Devoir maison

(à rendre le lundi 6 octobre)

Solution proposée.

1. **(2 pts)** Soit $z \in \mathbf{C}$. On a les équivalences

$$\begin{aligned} z \in G &\iff \exists d \in \mathbf{N}^*,\ z^d = 1 \\ &\iff \exists d \in \mathbf{N}^*,\ \exists n \in \mathbf{Z},\ z = e^{\frac{2\pi i n}{d}} \\ &\iff \exists\, (n,d) \in \mathbf{Z} \times \mathbf{N}^*,\ z = e^{2\pi i \frac{n}{d}} \\ &\iff \exists q \in \mathbf{Q},\ z = e^{2\pi i q} \\ &\iff z \in \operatorname{Im}\varphi \qquad \text{où l'on a défini } \varphi : \left\{ \begin{array}{ccc} \mathbf{Q} & \longrightarrow & \mathbf{C}^* \\ q & \longmapsto & e^{2\pi i q} \end{array} \right. . \end{aligned}$$

Par ailleurs, l'application φ est un morphisme de groupes de noyau $\operatorname{Ker}\varphi = \mathbf{Z}$, donc "passe" *modulo* $\mathbf{Z}$ et induit un isomorphisme sur son image

$$\left\{ \begin{array}{ccc} \mathbf{Q}/\mathbf{Z} & \xrightarrow{\sim} & \operatorname{Im}\varphi = G \\ \overline{q} & \longmapsto & e^{2\pi i q} \end{array} \right. .$$

2. **(1 pt)** On a explicitement $G_{p^0} = \left\langle \frac{1}{p^0} \right\rangle = \langle 1 \rangle = \langle 0 \rangle = \{0\}$: c'est le sous-groupe trivial. Il ne contient aucun élément d'ordre p.

(2 pts) Si $n < \infty$, alors $G_{p^n} = \mathbf{U}_{p^n}$ est un sous-groupe (d'après le cours) d'ordre p^n ; sinon, $G_{p^n} = G_{p^\infty} = \bigcup_{k \in \mathbf{N}^*} \mathbf{U}_k$ est aussi un sous-groupe (toujours d'après le cours) d'ordre cette fois infini (il contient tous les $\frac{1}{p^k}$ pour k décrivant $\mathbf{Z}$, lesquels sont distincts).

(2 pts) Soit $a \in G_{p^n}$. Supposons $n > 0$ (on a vu que$G_{p^0} = \{0\}$ ne contenait pas d'élément d'ordre p). On a les équivalences :

$$\begin{array}{c} a \text{ est d'ordre} \\ p \text{ dans } G_{p^n} \end{array} \iff \left\{ \begin{array}{c} a^p = 1 \neq a \\ a \in G_{p^n} \end{array} \right. \iff \left\{ \begin{array}{c} a \in \mathbf{U}_p \setminus \{1\} \\ a \in G_{p^n} \end{array} \right. \iff a \in G_{p^n} \cap \mathbf{U}_p \setminus \{1\} \overset{\mathbf{U}_p \subset G_{p^n}}{\iff} a \in \mathbf{U}_p \setminus \{1\} ,$$

ce qui montre que les éléments d'ordre p dans G_{p^n} sont : $\frac{1}{p}, \frac{2}{p}, ..., \frac{p-1}{p}$.

(1 pt) Lorsque $n < \infty$, le sous-groupe $G_{p^n} = \left\{ e^{2\pi i \frac{k}{p^n}} \ ;\ k \in \mathbf{Z} \right\} = \left\langle e^{\frac{2\pi i}{p^n}} \right\rangle$ est engendré par $\frac{1}{p^n}$.

