Rapport sur l'épreuve de mathématiques MPI1 2010 par François Charles, Mikaël de la Salle, Jérôme Germoni, Thomas Haettel (correcteurs), David Harari (concepteur et correcteur)

L'épreuve de 6 heures de mathématiques de la session 2010 portait sur le théorème de structure des groupes abéliens de torsion de type cofini. Plus précisément, fixons un nombre premier p et notons U_p le groupe multiplicatif des racines complexes de l'unité d'ordre une puissance de p ; le but du problème était d'établir que pour tout groupe abélien A de torsion p-primaire (i.e. tel que tout x de A soit d'ordre une puissance de p) et tel que l'ensemble des éléments d'ordre p soit fini, il existe un isomorphisme entre A et un produit direct $F \times U_p^r$, où F est un groupe fini (d'ordre une puissance de p). On notera en passant qu'en corollaire, un groupe abélien dont tous les éléments sont d'ordre fini et tel que pour tout p premier, l'ensemble des éléments d'ordre p est fini, est isomorphe à une somme directe sur tous les nombres premiers de groupes du type $F_p \times U_p^r$ avec F_p fini[1]

Le problème était (délibérément) plus facile que d'habitude cette année, le but étant d'éviter que de bons candidats ne soient bloqués par des questions trop ardues.[2] Par conséquent, il fallait résoudre correctement la totalité du problème pour avoir la note maximale de 20/20 (deux candidats y sont parvenus, et une dizaine s'en sont approchés de très près). Les notes ont été bien étalées, un quart environ des copies obtenant au moins 10/20. Ceci dit, les correcteurs ont été très sensibles à la qualité de la rédaction, et n'ont pas hésité à sanctionner les imprécisions et les preuves incomplètes. De ce fait, certains candidats ont peut-être été déçus par leur note quand ils avaient négligé certains détails importants (voir plus bas pour des exemples d'omissions de ce genre).

Un motif de satisfaction (un peu inattendu vu le peu d'algèbre générale restant au programme) a été le fait qu'un nombre conséquent de candidats ne se sont pas laissé déstabiliser par le cadre un peu inhabituel du problème, et ont montré une bonne maîtrise des notions algébriques (sous-groupes, morphismes) et arithmétiques (Bezout, $\mathbf{Z}/n\mathbf{Z}$) de base. Mentionnons seulement quelques erreurs standard : penser que l'égalité $nx = 0$ implique toujours $x = 0$ (quand x est un élément d'un groupe abélien et n un entier strictement positif), parler d' "espace vectoriel" sur $\mathbf{Z}/p^n\mathbf{Z}$ (alors que $\mathbf{Z}/p^n\mathbf{Z}$ n'est pas un corps si $n > 1$), se tromper de loi de groupes (entre $+$ et $\times$) pour utiliser la

[1]La notion de somme directe externe n'étant pas au programme, l'auteur a renoncé à inclure ce corollaire comme ultime question du problème.

[2]et aussi d'avoir une épreuve qui sélectionne suffisamment d'admissibles pour chacune des trois E.N.S.

propriété de morphisme, confondre les notions d'injectivité et de surjectivité d'une application. Certains candidats mélangent également allègrement les notions de groupe abélien et d'espace vectoriel.

Curieusement, ce sont les questions d'analyse de la partie I qui ont été les plus décevantes. Les questions (pourtant très simples) I.1.c) et I.1.d) ont parfois donné lieu à des pages de calcul incompréhensibles, des expressions telles que z^λ (avec z complexe et λ réel quelconque) ont fleuri bien qu'elles n'aient pas de sens, et la question (pourtant classique) du prolongement par continuité d'une application uniformément continue (fin de la partie I) a été un véritable massacre, y compris dans de très bonnes copies. Trop de candidats ne sont peut-être pas conscients que la rigueur et la précision ne doivent pas être oubliées même quand les questions paraissent familières.

Enfin, il y a encore un peu trop de rédactions désinvoltes (le candidat n'ayant pas envie de se fatiguer à vérifier des points pourtant non triviaux) et de copies mal présentées (écriture quasi-illisible, ratures incessantes alors qu'en 6 heures, on a le temps de travailler un peu au brouillon).

Ces remarques générales faites, voyons le déroulement du problème.

