



Algèbre et Arithmétique 3

Correction de l'exercice 6 de la feuille de TD 1

Ce qui suit ne doit pas être considéré comme un « corrigé-type », mais comme des indications (parfois succinctes, parfois non) sur les réponses aux questions de l'exercice et la façon d'y parvenir, et des commentaires sur les solutions trouvées dans les copies.

Voici tout d'abord quelques remarques générales inspirées par la lecture des copies :

- il est tout à fait normal voire souhaitable que vous communiquiez entre vous, mais pour que l'exercice soit profitable, chaque rédaction devrait être personnelle ; si vous recopiez la solution d'un autre, évitez au moins de recopier les bourdes et coquilles, ça fait mauvais genre. . .
- il faut respecter les conventions liées aux notations, notamment le fait que la notation additive est réservée aux groupes commutatifs, et *surtout* ne pas mélanger notations additive et multiplicative pour un même groupe ; rappelons qu'en notation additive le symétrique s'appelle opposé et pas inverse ; ces conventions ne sont pas là pour le plaisir de d'énoncer des règles rigides, mais parce que leur non respect est source de graves confusions, en particulier lorsqu'on travaille avec un anneau $(A, +, \times)$, où deux groupes, l'un $(A, +)$ noté additivement, l'autre $(A^\times, \times)$ noté multiplicativement, cohabitent : *je me réserve le droit de ne même pas lire en détail une solution d'exercice dans une copie d'examen si ces conventions ne sont pas respectées*
- il ne faut pas confondre les propriétés d'associativité et de commutativité, ni croire qu'il y a un lien entre les deux, par exemple que l'une entraîne l'autre ; il existe des groupes non commutatifs, donc avec une loi associative et non commutative, et l'exercice donnait en particulier l'exemple d'une loi de composition interne commutative non associative
- il faut s'habituer à utiliser et à manipuler avec pertinence les quantificateurs ; c'est plus facile à dire qu'à faire, mais tout effort manifeste dans ce sens sera grandement apprécié par le correcteur (et inversement. . .) ; un exemple (parmi d'autres) extrait des copies : la propriété exprimant qu'une loi de composition interne $\star$ sur un ensemble G admet un élément neutre **N'EST PAS**

$$\forall x \in G, \quad \exists e \in G, \quad x \star e = e \star x = x$$

- montrer qu'un couple $(G, \star)$ est un groupe et montrer qu'une partie H d'un groupe $(G, \star)$ est un sous-groupe de G , ça n'est *pas du tout* la même démarche ; je vous renvoie aux définitions du cours (qui ne sont pas là juste pour faire joli. . .) pour plus de détails ; rappelons notamment que dans le deuxième cas il n'y a aucune propriété d'associativité à vérifier.

Exercice 6

1 $(\mathbf{Z}, +)$ et $(\mathbf{C}^\times, \times)$ sont des groupes. Ici, il y avait tout un éventail de degrés de justification possibles, allant de « ils font partie des groupes de références vus en cours » (pourquoi pas, cela montre déjà que vous connaissez bien le cours) jusqu'à la vérification soigneuse des propriétés requises à partir de la construction de ces ensembles et des lois considérées (certains l'ont fait pour $\mathbf{C}^\times$, un seul l'a fait pour $\mathbf{Z}$).

$(\mathbf{Z}, \times)$ n'est pas un groupe. La loi admet 1 pour élément neutre et aucun élément n de $\mathbf{Z}$ ne vérifie $0 \times n = 1$.

$(\mathbf{C}^\times, +)$ n'est pas un groupe tout simplement parce que $+$ n'est pas une loi de composition interne sur $\mathbf{C}^\times$ (par exemple 1 et -1 sont dans $\mathbf{C}^\times$ mais pas leur somme).

$(\mathbf{N} \setminus \{0\}, \star)$ n'est pas un groupe car $\star$ n'est pas associative. Pour le démontrer, il faut absolument donner un exemple explicite, par exemple $(2 \star 1) \star 2 \neq 2 \star (1 \star 2)$. Alternativement, on pouvait aussi démontrer que $\star$ n'admettait pas d'élément neutre (ce qui nécessite un peu de soin pour être rédigé rigoureusement).

