DS4 de MP2
18.10.16

Devoir surveillé

Durée : 4 heures

Problème I – Ordre d'un élément et ordre d'un groupe abélien

Partie I – Généralités sur les ordres

I.1

a $x^{l-1} = x^{-1}$, donc $k \in \mathbb{Z}$ vérifie $(x^{l-1})^k = 1_G$ si et seulement si $x^k = 1_G$: l'ordre de x^{l-1} est l.

b Pour $m \in \mathbb{N}^*$ divisant l, on a $(x^m)^k = 1_G$ si et seulement si mk est multiple de l, si et seulement si k est multiple de l/m : l'ordre de x^m est l/m.

I.2

a Cours.

b Si G est cyclique, engendré par x d'ordre N, alors pour tout m divisant N, $x^{N/m}$ est d'ordre m.

Si, réciproquement, G vérifie la seconde propriété, alors il admet en particulier un élément d'ordre N, et il est donc cyclique.

I.3

a Soit t l'ordre de ab. Déjà, il est clair que $(ab)^{mn} = 1_G$, car a et b commutent (et donc $(ab)^{mn} = a^{mn}b^{mn}$). Ceci montre que t divise mn.

Comme $(ab)^{tm} = a^{tm}b^{tm} = b^{tm}$, n divise tm. Comme en outre n est premier avec m, n divise t (lemme de Gauss). De même, m divise t, puis, mn divise t (car $m \wedge n = 1$) : $t = mn$.

Autre preuve du fait que $t = mn$. Puisque $(ab)^t = 1_G$, on a $a^{-t} = b^t$, donc cet élément de G est à la fois dans $< a >$ et $< b >$: son ordre divise m et n qui sont premiers entre eux, donc son ordre vaut 1 puis $a^{-t} = b^t = 1_G$, donc t est multiple de m et de n, puis de leur produit (car $m \wedge n = 1$).

b Notons Ω_a l'ensemble des nombres premiers p tels que $v_p(m) \geqslant v_p(n)$, et notons Ω_b son complémentaire dans $\mathcal{P}$.

On pose

$$m' = \prod_{p \in \Omega_a} p^{v_p(m)} \quad \text{et} \quad n' = \prod_{p \in \Omega_b} p^{v_p(n)}$$

Il est clair que m' divise m (pour tout $p \in \mathcal{P}$, $v_p(m') \leqslant v_p(m)$), et que n' divise n. De plus, pour tout $p \in \mathcal{P}$, $v_p(m'n') = \max(v_p(m), v_p(n))$, et donc $m'n' = m \vee n$. Enfin, il est clair que $m' \wedge n' = 1$ (Ω_a et Ω_b sont disjoints).

On sait que $a^{m/m'}$ et $b^{n/n'}$ sont d'ordres respectifs m' et n' premiers entre eux, et donc que leur produit est d'ordre $m'n' = m \vee n$.

Partie II – Exposant d'un groupe abélien fini

II.1

a Il s'agit de montrer que Ω est non vide, ce qui est clair car $N \in \Omega$ d'après le théorème de Lagrange.

b Par définition de Ω et du ppcm,

$$\Omega = \left(\bigcap_{g \in G} \mathrm{o}(g)\mathbb{Z} \right) \cap \mathbb{N}^* = \mathrm{ppcm}(\mathrm{o}(g), g \in G)\mathbb{Z} \cap \mathbb{N}^*$$

d'où le résultat.

c Notons u l'ordre maximal d'un élément de G (un tel maximum existe car $\{\mathrm{o}(g), g \in G\}$ est une partie non vide de $\mathbb{N}^*$ majorée par N). Il s'agit de montrer que $u = r$. Nous savons déjà que u divise r. Réciproquement, soit $g \in G$, et soit k son ordre. Puisqu'il existe un élement de G d'ordre $u \vee k$, et que $u \vee k \geqslant u$, on a $u \vee k = u$ par définition de u, *i.e.* k divise u. Ceci donne donc $r|u$, puis $u = r$.

d Pour que $m \in \mathbb{N}^*$ soit l'ordre d'un élément de G, il faut que m divise r (r est le ppcm des ordres des éléments de G).

Réciproquement, puisque G admet un élément d'ordre r, il admet aussi un élément d'ordre tout diviseur de r préalablement fixé.

