Éléments de correction de l'examen Algèbre 3 (3mai 2016)

Attention : *il s'agit d'un corrigé volontairement succinct, qui ne constitue en aucun cas un modèle de rédaction.*

Exercice 1. Soit G un groupe fini d'élément neutre e dont la loi de groupe est notée multiplicativement.

1. Montrer que si H_1 et H_2 sont deux sous-groupes de G d'ordres a et b, et si a et b sont premiers entre eux, alors $H_1 \cap H_2 = \{e\}$. En déduire que, sous les mêmes hypothèses, l'application

$$\begin{array}{rcl} H_1 \times H_2 & \longrightarrow & G \\ (x_1, x_2) & \longmapsto & x_1 x_2 \end{array}$$

est injective et que le cardinal de G est supérieur ou égal à ab.

Comme $H_1 \cap H_2$ est un sous-groupe de H_1 et de H_2, son ordre divise celui de H_1 et celui de H_2, et il est donc égal à un. En particulier si deux couples (x_1, x_2) et (y_1, y_2) de $H_1 \times H_2$ sont tels que $x_1x_2 = y_1y_2$ alors $y_1^{-1}x_1 = y_2x_2^{-1} \in H_1 \cap H_2 = \{e\}$, donc $y_1^{-1}x_1 = y_2x_2^{-1} = e$, c'est-à-dire $x_1 = y_1$ et $x_2 = y_2$.
Attention : f n'est (en général) pas un morphisme de groupes (G n'est pas supposé abélien) et on ne peut donc pas établir son injectivité en étudiant son "noyau"...

2. Montrer que si H est un sous-groupe de G d'ordre p premier, alors H est cyclique, engendré par n'importe lequel de ses éléments différents de e.

C'est une application immédiate du théorème de Lagrange, puisque l'ordre du sous-groupe engendré par un élément de H est un diviseur de p, donc égal à p si cet élément n'est pas l'élément neutre.

3. Si p est un nombre premier, et si H_1 et H_2 sont deux sous-groupes d'ordre p de G, montrer qu'on a l'alternative

$$H_1 \cap H_2 = \{e\} \text{ ou } H_1 = H_2.$$

En déduire que si G contient deux sous-groupes d'ordre p distincts, alors il contient au moins p^2 éléments.

C'est essentiellement le même raisonnement qu'à la question précédente : $H_1 \cap H_2$ est un sous-groupe de H_1 et de H_2, donc son ordre vaut 1 ou p. Dans le premier cas, on a $H_1 \cap H_2 = \{e\}$, et dans le second $H_1 \cap H_2 = H_1 = H_2$. Si H_1 et H_2 sont distincts, alors le même raisonnement qu'à la question 1 montre que l'application $(x_1, x_2) \mapsto x_1x_2$, de $H_1 \times H_2$ dans G est injective, et donc G contient au moins p^2 éléments (les images des p^2 éléments de $H_1 \times H_2$ par cette application)

4. On suppose désormais que G est d'ordre 35. On se propose de montrer qu'il contient nécessairement au moins un élément d'ordre 5 et un élément d'ordre 7.

   (a) Justifier ce fait quand G est cyclique.

   Dans ce cas, $G =< x >$ avec x d'ordre 35, auquel cas x^7 est d'ordre 5 et x^5 est d'ordre 7.

On suppose dans la suite que G *n'est pas cyclique*.

Ceci implique en particulier que G ne contient pas d'élément d'ordre 35, donc que ses éléments, hormis le neutre, sont d'ordre 5 ou 7.

(b) En utilisant la question 3, montrer que G contient au moins un élément d'ordre 5.
Sinon, tous les éléments $\neq e$ de G, qui sont au nombre de 34, seraient d'ordre 7, ce qui implique en particulier que G contiendrait au moins deux sous-groupes d'ordre 7 distincts et que son cardinal serait supérieur à $7^2 = 49$, ce qui est évidemment absurde.

(c) Supposons, par l'absurde, que G ne contienne, hormis l'élément neutre, que des éléments d'ordre 5. Montrer qu'on a alors

$$|G| = 4k + 1$$

où k désigne le nombre de sous-groupes d'ordre 5 dans G.
Dans ce cas, tous les éléments $\neq e$ de G seraient d'ordre 5. Sachant qu'un groupe cyclique d'ordre 5 contient exactement 4 éléments d'ordre 5 et que deux sous-groupes cycliques d'ordre 5 distincts n'ont que l'élément neutre en commun, on pourrait donc regrouper les éléments de $G \setminus \{e\}$ par 4, selon le sous-groupe d'ordre 5 auquel ils appartiennent. On aurait donc

$$|G \setminus \{e\}| = 4k$$

c'est-à-dire

$$|G| = 4k + 1$$

où k désigne le nombre de sous-groupes d'ordre 5 de G. C'est évidemment absurde puisque $|G| = 35$ n'est pas congru à 1 modulo 4.