Partie **I**

I.1.a) était très facile et a été traité par la quasi-totalité des candidats. Dans I.1.b), beaucoup de candidats ont omis de démontrer (ou ne l'ont pas fait complètement) qu'il existait un a tel que $\int_0^a g(t)dt$ soit non nul. I.1.c) et I.1.d) étaient faciles, mais ont néanmoins donné lieu à des raisonnements inutilement compliqués alors qu'il suffisait de dériver l'identité $g(t+x) = g(t)g(x)$, puis d'utiliser l'équation différentielle satisfaite par g. I.1.e) a également été assez mal traitée avec des expressions fantaisistes du type z^λ, certains candidats ne comprenant pas que la seule difficulté était de montrer que le λ trouvé en I.1.d) était entier.

I.2. a souvent été bien traitée, même si les raisonnements dans I.2.b) ont parfois été flous. I.3.a) et I.3.b) ont également été souvent réussies. En revanche, presque tous les candidats ont (diversement) massacré I.3.c) : définition de $\bar{f}$ mal justifiée (pourquoi la limite obtenue via I.2.b) est-elle unique ?), vérification (qui n'est pas triviale) de la continuité de $\bar{f}$ omise, utilisation abusive d'un "prolongement par continuité" (qui n'existe pas en général et résulte de l'uniforme continuité, ce que la question avait justement pour but d'établir), conclusion incomplète...

Partie **II.**

II.1. n'était pas très difficile, même si pas mal de candidats n'ont pas bien compris que la difficulté de II.1.b) était de vérifier que g était bien définie. Certains n'ont pas non plus vu que II.1.c) était une conséquence du résultat

admis A), et ont tenté (sans succès) de définir directement un prolongement.[3] II.2. a souvent été correctement traitée, les candidats comprenant bien l'analogie avec une somme directe de sous-espaces vectoriels.

Partie **III.**

Cette partie présentait les résultats de base sur les groupes abéliens p-primaires. Les questions III.1. et III.2. permettaient de se familiariser avec cette notion et ont été assez bien traitées dans l'ensemble. La question III.3. était plutôt facile une fois qu'on avait vu qu'il fallait utiliser l'énoncé admis B). Néanmoins, les candidats ont très souvent oublié de démontrer que tous les éléments de G étaient diagonalisables. Dans la question III.4.a) il y a eu beaucoup d'erreurs, les candidats prétendant souvent qu'un morphisme injectif de A dans A était automatiquement surjectif (alors que A n'était pas supposé fini) ou encore justifiant l'injectivité en "divisant par m" (sic). III.4.b) était un corollaire facile.

Une bonne partie des candidats n'a pas vu que la seule difficulté de III.5. consistait à vérifier que la formule avait un sens. L'utilisation de la structure de $\mathbf{Z}/p\mathbf{Z}$-ev dans III.6.a) a en général été bien vue ; en revanche III.6.b) a donné lieu maintes fois à des erreurs, la plus fréquente consistant à penser que u_k était automatiquement surjectif. III.6.c) était sans doute la question la plus difficile du problème, le raisonnement (basé sur un "principe des tiroirs") étant assez subtil.

Partie **IV.**

Cette courte partie nécessitait un peu d'astuce, et n'a pas souvent été bien traitée. Il y a eu de nombreuses preuves incomplètes utilisant des assertions fausses du genre : "une intersection décroissante de groupes abéliens non nuls est non nulle" (alors qu'il fallait d'abord se ramener au cas où les dits groupes sont finis).

Partie **V.**

Cette partie assez technique n'a attiré que les très bons candidats. Après deux questions relativement tranquilles (V.1. et V.2.a)) venait l'assez complexe V.2.b), qui a très rarement été rédigée correctement, ce qui a coûté pas mal de points à ceux qui se sont contentés d'arguments vagues. V.3.a) et V.3.d) ont souvent été bien comprises (hormis les habituelles bêtises concernant les "espaces vectoriels sur $\mathbf{Z}/p^n\mathbf{Z}$"), tandis que les délicates V.3.b. et V.3.c. n'ont comme prévu été traitées que par les tout meilleurs.

[3]Un satisfecit moral par contre au candidat qui a fort correctement démontré A) en utilisant le lemme de Zorn. Un autre candidat savant a interprété II.1.c. comme le fait qu'un groupe divisible est "projectif" ; pas de chance, le terme correct est "injectif", qui est la notion duale...