II.2 Si $r = N$, alors G est cyclique puisqu'il possède un élément d'ordre N. Réciproquement, si G est cyclique, alors il possède un élément d'ordre N, donc $r = N$.

Pour $G = (\mathbb{Z}/2\mathbb{Z})^2$, $N = 4$ et $r = 2$.

II.3 Dans $\mathcal{S}_3$, l'exposant de G vaut 6, mais aucun élément de $\mathcal{S}_3$ n'est d'ordre 6.

Problème II – Une version faible du théorème des nombres premiers

Partie III – L'ensemble des nombres premiers est infini

III.1 Supposons que $\mathcal{P} = \{q_1, \dots, q_n\}$ (où $n \in \mathbb{N}^*$). L'entier $Q \overset{def}{=} q_1 \dots q_n + 1$ admet au moins un diviseur premier, différent de $q_1, \dots, q_n$, puisque $q_i \wedge Q = 1$ pour tout $i \in [\![1, n]\!]$, d'où une absurdité.

III.2

a Il s'agit d'une série géométrique de raison $\frac{1}{n} \in]0, 1[$, et de terme initial 1 : cette série converge et sa somme vaut $\frac{1}{1-\frac{1}{n}}$.

b Si nous supposons $\mathcal{P}$ fini, alors il existe un entier N tel que, pour tout entier n supérieur ou égal à p_N, on ait

$$\sum_{k=1}^{n} \frac{1}{k} \leqslant \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right)^{-1}$$

ce qui prouve la convergence de la série harmonique (son terme général est positif et la suite de ses sommes partielles est majorée), d'où une absurdité.

c D'après le résultat admis, on a, pour tout $N \in \mathbb{N}^*$

$$\sum_{k=1}^{p_N} \frac{1}{k} \leqslant \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right)^{-1}$$

et donc en prenant le logarithme

$$\ln\left(\sum_{k=1}^{p_N} \frac{1}{k}\right) \leqslant \sum_{i=1}^{N} \nu_i$$

et la divergence de la série harmonique permet à nouveau de conclure.

d Comme $\mu_k \sim \frac{1}{p_k} > 0$, les séries $\sum \mu_k$ et $\sum \frac{1}{p_k}$ ont même nature : d'après la question précédente, la série $\sum_k \frac{1}{p_k}$ diverge.

e La suite de terme général $\frac{p_{k+1}}{p_k}$ est clairement minorée par 1, donc, si on la suppose convergente, sa limite α est supérieur ou égale à 1. Si nous avions $\alpha > 1$, alors d'après le critère de d'Alembert, la série $\sum \frac{1}{p_k}$ convergerait, ce qui est exclu : $\alpha = 1$.

Partie IV – Minoration du ppcm des $2n + 1$ premiers entiers naturels non nuls

IV.1 Il s'agit d'établir, étant donné un nombre premier p inférieur ou égal à n, que

$$\max\{v_p(k), k \in [\![1, n]\!]\} = \left[\frac{\ln n}{\ln p}\right]$$

or ce maximum vaut clairement

$$\max\{s \in \mathbb{N}, p^s \leqslant n\}$$

d'où le résultat.

IV.2

a Pour tout $x \in [0, 1]$, $x(1 - x) \leqslant \frac{1}{4}$ (par exemple par étude de fonction), donc $(x(1 - x))^n \leqslant \frac{1}{4^n}$, et la croissance de l'intégrale permet de conclure.

b Pour tout $k \in [\![0,n]\!]$, $n+k+1 \in [\![1,2n+1]\!]$, donc $n+k+1$ divise d_{2n+1} par définition de ce ppcm.
c On a

$$I_n = \int_0^1 x^n \sum_{k=0}^{n} \binom{n}{k} x^k (-1)^{n-k} \mathrm{d}x = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \int_0^1 x^{n+k} \mathrm{d}x = \sum_{k=0}^{n} \frac{(-1)^{n-k}\binom{n}{k}}{n+k+1}$$

donc $d_{2n+1} I_n \in \mathbb{N}^*$ d'après la question précédente.

IV.3 On obtient $d_{2n+1} I_n \geqslant 1$, et donc $d_{2n+1} \geqslant 4^n$ d'après IV.2.a.