Exercice 2. On rappelle que $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ est muni d'une structure d'anneau pour les lois $+$ et $\cdot$ définies par

- $(x, y) + (x', y') = (x + x', y + y')$,
- $(x, y) \cdot (x', y') = (xx', yy')$

et que les éléments neutres pour ces deux lois sont respectivement $(0, 0)$ et $(1, 1)$.

1. Soit $H = \{(x, y) \in \mathbb{Z}^2 \mid x + y \text{ est pair}\}$.

(a) Montrer que $(H, +)$ est un sous-groupe du groupe additif $(\mathbb{Z}^2, +)$.
H est non vide car il contient $(0, 0)$. De plus, si $x + y$ et $x' + y'$ sont pairs, alors $(x' - x) + (y' - y) = (x' + y') - (x + y)$ l'est également. Autrement dit, si (x, y) et (x', y') appartiennent à H, alors $(x' + y') - (x, y)$ également.

(b) Montrer que l'application

$$\begin{array}{rccc} f: & \mathbb{Z}^2 & \longrightarrow & H \\ & (x, y) & \longmapsto & (x, 2y - x) \end{array}$$

est un isomorphisme de groupes.

On vérifie tout d'abord que f est à valeurs dans H, ce qui est clair vu que $x + 2y - x = 2y$ est pair pour tout couple $(x, y) \in \mathbb{Z}^2$. C'est clairement un morphisme de groupes, et il est injectif car son noyau est trivial, puisque $(x, 2y - x) = (0, 0)$ si et seulement si $(x, y) = (0, 0)$. Pour la surjectivité, il suffit de constater que si $x + y$ est pair, alors $\frac{x+y}{2} \in \mathbb{Z}$ et $(x, y) = f(x, \frac{x+y}{2})$.

2. Pour $d \in \mathbb{N}$, on pose
$$A_d = \left\{ (x, y) \in \mathbb{Z}^2 \mid x \equiv y \mod d \right\}.$$

(a) Montrer que A_d est un sous-anneau de $\mathbb{Z}^2$.

C'est presque immédiat grâce à la compatibilité des congruence avec l'addition et la multiplication. Il faut bien noter en particulier que $(1, 1)$ appartient à A_d, ce qui est une condition essentielle dans la définition d'un sous-anneau.

(b) Déterminer, en fonction de $d \in \mathbb{N}$, l'ensemble $A_d^\times$ des inversibles de A_d.

$$A_d^\times = \begin{cases} \{\pm(1,1)\} & \text{si } d \neq 2 \\ \{\pm(1,1), \pm(1,-1)\} & \text{si } d = 2 \end{cases}$$

(c) Les anneaux A_2 et A_3 sont-ils isomorphes ?

Non, puisqu'ils possèdent respectivement 4 et 2 éléments inversibles.

3. Inversement, si A est un sous-anneau de $\mathbb{Z}^2$, on pose
$$K = \{x \in \mathbb{Z} \text{ tels que } (x, 0) \in A\}.$$

(a) Montrer que K est un sous-groupe de $(\mathbb{Z}, +)$.

0 appartient à K puisque $(0, 0)$ appartient à A. De plus, si $(x, 0)$ et $(y, 0)$ appartiennent à A alors $(x - y, 0)$ appartient à A, ce qui permet de conclure que K est un sous-groupe de $\mathbb{Z}$.

(b) En déduire qu'il existe $d \in \mathbb{N}$ tel que $K = d\mathbb{Z}$ et que $A = A_d$.

Le théorème de structure des sous-groupes de $\mathbb{Z}$ permet d'affirmer l'existence d'un (unique) entier $d \in \mathbb{N}$ tel que $K = d\mathbb{Z}$. Par ailleurs, on a pour tout $(x, y) \in \mathbb{Z}^2$:
$$(x, y) = (x - y, 0) + (y, y)$$
Comme $(1, 1) \in A$, on a également $(y, y) \in A$ pour tout $y \in \mathbb{Z}$. Par conséquent
$$(x, y) \in A \Leftrightarrow (x - y, 0) \in A \Leftrightarrow x - y \in K = d\mathbb{Z} \Leftrightarrow (x, y) \in A_d.$$

Exercice 3. On rappelle que l'ensemble $\mathrm{GL}_2(\mathbb{R})$ des matrices réelles 2×2 inversibles est un groupe pour le produit matriciel, d'élément neutre la matrice identité.