Partie **VI.**

Cette dernière partie faisait la synthèse. Avec les indications fournies[4], elle était tout compte fait plutôt facile à condition de ne pas être trop épuisé en fin d'épreuve. Les quelques candidats qui sont arrivés jusque-là s'en sont bien sortis, hormis en VI.3. où il manquait presque systématiquement la justification qu'il y a bien p^k éléments dans le groupe des racines p^k-ième de l'unité de K (ce qui résultait de l'hypothèse de caractéristique zéro). Un (excellent) candidat a identifié le groupe U_p comme "le groupe des entiers p-adiques $\mathbf{Z}_p$", ce qui était savant mais légèrement inexact puisqu'il s'agit en fait de son dual $\mathbf{Q}_p/\mathbf{Z}_p$!

[4]Le concepteur aurait vraiment dû à ce stade être moins débonnaire et enlever les références indiquant quelles questions antérieures il fallait utiliser...

CORRIGÉ.

I

I.1 a) Pour tous t_1, t_2 dans $\mathbf{R}$, on a

$$g(t_1 + t_2) = f(e^{it_1}e^{it_2}) = f(e^{it_1})f(e^{it_2})$$

car f est un morphisme de S^1 dans S^1, d'où $g(t_1 + t_2) = g(t_1)g(t_2)$. Ainsi g est un morphisme de $(\mathbf{R}, +)$ dans $(S^1, \times)$.

b) Soit a fixé dans $\mathbf{R}$ tel que $\int_0^a g(t)dt \neq 0$ (a existe sinon en dérivant la fonction $a \mapsto \int_0^a g(t)dt$, on obtiendrait que g est identiquement nulle, or g est à valeurs dans S^1). Posons

$$F(x) = \int_x^{a+x} g(t)dt = \int_0^{a+x} g(t)dt - \int_0^x g(t)dt$$

Comme g est une application continue (par composition), l'application F est dérivable sur $\mathbf{R}$. Par ailleurs, un changement de variable donne

$$F(x) = \int_0^a g(t + x)dt = g(x) \int_0^a g(t)dt$$

d'après a). Ainsi g est dérivable comme quotient d'une fonction dérivable par une constante non nulle.

c) D'après a), on a $g(t + a) = g(t)g(a)$ pour tous réels a, t. En dérivant par rapport à t, on obtient $g'(t + a) = g(a)g'(t)$ d'où le résultat en faisant $t = 0$.

d) Le c) nous a donné une équation différentielle linéaire homogène à coefficients constants du premier ordre satisfaite par g. On sait alors qu'il existe des nombres complexes α et C tels que $g(t) = Ce^{\alpha t}$. D'après a), on a $g(0) = 1$ donc $C = 1$. D'autre part $g(1) \in S^1$ ce qui impose α imaginaire pur, d'où le résultat.

e) On note que $g(t+2\pi) = g(t)$ pour tout t de $\mathbf{R}$. En particulier $g(2\pi) = 1$ ce qui impose que λ est un entier k. Alors $f(e^{it}) = (e^{it})^k$ pour tout t de $\mathbf{R}$, ou encore $f(z) = z^k$ pour tout $z \in S^1$ puisque que tout élément de S^1 s'écrit e^{it} avec $t \in \mathbf{R}$.

I.2. a) On note que pour tout $k \in \mathbf{N}$, U_p contient le groupe des racines p^k-ièmes de l'unité qui est de cardinal p^k, donc U_p est infini puisque k peut être pris arbitrairement grand. Il est immédiat que $U_p \subset S^1$. Si maintenant $z_1^{p^k} = 1$ et $z_2^{p^l} = 1$ avec $k, l \in \mathbf{N}$ et $z_1, z_2 \in \mathbf{C}$, alors $z_1^{p^{k+l}} = 1$ et $z_2^{p^{k+l}} = 1$

donc $(z_1 z_2)^{p^{k+l}} = 1$ et $z_1 z_2 \in U_p$. D'autre part $1 \in U_p$ et $(1/z_1)^{p^k} = 1$ si $z_1^{p^k} = 1$. Finalement U_p est bien un sous-groupe de S^1.

b) Soit $z_0 = e^{2i\pi t_0}$ un élément de S^1 avec $t_0 \in [0,1]$. Soit $\varepsilon > 0$. Soit k un entier strictement positif tel que $1/p^k \leq \varepsilon$. On peut alors trouver un entier $s \in [0, p^k]$ tel que $s/p^k \leq t_0 \leq (s+1)/p^k$ (prendre la partie entière de $p^k t_0$). Posons $u = e^{\frac{2i\pi s}{p^k}}$. Alors $u \in U_p$ car $u^{p^k} = 1$. Par ailleurs $|t_0 - \frac{s}{p^k}| \leq \varepsilon$ donc $|z_0 - u| \leq 2\pi\varepsilon$ par inégalité des accroissements finis. Finalement U_p est dense dans S^1.