(2 pts) Supposons par l'absurde que G_{p^∞} soit engendré par un nombre fini d'éléments. Soient $\frac{a_i}{p^{n_i}}$ de tels générateurs. Appelons $N := \max n_i$. Alors tout élément engendré par les $\frac{a_i}{p^{n_i}}$ est une fraction de dénominateur p^N, donc appartient à G_{p^N}, donc est tués après p^N itérations : en particulier pour l'élément $\frac{1}{p^{N+1}}$ de G_{p^∞}, ce qui donne $\frac{1}{p} = 0$ [$\mathbf{Z}$], *i. e.* $\frac{1}{p} \in \mathbf{Z}$, ce qui est absurde.

3. **(1 pt)** L'inclusion $\supset$ est immédiate (1 est étranger avec n'importe quel entier). Soit $\frac{a}{b}$ un élément de H écrit sous forme irréductible. Soient (d'après Bézout) u et v des relatifs tels que $au + bv = 1$. Le u-ième itéré de $\frac{a}{b}$ reste dans H et vaut $u\frac{a}{b} = \frac{ua}{b} = \frac{1-vb}{b} = \frac{1}{b} - v = \frac{1}{b}$, d'où l'appartenance $b \in D_H$ voulue.

(1 pt) D_H est stable par diviseurs car H est stable par multiplication par tout entier (*i .e.* stable par itération). Montrons que D_H est stable par p. p. c. m. Soient a et b dans D_H. Soient $\lambda, \mu \in \mathbf{Z}$ tels que $\lambda a + \mu b = a \wedge b$. Reste alors dans H la somme $\mu\frac{1}{a} + \lambda\frac{l}{b} = \frac{a \wedge b}{ab} = \frac{1}{a \vee b}$, d'où $a \vee b \in D_H$.

(2 pts) Montrons alors que $H_{D_H} = H$. Soit $g \in H_{D_H}$, mettons $g = \sum \frac{a_i}{d_i}$ pour certains $d_i \in D_H$: par définition de D_H, les $\frac{1}{d_i}$ sont alors dans H, donc les itérés $\frac{a_i}{d_i}$ aussi, donc leur somme g aussi. Soit réciproquemet $\frac{a}{b} \in H$ avec a et b étrangers. Alors $b \in D_H$, donc $\frac{1}{b} \in H_{D_H}$, donc le a-ième itéré $\frac{a}{b}$ reste dans H_{D_H}, *c. q. f. d.*.

(2 pts) Soit $D \subset \mathbf{N}^*$ stable par p. p. c. m. et diviseurs. Il est clair que le sous-groupe engendré H_D est un sous-groupe. Montrons alors l'égalité $D_{H_D} = D$. Soit $d \in D$: alors $\frac{1}{d} \in H_d$, donc le dénominateur d tombe dans D_{H_d}. Soit réciproquement $d \in D_{H_D}$, mettons $\frac{1}{d} = \sum \frac{a_i}{d_i}$ pour certains $d_i \in D$: alors $\frac{1}{d}$ est de la forme (après réduction au plus petit commun dénominateur) $\frac{?}{\bigvee d_i}$, d'où la divisibilité $d \mid \bigvee d_i$ et (par hypothèses sur D) l'appartenance $d \in D$

(2 pts) Montrons que

l'image des sous-groupes finis sont les ensembles de diviseurs d'entiers fixés.

Supposons H fini. On peut alors borner les dénominateurs de ses éléments (tous écrits sous forme irréductible), *i. e.* borner D_H : notons $N := \max D_H$. Puisque D_H est stable par diviseurs, il contient tous ceux de N. Soit par aileurs $d \in D_H$: le p. p. c. m. $d \vee N$ restant dans D_H, il doit être plus petit que son maximum N, ce qui force l'égalité $d \vee N = N$ et la divisibilité $d \mid N$. Finalement, D_H est l'ensemble des diviseurs d'un même entier (son maximum). Réciproquement, si D est l'ensemble des diviseurs d'un entier N, alors itérer $\frac{1}{N}$ donne $\frac{1}{d}$ pour n'importe quel $d \in D$, d'où l'inclusion $\left\langle \frac{1}{N} \right\rangle \subset \left\langle \frac{1}{d} \ ; \ d \in D \right\rangle = H_D$, l'inclusion réciproque étant immédiate (vu que $N \in D$) ; ainsi H_D est-il fini (de cardinal N).