Soit G l'ensemble des matrices 2×2 de la forme $\begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix}$ avec $a \in \mathbb{Z}$ et $\varepsilon \in \{-1, 1\}$.

1. Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

C'est évident, en constatant que la matrice identité $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ appartient à G et en utilisant la formule

$$\begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & \varepsilon' \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix} \begin{pmatrix} 1 & -\varepsilon' b \\ 0 & \varepsilon' \end{pmatrix} = \begin{pmatrix} 1 & \varepsilon'(a-b) \\ 0 & \varepsilon\varepsilon' \end{pmatrix}.$$

Soit n un entier naturel ≥ 2 fixé. On pose

$$H = \left\{ \begin{pmatrix} 1 & nk \\ 0 & 1 \end{pmatrix}, k \in \mathbb{Z} \right\}.$$

2. Montrer que H est un sous-groupe normal (ou distingué) de G.

   Le fait que H soit un sous-groupe découle de la formule

$$\begin{pmatrix} 1 & nk \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n\ell \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & nk \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -n\ell \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n(k-\ell) \\ 0 & 1 \end{pmatrix}.$$

   Le fait qu'il soit distingué découle de la formule

$$\begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix}^{-1} \begin{pmatrix} 1 & nk \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix} = \begin{pmatrix} 1 & -\varepsilon a \\ 0 & \varepsilon \end{pmatrix} \begin{pmatrix} 1 & nk \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix} = \begin{pmatrix} 1 & \varepsilon nk \\ 0 & 1 \end{pmatrix}.$$

3. Montrer que pour tout élément $g = \begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix} \in G$ il existe un unique entier $r \in \{0, \ldots, n-1\}$ et un unique élément h de H tels que

$$g = \begin{pmatrix} 1 & r \\ 0 & \varepsilon \end{pmatrix} h.$$

   Si $h = \begin{pmatrix} 1 & nq \\ 0 & 1 \end{pmatrix}$ est un élément de H, on a

$$\begin{pmatrix} 1 & r \\ 0 & \varepsilon \end{pmatrix} h = \begin{pmatrix} 1 & r+nq \\ 0 & \varepsilon \end{pmatrix}.$$

   Ainsi, pour que $h = \begin{pmatrix} 1 & nq \\ 0 & 1 \end{pmatrix}$ et $r \in \{0, \ldots, n-1\}$ vérifient la relation

$$\begin{pmatrix} 1 & r \\ 0 & \varepsilon \end{pmatrix} h = g = \begin{pmatrix} 1 & a \\ 0 & \varepsilon \end{pmatrix},$$

   il faut et il suffit que q et r soient respectivement le quotient et le reste de la division euclidienne de a par n. Ceci assure l'existence et l'unicité du couple (r, h) cherché.

   En déduire l'ordre du groupe G/H.

   En particulier, G/H est d'ordre $2n$, puisqu'il y a exactement $2n$ matrices $\begin{pmatrix} 1 & r \\ 0 & \varepsilon \end{pmatrix}$ avec $\varepsilon = \pm 1$ et $r \in\in \{0, \ldots, n-1\}$.

4. (a) Exhiber un élément x d'ordre 2 et un élément y d'ordre n dans G/H qui soient tels que

$$xyx = y^{-1}.$$

Soient $X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $Y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Alors, leurs classes x et y modulo H conviennent.

(b) Montrer que G/H est isomorphe au groupe diédral D_{2n} des isométries d'un polygone régulier à n sommets.

Avec des notations standard, on note r une rotation de centre O, isobarycentre du polygone, et d'angle $\dfrac{2\pi}{n}$, et s l'une (quelconque) des réflexions d'axe passant par O et un sommet. Avec les notations précédentes, on remarque que tout élément de G peut s'écrire sous la forme

$$\begin{pmatrix} 1 & a \\ 0 & (-1)^i \end{pmatrix} = X^i Y^a$$

avec $i = 0$ ou 1 et $a \in \mathbb{Z}$. On considère alors l'application ϕ de G dans D_{2n} qui applique $\begin{pmatrix} 1 & a \\ 0 & (-1)^i \end{pmatrix}$ sur $s^i r^a$. On vérifie aisément qu'il s'agit d'un morphisme de groupes, grâce à la relation $XYX = Y^{-1}$. On montre ensuite que ϕ est surjectif (c'est immédiat) et de noyau $\ker \phi = H$. Le théorème de factorisation fournit alors l'isomorphisme cherché.