I.3. a) Soient z_1, z_2 dans U_p. Alors $f(z_2) - f(z_1) = f(z_1)f(z_2/z_1) - f(z_1)$ car f est un morphisme. Comme f est à valeurs dans S^1, on obtient

$$|f(z_2) - f(z_1)| = |f(z_2/z_1) - 1|$$

Soit $\varepsilon > 0$. Comme f est continue en 1, on peut trouver $\eta > 0$ tel que pour tout z dans S^1 tel que $|z-1| \leq \eta$, on ait $|f(z)-1| \leq \varepsilon$. Alors, si $|z_2 - z_1| \leq \eta$, on a $|z_2/z_1 - 1| \leq \eta$ donc $|f(z_2/z_1) - 1| \leq \varepsilon$ soit $|f(z_2) - f(z_1)| \leq \varepsilon$. Finalement f est uniformément continue sur U_p.

b) La suite (x_n) est de Cauchy. Avec a), on voit immédiatement que $f(x_n)$ est de Cauchy dans S^1, qui est une partie complète de $\mathbf{C}$ (car fermée dans $\mathbf{C}$, qui est complet). Ainsi $f(x_n)$ converge dans S^1.

c) (Question difficile, mais méthode classique). Soit $x \in S^1$. D'après I.2.b), on peut écrire x comme limite d'une suite (x_n) d'éléments de U_p, et d'après I.3.a), on peut poser $\bar{f}(x) = \lim(f(x_n))$: cette limite ne dépend pas de la suite (x_n) choisie, car si (y_n) est une autre suite d'éléments de U_p convergeant vers x, alors la suite "mélangée" (z_n) (définie en prenant $z_{2n} = x_n$ et $z_{2n+1} = y_n$) doit aussi vérifier que $(f(z_n))$ converge.

Il reste à montrer que $\bar{f}$ est continue. Soit $\varepsilon > 0$ et soit η comme en a). Soient y, z dans S^1 avec $| y - z | \leq \eta/2$. Par densité de U_p, on peut trouver des suites (y_n), (z_n) d'éléments de U_p convergeant respectivement vers y, z. Pour n assez grand, on a alors $| y_n - z_n | \leq \eta$, donc $| f(y_n) - f(z_n) | \leq \varepsilon$ via a). Maintenant par définition de $\bar{f}$, les suites $(f(y_n))$, $(f(z_n))$ convergent respectivement vers $\bar{f}(y)$, $\bar{f}(z)$, d'où en passant à la limite : $| \bar{f}(y) - \bar{f}(z) | \leq \varepsilon$, ce qui montre que $\bar{f}$ est (uniformément) continue.

L'unicité de $\bar{f}$ résulte du principe de prolongement des identités, U_p étant dense dans S^1. Ce principe donne aussi immédiatement que $\bar{f}$ est un morphisme. Le I.1.e) permet alors de conclure qu'il existe $k \in \mathbf{Z}$ tel que $f(z) = z^k$ pour tout z de U_p.

II

1. a) Soit $x \in B_a$. Par définition de B_a, x s'écrit $x = b + ka$ avec $b \in B$ et $k \in \mathbf{Z}$. Si $x = b' + k'a$ avec $b' \in B$ et $k' \in \mathbf{Z}$, on a $b' - b = (k - k')a$ d'où

$(k-k')a \in B$. Par hypothèse ceci implique $k = k'$, puis $b = b'$ d'où l'unicité cherchée. On peut alors définir g en posant $g(b+ka) = f(b)$ pour tout $b \in B$ et tout $k \in \mathbf{Z}$. L'unicité de l'écriture $x = b + ka$ donne immédiatement que g est bien défini et que c'est un morphisme de B_a dans D qui prolonge f.

b) (Question difficile). Comme B est un sous-groupe de A, l'ensemble des $n \in \mathbf{Z}$ tels que $na \in B$ est un sous-groupe H de $\mathbf{Z}$ (c'est l'image réciproque de B par le morphisme $n \mapsto na$ de $\mathbf{Z}$ dans A). Comme H est par hypothèse non trivial, on sait alors qu'il est de la forme $l\mathbf{Z}$ avec $l > 0$, ce qui montre que $l = m$ (c'est le plus petit élément > 0 de H) et m est bien un générateur de H.

