Correction du contrôle continu n°1
Durée 2h

Question de cours : Voir le cours

Exercice 1. Soit H l'ensemble des matrices de type $\begin{pmatrix} 1 & 0 & x \\ -x & 1 & -x^2/2 \\ 0 & 0 & 1 \end{pmatrix}$ où $x \in \mathbb{R}$.

(1) On montre que H est le sous-groupe du groupe multiplicatif $SL(3,\mathbb{R})$ des matrices de déterminant 1 ou bien du groupe multiplicatif $GL(3,\mathbb{R})$ des matrices inversibles 3×3 à coefficients dans $\mathbb{R}$. On note I_3 la matrice identité 3×3.
Posons

$$M(x) = \begin{pmatrix} 1 & 0 & x \\ -x & 1 & -x^2/2 \\ 0 & 0 & 1 \end{pmatrix}$$

pour tout $x \in \mathbb{R}$. On a $I_3 = M(0)$ donc H est non vide. De plus, $\det M(x) = 1 \neq 0$, donc

$$H \subset SL(3,\mathbb{R}) \subset GL(3,\mathbb{R}).$$

Soit $x, y \in \mathbb{R}$. On calcule le produit

$$M(x)M(y) = \begin{pmatrix} 1 & 0 & x+y \\ -x-y & 1 & -xy - y^2/2 - x^2/2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x+y \\ -(x+y) & 1 & -(x+y)^2/2 \\ 0 & 0 & 1 \end{pmatrix} = M(x+y).$$

Donc, H est stable par produit de matrices et le produit est commutatif.
De là, $M(x)M(-x) = M(x-x) = M(0) = I_3$. Donc, H est stable par passage à l'inverse avec $M(x)^{-1} = M(-x)$. Par conséquent, H est un sous-groupe commutatif du groupe $(SL(3,\mathbb{R}), \times)$, et donc H muni du produit de matrices est un groupe commutatif.

(2) On considère l'application $\varphi : \mathbb{R} \to HF$ définie par $\varphi(x) = M(x)$. Vu les calculs faits précédemment, pour tout $x, y \in \mathbb{R}$, on a $\varphi(x+y) = M(x+y) = M(x)M(y) = \varphi(x) \times \varphi(y)$. Donc φ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(H, \times)$.

(3) On vérifie que le morphisme de groupes $\varphi : \mathbb{R} \to G$ est bijectif. Tout d'abord, $\varphi(x) = I_3 \iff x = 0$, donc $\ker \varphi = \{0\}$ et φ est injectif sur $\mathbb{R}$. La surjectivité est immédiate par définition de $\varphi = M$. Les groupes $(\mathbb{R}, +)$ et $(H, \times)$ sont bien isomorphes.

Exercice 2. Notons $G = \{e, a, b, c, d\}$ un groupe d'ordre 5 d'élément neutre e.

(1) L'ordre d'un élément de G divise 5. Le nombre 5 étant premier, a, b, c et d sont d'ordre 5, le neutre e étant le seul élément d'ordre 1.

(2) Ainsi, a, b, c et d sont tous des générateurs de G, qui est un groupe monogène, donc abélien.

(3) G est un groupe monogène d'ordre 5 donc il est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ par l'isomorphisme $\overline{x} \mapsto a^x$. En d'autres termes, à un isomorphisme près, il existe un unique groupe d'ordre 5.

Exercice 3. Soit $(G, .)$ un groupe dans lequel tout élément distinct de l'élément neutre est d'ordre 2. Notons e l'élément neutre du groupe $(G, .)$ et a un élément de G distinct de e. On pose $H = \{e, a\}$.

(1) Soit $x, y \in G$. Par hypothèse, $x^2 = e = y^2$ et aussi $x.y.x.y = (x.y)^2 = e$. Donc,

$$y.x = x^2.(y.x).y^2 = x.(x.y.x.y).y = x.y$$

et le groupe G est abélien. Exemple d'un tel sous-groupe d'ordre > 2 : $G = \{I, -I, J, -J\}$ muni de $\times$ où I est la matrice identité 2×2 et $J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(2) H est une partie non vide du groupe G. Sa table de composition est donnée par $\begin{array}{c|cc} . & e & a \\ \hline e & e & a \\ a & a & e \end{array}$. Donc, H est stable par composition et par passage à l'inverse (tout élément de G est son propre inverse). Donc H est un sous-groupe de G d'ordre 2.

(3) Par définition d'ensemble quotient

$$G/H = \{\overline{x} \mid x \in G\} \text{ avec } \overline{x} = \{y \in G : x^{-1}.y \in H\} = \{x, x.a\}.$$

On vérifie d'abord que $\overline{x.y}$ est indépendant du choix des représentants des classes de $\overline{x}$ et $\overline{y}$. En effet, si $\overline{x} = \overline{u}$ et $\overline{y} = \overline{v}$, alors $u = x$ ou $x.a$ et $v = y$ ou $y.a$. Donc, G étant abélien, $u.v = x.y.a^2 = x.y$ ou $x.y.a$. autrement dit $\overline{x.y} = \overline{u.v}$. On peut alors définir une loi de composition interne sur G/H par $\overline{x} * \overline{y} = \overline{x.y}$.
La loi . étant associative et commutative, $*$ l'est aussi.
Son neutre est $\overline{e} = H = \{e, a\}$.
Puis, $\overline{x} * \overline{x} = \overline{x.x} = \overline{e}$, autrement dit tout élément $\overline{x}$ est inversible d'inverse lui-même.
En conclusion, l'ensemble quotient G/H muni de la loi $\overline{x} * \overline{y} = \overline{x.y}$ est un groupe abélien et tout élément de G/H distinct du neutre est d'ordre 2.

