Groupes

Marc SAGE

2 juillet 2006

Table des matières

1 Pour s'échauffer

Lesquels parmi les groupes additifs $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, et $\mathbb{Z}^2$ sont isomorphes ?

Solution proposée.
Nous allons montrer qu'aucun n'est isomorphe à l'autre.
Déjà, $\mathbb{R}$ est le seul à ne pas être dénombrable, ce qui montre qu'il n'est pas isomorphe aux trois autres.
Soit $f : \mathbb{Q} \longrightarrow \mathbb{Z}$ un isomorphisme. Pour tout entier q non nul, on a

$$f(1) = f\left(\frac{1}{q} + ... + \frac{1}{q}\right) = qf\left(\frac{1}{q}\right) \in q\mathbb{Z},$$

ce qui montre que $f(1)$ divisible par tout entier non nul. On doit donc avoir $f(1) = 0$, *absurde* par injectivité de f.
Soit $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ un isomorphisme. Pour des entiers a et b, on a

$$f(a,b) = f(a,0) + f(0,b) = f\left(\underbrace{1 + ... + 1}_{a}, 0\right) + f\left(0, \underbrace{1 + ... + 1}_{b}\right) = af(1,0) + bf(0,1),$$

de sorte qu'en prenant $\begin{cases} a = -f(0,1) \\ b = f(1,0) \end{cases}$ on obtienne $f(a,b) = 0$, d'où $a = b = 0$ par injectivité de f. Cela force $f = 0$: contradiction.
Soit $f : \mathbb{Z}^2 \longrightarrow \mathbb{Q}$ un isomorphisme. Pour des entiers a et b, on a comme précédemment

$$f(a,b) = af(1,0) + bf(0,1),$$

de sorte qu'en prenant $\begin{cases} a = -f(0,1)\, d \\ b = f(1,0)\, d \end{cases}$ où d est un dénominateur commun aux fractions $f(1,0)$ et $f(0,1)$ on obtienne $f(da, db) = 0$, d'où contradiction comme avant.

2 Lemme de Dedekind

Soit $n \geq 2$, G un monoïde et $\sigma_1, ..., \sigma_n : G \longrightarrow K^*$ des morphismes multiplicatifs deux à deux distincts. Montrer que

$$\forall \overrightarrow{\lambda} \in K^n,\ \lambda_1\sigma_1 + ... + \lambda_n\sigma_n = 0 \implies \overrightarrow{\lambda} = 0.$$

En d'autres termes, les σ_i sont linéairement K-indépendants dans le K-espace vectoriel des applications de G dans K.

Démonstration.
Par l'absurde. On suppose $\sum_{i=1}^{n} \lambda_i\sigma_i = 0$ où les λ_i ne sont pas tous nuls avec n minimal. Alors, pour tous x, y dans G, on a

$$0 = \left[\sum_i \lambda_i\sigma_i\right](xy) = \left[\sum_i \lambda_i\sigma_i(x)\,\sigma_i\right](y),$$

d'où pour tout j :

$$\sum_i \lambda_i(\sigma_i(x) - \sigma_j(x))\,\sigma_i = \sum_i \lambda_i\sigma_i(x)\,\sigma_i - \sigma_j(x)\sum_i \lambda_i\sigma_i = 0 - 0 = 0$$

Par minimalité de n (remarquer qu'on a tué l'un des scalaires devant les σ_i), on doit avoir a

$$\lambda_i(\sigma_i(x) - \sigma_j(x)) = 0$$

pour tous i, j. En particulier, pour un i tel que $\lambda_i \neq 0$ et pour un $j \neq i$ (possible car $n \geq 2$), on obtient $\sigma_i(x) - \sigma_j(x) = 0$, et ce pour tout x de G, *i.e.* $\sigma_i = \sigma_j$, *absurde* car les σ_i sont deux à deux distintcs.

3 K^* est cyclique pour K corps fini

Soit K un corps et G un sous-groupe fini de K^*. En classifiant les éléments de G selon leur ordre, montrer que G est cyclique. On rappelle au besoin l'identité $\sum_{d|n} \varphi(d) = n$.

Solution proposée.
Notons n le cardinal du groupe G. En notant Ω_d les éléments de G d'ordre d, lequel doit diviser n par Lagrange, on partionne

$$G = \coprod_{d|n} \Omega_d.$$

Pour un $g \in \Omega_d$, les éléments $1, g, g^2, ..., g^{d-1}$ sont distincts et racines du polynôme $X^d - 1$, donc l'ensemble des racines $X^d - 1$ est exactement l'engendré $\langle g \rangle$, ce qui montre que ces engendrés sont les mêmes :

$$\forall g \in \Omega_d,\ \langle g \rangle = \left\{\text{racines de } X^d - 1\right\}.$$

Fixons un élement g_d dans Ω_d. Un autre élément de Ω_d, disons g, appartient à $\langle g \rangle = \langle g_d \rangle$, donc s'écrit g_d^k pour un certain k. En introduisant le pgcd $\delta = d \wedge k$, on a

$$g^{\frac{d}{\delta}} = \left(g_d^k\right)^{\frac{d}{\delta}} = \left(g_d^d\right)^{\frac{k}{\delta}} = 1,$$

ce qui montre que l'ordre d de g divise $\frac{d}{\delta}$, d'où $\delta = 1$. Tout élément de Ω_d s'écrit donc comme une puissance de g_d qui est première avec d, d'où l'inclusion

$$\Omega_d \subset \left\{g_d^k\ ;\ d \wedge k = 1\right\}.$$

En prenant les cardinaux, on obtient la majoration

$$|\Omega_d| \leq \varphi(d).$$

Or, les Ω_d partionnant G, on doit avoir

$$n = |G| = \sum_{d|n} |\Omega_d| \leq \sum_{d|n} \varphi(n) = n,$$

ce qui force l'égalité partout : en particulier, $|\Omega_n| = \varphi(n) > 0$, d'où l'existence d'un élément d'ordre n et la cyclicité de G.

Remarque. Un corollaire immédait est la cyclicité de K^* pour K corps fini, vu K^* est alors un sous-groupe fini de K^*.

4 Groupes fini d'exposant ≤ 2

Soit G un groupe fini où tout élément est involutif :

$$\forall g \in G,\ g^2 = 1.$$

Montrer que G est isomorphe au groupe additif $\mathbb{F}_2^n$ pour un certain entier n (où $\mathbb{F}_2 = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ désigne le corps à deux éléments).

On commencera par montrer que G est abélien, puis on pourra considérer une famille génératrice de G minimale, ou bien mettre une structure de $\mathbb{F}_2$-ev sur G.