Montrons alors que g est bien définie (i.e. la définition de $g(b + ka)$ ne d'épend pas de l'écriture $b + ka$ d'un élément de B_a, qui n'est plus unique comme en a)). Si un élément x de B_a s'écrit $x = b + ka = b' + k'a$ (avec $b, b' \in B$ et $k, k' \in \mathbf{Z}$), alors $(b' - b) = (k - k')a$. Comme H est engendré par m, on obtient que $(k' - k)$ (qui est dans H) est divisible par m, soit $k' = k + mr$ avec $r \in \mathbf{Z}$. Alors

$$f(b) + kd = f(b' + mra) + kd = f(b') + rf(ma) + kd =$$

$$f(b') + rf(b_0) + kd = f(b') + (rm + k)d = f(b') + k'd$$

ce qui montre que g est bien définie.

Il est alors immédiat que g est un morphisme de B_a dans D qui prolonge f.

c) Que l'on soit dans le cas de la question a) ou de la question b), on a vu que f se prolongeait à B_a (qui contient strictement B si $a \notin B$) : en effet dans le cas b) l'existence de $d \in D$ tel que $f(b_0) = md$ est assurée par l'hypothèse que D est divisible. Il suffit alors d'appliquer le résultat A) admis dans l'introduction pour conclure.

2. a) On applique II.1.c) à l'identité $f : D \to D$. Il existe donc un morphisme $\pi : A \to D$ qui prolonge Id_D, ce qui signifie $\pi(x) = x$ pour tout x de D.

b) On prend pour S le noyau de π. Alors $S \cap D = \{0\}$ puisque π est l'identité sur D. D'autre part tout x de A s'écrit $x = \pi(x) + (x - \pi(x))$ avec $\pi(x) \in D$ et $(x - \pi(x)) \in S$ puisque $\pi(\pi(x)) = \pi(x)$. On a donc l'existence de la décomposition $x = d + s$. L'unicité se déduit immédiatement de ce que $S \cap D = \{0\}$ (bien entendu ceci est tout à fait analogue à une décomposition en somme directe associée à un projecteur dans un espace vectoriel).

Il est alors clair que l'application de $D \times S$ dans A qui envoie (d, s) sur $d + s$ est un isomorphisme de groupes.

III

1. Par définition tout élément x de U_p vérifie $x^{p^k} = 1$ pour un certain $k \in \mathbf{N}$, donc U_p est p-primaire. Il est p-divisible car si $x \in U_p$ vérifie $x^{p^k} = 1$, alors il existe un nombre complexe z tel que $z^p = x$ vu que $\mathbf{C}$ est algébriquement clos. Alors $z^{p^{k+1}} = 1$ et $z \in U_p$.

2. Si m est une puissance de p, alors comme $mx = 0$ pour tout x de $\mathbf{Z}/m\mathbf{Z}$, on obtient que $\mathbf{Z}/m\mathbf{Z}$ est p-primaire. Respectivement si $\mathbf{Z}/m\mathbf{Z}$ est p-primaire, alors il existe un entier k tel que $p^k.\bar{1} = \bar{0}$ dans $\mathbf{Z}/m\mathbf{Z}$ donc m divise p^k et m est de ce fait une puissance de p.

Si maintenant p divise m, alors $\mathbf{Z}/m\mathbf{Z}$ n'est pas p-divisible car $\bar{1}$ n'est pas dans l'image de la multiplication par p (sinon on aurait un entier x tel que m divise $px-1$, donc p diviserait 1). Réciproquement si p ne divise pas m, alors la multiplication par p est injective dans $\mathbf{Z}/m\mathbf{Z}$ via le lemme de Gauss (vu que p est premier avec m), donc surjective par finitude de $\mathbf{Z}/m\mathbf{Z}$ et $\mathbf{Z}/m\mathbf{Z}$ est bien p-divisible.

Finalement $\mathbf{Z}/m\mathbf{Z}$ est p-primaire ssi m est une puissance de p. $\mathbf{Z}/m\mathbf{Z}$ est p-divisible ssi m est premier avec p.

