Lycée Carnot
ECS 4 – Mathématiques
A. Troesch

Pour le 17 septembre 2005

Devoir Maison n° 2 – ensembles et applications : Groupes, lemme des cinq

Partie I – Groupes.

Soit G un ensemble, muni d'une loi (multiplication par exemple) $(x,y) \mapsto x \cdot y$. On dit que G est un groupe si :

1. *la loi est associative : $\forall x,y,z \in G,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$;*
2. *il existe dans G un élément e appelé « neutre », et noté tel que : $\forall x \in G,\ e \cdot x = x \cdot e = x$;*
3. *pour tout élément x de G, il existe un élément x' de G tel que $x \cdot x' = x' \cdot x = 0$. L'élément x' est appelé inverse de x et est noté x^{-1}*

On dit de plus que le groupe est commutatif (ou abélien) si la loi est commutative : $\forall x, y \in G,\ x \cdot y = y \cdot x$. Lorsque G est un groupe abélien, on préfère souvent une notation additive à une notation multiplicative pour la loi. Par exemple, l'associativité s'écrit alors $(x+y)+z = x+(y+z)$. On appelle dans ce cas « opposé » l'inverse de x, et on le note $-x$ au lieu de x^{-1}.
On note souvent le neutre 1 (en notation multiplicative) ou 0 (en notation additive).

1. Exemples.
   (a) Montrer que $\mathbb{Z}$ muni de l'addition usuelle est un groupe abélien. Même question pour $\mathbb{R}$ et pour $\mathbb{C}$.
   (b) Est-ce que $\mathbb{N}$ muni de l'addition usuelle est un groupe ?
   (c) Montrer que $\{0\}$ muni de l'addition définie par $0+0=0$ est un groupe abélien. On note plus simplement 0 ce groupe.
   (d) Montrer que $\{0,1\}$ est un groupe abélien lorsqu'on le munit de l'addition définie par :
   $$0+0=0, \qquad 0+1=1+0=1 \qquad 1+1=0.$$
   Ce groupe est noté $\mathbb{Z}/2\mathbb{Z}$ (lire : « $\mathbb{Z}$ sur 2 $\mathbb{Z}$ »).
   (e) *Plus généralement, on munit $\{0,1,\dots,n-1\}$ de l'addition $\dot{+}$ (le point sert à la distinguer de l'addition usuelle dans $\mathbb{N}$) suivante : pour tout i et tout j de $\{0,\dots,n-1\}$, $i \dot{+} j$ est défini comme étant le reste de la division euclidienne de $i+j$ par n. Ainsi, $i \dot{+} j$ est le seul entier de $\{0,1,\dots,n-1\}$ tel que $i+j \equiv i \dot{+} j \mod n$.*
   Montrer qu'on définit ainsi un groupe abélien. Ce groupe est noté $\mathbb{Z}/n\mathbb{Z}$.
   (f) $\mathbb{R}^*$ muni de l'addition usuelle est-il un groupe ? $\mathbb{R}^*$ muni de la multiplication habituelle est-il un groupe ? Est-il abélien ? On note ce groupe $(\mathbb{R}^*, \times)$.
   (g) Mêmes questions avec le groupe multiplicatif $(\mathbb{C}^*, \times)$.
   (h) Soit E un ensemble. Montrer que E^E l'ensemble des fonctions de E dans lui-même muni de la loi de composition des fonctions est un groupe. Est-il abélien ?
2. Soit G et H deux groupes. On munit $G \times H$ de l'addition suivante :
   $$\forall (g,g') \in G^2,\ \forall (h,h') \in H^2, (g,h) \cdot (g',h') = (g \cdot g', h \cdot h').$$
   Montrer que l'on définit ainsi une structure de groupe sur $G \times H$, et que ce groupe est abélien si G et H sont abéliens.
3. Soit G un groupe, et soit $H \subset G$ un sous-ensemble de G.
   (a) Montrer que pour que H soit un groupe, il suffit que :
   - H soit non vide,
   - pour tout x et tout y de H, $x \cdot y$ soit encore un élément de H (stabilité de H par la loi de G).
   - pour tout x de H, x^{-1} est encore dans H.

