

1) et 2)

J'ai appris *a posteriori* que le cours vous signalait tous les  $a\mathbf{Z}$  comme sous-groupes de  $\mathbf{Z}$ , et vous disait même que tout sous-groupe de  $\mathbf{Z}$  est de cette forme. Les questions 1 et 2 font donc double emploi avec le cours, auquel je renvoie. Je souligne tout de même que la question 2 b) a été étonnamment maltraitée, je m'attendais à ce que vous fussiez plus nombreux à savoir que :

Toute partie non vide de  $\mathbf{N}$  admet un plus petit élément.

Ceux qui ne le savaient pas pourront, s'ils le souhaitent, le recopier cinq cents fois (c'est facultatif).

3) Un exemple simple en est  $\{(k, k) \mid k \in \mathbf{Z}\}$ . Vérifier que c'est un sous-groupe est facile mais prend quelques lignes, que je crains inévitables en l'état de ce que je sais figurer dans votre cours.

4) Le mieux est de faire soigneusement les inclusions dans les deux sens.

\* Soit  $(x, y) \in \mathbf{Z} \times 6\mathbf{Z}$ . Par les hypothèses sur  $H_x$  et  $H_y$ , les couples  $(x, 0)$  et  $(0, y)$  sont tous deux dans le sous-groupe  $H$ , qui est stable par addition. Leur somme y est donc aussi, or leur somme c'est  $(x, y)$ .

\* Soit  $(x, y) \in H$ . Vu l'hypothèse sur  $H_x$ ,  $(x, 0) \in H$ . Comme  $H$  est un sous-groupe,  $(x, y) - (x, 0) \in H$ , c'est-à-dire  $(0, y) \in H$ . Vu l'hypothèse sur  $H_y$ ,  $y \in 6\mathbf{Z}$ . On en conclut que  $(x, y) \in \mathbf{Z} \times 6\mathbf{Z}$ .

5) Là aussi je recommande la double inclusion.

\*  $5\mathbf{Z} \times \{0\} = H_x \cap H$  (c'est l'intersection de  $H$  avec quelque chose).

\* Dans l'autre sens, soit  $(x, y) \in H$ . Alors d'une part  $(5x, 5y) = (x, y) + (x, y) + (x, y) + (x, y) + (x, y) \in H$  et d'autre part  $(5x, 0) \in H$ , vu l'hypothèse sur  $H_x$ . Leur différence est donc aussi dans  $H$ , différence qui vaut  $(0, 5y)$ . Cet élément de  $H$  est dans  $H_y$  puisque sa première coordonnée est nulle, donc il est nul vu l'hypothèse sur  $H_y$ . Donc  $5y = 0$ , donc  $y = 0$ , donc  $(x, y) \in H_x$  c'est-à-dire  $(x, y) \in 5\mathbf{Z} \times \{0\}$ .

6) L'ensemble des éléments dont la somme des deux coordonnées est paire convient. Il n'est pas trop long de vérifier que c'est un sous-groupe si on prend la précaution de le présenter sous cette forme.

7) Plein de façons de faire, mais aucune n'est absolument évidente. En voici une, ce n'est pas la seule.

On va montrer un peu plus, à savoir qu'il n'existe pas de morphisme injectif de  $\mathbf{Z}^2$  vers  $\mathbf{Z}$ . Soit en effet  $\varphi$  un morphisme de  $\mathbf{Z}^2$  vers  $\mathbf{Z}$ . Notons  $a = \varphi(1, 0)$  et  $b = \varphi(0, 1)$ . On constate alors que  $\varphi(b, -a) = b\varphi(1, 0) - a\varphi(0, 1) = 0$  (j'ai utilisé implicitement que pour  $\varphi$  morphisme de groupes additif,  $x$  dans le groupe de départ et  $k \in \mathbf{Z}$ ,  $\varphi(kx) = k\varphi(x)$  qui est facile à montrer à supposer qu'on ne le sache pas déjà). Donc de deux choses l'une : ou bien  $(b, -a) \neq (0, 0)$  et alors on a trouvé un élément non nul dans le noyau, donc  $\varphi$  n'est pas injectif, ou bien  $(b, -a) = (0, 0)$  mais alors  $a = 0$  donc  $\varphi(1, 0) = 0$  et là aussi on a sous la main un élément non nul du noyau. Le morphisme  $\varphi$  n'est donc pas injectif.