3. Comme G est p-primaire, tout élément de G annule un polynôme du type $X^{p^k} - 1$, qui est scindé à racines simples. D'après le théorème de décomposition des noyaux, tous les éléments de G sont diagonalisables. D'après un résultat rappelé dans l'introduction, les éléments de G sont simultanément diagonalisables. Ainsi il existe une matrice inversible u telle que le sous-groupe uGu^{-1} (qui est conjugué de G, donc isomorphe à G) soit composé de matrices diagonales; on peut donc supposer que tous les éléments de G sont des matrices diagonales. Pour $g \in G$, notons g_i le i-ème coefficient diagonal de g (qui est dans U_p car G est p-primaire). Alors $g \mapsto (g_i)$ est un morphisme injectif de G dans $(U_p)^n$, d'où le résultat.

Remarque : La question VI.2.b) donne en fait que G est isomorphe à un produit $F \times (U_p)^r$ avec F fini p-primaire. Si on connaît la structure des groupes abéliens finis, on obtient de plus que F est un produit de s groupes cycliques p-primaires avec $s + r \leq n$ vu que $G[p]$ est de cardinal p^{r+s} et le cardinal de $(U_p)^n[p]$ est p^n.

4. a) Soit $x \in A$. Soit $k \in \mathbf{N}^*$ tel que $p^k x = 0$. Par Bezout, on peut trouver des entiers u, v tels que $mu + p^k v = 1$. Alors $x = (mu + p^k v)x = m(ux)$, donc x est dans l'image du morphisme de multiplication par m. Comme x est arbitraire, on a montré que ce morphisme était surjectif. Si de plus $mx = 0$, on trouve $x = 0$ donc le dit morphisme a bien un noyau trivial, i.e. il est aussi injectif.

b) Soit $n \in \mathbf{N}^*$, on écrit $n = p^k m$ avec m premier à p. Alors le morphisme $x \mapsto nx$ est composé de la multiplication par p (k fois) qui est surjective parce que A est p divisible, et de la multiplication par m qui est bijective d'après a). Ainsi $x \mapsto nx$ est surjective de A dans A, i.e. A est divisible.

5. Le seul point non trivial est que la formule a un sens. C'est le cas car si λ et μ sont des entiers avec $\bar{\lambda} = \bar{\mu}$, alors $(\lambda - \mu)$ est divisible par p d'où $\lambda x = \mu x$ vu que $px = 0$ pour tout x de $A[p]$.

6. a) Comme $A[p]$ est fini, c'est un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel de dimension finie, il est donc en particulier isomorphe comme groupe à $(\mathbf{Z}/p\mathbf{Z})^r$, où r est sa dimension.

b) L'application u_k est clairement un morphisme de groupe de noyau $A[p]$. Son image est incluse dans $A[p^k]$, donc par le théorème de Lagrange (résultat admis C) de l'introduction), le cardinal de son image divise celui (noté m_k) de $A[p^k]$. Comme le cardinal de $A[p^{k+1}]$ est le produit de celui du noyau de u_k avec celui de l'image de u_k (cf. rappel C) de l'introduction), on obtient que m_{k+1} divise $m_1 m_k$. D'après a), le cardinal de m_1 est une puissance de p d'où le résultat par récurrence sur k. Si maintenant A est un groupe abélien fini p-primaire, la suite des $A[p^k]$ (qui est croissante) est forcément stationnaire, donc $A = A[p^k]$ pour un certain k et le cardinal de A est donc une puissance de p. Réciproquement un groupe abélien fini A de cardinal p^l vérifie $p^l x = 0$ pour tout x de A (en effet le sous-groupe engendré par x est cyclique, de cardinal divisant p^l d'après le théorème de Lagrange), donc est p-primaire.

c) (Question difficile). Soit x_1 une solution. Alors toute solution x est de la forme $x = x_1 + y$ avec $y \in A[p]$. Ainsi il n'y a qu'un nombre fini de solutions, disons $x_1, ..., x_l$. Si aucune de ces solutions n'était dans $\bigcap_{k \in \mathbf{N}^*} p^k A$, il existerait (par finitude) un entier $s > 0$ tel qu'aucun des x_i ne soit dans $p^s A$. Alors x_0 ne serait pas dans $p^{s+1} A$, contradiction. On en conclut que $\bigcap_{k \in \mathbf{N}^*} p^k A$ est un groupe p-divisible.

