

STRUCTURES ALGÉBRIQUES

✠ ***Exercice 1.*** [$\circ$]
Soit E un ensemble fini. On note A le sous-ensemble de E^E constitué des applications qui ne sont pas bijectives. Démontrer que A est stable pour la loi $\circ$.
Cela fournit un exemple de magma associatif, non commutatif et sans élément neutre.

Soient $f, g \in A$. Par l'absurde, supposons que $f \circ g \notin A$. Cela signifie que $f \circ g$ est bijective. On sait alors que f est surjective et g est injective. Mais comme E est un ensemble fini, le théorème Bonux nous dit que f et g sont en fait des bijections, c'est-à-dire $f, g \notin A$. C'est absurde ! Donc

$$\boxed{A \text{ est stable pour la loi } \circ.}$$

✠ ***Exercice 2.*** [$\star$] (Produit ensembliste de sous-groupes)
Soient $(G, *)$ un groupe et H, K deux sous-groupes de G. On pose

$$HK = \{h * k : h \in H,\ k \in K\} \qquad \text{et} \qquad KH = \{k * h : h \in H,\ k \in K\}$$

1. Dans cette question, on suppose que G est abélien. Démontrer que HK est un sous-groupe de G et que c'est le plus petit sous-groupe de G qui contient H et K.
2. Dans cette question, on ne suppose plus que G est abélien. Démontrer que HK est un sous-groupe de G si, et seulement si, $HK = KH$.

1. On a $e = e * e$ avec $e \in H$ et $e \in K$ donc $e \in HK$.

   Soit $g_1, g_2 \in HK$. Il existe $h_1, h_2 \in H$ et $k_1, k_2 \in K$ tels que $g_1 = h_1k_1$ et $g_2 = h_2k_2$. On a alors ${g_1g_2}^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1{k_2}^{-1}{h_2}^{-1} = (h_1{h_2}^{-1})(k_1{k_2}^{-1}) \in HK$ où troisième égalité découle du fait que G est abélien.

   On en conclut que
   $$\boxed{HK \text{ est un sous-groupe de } G.}$$

   Pour démontrer que HK est le plus petit sous-groupe de G qui contient H et K, il suffit de vérifier que tout sous-groupe qui contient H et K contient aussi HK. Or, si G' est un sous-groupe de G qui contient H et K, la stabilité de la loi nous dit que G' contient tous les produits d'un élément de H par un élément de K, et donc que G' contient HK. Le tour est joué ! Ainsi,

   $$\boxed{HK \text{ est le plus petit sous-groupe de } G \text{ qui contient } H \text{ et } K.}$$

2. On raisonne par double-implication.

   $\Rightarrow$ Supposons que HK est un sous-groupe de G.

   Pour démontrer que $HK = KH$, on procède par double-inclusion.

   $\supset$ Soit $x \in KH$. Il existe $k \in K$ et $h \in H$ tel que $x = kh$. Alors $x^{-1} = h^{-1}k^{-1} \in HK$ car $h^{-1} \in H$ et $k^{-1} \in K$ puisque H et K sont des sous-groupes. Comme HK est un sous-groupe, on en déduit que $x \in HK$. Donc $KH \subset HK$.

   $\subset$ Soit $x \in HK$. Comme HK est un sous-groupe de G, on sait que $x^{-1} \in HK$. Par conséquent, il existe $h \in H$ et $k \in K$ tel que $x^{-1} = hk$. Dès lors, on a $x = k^{-1}h^{-1} \in KH$ car $k^{-1} \in K$ et $h^{-1} \in H$ puisque H et K sont des sous-groupes. Donc $KH \supset HK$.

$\Leftarrow$ Supposons que $HK = KH$.

On a $e = e * e$ avec $e \in H$ et $e \in K$ donc $e \in HK$.