8) Comme plus haut, on attendait que vous utilisassiez la proposition que j'ai mise en relief et que, le cas échéant, vous recopiez cinq cent fois de plus.

9) Comme  $0 < D$  la division euclidienne suggérée existe. On l'effectue donc : on écrit  $v = Dq + r$  où  $0 \leq r < D$ . L'élément  $q(C, D)$  est alors dans  $H$  puisque  $(C, D)$  est dans  $H$ , donc aussi la différence  $(u, v) - q(C, D) = (u - qC, r)$ . Or par définition de  $D$  le sous-groupe  $H$  ne contient pas d'éléments dont la deuxième coordonnée est un entier strictement entre 0 et  $D$ , donc  $r = 0$  ce qui prouve que  $D$  divise  $v$ .

10) On continue avec les notations du 9) (l'énoncé aurait d'ailleurs dû dire que  $u$  et  $v$  étaient les mêmes qu'à la question précédente, désolé pour ceux qui ne l'ont pas compris, c'est ma faute). On en est à savoir que  $(u - qC, 0)$  est un élément de  $H$ , et cet élément est dans  $H_x$  puisque sa deuxième coordonnée est nulle. Vu l'hypothèse sur  $H_x$  cet élément est nul, donc  $u = qC$  ce qui, à la suite du  $v = qD$  obtenu à la question précédente, pourvu que  $(u, v) = q(C, D)$ .

11) On introduit  $\varphi : \mathbf{Z} \rightarrow H$  qui à  $k$  associe  $k(C, D)$ . Comme  $D$  n'est pas nul, si  $\varphi(k) = 0$  alors  $k = 0$  donc  $\text{Ker } \varphi = \{0\}$  et  $\varphi$  est injective. La question 10 a prouvé que  $\varphi$  était surjective. Enfin  $\varphi$  est un morphisme, ce qu'on montre directement par calcul très facile et fastidieux. Comme un tel calcul serait répété dans la suite, on affirmera une bonne fois pour toutes (et on montrera si on est méticuleux) que pour tout  $(c, d)$  fixé dans  $\mathbf{Z}^2$  l'application  $k \mapsto k(c, d)$  est un morphisme injectif de  $\mathbf{Z}$  dans  $\mathbf{Z}^2$ .

12) J'ai réalisé en corrigeant les copies que cette question était plus difficile que je ne la sentais, parce que bien que sa solution ne nécessite aucune idée originale, les idées qui y sont ne vous sont certainement pas familières. Je commence donc par souligner que pas mal de monde m'a rendu une solution correcte qui recopiait en gros les preuves des questions 1) et 2) en y ajoutant quelques parenthèses, virgules et zéros. C'est tout à fait honnête et me convient. Comme on est là pour progresser voyons comment on peut faire pour ne pas refaire trente fois la même chose : on peut profiter du fait que le fait que les calculs se reproduisent à l'identique, c'est le symptôme de l'existence d'un isomorphisme, et faire l'effort d'explicitier cet isomorphisme,

après quoi tout tombe tout cuit. Essayons donc cette solution plus “savante”.

Vu le principe général énoncé juste plus haut, l'application  $\varphi : \mathbf{Z} \rightarrow \mathbf{Z}^2$  définie par  $k \mapsto k(1, 0) = (k, 0)$  est un morphisme injectif. Celle obtenue par restriction de son ensemble d'arrivée à  $\varphi(\mathbf{Z}) = \mathbf{Z} \times \{0\}$  est donc un isomorphisme. Les sous-groupes de  $\mathbf{Z} \times \{0\}$  sont alors plus ou moins clairement les images des sous-groupes de  $\mathbf{Z}$  par cet isomorphisme, et ce sont donc les  $a\mathbf{Z} \times \{0\}$ . Il existe donc un  $a$  tel que  $H_x = a\mathbf{Z} \times \{0\}$ . On peut poser  $A = |a|$  et noter qu'il n'est pas nul parce qu'on a supposé  $H_x \neq \{(0, 0)\}$ .