4. **(1 pt)** Soit $\alpha \in \overline{\mathbf{N}}^{\mathbf{P}}$. Montrons que D_α est stable par p. p. c. m. Soient $\prod p^{v_p}$ et $\prod p^{w_p}$ dedans : leur p. p. c. m vaut $\prod p^{\max\{v_p, w_p\}}$ et les comparaisons $v_p, w_p \leq \alpha_p$ équivalent à celles $\max\{v_p, w_p\} \leq \alpha_p$. Montrons que D_α est stable par diviseurs. Un diviseur de $\prod p^{v_p}$ est de la forme $\prod p^{k_p}$ où $k_p \leq v_p$ pour tout $p \in \mathbf{P}$, d'où les comparaisons $k_p \leq v_p \leq \alpha_p$. Nous venons de montrer que l'application $\beta \mapsto D_\beta$ est bien définie.

(1 pt) Soit $\alpha \in \overline{\mathbf{N}}^{\mathbf{P}}$ et fixons un $p \in \mathbf{P}$. Alors tout élément de D_α a une valuation p-adique plus petite que α_p. Dans le cas "α_p fini", cette valuation majorante est atteinte (par exemple en $p^{\alpha_p} \in D_\alpha$) ; dans le cas "$\alpha_p$ infini", elle ne l'est bien sûr jamais. Dans tous les cas, on peut décrire $\alpha_p = \sup_{\overline{\mathbf{N}}} \{v_p(d) \ ; \ d \in D\}$ (où le sup devient un max ssi $\alpha_p < \infty$), ce qui montre que l'application $\beta \mapsto D_\beta$ admet un inverse à gauche

$$D \mapsto \left(\sup_{\overline{\mathbf{N}}} \{v_p(d) \ ; \ d \in D\} \right)_{p \in \mathbf{P}}.$$

Montrons que cet inverse à gauche est un inverse tout court, ce qui conclura.

(2 pts) Soit D une partie de $\mathbf{N}$ stable par p. p. c. m. et par diviseurs. Posons $\alpha := \left(\sup_{\overline{\mathbf{N}}} \{v_p(d) \ ; \ d \in D\}\right)_{p \in \mathbf{P}}$. On veut montrer l'égalité $D = D_\alpha$. Soit $d \in D$: pour tout premier p, on a $p^{v_p(d)} \mid d$, donc la valuation $v_p(d)$ minore le *supremum* α_p, d'où l'on déduit (faisant varier p) l'appartenance $d \in D_\alpha$. Soit à présent $\delta \in D_\alpha$. Puisque D est stable par p. p. c. m. et que δ est le p. p. c. m. des $p^{v_p(\delta)}$, il suffit pour montrer $\delta \in D$ de prouver que tous les $p^{v_p(\delta)}$ sont dans D. Or, par définition du *supremum* α_p, il y a un $\Delta \in D$ tel que[1] $v_p(\Delta) \geq v_p(\delta)$: la partie D étant stable par diviseurs, elle contiendra $p^{v_p(\Delta)}$ (qui divise Δ), donc aussi $p^{v_p(\delta)}$ (puisque $v_p(\delta) \leq v_p(\Delta)$), *c. q. f. d.*.