Solution proposée.
Soit a et b dans G. On peut écrire

$$ab = a1b = a(ab)^2 b = a(abab)b = a^2(ba)b^2 = ba,$$

d'où le caractère abélien de G. On notera désormais la loi de groupe additivement.

Considérons comme indiqué une famille génératrice $g_1, ..., g_n$, qui existe quitte à prendre tous les éléments de G – c'est là que l'hypothèse de finitude intervient. L'ensemble des cardinaux de telles familles est une partie non vide de $\mathbb{N}$, donc admet un élément minimal, que l'on peut supposer être n.

L'hypothèse de génération signifie exactement que le morphisme de groupes

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{F}_2^n & \longrightarrow & G \\ (\alpha_1, ..., \alpha_n) & \longmapsto & \alpha_1 g_1 + ... + \alpha_n g_n \end{array} \right.$$

est surjectif (φ est bien défini par l'hypothèse d'involution), et la minimalité de n implique l'injectivité de φ : en effet, si l'on suppose $\sum \alpha_i g_i = 0$ où le n-uplet (α_i) est non-nul, alors l'un des α_i vaut 1, mettons $\alpha_{i_0} = 1$, de sorte que g_{i_0} est engendré par les autres g_i : en le retirant, on obtient une famille génératrice de G strictement plus petite que $(g_1, ..., g_n)$, contredisant la minimalité de n. Finalement, φ est un isomorphisme de groupes, ce qui conclut.

Une autre approche consiste à munir G d'une structure de $\mathbb{F}_2$-ev. On dispose déjà d'une loi interne $+$; on va définir une loi externe $\cdot$ de la seule façon possible :

$$\left\{ \begin{array}{l} 0 \cdot g = 0 \\ 1 \cdot g = g \end{array} \right. .$$

Il est aisé de vérifier les axiomes d'un ev. G étant fini, il est de dimension finie n, donc isomorphe à $\mathbb{F}_2^n$ en tant qu'ev, *a fortiori* en tant que groupes abéliens. Joli, non ?

Remarque. En fait, prendre une famille génératrice minimale revient, en termes vectoriels, à considérer une *base*. On ne fait donc, dans la première méthode, que redémontrer qu'un K-ev de dimension d est isomorphe à K^d (avec $K = \mathbb{Z}$, ce qui est quand même tout à fait différent d'un corps).

5 Une caractérisation des groupes abéliens d'ordre impair

Soit G un groupe fini muni d'un automorphisme f involutif tel que $\operatorname{Fix} f = \{1\}$. *Montrer que G est commutatif.*

Solution proposée.

Si G était abélien, tout $a \in G$ commuterait avec $f(a)$, ce qui s'écrit

$$af(a) = f(a)\, a = f(a)\, f(f(a)) = f(af(a)) \implies af(a) \in \operatorname{Fix} f \implies f(a) = a^{-1}.$$

Notre automorphisme est donc nécessairement l'inversion. Réciproquement si l'on prouve que $f = \cdot^{-1}$, on aura montré que G est abélien :

$$ab = f\left(a^{-1}\right) f\left(b^{-1}\right) = f\left(a^{-1}b^{-1}\right) = f\left((ba)^{-1}\right) = ba.$$

Arrêtons là l'analyse.

Nous n'avons pas encore utilisé l'hypothèse G fini. Il est très souvent judicieux sous cette hypohtèse de finitude d'exhiber une gentille application de G dans G qui est injective afin de conclure à sa surjectivité et espérer avancer. La condition $\operatorname{Fix} f = \{1\}$ ressemble à de l'injectivité (penser à l'analogue linéaire $\operatorname{Ker} f = \{0\}$), mais il nous faudrait deux variables. Qu'à cela ne tienne, on les fait apparaître :

$$a = b \iff ab^{-1} = 1 \iff ab^{-1} \in \operatorname{Fix} f \iff f\left(ab^{-1}\right) = ab^{-1} \iff a^{-1} f(a) = b^{-1} f(b).$$

L'application $\varphi : a \mapsto a^{-1} f(a)$ est par conséquent injective, donc surjective, donc atteint tout $a \in G$ en un $x \in G$. On en déduit $f = \cdot^{-1}$ en regardant naturellement le produit :

$$af(a) = \varphi(x)\, f(\varphi(x)) = x^{-1} f(x)\, f\left(x^{-1} f(x)\right) = x^{-1} f(x)\, f(x)^{-1}\, x = 1, \ CQFD.$$

Remarque. En regroupant les éléments de G en paires $\{a, f(a)\}$, qui sont toutes (par injectivité de f) de cardinal 2 à l'exception de $\{1, f(1)\} = \{f(1)\}$, on voit que G est d'ordre impair.

Réciproquement, si G est un groupe abélien fini d'ordre n impair, alors l'inversion est un morphisme dont les points fixes ont un ordre divisant 2 (ils vérifient $a = a^{-1}$, *i.e.* $a^2 = 1$) et n (par Lagrange). Le seul point fixe de l'inversion est donc 1, d'où un automorphisme involutif f tel que $\operatorname{Fix} f = \{1\}$.

6 Premier théorème de Sylow

Soit G un groupe fini de cardinal $n = \prod p_i^{\alpha_i}$. Nous allons montrer que G admet des sous-groupes d'ordre $p_i^{\beta_i}$ pour tout i et pour tout $\beta_i \leq \alpha_i$. Ceci constitue une réciproque partielle au théorème de Lagrange.

• *Soit G un groupe fini abélien et p un premier divisant son cardinal. Montrer que G admet un sous-groupe d'ordre p.*

• *On ne suppose plus G abélien. En introduisant la relation d'équivalence "être conjugués", i.e.*

$$x \sim y \iff \exists g \in G,\ y = gxg^{-1}$$

montrer l'existence de sous-groupes stricts H_i tel que

$$|G| = |Z(G)| + \sum_i \frac{|G|}{|H_i|}.$$

• *Conclure.*

Solution proposée.

• Considérons un système $(g_1, ..., g_r)$ de générateurs de G ; un tel système existe car G est fini (prendre au besoin tous les éléments du groupe). En notant $H := \langle g_1 \rangle \times ... \langle g_r \rangle$, le morphisme

$$\varphi : \left\{ \begin{array}{ccc} H & \longrightarrow & G \\ (a_1, ..., a_r) & \longmapsto & a_1 ... a_r \end{array} \right.$$

est alors surjectif (G est abélien !), d'où l'isomorphisme

$$G \simeq {}^{H}\!/_{\operatorname{Ker}\varphi}.$$

En prenant les cardinaux, $|G|$ doit diviser $|H|$, lequel vaut le produit des ordres ω_i des g_i, donc p divise $\prod \omega_i$, et étant premier il divise l'un des ω_i, mettons $\omega_i = kp$. L'élément g_i^k est alors d'ordre p et son engendré fournit le sous-groupe cherché.