13) Ce coup-ci on récupère encore le résultat abstrait écrit en conclusion du 11, cette fois pour  $(c, d) = (A, 0)$ . Comme plus haut, la restriction de ce morphisme où on remplace l'ensemble d'arrivée par l'image de  $\varphi$  est un isomorphisme, celui qui répond à la question.

14) a) Une dernière fois, vous pourrez recopier cinq cents fois l'énoncé que j'ai mentionné au début de ce corrigé. Si vous ne l'avez toujours pas mémorisé, recommencez encore cinq cents fois, mais pas davantage - le cas serait désespéré.

b) Simple calcul pas passionnant.

c) Soit  $(m, n)$  un élément du noyau de  $\varphi$ . Cela signifie que  $(mA + nC, nD) = (0, 0)$ . Comme  $D$  est le plus petit élément d'une partie de  $\mathbf{N}^*$ , il n'est pas nul, donc  $n = 0$ , donc  $(mA, 0) = (0, 0)$  et comme  $A \neq 0$ ,  $m = 0$ . Le noyau de  $\varphi$  est donc réduit à  $\{(0, 0)\}$  et  $\varphi$  est donc injectif.

d) Découle du fait que  $(A, 0)$  et  $(C, D)$  sont dans  $H$ , je n'écris pas les détails.

e) Soit  $(u, v)$  dans  $H$ . On va procéder en gros comme aux questions 9 et 10, en adaptant le scénario aux nouvelles circonstances. D'abord on fait la division euclidienne de  $v$  par  $D$ , soit  $v = qD + r$  où  $0 \leq r < D$ ; puis on remarque que  $(u, v) - q(C, D)$  est dans  $H$  et, exactement comme au 9, on en conclut que  $r = 0$ . Les choses ne se passent pas tout à fait pareil qu'au 10 : l'information selon laquelle  $(u - qC, 0) \in H$  et donc  $(u - qC, 0) \in H_x$  permet seulement de garantir qu'il existe un  $k$  tel que  $u - qC = kA$ . Mais cette information donne :

$$(u, v) = (kA + qC, qD) = k(A, 0) + q(C, D) = \varphi(k, q)$$

et on conclut finalement que  $(u, v) \in \varphi(\mathbf{Z}^2)$ .

f) C'est juste une mise bout à bout des infos :  $\varphi$  est injective, donc est un isomorphisme entre son départ et son image, c'est-à-dire entre  $\mathbf{Z}^2$  et  $H$ .

15) Il ne faut pas oublier de considérer le groupe  $\{(0, 0)\}$ , isomorphe au groupe additif  $\{0\}$ . Voilà qui est fait, on en est débarrassé. Soit maintenant  $H$  non réduit à un singleton. Si  $H_x$  est réduit à un singleton, la troisième partie a montré que  $H$  était isomorphe à  $\mathbf{Z}$ . Sinon, si  $H = H_x$  la question 13 a montré que  $H$  était isomorphe à  $\mathbf{Z}$  tandis que si  $H \neq H_x$  la question 14 a montré que  $H$  était isomorphe à  $\mathbf{Z}^2$ . Enfin et accessoirement on sait depuis la question 7 que  $\mathbf{Z}$  et  $\mathbf{Z}^2$  ne sont pas isomorphes l'un à l'autre (et ne sont évidemment pas isomorphes au groupe à un élément, avec qui ils seraient bien en peine de se mettre en bijection, gros qu'ils sont).

On en conclut donc :

tout sous-groupe additif de  $\mathbf{Z}^2$  est isomorphe à un et un seul des trois modèles suivants :  $\{0\}$ ,  $\mathbf{Z}$  et  $\mathbf{Z}^2$ .