Remarque : Sans l'hypothèse de finitude de $A[p]$, le résultat est faux. En d'autres termes, le sous-groupe des éléments infiniment p-divisibles peut ne pas être lui-même un groupe p-divisible.

Voir par exemple

http://www.jmilne.org/math/Books/add/addendaB.pdf, page 12.

IV

1. Pour tout $x \neq 0$ de $A[p]$, il existe un entier $m \in \mathbf{N}^*$ tel que $x \notin p^m A$. Comme $A[p]$ est fini, on peut choisir un tel m qui convient pour tous les x non nuls de $A[p]$, et on obtient alors $p^m A \cap A[p] = \{0\}$.

2. Soit $x \in A$. Alors il existe $k > 0$ (qu'on peut supposer $> m$) tel que $p^k x = 0$. Alors $p^{k-1}x \in p^m A \cap A[p]$ donc $p^{k-1}x = 0$. Par récurrence descendante sur k, on obtient alors $p^m x = 0$. Finalement $A = A[p^m]$ et d'après III.6.b., A est fini.

V

1. Ici l'hypothèse que A est p-divisible implique que l'application u_k de II.6.b) a pour image exactement $A[p^k]$ car tout élément x de $A[p^k]$ s'écrit $x = py$ avec $y \in A$, ce qui force $y \in A[p^{k+1}]$. Comme le noyau de u_k est $A[p]$, on obtient $m_{k+1} = m_1 m_k$, où m_k désigne le cardinal de $A[p^k]$. Comme $m_1 = p^r$, on obtient par récurrence sur k que le cardinal m_k de $A[p^k]$ est p^{kr}.

2. a) Comme A est p-divisible, on construit la suite (x_n) par récurrence en choisissant x_{n+1} arbitrairement dans A tel que $px_{n+1} = x_n$, une fois les n premiers termes de la suite construits. Alors $p^{n-1}x_n \neq 0$ et $p^n x_n = 0$ vu que $p^{n-1}x_n = x_1$ (par récurrence sur $n \in \mathbf{N}^*$). Ainsi l'ordre de x_n ne divise pas p^{n-1} et comme il divise p^n, c'est p^n, ce qui signifie que x_n est un générateur de $A[p^n]$ puisque d'après V.1 le groupe $A[p^n]$ est de cardinal p^n.

b) (Question difficile). Comme $A[p^n]$ est cyclique d'ordre p^n engendré par x_n, on définit un isomorphisme Φ_n de $A[p^n]$ sur le sous-groupe $C_{p^n} \subset U_p$ des racines p^n-ièmes de l'unité en envoyant x_n sur $\zeta_{p^n} := e^{\frac{2i\pi}{p^n}}$. Définissons $\Phi : A \to U_p$ par $\Phi(x) = \Phi_n(x)$ si $x \in A[p^n]$. Alors Φ est bien défini car d'une part A est la réunion des $A[p^n]$ (vu que A est p-primaire); d'autre part si x est dans $A[p^n]$ et dans $A[p^m]$ avec par exemple $m > n$, on a bien $\Phi_n(x) = \Phi_m(x)$ vu que si $x = kx_n$, alors $x = kp^{m-n}x_m$ (et $\Phi_n(x_n) = \Phi_m(x_m)^{m-n}$ par définition des Φ_n). Il est alors immédiat que Φ est un isomorphisme car chaque Φ_n l'est et U_p est la réunion des C_{p^n}.

3. a) Comme on l'a vu en III.6.a), r est la dimension de $A[p]$ comme espace vectoriel sur $\mathbf{Z}/p\mathbf{Z}$. Soit donc une base $(a_1, ..., a_r)$ de cet espace vectoriel. La conclusion cherchée traduit exactement le fait que c'est une famille libre.

b) (Question difficile). On construit la suite $(x_{i,n})$ exactement comme la suite (x_n) de V.2.a). L'application donnée est alors bien définie car pour $\lambda_i \in \mathbf{Z}$, $\lambda_i x_{i,n}$ ne dépend que de la classe de λ_i modulo p^n vu que $p^n x_{i,n} = 0$. C'est de manière évidente un morphisme de groupes. Pour montrer que c'est un isomorphisme, il suffit de voir que son noyau est trivial vu que par V.1., les ensembles de départ et d'arrivée ont même cardinal. Montrons ceci par récurrence sur n. Si $\sum_{i=1}^r \lambda_i x_{i,n} = 0$, alors en multipliant par p^{n-1}, on obtient

$$\sum_{i=1}^{r} \lambda_i a_i = 0$$

ce qui donne (d'après a)) que λ_i est divisible par p, soit $\lambda_i = p\mu_i$ avec $\mu_i \in \mathbf{Z}$. Ainsi $\sum_{i=1}^r \mu_i x_{i,n-1} = 0$ et par hypothèse de récurrence chaque μ_i est divisible par p^{n-1}, donc λ_i est divisible par p^n, i.e. $\lambda_i = \bar{0}$ dans $\mathbf{Z}/p^n\mathbf{Z}$ comme on voulait.