Soient $g_1, g_2 \in HK$. Il existe $h_1, h_2 \in H$ et $k_1, k_2 \in K$ tels que $g_1 = h_1 k_1$ et $g_2 = h_2 k_2$. On a alors $g_1 {g_2}^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 {k_2}^{-1} {h_2}^{-1}$. Or $k_1 {k_2}^{-1} {h_2}^{-1} \in KH$ car $k_1 {k_2}^{-1} \in K$ et ${h_2}^{-1} \in H$ puisque H et K sont des sous-groupes, donc $k_1 {k_2}^{-1} {h_2}^{-1} \in HK$. Cela permet d'affirmer l'existence de $h_3 \in H$ et $k_3 \in K$ tels que $k_1 {k_2}^{-1} {h_2}^{-1} = h_3 k_3$. D'où $g_1 {g_2}^{-1} = h_1 h_3 k_3 \in HK$ car $h_1 h_3 \in H$ et $k_3 \in K$ car H est un sous-groupe.

On en déduit que HK est un sous-groupe de G.

En conclusion,

$$\boxed{HK \text{ est un sous-groupe de } G \text{ si, et seulement si, } HK = KH.}$$

✠ ***Exercice 3.*** [$\star$] (Produits direct et demi-direct de groupes)

Soient $(G, *)$ et $(H, \star)$ deux groupes.

1. (Cours) On définit sur $G \times H$ la loi $\otimes$ par

$$\forall (g_1, h_1), (g_2, h_2) \in G \times H, \qquad (g_1, h_1) \otimes (g_2, h_2) = (g_1 * g_2 \,,\, h_1 \star h_2).$$

Démontrer que $(G \times H, \otimes)$ est un groupe, appelé *produit direct* de G par H.

2. Soit $\varphi : (H, \star) \longrightarrow \big(\mathrm{Aut}(G), \circ\big)$ un morphisme de groupe. On définit sur $G \times H$ la loi $\boxtimes$ par

$$\forall (g_1, h_1), (g_2, h_2) \in G \times H, \qquad (g_1, h_1) \boxtimes (g_2, h_2) = \big(g_1 * \varphi(h_1)(g_2) \,,\, h_1 \star h_2\big).$$

   a) Démontrer que $(G \times H, \boxtimes)$ est un groupe, appelé *produit semi-direct* de G par H relativement à φ. On le note $G \rtimes_\varphi H$.

   b) Que reconnait-on lorsque φ est le morphisme trivial (i.e. $\forall h \in H,\ \varphi(h) = \mathrm{Id}_G$).

1. Cf cours.
2. a) La loi $\boxtimes$ est clairement interne.

La loi $\boxtimes$ est associative car, pour tous $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$, on a

$$\begin{aligned}
& \big((g_1, h_1) \boxtimes (g_2, h_2)\big) \boxtimes (g_3, h_3) \\
= \ & \big(g_1 * \varphi(h_1)(g_2) \,,\, h_1 \star h_2\big) \boxtimes (g_3, h_3) \\
= \ & \big(\big(g_1 * \varphi(h_1)(g_2)\big) * \varphi(h_1 \star h_2)(g_3) \,,\, (h_1 \star h_2) \star h_3\big) \\
= \ & \big(g_1 * \big(\varphi(h_1)(g_2) * \varphi(h_1 \star h_2)(g_3)\big) \,,\, h_1 \star (h_2 \star h_3)\big) && \text{associativité de } * \text{ et de } \star \\
= \ & \big(g_1 * \big(\varphi(h_1)(g_2) * \varphi(h_1)\big(\varphi(h_2)(g_3)\big)\big) \,,\, h_1 \star (h_2 \star h_3)\big) && \text{car } \varphi \text{ est un morphisme} \\
= \ & \big(g_1 * \varphi(h_1)\big(g_2 * \varphi(h_2)(g_3)\big) \,,\, h_1 \star (h_2 \star h_3)\big) && \text{car } \varphi(h_1) \text{ est un morphisme} \\
= \ & (g_1, h_1) \boxtimes \big(g_2 * \varphi(h_2)(g_3), h_2 \star h_3\big) \\
= \ & (g_1, h_1) \boxtimes \big((g_2, h_2) \boxtimes (g_3, h_3)\big).
\end{aligned}$$

Le couple () est neutre pour $\boxtimes$ car, pour tout $(g, h) \in G \times H$, on a

$$\begin{aligned}
(e_G, e_H) \boxtimes (g, h) &= \big(e_G * \varphi(e_H)(g) \,,\, e_H \star h\big) \\
&= \big(\mathrm{Id}_G(g) \,,\, h\big) && \text{car } \varphi \text{ est un morphisme} \\
&= (g, h)
\end{aligned}$$

et

$$\begin{aligned}
(g, h) \boxtimes (e_G, e_H) &= \big(g * \varphi(h)(e_G) \,,\, h \star e_H\big) \\
&= \big(g * e_G \,,\, h \star e_H\big) && \text{car } \varphi(h) \text{ est un morphisme} \\
&= (g, h).
\end{aligned}$$