(4) Bonus : Supposons que l'ordre n de G est fini $\geqslant 2$. S'il est d'ordre 2, alors c'est bon. Sinon, il est d'ordre > 2 et il admet un sous-groupe non trivial $H = \{e, a\}$ d'ordre 2. On pose alors $G_1 = G/H$ et, d'après le théorème de Lagrange, on a $n = 2 \times \text{card}G_1$.
Et on recommence : si $\text{card}G_1 = 2$, c'est fini ($n = 2^2$) ; sinon $\text{card}G_1 > 2$ et comme dans le groupe quotient G_1 tout élément distinct du neutre est d'ordre 2, il admet aussi un sous-groupe non trivial H_1 d'ordre 2. On pose alors $G_2 = G_1/H_1$ et on a $n = 2 \times \text{card}G_1 = 2 \times 2 \times \text{card}G_2$. On réitère le procédé qui s'arrête car G est fini. Ainsi, $n = 2 \times 2 \times \cdots \times 2$ est une puissance de 2.

Exercice 4. On note $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$ les 8 éléments du groupe $(\mathbb{Z}/8\mathbb{Z}, +)$.

(1) Le sous-groupe engendré par $\overline{1}$ est $\langle \overline{1} \rangle = \{k\overline{1} \mid k \in \mathbb{Z}\} = \{\overline{k} \mid k \in \mathbb{Z}\} = \mathbb{Z}/8\mathbb{Z}$. Donc, le groupe $(\mathbb{Z}/8\mathbb{Z}, +)$ est cyclique (monogène et fini) engendré par $\overline{1}$.
Les générateurs de $(\mathbb{Z}/8\mathbb{Z}, +)$ sont les $\overline{m}$ où m est premier avec 8. Les générateurs sont donc $\overline{1}$, $\overline{3}$, $\overline{5}$,$\overline{7}$.

(2) D'après le théorème de Lagrange, les sous-groupes de $(\mathbb{Z}/8\mathbb{Z}, +)$ sont d'ordre un diviseur de 8, donc d'ordre 1, 2, 4 ou 8.
Les sous-groupes d'ordre 1 et 8 sont les sous-groupes triviaux $\{\overline{0}\}$ et $\mathbb{Z}/8\mathbb{Z}$ respectivement.
Les sous-groupes d'ordre 2 contiennent le neutre $\overline{0}$ et un élément d'ordre 2. La seule possibilité est donc $\{\overline{0}, \overline{4}\}$.
Les sous-groupes d'ordre 4 contiennent le neutre $\overline{0}$ et des éléments d'ordre 2 ou 4. Ils ne contiennent aucun générateur. La seule possibilité est donc $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$.

(3) La classe $\overline{3}$ est inversible pour le produit si et seulement si il existe $x \in [\![0, 7]\!]$ tel que $\overline{3} \times \overline{x} = \overline{1}$, autrement dit $3x \equiv 1(8)$, soit encore 3 et 8 sont premiers entre eux. Donc, $\overline{3}$ est inversible. De la même manière $\overline{4}$ n'est pas inversible (il n'est pas premier avec 8). Pour déterminer l'inverse de $\overline{3}$, on détermine les coefficients de Bezout dans l'identité $3x + 8y = 1$, on trouve facilement $x = 3$ (et $y = -1$). Donc l'inverse de $\overline{3}$, c'est $\overline{3}$.

(4) On considère le groupe produit $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$ muni de l'addition encore notée $+$:

$$(\widetilde{x_1}, \widetilde{x_2}, \widetilde{x_3}) + (\widetilde{y_1}, \widetilde{y_2}, \widetilde{y_3}) = (\widetilde{x_1 + y_1}, \widetilde{x_2 + y_2}, \widetilde{x_3 + y_3}).$$

C'est un groupe fini à 8 éléments et chacun des ses éléments est son propre opposé. Si les groupes additifs $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$ et $\mathbb{Z}/8\mathbb{Z}$ étaient isomorphes, il existerait une isomorphisme φ de $\mathbb{Z}/8\mathbb{Z}$ vers $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$. Alors, $\varphi(\overline{1})$ serait d'ordre 2 et :

$$\varphi(\overline{2}) = \varphi(\overline{1} + \overline{1}) = \varphi(\overline{1}) + \varphi(\overline{1}) = \widetilde{0}.$$

φ étant injective, il viendrait, $\overline{2} = \overline{0}$ ce qui est faux. Donc les groupes ne sont pas isomorphes.