c) On observe que si $m > n$, alors on a $x_{i,n} = p^{m-n}x_{i,m}$, ce qui donne immédiatement que A_i est un sous-groupe de A. L'application donnée est clairement un morphisme de groupes. Il est surjectif car son image contient tous les $A[p^n]$ d'après b). Soit (y_i) un élément de son noyau, chaque y_i s'écrit $y_i = \lambda_i x_{i,n_i}$ avec $\lambda_i \in \mathbf{Z}$ et $n_i \in \mathbf{N}^*$, mais nous pouvons supposer que tous les n_i sont égaux à un même n (en prenant pour n le plus grand des n_i). Alors $\sum_{i=1}^r y_i = 0$ donne que tous les λ_i sont divisibles par p^n d'après b), donc $y_i = \lambda_i x_{i,n} = 0$ puisque $p^n x_{i,n} = 0$.

d) Il suffit d'après c) de voir que chaque A_i est isomorphe à U_p. Mais A_i est un groupe p-primaire et p-divisible (vu que $px_{i,n+1} = x_{i,n}$) avec $A_i[p]$ de cardinal p (c'est le groupe engendré par $x_{i,1} = a_i$) d'où la conclusion avec V.2.b).

VI

1. Il est immédiat que D est un sous-groupe de A. Soit $x \in D$. Par définition x s'écrit comme une somme finie $x = \sum_{i=1}^r x_i$, où chaque x_i est dans l'un des groupes D_i. Comme chaque D_i est p-divisible, on peut trouver $y_i \in D_i$ tel que $x_i = pd_i$. Alors $x = py$ avec $y = \sum_{i=1}^r y_i$ (donc $y \in D$), ce qui montre que D est p-divisible. D'autre part D est p-primaire (car c'est un sous-groupe de A), il est donc divisible d'après III.4.b). Enfin, tout sous-groupe divisible de A est l'un des D_i par définition des D_i, donc il est inclus dans D.

2. a) Comme D est divisible, on a en particulier $D \subset \bigcap_{k\in\mathbf{N}^*} p^k A$. Maintenant d'après III.6.c) le groupe $\bigcap_{k\in\mathbf{N}^*} p^k A$ est p-divisible, donc divisible puisqu'il est p-primaire. D'après VI.1., on a $\bigcap_{k\in\mathbf{N}^*} p^k A \subset D$, soit finalement $D = \bigcap_{k\in\mathbf{N}^*} p^k A$.

On remarque alors que $D \cap S = \{0\}$ (d'après l'unicité de la décomposition dans II.2.b)), ce qui donne a fortiori que $\bigcap_{k\in\mathbf{N}^*} p^k S = \{0\}$. Comme $A[p]$ est fini, $S[p]$ est fini et IV.2. s'applique à S, qui est donc fini.

b) D'après II.2.b), le groupe A est isomorphe à $S \times D$. Comme D est p-primaire et p-divisible avec $D[p]$ fini, V.3.d) donne qu'il est isomorphe à U_p^r pour un certain entier r. Comme S est fini et p-primaire, on obtient le résultat en posant $F = S$.

3. Il est immédiat de voir que μ_{p^∞} est un sous-groupe de K^* (même argument qu'en I.2.a)). Il est p-primaire, et p-divisible car K est algébriquement

clos (même argument qu'en III.1). D'autre part l'équation $x^p = 1$ a exactement p solutions dans K (qui sont dans μ_{p^∞} par définition de μ_{p^∞}), car K est algébriquement clos et la dérivée px^{p-1} de $x^p - 1$ n'a pas de racine commune avec $x^p - 1$ (il n'y a donc pas de racine multiple; c'est ici qu'on utilise l'hypothèse que la caractéristique de K est nulle). On peut donc appliquer V.2.b) pour en conclure que μ_{p^∞} est isomorphe à U_p.