2 Pour $\{-1, 1\}$, on pouvait prendre la multiplication usuelle. On vérifie alors facilement (quoique fastidieusement) que les propriétés requises sont bien vérifiées. Ou bien on dit par exemple : $\{-1, 1\}$ est un sous-groupe de $(\mathbf{Q}^\times, \times)$ (ou $\mathbf{R}^\times$, etc...) donc $\{-1, 1\}$ muni de la loi induite par $\times$ est bien un groupe (en supposant bien sûr connu que $(\mathbf{Q}^\times, \times)$ est un groupe).

Pour $\mathbf{R}^2$ la loi la plus naturelle était bien entendue l'addition composante par composante, utilisée notamment en algèbre linéaire. Il est à noter que l'énoncé demandait de *construire* la loi, donc il était a priori un peu sec de se contenter de dire « On prend la loi $+$ sur $\mathbf{R}^2$ » (rappeler au moins comment $+$ est défini!). Les vérifications à mener sont alors faciles quoique comme toujours un peu fastidieuses.

3 La lecture de la table montre que $\star$ admet a pour élément neutre, que la loi $\star$ est commutative et que tout élément de $\{a, b, c\}$ admet un symétrique (lui-même). Ainsi $(\{a, b, c\}, \star)$ est un groupe si et seulement si $\star$ est associative. Mais $\star$ n'est pas associative, par exemple on vérifie par le calcul que $(b \star b) \star c \neq b \star (b \star c)$. Alternativement, on peut utiliser comme indiqué en cours le théorème de Lagrange : si $(\{a, b, c\}, \star)$ était un groupe, b serait un élément d'ordre 2, mais 2 ne divise pas le cardinal de $\{a, b, c\}$, contradiction.

4 La réunion de deux sous-groupes n'est pas un sous-groupe en général. Un contre exemple a été donné en TD. Démontrer que la réunion de deux sous-groupes en est un si et seulement si l'un est inclus dans l'autre n'était absolument pas demandé ici (ce résultat peut certes éventuellement faciliter la production d'un contre-exemple, mais ici il n'était pas dur de trouver un contre-exemple en se basant uniquement sur le contenu du cours).

L'intersection de deux sous-groupes en est un. Ce résultat énoncé en cours n'avait pas été démontré, ici c'était bien entendu l'occasion de faire la démonstration! Voici un exemple de rédaction : soit G un groupe (noté multiplicativement) d'élément neutre e , H et K deux sous-groupes de G . Comme H et K sont des sous-groupes, $e \in H$ et $e \in K$ donc $e \in H \cap K$. Soient x et y des éléments de $H \cap K$. Comme x et y sont dans H (respectivement dans K) et que H (respectivement K) est un sous-groupe de G , on a $x.y \in H$ (respectivement $x.y \in K$). Donc $x.y \in H \cap K$. Comme x est dans H (respectivement dans K) et que H (respectivement K) est un sous-groupe de G , on a $x^{-1} \in H$ (respectivement $x^{-1} \in K$) donc $x^{-1} \in H \cap K$. Finalement $H \cap K$ est bien un sous-groupe de K .

Un certain nombre de copies utilisent la caractérisation suivante d'un sous-groupe : H est un sous-groupe de G si et seulement si $e \in H$ et pour tous $x, y \in G$, on a $x.y^{-1} \in H$ (variante : si et seulement si H est non vide et pour tous $x, y \in G$, on a $x.y^{-1} \in H$). Je signale juste que ce n'est pas la définition donnée en cours, qu'il n'est pas dur de montrer que c'est une définition équivalente et j'espère que ceux qui ont utilisé cette variante savent le faire.

5 Avec un tout petit peu d'imagination, les exemples ne manquent pas. Un des exemples les plus simples est sans doute $(\mathbf{N} \setminus \{0\}, +)$. Attention, $(\mathbf{Z} \setminus \{0\}, +)$ n'est pas un exemple valable (voyez-vous pourquoi?)