• On laissera au lecteur le soin de vérifier que l'on parle bien d'une relation d'équivalence. En notons Ω_x la classe d'un élément x de G et en prenant un représentant x_i dans chaque classe *distincte* Ω_i, les Ω_i partitionnent G, d'où la relation des cardinaux

$$|G| = \sum |\Omega_i| .$$

Pour faire apparaître le cardinal du centre, on remarque que la classe d'un élément c du centre est réduit au singleton $\{c\}$, et réciproquement. On peut donc réécrire

$$|G| = |Z(G)| + \sum |\Omega_i|$$

où la somme porte sur les classes non triviales. On aimerait bien pouvoir écrire

$$|\Omega_i| = \frac{|G|}{|H_i|}$$

où H_i est un sous-groupe de G (il sera automatiquement strict puisque $|\Omega_i| \geq 2$), ce qui pourrait se faire si l'on avait un isomorphisme

$$\Omega_i \simeq {}^{G}\!/_{H_i}.$$

On se contentera d'une bijection, vu que Ω_i n'a aucune raison d'être muni d'une structure de groupe. Cela sent la factorisation canonique d'applications à plein nez :

$$\operatorname{Im} f \simeq {}^{G}\!/_{\equiv} \text{ où } a \equiv b \iff f(a) = f(b) .$$

On veut une application d'image Ω_i, donc il est naturel de considérer l'application

$$f_i : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & gx_ig^{-1} \end{array} \right. .$$

Deux élément a et b auront même image ssi

$$ax_ia^{-1} = bx_ib^{-1} \iff \left(b^{-1}a\right) x_i = x_i \left(b^{-1}a\right) \iff a \in bH_i$$

où H_i est le sous-groupe des éléments de G qui commutent avec x_i. La factorisation de f_i donne alors une bijection $\Omega_i \simeq {}^{G}\!/_{H_i}$, *CQFD.*

• Soit p^α divisant $n = |G|$ où p est premier ; montrons par récurrence sur n qu'il y a un sous-groupe de G d'ordre p^α. Pour $n = 2$, le résultat est clair. Ensuite, on reprend l'égalité

$$|G| = |Z(G)| + \sum_i \frac{|G|}{|H_i|}$$

prouvée au second point.

S'il y a un i tel que p^α divise $|H_i|$, on conclut par récurrence vu que $|H_i| < n$.

Sinon, p divise $\frac{|G|}{|H_i|}$ pour tout i, donc divise le cardinal du centre. Ce dernier étant abélien, le premier point s'applique : il y a un sous-groupe Z du centre de cardinal p. L'idée est alors de quotient G par ce sous-groupe (abélien), d'en extraire par récurrence un sous-groupe $\mathcal{H}$ d'ordre $p^{\alpha-1}$ (noter que $\left|{}^{G}\!/_{Z}\right| = \frac{|G|}{|Z|} = \frac{n}{p} < n$), puis de remonter à G en posant pour H la réunion des élements de $\mathcal{H}$. L'intérêt est qu'alors $\mathcal{H} = {}^{H}\!/_{Z}$, d'où le cardinal de H souhaité :

$$|H| = |Z|\,|\mathcal{H}| = pp^{\alpha-1} = p^a.$$

Un dessin où l'on découpe (*i.e.* "quotiente") G selon les classes modulo Z pourra aider à voir ce que l'on fait.

Remarque. Si $|G| = \prod p_i^{\alpha_i}$, un sous-groupe de G d'ordre $p_i^{\alpha_i}$ est appelé *p_i-Sylow* de G. Leur étude apporte de nombreuses informations sur la structure du groupe.

Les deuxième et troisième théorèmes de Sylow (on vient de montrer le premier) affirment d'une part que tous les p-Sylow sont conjugués (la réciproque étant claire), d'autre part que leur nombre divise n et est congru à 1 modulo p.

Les deux prochains exercices illustrent l'utilisation des trois théorèmes de Sylow dans des problèmes de classification.

7 Groupes de cardinal pq cycliques : vers le produit semi-direct

Soit G un groupe de cardinal pq avec $p < q$ premiers tels que p ne divise pas $q - 1$. On veut montrer que G est cyclique.

1. *Montrer, à l'aide des théorèmes de Sylow énoncés à l'exercice précédent, que G admet exactement quatre sous-groupes : $\{1\}$, un unique p-Sylow S, un unique q-Sylow T, G.*
2. *Conclure si G est abélien.*
3. *Dans le cas général, mettre une structure de groupe sur $S \times T$ telle que l'application considérée à la question précédente soit un morphisme de groupes.*
4. *Conclure.*

Solution proposée.

1. Soit H un sous-groupe de G. Par le théorème de Lagrange, son cardinal divise celui de G, donc vaut l'une des quatre valeurs $1, p, q, pq$. Les premier et dernier cas sont triviaux : $H = \{1\}$ et $H = G$. Dans les deux autres, H est un sous-groupe de Sylow de G. Regardons le nombre de ces derniers à l'aide de considérations arithmétiques et du troisième théorème de Sylow.

   Soit n_p le nombre de p-Sylow de G. Sylow nous dit que n_p divise pq et est congru à 1 modulo p. Cette dernière congruence montre que n_p n'est pas un multiple de p, donc est premier avec p ; comme il divise pq, il divise q, donc vaut 1 ou q. Si n_p valait q, ce dernier vaudrait 1 modulo p, d'où $p \mid q - 1$, ce qui est exclu par les hypothèses.

   On montrerait de même que le nombre n_q de q-Sylow de G divise p, d'où $n_q \leq p < q$; mais l'on sait de plus que $n_q \equiv 1\,[q]$, ce qui force $n_q = 1$.

   On notera S et T les uniques p-Sylow et q-Sylow de G. Noter qu'ils sont cycliques. Par ailleurs, le second théorème de Sylow nous disent que tous les p Sylow sont conjugués : mais il n'y a qu'un seul, S, lequel doit par conséquent être stable par conjugaison.

2. Si G est abélien, l'application suivante est un morphisme de groupes :

$$\pi : \left\{ \begin{array}{ccc} S \times T & \longrightarrow & G \\ (s,t) & \longmapsto & st \end{array} \right. .$$

Les cardinaux étant les mêmes au départ et à l'arrivée, montrons que π est injectif. Cela montrera que π est bijectif, et G sera isomorphe au produit $S \times T \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{q\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{pq\mathbb{Z}}$ cyclique (lemme chinois).