Partie V – Majoration du produit des N premiers nombres premiers

V.1 Laissée au lecteur

V.2 On sait que $\binom{2m+1}{m} = \binom{2m+1}{m+1}$, et que

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1} = 2 \cdot 4^m$$

Il vient donc :

$$2 \cdot \binom{2m+1}{m} = \binom{2m+1}{m} + \binom{2m+1}{m+1} \leqslant \sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2 \cdot 4^m,$$

puis le résultat demandé.

V.3 Soit p_k un diviseur premier du produit $P(2m+1, m+1)$. Ce nombre divise le produit $\left(\binom{2m+1}{m}\right)(m!(m+1)!)$ $(= (2m+1)!)$, et est premier avec le second terme de ce produit, donc divise le premier terme $\binom{2m+1}{m}$ (lemme de Gauss). Les nombres premiers p_k (compris entre $m+1$ et $2m$) divisant $\binom{2m+1}{m}$ et étant premiers entre eux deux à deux, leur produit $P(2m+1, m+1)$ divise $\binom{2m+1}{m}$.

V.4 Si $K(m+1) \leqslant 4^{m+1}$, alors, en vertu de ce que précède :

$$K(2m+1) = K(m+1) P(2m+1, m+1) \leqslant 4^{m+1} 4^m \leqslant 4^{2m+1}.$$

V.5

a On raisonne par récurrence sur n, en écartant le cas évident où $n = 1$:

$$\forall\, k \in [\![1,n]\!], K(k) \leqslant 4^k$$

L'amorçage en $n = 2$ est aisé ($0 \leqslant 4$ et $2 \leqslant 16$).

Soit $n \in \mathbb{N}$, $n \geqslant 2$. On suppose l'assertion vérifiée au rang n, montrons-la au rang $n+1$: raisonnons par disjonction des cas :

- ◇ si $n+1$ est premier, il existe alors $m \in \mathbb{N}^*$ tel que $n+1 = 2m+1$ (car cet entier premier vaut au moins 3 donc est impair, d'où l'intérêt d'amorcer la récurrence en 2), l'hypothèse de récurrence et la question précédente montre que $K(n+1) \leqslant 4^{n+1}$;
- ◇ si $n+1$ n'est pas premier, alors $K(n+1) = K(n) \leqslant 4^n \leqslant 4^{n+1}$ (la première inégalité étant justifiée par l'hypothèse de récurrence).

b On a prouvé cette inégalité si $x \in \mathbb{N}^*$, et, si $x \in \mathbb{R}_+^* \setminus \mathbb{N}^*$, alors $K(x) = K([x]) \leqslant 4^{[n]} \leqslant 4^x$.

Partie VI – $N(x) = \Theta\left(\frac{x}{\ln(x)}\right)$

VI.1 On a bien sûr $S(x) \leqslant (2\ln 2)x$.

VI.2

a Soit k un entier naturel non nul :

$$\begin{aligned}
\int_2^{p_k} S(t) f'(t) \mathrm{d}t &= \sum_{j=1}^{k-1} \int_{p_j}^{p_{j+1}} S(t) f'(t) \mathrm{d}t \\
&= \sum_{j=1}^{k-1} \left(\ln \prod_{1 \leqslant i \leqslant j} p_i \right) (f(p_{j+1}) - f(p_j)) \\
&= \sum_{j=2}^{k} \left(\ln \prod_{1 \leqslant i \leqslant j-1} p_i \right) f(p_j) - \sum_{j=1}^{k-1} \left(\ln \prod_{1 \leqslant i \leqslant j} p_i \right) f(p_j) \\
&= -\sum_{i \in [\![1,k]\!]} \ln(p_i) f(p_i) + S(p_k) f(p_k).
\end{aligned}$$

b On en déduit la relation

$$\sum_{i\in[\![1,N(x)]\!]} \ln(p_i)f(p_i) = S(x)f(x) - \int_2^x S(t)f'(t)\mathrm{d}t$$

en remarquant que

$$\int_{p_{N(x)}}^x S(t)f'(t)\mathrm{d}t = S(p_{N(x)})(f(x) - f(p_{N(x)})) = S(x)f(x) - S(p_{N(x)})f(p_{N(x)}).$$