   On dit que H est un *sous-groupe* de G.
   (b) Montrer que $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$.
   (c) Soit $n \in \mathbb{N}^*$. On note $n\mathbb{Z} = \{n \cdot x,\ x \in \mathbb{Z}\}$ (l'ensemble des multiples de n). Montrer que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

(d) On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ l'ensemble des complexes de module 1. Montrer que S^1 est un sous-groupe de $(\mathbb{C}^*, \times)$.
(e) Soit G un groupe de neutre 1, et soit H un sous-groupe de G. Montrer que $1 \in H$.
(f) Soit H et K deux sous-groupes d'un groupe G. Montrer que $H \cap K$ est un sous-groupe de G.
(g) $H \cup K$ est-il forcément un sous-groupe de G ?

Partie II – Morphismes de groupes

Soit G et H deux groupes, dont la loi est notée multiplicativement. On note 1_G et 1_H les neutres respectifs de G et H. Un homomorphisme (ou morphisme de groupes) de G vers H est une application $f : G \longrightarrow H$ telle que pour tout $(x, y) \in G^2$, $f(x \cdot y) = f(x) \cdot f(y)$.
Soit $f : G \longrightarrow H$ un homomorphisme. On définit :
- *le noyau de f : $\mathrm{Ker}(f) = \{x \in G \mid f(x) = 1_H\}$*
- *l'image de f : $\mathrm{Im}(f) = \{y \in H \mid \exists x \in G,\ f(x) = y\} = f(G)$.*

Un homomorphisme bijectif est appelé isomorphisme.

1. Soit $f : G \longrightarrow H$ un homomorphisme. Montrer que $f(1_G) = 1_H$.
2. Montrer que $\mathrm{Ker}(f)$ est un sous-groupe de G et que $\mathrm{Im}(f)$ est un sous-groupe de H.
3. Exemples (attention, dans la plupart des exemples, les groupes sont additifs, et le neutre est 0 et non 1)
   (a) Soit $n \in \mathbb{N}$, et soit $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ défini par $f(m) = n \cdot m$. Montrer que f est un homomorphisme, et déterminer sont noyau et son image.
   (b) Même question avec $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, où $f(m)$ est le reste de la division euclidienne de m par n, donc l'unique entier k de $\{0, \dots, n-1\}$ tel que $m \equiv k \mod n$.
   (c) Même question avec $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \times)$ défini par $f(x) = \mathrm{e}^x$.
   (d) Même question avec $f : (\mathbb{R}, +) \longrightarrow S^1$ défini par $f(x) = \mathrm{e}^{\mathrm{i}\,x}$.
4. Soit $f : G \longrightarrow H$ un homomorphisme. Montrer que f est surjective si et seulement si $\mathrm{Im}(f) = H$ et que f est injective si et seulement si $\mathrm{Ker}(f) = 1_G$.
5. Les homomorphismes de la question 3 sont-ils injectifs ? surjectifs ? Lesquels sont des isomorphismes ?
6. Soit G un groupe (additif), de neutre 0_G. On considère le groupe 0 de la question I-1c.
   (a) Montrer qu'il existe un unique homomorphisme de 0 vers G. Préciser son noyau et son image. Est-ce une injection ? une surjection ? un isomorphisme ? On note 0 ce morphisme.
   (b) Montrer qu'il existe un unique homomorphisme de G vers 0. Préciser son noyau et son image. Est-ce une injection ? une surjection ? un isomorphisme ? On note également 0 ce morphisme.
7. Soit G, H et K trois groupes, et $f : G \to H$ et $g : H \to K$ deux homomorphismes. Montrer que $g \circ f$ est un homomorphisme.

Partie III – Suites exactes

Soit $G_1, \dots, G_n$ des groupes, et $f_1 : G_1 \to G_2, \dots, f_{n-1} : G_{n-1} \to G_n$ des homomorphismes :

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-2}} G_{n-1} \xrightarrow{f_{n-1}} G_n.$$

1. Montrer que pour tout $i \in [\![1, n-2]\!]$, $f_{i+1} \circ f_i = 0$ si et seulement si $\mathrm{Im}(f_i) \subset \mathrm{Ker}(f_{i+1})$.