Partant de $st = 1$, on a $s = t^{-1} \in T$, donc l'ordre de s divise l'ordre $|T| = q$; or, l'ordre de $s \in S$ doit aussi diviser $|S| = p$. Les entiers p et q étant étrangers, l'ordre de s vaut 1, d'où $s = 1$ puis $t = 1$, *CQFD.*

3. Dans le cas général, la loi $(s,t)\,(s',t') = (ss',tt')$ ne fait pas de π un morphisme :

$$\pi\left((s,t)\,(s',t')\right) = \pi\left((ss',tt')\right) = ss'tt' \neq sts't' = \pi\,(s,t)\,\pi\,(s',t')\,.$$

On va alors "tordre" la loi produit pour mettre les termes du produit $ss'tt'$ dans le "bon" ordre. Il s'agit surtout de tordre les deux termes du milieu $s't$ en ts'. Cela peut se faire en conjuguant s' par t, le résultat restant bien dans S car ce dernier est stable par conjugaison. On essaie donc la loi

$$(s,t) * (s',t') := \left(s\ \underline{ts't^{-1}}, tt'\right).$$

Elle a le bon goût de faire de π un morphisme :

$$\pi\left((s,t) * (s',t')\right) = \pi\left(sts't^{-1}, tt'\right) = sts't' = \pi\,(s,t)\,\pi\,(s',t')\,.$$

Mais il n'est pas évident qu'il s'agisse d'une loi de groupe ! Il faut vérifier les trois axiomes.

Le couple $(1,1)$ est neutre :

$$\left\{ \begin{array}{l} (s,t) * (1,1) = \left(st1t^{-1}, t1\right) = (s,t) \\ (1,1) * (s,t) = \left(11s1^{-1}, 1t\right) = (s,t) \end{array} \right. .$$

L'inverse de (s,t), en cherchant un peu, se trouve être $\left(t^{-1}s^{-1}t, t^{-1}\right)$:

$$\left\{ \begin{array}{l} (s,t) * \left(t^{-1}s^{-1}t, t^{-1}\right) = \left(stt^{-1}s^{-1}tt^{-1}, tt^{-1}\right) = (1,1) \\ \left(t^{-1}s^{-1}t, t^{-1}\right) * (s,t) = \left(t^{-1}s^{-1}tt^{-1}st, t^{-1}t\right) = (1,1) \end{array} \right. .$$

L'associativité est la chose la moins évidente à vérifier :

$$\left\{ \begin{array}{c} ((s,t) * (u,v)) * (x,y) = \left(stut^{-1}, tv\right) * (x,y) = \left(stut^{-1}tvx\,(tv)^{-1}, tvy\right) \\ (s,t) * ((u,v) * (x,y)) = (s,t) * \left(uvxv^{-1}, vy\right) = \left(stuvxv^{-1}t^{-1}, tvy\right) \end{array} \right.$$

et ces valeurs sont les mêmes.

Le groupe ainsi obtenu est appelé *produit semi-direct*[1] de S par T, et est noté $S \rtimes T$,

4. Pour conclure, il faudrait montrer que $S \rtimes T$ est cyclique. Soit s et t des générateurs de S et T respectivement. Montrons que (s,t) est un générateur en calculant ses puissances.

Il suffit de montrer que son ordre vaut pq, *i.e.* qu'il est différent de 1 (clair), p ou q (moins clair). Un calcul des premières valeurs ainsi qu'une récurrence immédiate permettent de montrer que $(s,t)^n = \left((st)^n\,t^{-n}, t^n\right)$:

$$(s,t)^{n+1} = (s,t) * \left((st)^n\,t^{-n}, t^n\right) = \left(st\,(st)^n\,t^{-n}t^{-1}, t^{n+1}\right) = \left((st)^{n+1}\,t^{-(n+1)}, t^{n+1}\right).$$

Si (s,t) était d'ordre p, la seconde coordonée indiquerait $t^p = 1$, ce qui est impossible puisque t est d'ordre q premier avec p. Si (s,t) était d'ordre q, la première coordonée dirait $(st)^q = 1$, de sorte que le sous-groupe $\langle st \rangle$ de G (qui n'est pas trivial) serait d'ordre q, donc vaudrait T. Mais il doit contenir st, d'où $s \in T$ et la contradiction.

L'exercice qui suit propose un critère plus général de cyclicité. On pourrait très bien adapter et simplifier la démonstration suivante à l'exercice qui précède, mais nous n'aurions alors pas eu l'occasion de parler de produit semi-direct, ce qui aurait été fort dommage :-).

[1] Plus généralement, si un groupe H agit sur une autre groupe N par automorphisme (*i.e.* si l'on se donne un morphisme de groupes $\varphi : H \longrightarrow \mathrm{Aut}\,N$), on peut définir une loi "tordue" sur le produit $N \times H$ par

$$(n,h)\,(n',h') = \left(n\ \underline{h \cdot n'}, hh'\right).$$

On vérifie qu'il s'agit d'un groupe, noté $N \rtimes_\varphi H$, appelé *produit semi-direct* de $N \times H$ par φ.

Observer que la barre dans le signe $\rtimes$ est du côté du groupe qui agit sur l'autre. On aurait très bien pu munir le produit $H \times N$ d'une loi semblable, d'où un produit semi-direct $H \ltimes_\varphi N$.

8 Un critère de cyclicité

Soit G un groupe d'ordre n. On suppose que n est premier avec $\varphi(n)$. On va montrer que G est cyclique.
• *Montrer que n s'écrit $\prod p_i$ avec les p_i des premiers tous distincts et tels qu'aucun d'eux ne divise $\prod(p_i - 1)$.*
• *Si G est abélien, conclure en considérant le produit des p_i-Sylow.*
• *Soit p l'un des p_i. Montrer que G admet un unique p-Sylow S et que ce dernier est stable par conjugaison.*
• *Montrer que l'on a une injection de ${}^{G}\!/_{Z(S)}$ dans $\operatorname{Aut} S$ où $Z(S)$ désigne le centre de S. En déduire que G commute avec tous ses p-Sylow, puis conclure.*

Solution proposée.
• Décomposons n en $\prod p_i^{\alpha_i}$, de sorte que $\varphi(n)$ se calcule par

$$\varphi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1).$$

Puisque $\varphi(n)$ est premier avec n, tous les α_i doivent valoir 1 et aucun des p_i ne doit diviser $\prod(p_i - 1)$.
• Soit S_i un p_i-Sylow de G : il est cyclique car de cardinal p_i premier, donc $\simeq {}^{\mathbb{Z}}\!/_{p_i\mathbb{Z}}$. Dans le cas abélien, l'application

$$\pi : \left\{ \begin{array}{ccc} \prod S_i & \longrightarrow & G \\ \overrightarrow{s} & \longmapsto & \prod s_i \end{array} \right.$$

est un morphisme de groupes. Montrons que π est injectif. Par l'égalité des cardinaux, π sera alors bijectif, d'où les isomorphismes

$$\prod S_i \simeq \prod {}^{\mathbb{Z}}\!/_{p_i\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{p_1 \ldots p_r\mathbb{Z}} \text{ (lemme chinois)}$$

et la conclusion.