VI.3 On prend $f = \frac{1}{\ln}$. La précédente l'inégalité donne immédiatement

$$\sum_{1\leqslant k\leqslant N(x)} 1 = \frac{S(x)}{\ln(x)} + \int_2^x \frac{S(t)}{t\ln(t)^2}\mathrm{d}t$$

et donc, d'après VI.1 :

$$N(x) \leqslant 2\ln 2\left(\frac{x}{\ln x} + \int_2^x \frac{\mathrm{d}t}{(\ln t)^2}\right).$$

VI.4

a L'étude demandée est standard : la fonction considérée ψ est strictement décroissante de $\ln 2$ à 2, puis strictement croissante sur $[2,+\infty[$. En cas d'existence de u_0, on doit avoir $u_0 \in [2,+\infty[$, d'où l'unicité (par stricte croissance - donc injectivité- de ψ sur cet intervalle). Comme ψ est continue tend vers $+\infty$ en $+\infty$, et que $\psi(2) < \psi(\ln 2)$ l'existence est prouvée (théorème des valeurs intermédiaires)

b On en déduit, pour tout $x > e^{u_0}$, en majorant ψ par $\psi(x) = x/(\ln(x))^2$ sur $[\ln(2),\ln(x)]$, puis en intégrant :

$$\int_{\ln 2}^{\ln x} \frac{e^u}{u^2}\mathrm{d}u \leqslant \int_{\ln 2}^{\ln x} \frac{e^{\ln x}}{(\ln x)^2}\mathrm{d}u = \frac{x}{(\ln x)^2}(\ln x - \ln 2).$$

c En effectuant le changement de variable $t = e^u$ de classe $\mathcal{C}^1$ sur $[\ln 2, \ln x]$, on obtient :

$$\int_2^x \frac{\mathrm{d}t}{(\ln t)^2} = \int_{\ln 2}^{\ln x} \frac{e^u}{u^2}\mathrm{d}u \leqslant \frac{x}{(\ln x)^2}(\ln x - \ln 2) \leqslant \frac{x}{(\ln x)}.$$

L'inégalité demandée résulte alors immédiatement de ce qui précède.

VI.5 Nous avons établi que $4^n \leqslant d_{2n+1}$, et que

$$d_{2n+1} = \prod_{i\in[\![1,N(2n+1)]\!]} p_i^{\left\lfloor \frac{\ln(2n+1)}{p_i}\right\rfloor}$$

En prenant le logarithme, il vient

$$2n\ln(2) \leqslant \sum_{i\in[\![1,N(2n+1)]\!]} \left\lfloor \frac{\ln(2n+1)}{p_i}\right\rfloor \ln(p_i)$$

et donc

$$2n\ln(2) \leqslant N(2n+1)\ln(2n+1)$$

puis

$$N(2n+1) \geqslant \frac{2n\ln(2)}{\ln(2n+1)}$$

En prenant $x > 3$, et n l'entier tel que $2n+1 \leqslant x < 2n+3$, on a

$$N(x) = N(2n+1) \geqslant \frac{2n\ln(2)}{\ln(2n+1)} \geqslant \ln(2)\frac{x-3}{\ln(x)}$$

et on a donc bien

$$N(x) \geqslant \frac{\ln 2}{2}\frac{x}{\ln x}$$

au voisinage de $+\infty$.

VI.6

a On a admis le théorème des nombres premiers. Il nous donne en particulier

$$N(p_n) \sim \frac{p_n}{\ln(p_n)}$$

i.e. (puisque $N(p_n) = n$)

$$\frac{n \ln(p_n)}{p_n} \sim 1$$

puis en prenant le logarithme

$$\ln(n) + \ln(\ln(p_n)) - \ln(p_n) = \mathrm{o}(1)$$

puis

$$\ln(p_n) \sim \ln(n)$$

Il vient bien alors

$$p_n \sim n \ln(n)$$

b La série $\sum \frac{1}{p_n}$ a même nature que $\sum \frac{1}{n \ln(n)}$ (par équivalence et positivité des termes généraux de ces séries).

Or on montre la divergence de $\sum \frac{1}{n \ln(n)}$ par comparaison série-intégrale par exemple, d'où le résultat.

c Grâce à l'équivalent $p_n \sim n \ln(n)$, on obtient $\frac{p_{n+1}}{p_n} \sim \frac{(n+1)\ln(n+1)}{n \ln(n)} \sim 1$, et la suite de terme général $\frac{p_{n+1}}{p_n}$ converge donc vers 1.