5. **(2 pts)** Regardons d'abord le cas $k, l < \infty$. Explicitons $D_\beta = \left\{p^a q^b \ ; \ a \leq k \text{ et } b \leq l\right\}$: c'est l'ensemble des diviseurs de $p^k q^l$. On en déduit $H_\beta = \left\langle \frac{1}{p^k}, \frac{1}{q^l} \right\rangle$. On veut donc un isomorphisme de $\left\langle \frac{1}{p^k} \right\rangle \times \left\langle \frac{1}{q^l} \right\rangle$ sur $\left\langle \frac{1}{p^k}, \frac{1}{q^l} \right\rangle$. Essayons la somme, qui est clairement un morphisme surjectif[2] : montrons son injectivité. Soient $a, b \in \mathbf{Z}$ tels que $\frac{a}{p^k} + \frac{b}{q^l} = 0$. Remarquer l'égalité $p \wedge q = 1$ puisque p et q sont des premiers distincts. Multiplier par q^l donne alors $\frac{aq^l}{p^k} = 0$, *i. e.* $p^k \mid aq^l$, *i. e.* (car $p \wedge q = 1$) $p^k \mid a$, *i. e.* $\frac{a}{p^k} = 0$, d'où $\frac{b}{q^l} = -\frac{a}{p^k} = 0$, ce qui conclut.

(1 pt) Supposons à présent $k < \infty = l$. On veut alors un isomorphisme de $\left\langle \frac{1}{p^k} \right\rangle \times \left\langle \frac{1}{q}, \frac{1}{q^2}, \frac{1}{q^3}, ... \right\rangle$ sur $\left\langle \frac{1}{p^k}, \frac{1}{q}, \frac{1}{q^2}, \frac{1}{q^3}, ... \right\rangle$. L'argument ci-dessus fonctionne alors sans rien changer. Même chose lorsque $k = \infty = l$.

(3 pts) Montrons plus généralement[3] que

pour tous α et $\beta \in \overline{\mathbf{N}}^{(\mathbf{P})}$ à supports disjoints, on a $H_{\alpha \sqcup \beta} = H_\alpha \oplus H_\beta$

où l'on noté $\alpha \sqcup \beta$ la famille concaténée $p \mapsto \begin{cases} \alpha_p \text{ si } p \in \operatorname{Supp} \alpha \\ \beta_p \text{ si } p \in \operatorname{Supp} \beta \end{cases}$.

[1] si α_p est fini, on peut imposer $v_p(\Delta) = \alpha_p$, sinon on peut imposer $v_p(\Delta)$ aussi grand que voulu

[2] pour toutes parties A et B d'un même groupe abélien, on a toujours l'égalité $\langle A \cup B \rangle = \langle A \rangle + \langle B \rangle$

[3] Ce qui précède traite les familles dont les supports sont des singletons. Pourquoi alors faire *ensuite* une preuve qui englobe la première ? pourquoi ne pas l'avoir fait de suite pour nous économiser ? Parce que la première preuve *nourrit notre intuition*, en nous donnant un cas particulier, de la preuve générale à venir, ce qui nous permettra de mieux appréhender cette dernière.

Soient de tels α et β. En calculant

$$\begin{aligned} D_{\alpha\sqcup\beta} &= \left\{ \prod_{p\in\operatorname{Supp}\alpha\sqcup\beta} p^{u_p} \ ;\ \forall p\in\operatorname{Supp}(\alpha\sqcup\beta)\,,\ u_p\le[\alpha\sqcup\beta]_p \right\} \\ &= \left\{ \prod_{p\in\operatorname{Supp}\alpha} p^{v_p} \prod_{q\in\operatorname{Supp}\beta} q^{w_q} \ ;\ \begin{array}{c}\forall p\in\operatorname{Supp}\alpha,\ v_p\le\alpha_p\\ \forall q\in\operatorname{Supp}\beta,\ w_q\le\beta_q\end{array} \right\} \\ &= \left\{ \prod_{p\in\operatorname{Supp}\alpha} p^{v_p} \ ;\ \forall p\in\operatorname{Supp}\alpha,\ v_p\le\alpha_p \right\} \left\{ \prod_{q\in\operatorname{Supp}\beta} q^{w_q} \ ;\ \forall q\in\operatorname{Supp}\beta,\ w_q\le\beta_q \right\} \\ &= D_\alpha D_\beta, \text{ on peut décrire } H_{\alpha\sqcup\beta}=H_{D_{\alpha\sqcup\beta}}=H_{D_\alpha D_\beta}=\left\langle \frac{1}{de} \ ;\ \begin{array}{c} d\in D_\alpha\\ e\in D_\beta\end{array} \right\rangle. \end{aligned}$$