$\operatorname{Ker}\pi$ est un sous-groupe de $\prod S_i$, donc du type $\prod K_i$ où K_i est un sous-groupe de S_i, *i.e.* $K_i = S_i$ ou $\{1\}$. Puisque la partie

$$\{1\} \times \ldots \times \{1\} \times S_i \times \{1\} \times \ldots \times \{1\}$$

est envoyée sur S_i par π, les K_i sont tous réduits à $\{1\}$, *CQFD.*
• Soit S et T deux p-Sylow (cycliques) de G. En considérant la projection canonique modulo S, l'ordre de l'image d'un générateur de T divise p, donc vaut ou bien p, mais alors ${}^{G}\!/_{S}$ contient un élément d'ordre p, qui est exclu au vu des cardinaux, ou bien 1, auquel cas T est envoyé sur le neutre de ${}^{G}\!/_{S}$, *i.e.* $T \subset S$. Par symétrie on a l'égalité, d'où l'unicité de S. Les conjugués de S étant clairement des p-Sylow, S est donc stable par conjugaison.
• Considérons l'application

$$\left\{ \begin{array}{ccc} G & \longrightarrow & \operatorname{Aut} S \\ g & \longmapsto & s \mapsto gsg^{-1} \end{array} \right. ,$$

qui est bien définie par le point qui précède. Son noyau est exactement le centre de S, d'où l'injection souhaitée en passant au quotient. On peut donc voir ${}^{G}\!/_{Z(S)}$ comme un sous-groupe de $\operatorname{Aut} S$; son cardinal $\frac{n}{|Z(S)|}$ doit par conséquent diviser celui de $\operatorname{Aut} S$. S étant isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, son groupe des automorphismes est $\simeq \left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^*$ (envoyer un automorphisme f sur $f(1)$), donc $\frac{n}{|Z(S)|}$ doit diviser $p-1$, et puisque n est premier avec $p-1$, n doit diviser $|Z(S)|$. $Z(S)$ vaut par conséquent G tout entier, donc un élément quelconque de G commute avec S, et ce pour tous les p_i. Cela suffit à montrer que l'application π utilisée au second point est un morphisme de groupes, ce qui conclut.

9 Entremets

Soit G un groupe dont le quotient par son centre Z est cyclique. Montrer que G est abélien.

Solution proposée.
Soit a un élément de G dont la classe $\overline{a}$ modulo Z engendre ${}^{G}\!/_{Z}$. Prenons deux éléments g et g' dans G dont on veut montrer qu'ils commutent. Leurs classes modulo Z sont des puissances de $\overline{a}$, mettons $\overline{g} = \overline{a}^n = \overline{a^n}$. Il y a donc un $z \in Z$ tel que $g = za^n$. De même, on peut écrire $g' = z'a^{n'}$ avec $z' \in Z$. Il est alors clair que g et g' commutent :

$$gg' = zz'a^{n+n'} = g'g.$$

10 Prolongement des caractères

On appelle *caractère* d'un groupe G tout morphisme $\chi : G \longrightarrow \mathbb{C}^*$ à valeur dans le groupe multiplicatif des complexes non nuls.

Soit G un groupe abélien, H un sous-groupe de G et χ un caractère de H. Montrer que χ se prolonge en un caractère de G.

Solution proposée.

Essayons de prolonger χ petit à petit, en rajoutant à H un élément a qui n'est pas dans H. Si l'on y parvient, il suffira de répéter l'opération tant que le groupe $\langle H, a\rangle$ ne vaudra pas G tout entier, procédé qui est assuré de terminer étant donnée la finitude de G.

On veut prolonger χ à $\langle H, a\rangle$; on a envie de poser

$$\overline{\chi}\left(ha^r\right) = \chi\left(h\right)\chi\left(a\right)^r,$$

mais $\chi(a)$ n'a aucun sens. Cependant, il y a une puissance de a qui tombe dans H : considérer l'ordre n de la classe de a dans ${}^{G}\!/_{H}$. Ainsi, $\chi(a^n)$ a un sens, et puisqu'on doit avoir $\overline{\chi}(a^n) = \overline{\chi}(a)^n$, le complexe $\overline{\chi}(a)$ doit être défini comme une racine n-ième de $\overline{\chi}(a^n) = \chi(a^n)$. Il faut donc poser

$$\overline{\chi}\left(ha^r\right) = \chi\left(h\right)\alpha^r.$$

où α est une telle racine. Sous cette forme, il est clair que $\overline{\chi}$ est un morphisme qui prolonge χ, mais rien ne garantit encore la validité de la formule ci-dessus.

Pour que $\overline{\chi}$ soit bien défini, il s'agit de montrer que

$$ha^r = 1 \implies \chi\left(h\right)\alpha^r = 1.$$

En effet, si l'on a deux écritures $ha^r = h'a^{r'}$ d'un même élément de $\langle H, a\rangle$, l'implication précédente donne

$$h'h^{-1}a^{r'-r} = 1 \implies \chi\left(h'h^{-1}\right)\alpha^{r'-r} = 1 \implies \chi\left(h'\right)\alpha^{r'} = \chi\left(h\right)\alpha^r$$

puisque χ est un morphisme. Partant de $ha^r = 1$, la puissance $a^r = h^{-1}$ est dans H, donc r est un multiple de l'ordre de a dans ${}^{G}\!/_{H}$ (*i.e.* n), mettons $r = ns$, ce qui donne $1 = h\ (a^n)^s$. On peut appliquer χ vu que tout le monde est dans H :

$$1 = \chi\left(h\right)\ \chi\left(a^n\right)^s = \chi\left(h\right)\ \left(\alpha^n\right)^s = \chi\left(h\right)\ \alpha^r,\ \textit{CQFD.}$$

11 Dévissage de groupes à l'aide d'une rétraction

Soit H un sous-groupe d'un groupe G abélien et $\rho : G \longrightarrow G$ une rétraction *de G sur H,* i.e. *un morphisme vérifiant* $\begin{cases} \rho_{|H} = \mathrm{Id}_H \\ \rho\left(G\right) \subset H \end{cases}$ *. Montrer que G est isomorphe à ${}^{G}\!/_{H} \times H$.*

Solution proposée.