Si cette condition est vérifiée, on parle de suite de morphismes.
On dit que $G_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} G_n$ est une suite exacte *si et seulement si :*

$$\forall i \in [\![1, n-2]\!], \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}).$$

2. (a) Quelle propriété sur f est traduite par le fait que $0 \longrightarrow G \xrightarrow{f} H$ est une suite exacte ? (le premier morphisme étant le morphisme nul 0).
   (b) Quelle propriété sur f est traduite par le fait que $G \xrightarrow{f} H \longrightarrow 0$ est une suite exacte ?
3. Montrer que $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$ une suite exacte (le morphisme $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ étant celui défini en II-3b, et le morphisme $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ étant la multiplication par n).

4. Même question avec $0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{f} \mathbb{Z}/4\mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$, où f est défini par $f(0) = 0$ et $f(1) = 2$, et g est défini par $g(0) = g(2) = 0$ et $g(1) = g(3) = 1$ (vérifier d'abord que f et g sont des homomorphismes).
5. Soit G et H deux groupes. Montrer que $0 \longrightarrow G \xrightarrow{f} G \times H \xrightarrow{g} H \longrightarrow 0$ est une suite exacte, où f est l'injection sur le premier facteur, et g est la projection sur le second facteur.

Partie IV – Lemme des quatre, lemme des cinq.
On considère le carré suivant, où tous les ensembles sont des groupes additifs, et toutes les applications sont des homomorphismes :

$$\begin{tikzcd}
G_1 \arrow[r, "f"] \arrow[d, "\alpha"'] & G_2 \arrow[d, "\beta"] \\
H_1 \arrow[r, "g"'] & H_2
\end{tikzcd}$$

On dit que ce carré est commutatif si $g \circ \alpha = \beta \circ f$.

1. **Lemme des cinq, version faible.**
   On considère le diagramme suivant de groupes et d'homomorphismes :

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0,
\end{tikzcd}$$

   où les deux lignes sont des suites exactes, et les deux carrés sont commutatifs.
   (a) Montrer que si α et γ sont injectives, alors β aussi.
   Indication : considérer $x \in B$ tel que $\beta(x) = 0$. En considérant $\gamma \circ g$, montrer que $g(x) = 0$, puis qu'il existe $y \in A$ tel que $f(y) = x$. En considérant $f' \circ \alpha$, en conclure que $x = 0$. (Cette démarche s'appelle une « chasse au diagramme » ; remarquez que c'est la recherche d'éléments s'envoyant sur 0 par les flèches horizontales qui permet de remonter vers la gauche du diagramme)
   (b) Montrer que si α et γ sont surjectives, alors β aussi.
   Indication : soit $y \in B'$; en considérant $\gamma \circ g$ trouver $x \in B$ tel que $y - \beta(x) \in \mathrm{Ker}(g')$. En utilisant la surjectivité de α, trouver $x' \in B$ tel que $\beta(x') = y - \beta(x)$. Conclure.
   (c) Montrer que si α et γ sont des isomorphismes, alors β aussi.
2. **Lemme des quatre.**
   On considère le diagramme suivant de groupes et morphismes de groupes :

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"'] & C \arrow[r, "h"] \arrow[d, "\gamma"] & D \arrow[d, "\delta"] \\
A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D',
\end{tikzcd}$$

   dans lequel les deux lignes sont des suites exactes, et les trois carrés sont commutatifs. En s'inspirant des méthodes de la question précédente, montrer les résultats suivants :
   (a) Si β et δ sont injectives et α est surjective, alors γ est injective. (Indication : utiliser les 3 hypothèses)
   (b) Si α et γ sont surjectives et δ est injective, alors β est surjective.
3. **Lemme des cinq, version forte.**
   On considère maintenant le diagramme suivant de groupes et morphismes de groupes :

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"'] & C \arrow[r, "h"] \arrow[d, "\gamma"] & D \arrow[r, "k"] \arrow[d, "\delta"] & E \arrow[d, "\varepsilon"] \\
A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D' \arrow[r, "k'"] & E',
\end{tikzcd}$$

   dans lequel les deux lignes sont des suites exactes, et les quatre carrés sont commutatifs.
   (a) Montrer à l'aide de la question 2 que si α, β, δ et ε sont des isomorphismes, il en est de même de γ.
   (b) Donner des conditions suffisantes pour que γ soit injective ; pour que γ soit surjective.
   (c) En déduire des conditions suffisantes moins fortes qu'en (a) pour que γ soit un isomorphisme.
   (d) Retrouver la version faible du lemme des cinq à partir de cette version.