Ce dernier sous-groupe contient $\left\langle \frac{1}{d}\ ;\ d\in D_\alpha\right\rangle = H_\alpha$ (prendre e égal à 1) et de même H_β, donc leur somme $H_\alpha+H_\beta$. Réciproquement, il est clair qu'un élément de $H_\alpha+H_\beta=\left\langle \frac{1}{d}\ ;\ d\in D_\alpha\right\rangle+\left\langle \frac{1}{e}\ ;\ e\in D_\beta\right\rangle$ est (après réduction à un même dénominateur) de la forme $\frac{?}{de}$ pour un $(d,e)\in D_\alpha\times D_\beta$, ce qui prouve l'égalité $H_{\alpha\sqcup\beta}=H_\alpha+H_\beta$. Montrons enfin que la somme est directe. (On reprend la démonstration effectuée pour les supports-singletons.) Soient $a,b\in\mathbf{Z}$ et $(d,e)\in D_\alpha\times D_\beta$ tels que $\frac{a}{d}+\frac{b}{e}=0$. Observer l'égalité $d\wedge e=1$ puisque α et β sont à supports disjoints. Multiplier par e donne alors $\frac{ae}{d}=0$, *i. e.* $d\mid ae$, *i. e.* (puisque $d\wedge e=1$) $d\mid a$, *i. e.* $\frac{a}{d}=0$, d'où $\frac{b}{e}=-\frac{a}{d}=0$, ce qui conclut.

(1 pt) Soit $\alpha\in\overline{\mathbf{N}}^{(\mathbf{P})}$. Pour tout $p\in\mathbf{P}$, notons δ^p la famille de support $\{p\}$ qui envoie p sur α_p (observer alors l'égalité $H_{\delta^p}=G_{p^{\alpha_p}}$). En décomposant la famille α selon la concaténée des δ^p lorsque p décrit $\operatorname{Supp}\alpha$, le résultat précédent (qui nous dit en substance que l'application H transforme $\sqcup$ en $\oplus$) permet d'obtenir (via une récurrence immédiate) la description

$$H_\alpha=H_{\bigsqcup_{p\in\operatorname{Supp}\alpha}\delta^p}=\bigoplus_{p\in\operatorname{Supp}\alpha}H_{\delta^p}=\bigoplus_{p\in\operatorname{Supp}\alpha}G_{p^\alpha}.$$

6. **(1 pt)** Observer tout d'abord que, vu l'équivalence (valide pour toutes familles $\alpha,\beta\in\overline{\mathbf{N}}^{(\mathbf{P})}$)

$$H_\alpha\subset H_\beta\iff\forall p\in\mathbf{P},\ \alpha_p\le\beta_p,$$

les sous-groupes de G_{p^n} sont de la forme G_{p^m}. En particulier, les sous-groupes non trivaux de G_{p^n} ont (exactement) p éléments d'ordre au plus p.

(1 pt) Les groupes A et B étant des facteurs du produit $A\times B\simeq G_{p^n}$, ils sont isomorphes à des sous-groupes de G_{p^n}, donc sont des G_{p^m}. Si aucun d'eux n'est le groupe trivial, ils ont chacun p éléments d'ordre au plus p, ce qui fournit p^2 couples dans $A\times B$ d'ordre au plus p. Or G_{p^n} contient (au plus) p éléments d'ordre au plus p, d'où la comparaison $p^2\ge p$, ce qui contredit la primalité de p.