Nous allons expliciter l'isomorphisme. Dans cet esprit, il n'y a pas trente-six mille manières de procéder. On veut un morphisme à valeurs dans un produit, il s'agit d'en trouver plusieurs à valeurs dans chaque composante. Dans le cas qui nous intéresse, le morphisme canonique à valeurs dans ${}^{G}\!/_{H}$ est donné par la projection canonique π, et pour atterrir dans H la rétraction de l'énoncé nous tend les bras. Montrons donc que le morphisme

$$\pi \times \rho : \begin{cases} G & \longrightarrow & {}^{G}\!/_{H} \times H \\ g & \longmapsto & \left(\pi\left(g\right), \rho\left(g\right)\right) \end{cases}$$

est bijectif.

Pour l'injectivité, on part de $\begin{cases} \pi\left(g\right) = 1 \\ \rho\left(g\right) = 1 \end{cases}$. La première ligne nous dit que $g \in H$, d'où (par propriété de ρ) $1 = \rho\left(g\right) = g$.

La surjectivité est (un peu) plus délicate. Soit $\left\{ \begin{array}{c} \pi(g') \in {}^{G}\!/_{H} \\ h' \in H \end{array} \right.$ que l'on cherche à atteindre par un $g \in G$. Cela s'écrit

$$\left\{ \begin{array}{c} \pi(g) = \pi(g') \\ \rho(g) = h' \end{array} \right. \iff \left\{ \begin{array}{c} \exists h \in H,\ g = hg' \\ h' = \rho(g) \end{array} \right. \iff \left\{ \begin{array}{c} \exists h \in H,\ g = hg' \\ h' = h\rho(g') \end{array} \right. \iff \left\{ \begin{array}{c} g = hg' \\ h = \frac{h'}{\rho(g')} \end{array} \right. .$$

Il suffit donc de prendre $g = \frac{g'h'}{\rho(g')}$.

Remarque. La propriété $G \simeq {}^{G}\!/_{H} \times H$, bien que très alléchante d'un point de vue calcul formel, n'est pas du tout vraie en général. Prendre par exemple n'importe quel groupe cyclique G d'ordre n^2 et un sous-groupe H d'ordre n, à l'instar de $\{-1, 1\} \subset \{1, i, -1, -i\}$: tous les éléments de ${}^{G}\!/_{H} \times H$ sont tués après n itérations, mais G contient un élément d'ordre n^2.

12 Exposant d'un groupe

On appelle *exposant* d'un groupe G le ppcm des ordres de ses éléments (qui peut être infini).
On notera $\omega(g)$ l'ordre d'un élément $g \in G$ et $a \vee b$ le ppcm des entiers a et b.

Montrer que l'exposant d'un groupe abélien fini G est atteint, i.e.

$$\exists g_0 \in G,\ \omega(g_0) = \bigvee_{g \in G} \omega(g)$$

Solution proposée.
Comme dans tous les problèmes de groupes finis, c'est la décomposition du cardinal de notre groupe qui contient la "complexité" du groupe :

$$n = \prod p_i^{\alpha_i}.$$

L'énoncé demande de trouver un élément g_0 de G dont l'ordre est multiple des ordres de tous les autres éléments. Puisque l'ordre d'un $g \in G$ est de la forme $\prod p_i^{\gamma_i}$ (il divise l'ordre de G), les puissances γ_i du g_0 que l'on cherche doivent être plus grandes que les γ_i de tous les $g \in G$. D'où l'idée de considérer, parmi les éléments d'ordre une puissance de p_i (il y a toujours au moins le neutre), un élément g_i tel que cette puissance soit maximale, disons $\omega(g_i) = p^{\beta_i}$. Un lemme classique assure que le produit $g_0 = \prod g_i$ est d'ordre $\prod p^{\beta_i}$.
Vérifions que tout ce passe comme on le souhaite. Soit $\prod p_i^{\gamma_i}$ l'ordre d'un $g \in G$. Alors g puissance $\prod_{j \neq i} p_j^{\gamma_j}$ est d'ordre $p_i^{\gamma_i}$, donc $\gamma_i \leq \beta_i$ par maximalité de β_i, et ce pour tout i, ce qui montre que $\omega(g) \mid \omega(g_0)$. Ploum.

13 Structure des groupes abéliens finis

Soit G un groupe abélien fini. À l'aide des trois exercices précédents, montrer que G est isomorphe à un produit de ${}^{\mathbb{Z}}\!/_{d_i\mathbb{Z}}$ avec les relations de divisibilité $d_i \mid d_{i+1}$ et unicité de tels d_i :

$$\left\{ \begin{array}{c} G \simeq {}^{\mathbb{Z}}\!/_{d_1\mathbb{Z}} \times ... \times {}^{\mathbb{Z}}\!/_{d_n\mathbb{Z}} \\ d_1 \mid d_2 \mid ... \mid d_n \end{array} \right. .$$

Pour l'unicité des d_i, on pourra montrer l'isomorphisme suivant :

$$a\,{}^{\mathbb{Z}}\!/_{b\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{\frac{b}{a \wedge b}\mathbb{Z}}.$$

Solution proposée.

Existence.

Si le résultat à montrer est juste (et il l'est), l'exposant de G apparaît comme étant le plus grand des d_i. On peut voir l'amorce d'une récurrence en dévissant successivement G à l'aide des ${}^{\mathbb{Z}}\!/_{d_i\mathbb{Z}}$. Le point délicat sera d'exhiber la rétraction.

Soit $a \in G$ d'odre l'exposant e de G. Le sous-groupe H engendré par a est cyclique de cardinal e, donc isomorphe au groupe μ_e des racines e-ièmes de l'unité ; on a ainsi un caractère $\chi : H \longrightarrow \mu_e$, qui se prolonge en un caractère $\overline{\chi} : G \longrightarrow \mathbb{C}^*$. Mais l'intérêt de considérer l'exposant de G est que ce nouveau caractère reste à valeurs dans μ_e :

$$\forall g \in G,\ g^e = 1 \implies \overline{\chi}(g)^e = 1.$$

On peut donc considérer le morphisme $\chi^{-1} \circ \overline{\chi}$, qui est trivialement une rétraction de G sur H, d'où un dévissage

$$G \simeq {}^{G}\!/_{H} \times H \simeq G' \times {}^{\mathbb{Z}}\!/_{e\mathbb{Z}}$$

où $G' = {}^{G}\!/_{H}$. Pour conclure la récurrence, il faudrait montrer que l'exposant e' de G' divise e. Mais cela est évident : en considérant un élément $\pi(b)$ de G' d'ordre e', l'identité $b^e = 1$ passe modulo H :

$$\pi(b)^e = \pi(b^e) = \pi(1) = 1 \implies e' \mid e.$$

Unicité

Il s'agit essentiellement d'une affaire de combinatoire.

Montrons l'isomorphisme donné. Un démarche naturelle est de regarder la multiplication par a :

$$\varphi : \left\{ \begin{array}{ccc} {}^{\mathbb{Z}}\!/_{\frac{b}{a\wedge b}\mathbb{Z}} & \longrightarrow & a\,{}^{\mathbb{Z}}\!/_{b\mathbb{Z}} \\ \widetilde{x} & \longmapsto & \overline{ax} \end{array} \right.$$

où les barres et tildes marquent respectivement les classes modulos b et $\frac{b}{a\wedge b}$. Est-ce le morphisme φ est bien défini ?

$$\widetilde{x} = \widetilde{y} \implies \frac{b}{a\wedge b} \mid y - x \implies \underbrace{\frac{a}{a\wedge b}}_{\text{entier}} b \mid ay - ax \implies \overline{ay} = \overline{ax}, \text{ OK.}$$

A-t-on l'injectivité de φ ?

$$\overline{ax} = \overline{0} \implies b \mid ax \implies \frac{b}{a\wedge b} \mid \frac{a}{a\wedge b}x \implies \frac{b}{a\wedge b} \mid x \implies \widetilde{x} = \widetilde{0}$$

car $\frac{b}{a\wedge b}$ et $\frac{a}{a\wedge b}$ sont premiers entre eux. La surjectivité de φ étant claire, l'isomorphisme est montré.

Supposons à présent que G se décompose de deux manières

$$\prod_{i=1}^{m} {}^{\mathbb{Z}}\!/_{c_i\mathbb{Z}} \simeq G \simeq \prod_{j=1}^{n} {}^{\mathbb{Z}}\!/_{d_j\mathbb{Z}}$$

avec les divisibilités $\left\{ \begin{array}{c} c_i \mid c_{i+1} \\ d_j \mid d_{j+1} \end{array} \right.$. En regardant les d_1-ièmes itérés des éléments de G (ce qui revient à multiplier la relation ci-dessus par d_1), on obtient (en utilisant l'isomorphisme donné)

$$\prod_{i=1}^{m} {}^{\mathbb{Z}}\!/_{\frac{c_i}{d_1\wedge c_i}\mathbb{Z}} \simeq \prod_{j=1}^{n} {}^{\mathbb{Z}}\!/_{\frac{d_j}{d_1\wedge d_j}\mathbb{Z}} = \prod_{j=1}^{n} {}^{\mathbb{Z}}\!/_{\frac{d_j}{d_1}\mathbb{Z}} \text{ car } d_1 \mid d_j$$

d'où en prenant les cardinaux

$$\prod_{i=1}^{m} \frac{c_i}{c_i \wedge d_1} = \prod_{j=1}^{n} \frac{d_j}{d_1}.$$

Or, en regardant le cardinal de $G \simeq \prod_{j=1}^{n} {}^{\mathbb{Z}}\!/_{d_j\mathbb{Z}}$, on voit que $\prod c_i$ et $\prod d_j$ ont même valeur, ce qui permet de simplifier la relation précédente et d'en tirer

$$d_1^n = \prod_{i=1}^{m} (c_i \wedge d_1) \leq \prod_{i=1}^{m} d_1 = d_1^m \implies n \leq m.$$

Par symétrie, il vient $n = m$, puis le cas d'égalité impose $c_1 \wedge d_1 = d_1$, d'où $d_1 \mid c_1$ et l'égalité $c_1 = d_1$ par symétrie.

On regarde ensuite les d_2-ièmes itèrés de G, et on recommence le même procédé, en tenant compte de l'égalité $c_1 = d_1$, pour aboutir à $c_2 = d_2$, et ainsi de suite. L'égalité $n = m$ assure que l'on épuise les c_i en même temps que les d_j, ce qui conclut la preuve.

14 Indécomposabilité des sous-groupes de Prüffer

Donnons-nous un nombre premier p. On se place sur le cercle unité $\mathbb{S}_1$ du plan complexe, et on considère le groupe

$$\mathcal{G} = \left\langle e^{2\pi i \frac{1}{p^\alpha}} \ ; \alpha \in \mathbb{N} \right\rangle$$

des éléments de $\mathbb{S}_1$ d'ordre une puissance de p.

Montrer que $\mathcal{G}$ est indécomposable, i.e. *que*

$$\mathcal{G} \overset{\text{groupes}}{\simeq} A \times B \implies \left\{ \begin{array}{l} A \simeq 0 \\ B \simeq \mathcal{G} \end{array} \right. \text{ ou } \left\{ \begin{array}{l} A \simeq \mathcal{G} \\ B \simeq 0 \end{array} \right. .$$

On pourra montrer que les sous-groupes stricts de $\mathcal{G}$ sont tous finis.

Solution proposée.

Regardons tout d'abord à quoi ressemble notre groupe $\mathcal{G}$. On commence déjà par se débarasser des $e^{2\pi i}$ en passant de $\mathbb{S}_1$ à $\mathbb{R}/\mathbb{Z}$ via l'isomorphisme de groupes

$$f : \left\{ \begin{array}{ccc} (\mathbb{S}_1, \times) & \longrightarrow & \left(\mathbb{R}/\mathbb{Z}, +\right) \\ e^{2\pi i x} & \longmapsto & x \end{array} \right. ,$$

de sorte que décrire $\mathcal{G}$ devient plus commode :

$$\mathcal{G} \simeq f(\mathcal{G}) = \left\langle \frac{1}{p^\alpha} \ ; \alpha \in \mathbb{N} \right\rangle = \left\{ \sum_{\alpha \geq 1} \frac{k_\alpha}{p^\alpha} \ ; (k_\alpha) \in \mathbb{Z}^{(\mathbb{N})} \right\} := G$$

(α est pris ≥ 1 car on raisonne modulo $\mathbb{Z}$).

Revenons à l'énoncé. Supposons $\mathcal{G} \overset{\varphi}{\simeq} A \times B$. Il est bon de remarquer qu'on dispose d'une suite de morphismes injectifs

$$\left\{ \begin{array}{ccccccc} A & \overset{i_A}{\hookrightarrow} & A \times B & \overset{\varphi^{-1}}{\longrightarrow} & \mathcal{G} & \overset{f^{-1}}{\longrightarrow} & G \\ a & \longmapsto & (a, 1_B) & & & & \end{array} \right.$$

et donc que A peut être vu comme un sous-groupe de G. Ce qui nous amène naturellement à étudier les sous-groupes de G pour savoir à quoi ressemble A.

Le point fondamental à remarquer est que, pour un élément $\sum_{\alpha \geq 1} \frac{k_\alpha}{p^\alpha}$, que l'on peut toujours écrire

$$\sum_{\alpha=1}^{n} \frac{k_\alpha}{p^\alpha} \text{ avec } k_n \notin p\mathbb{Z},$$

c'est l'entier n qui est la donnée cruciale pour l'étude des sous-groupes.

En effet, si l'on borne cet entier n, mettons $n \leq M$, alors on obtient clairement un sous-groupe

$$G_M = \left\{ \sum_{\alpha=1}^{M} \frac{k_\alpha}{p^\alpha} \ ; (k_1, ..., k_M) \in \mathbb{Z}^M \right\} = \left\langle \frac{1}{p}, \frac{1}{p^2}, ..., \frac{1}{p^M} \right\rangle .$$

On a aussi un sous-groupe évident :

$$G_\infty = \left\langle \frac{1}{p}, \frac{1}{p^2}, ..., \frac{1}{p^n}, ... \right\rangle = G.$$

On va montrer que les G_n pour $n \in \mathbb{N} \cup \{\infty\}$ sont les seuls sous-groupes de G en utilisant le lemme suivant (qui étudie la donnée cruciale décrite ci-dessus).

Lemme.

Si un sous-groupe H de G contient un élément $x = \sum_{\alpha=1}^{n} \frac{k_\alpha}{p^\alpha}$ avec $k_n \notin \mathbb{Z}p$, alors H contient G_n.

Pour montrer cela, on récurre sur n. Le cas $n = 0$ étant trivial, on prendra $n \geq 1$

On va commencer par récupérer le terme $\frac{1}{p}$ dans H. Puisque la multiplication dans $\mathbb{N}$ est l'itération de l'addition, les sous-groupes additifs de G (ceux qui nous intéressent) sont stables par multiplication par un entier. Ainsi, H contient

$$p^{n-1}x = k_1 p^{n-1} + ... + k_{n-1} + \frac{k_n}{p} = \frac{k_n}{p}.$$

Puisque p est premier, l'hypothèse $k_n \notin p\mathbb{Z}$ signifie $k_n \wedge p = 1$, d'où par Bézout des entiers u et v tels que

$$k_n u + pv = 1.$$

On en déduit que H contient

$$u\frac{k_n}{p} = \frac{uk_n}{p} = \frac{1-pv}{p} = \frac{1}{p} - v = \frac{1}{p},$$

donc aussi l'élément

$$p \times \left(x - k_1 \frac{1}{p} \right) = \sum_{\alpha=1}^{n-1} \frac{k_{\alpha+1}}{p^\alpha}.$$

Par récurrence on obtient $G_{n-1} \subset H$. On peut alors récupérer le terme $\frac{1}{p^n}$. En effet, H contient

$$x - \sum_{\alpha=1}^{n-1} \frac{k_\alpha}{p^\alpha} = \frac{k_n}{p^n},$$

donc le terme

$$u\frac{k_n}{p^n} + \frac{v}{p^{n-1}} = \frac{1-pv}{p^n} + \frac{v}{p^{n-1}} = \frac{1}{p^n}.$$

Ainsi,

$$G_n = \left\langle G_{n-1}, \frac{1}{p^n} \right\rangle \subset H.$$

Ce lemme étant prouvé, la structure des sous-groupes de G tombe d'elle même.

En effet, soit H un sous-groupe de G. Notons

$$M = \max_{\mathbb{N}\cup\{\infty\}} \left\{ n \; ; H \text{ contient un } \sum_{\alpha=1}^{n} \frac{k_\alpha}{p^\alpha} \text{ avec } k_n \notin p\mathbb{Z} \right\}.$$

- Si M est fini, alors clairement $H \subset G_M$, et par le lemme $G_M \subset H$, d'où $G = G_M$.
- Si $M = \infty$, alors H contient un $\sum_{\alpha=1}^{n} \frac{k_\alpha}{p^\alpha}$ avec $k_n \notin \mathbb{Z}p$ et n arbitrairement grand, donc contient (par le lemme) tous les G_n, *i.e.* tous les $\widetilde{\frac{1}{p^n}}$, *i.e.* G ; d'où $H = G$.

Ainsi,

les sous-groupes de G sont exactement les G_n pour $n \in \mathbb{N} \cup \{\infty\}$.

On remarquera par ailleurs, pour suivre les indications de l'énoncé, que les $G_{n<\infty}$ sont finis. En effet, on peut toujours écrire

$$G_n = \left\{ \sum_{\alpha=1}^{n} \frac{k_\alpha}{p^\alpha} \; ; (k_1, ..., k_n) \in \{0, ..., p-1\}^n \right\}$$

en écrivant les k_α en base p, d'où

$$\#G_n = \#\{0, ..., p-1\}^n = p^n.$$

Concluons. On part de $\mathcal{G} \overset{\varphi}{\simeq} A \times B$ et on se souvient du diagramme

$$\left\{ \begin{array}{ccccccc} A & \overset{i_A}{\hookrightarrow} & A \times B & \overset{\varphi^{-1}}{\longrightarrow} & \mathcal{G} & \overset{f^{-1}}{\longrightarrow} & G \\ a & \longmapsto & (a, 1_B) & & & & \end{array} \right. .$$

On vient de voir que $\left\{ \begin{array}{l} f^{-1}\varphi^{-1} i_A (A) = G_a \\ f^{-1}\varphi^{-1} i_B (B) = G_b \end{array} \right.$ en tant que sous-groupes de G, où $a, b \in \mathbb{N} \cup \{\infty\}$. Regardons les quatre cas possibles – en fait trois, par symétrie de A et B.

Si a et b sont finis, on devrait avoir

$$\#\mathcal{G} = \#(A \times B) = \#(G_a \times G_b) = \#G_a \times \#G_b \leq p^a p^b < \infty,$$

absurde car G est infini (il contient tous les $\frac{1}{p^\alpha}$ pour $\alpha \geq 1$).

Si a et b sont infinis, on aurait l'isomorphisme

$$G \simeq G \times G.$$

En remarquant que les éléments d'ordre au plus p^n dans G sont exactement les éléments de G_n, et que (du coup) les éléments d'ordre au plus p^n dans $G \times G$ sont exactement les éléments de $G_n \times G_n$, on obtient une contradiction en prenant les cardinaux ("être d'ordre au plus ω" est une notion qui passe à l'isosomorphisme).

Dans le cas contraire, disons si a est fini et $b = \infty$, le même argument tient la route : être d'ordre au plus p^a dans $G \times G_a$ signifie être dans $G_a \times G_a$, ce qui impose l'égalité des cardinaux

$$|G_a \times G_a| = |G_a| \implies a = 0 \implies G_a \simeq \{0\}\,,\ \textit{CQFD.}$$