Tout élément (g,h) de $G\times H$ est inversible pour $\boxtimes$ d'inverse $\big(\varphi(h)^{-1}(g^{-1})\,,\,h^{-1}\big)$. En effet, on a

$$\begin{aligned}(g,h)\boxtimes\big(\varphi(h)^{-1}(g^{-1})\,,\,h^{-1}\big) &= \big(g*\varphi(h)\big(\varphi(h)^{-1}(g^{-1})\big)\,,\,h\star h^{-1}\big)\\ &= \big(g*g^{-1}\,,\,h\star h^{-1}\big)\\ &= (e_G,e_H)\end{aligned}$$

et

$$\begin{aligned}\big(\varphi(h)^{-1}(g^{-1})\,,\,h^{-1}\big)\boxtimes(g,h) &= \big(\varphi(h)^{-1}(g^{-1})*\varphi(h^{-1})(g)\,,\,h^{-1}\star h\big)\\ &= \big(\varphi(h^{-1})(g^{-1})*\varphi(h^{-1})(g)\,,\,h^{-1}\star h\big) && \text{car } \varphi \text{ est un morphisme}\\ &= \big(\varphi(h^{-1})(g^{-1}*g)\,,\,h^{-1}\star h\big) && \text{car } \varphi(h^{-1}) \text{ est un morphisme}\\ &= \big(\varphi(h^{-1})(e_G)\,,\,h^{-1}\star h\big)\\ &= (e_G,e_H) && \text{car } \varphi(h^{-1}) \text{ est un morphisme}\end{aligned}$$

En conclusion,

$$\boxed{(G\times H,\boxtimes) \text{ est un groupe.}}$$

b) Dans le cas où φ est le morphisme trivial, on a, pour tous $(g_1,h_1),(g_2,h_2)\in G\times H$,

$$(g_1,h_1)\boxtimes(g_2,h_2)=\big(g_1*\varphi(h_1)(g_2)\,,\,h_1\star h_2\big)=\big(g_1*\mathrm{Id}_G(g_2)\,,\,h_1\star h_2\big)=(g_1*g_2\,,\,h_1\star h_2).$$

Donc

$$\boxed{\begin{array}{c}\text{dans le cas où } \varphi \text{ est le morphisme trivial, le produit semi-direct}\\ \text{de } G \text{ par } H \text{ relativement à } \varphi \text{ est le produit direct de } G \text{ par } H.\end{array}}$$

✠ *Exercice 4.* [$\star$]
Soient $(A,+,\times)$ un anneau non réduit à $\{0\}$ et $a,b\in A$. On suppose que $ab+ba=1$ et $a^2b+ba^2=a$. Démontrer que $a=2a^2b=2ba^2$. En déduire que a est inversible et donner son inverse.

En multipliant $ab+ba=1$ par a à gauche, on obtient $a^2b+aba=a$. En multipliant la même relation par a à droite, on obtient $aba+ba^2=a$. En comparant ces deux relations avec l'hypothèse $a^2b+ba^2=a$, on en déduit que $aba=a^2b=ba^2$. En reportant dans $a^2b+ba^2=a$, il vient

$$\boxed{a=2a^2b=2ba^2.}$$

L'égalité $a=2a^2b$ nous dit que $ba=2ba^2b$ et l'égalité $a=2ba^2$ nous dit que $ab=2ba^2b$, donc $ab=ba$. Comme $ab+ba=1$, il s'ensuit que $2ab=2ba=1$. Par conséquent,

$$\boxed{a \text{ est inversible et } a^{-1}=2b.}$$

✠ *Exercice 5.* [$\bigstar$]
Soient $(A,+,\times)$ un anneau tel que $\forall a,b\in A,\ ba=\pm ab$. Démontrer que A est commutatif.

On introduit le centre Z de A et son « anticentre » Z' définis par

$$Z=\{a\in A:\forall x\in A,\ ax=xa\}\qquad\text{et}\qquad Z'=\{a\in A:\forall x\in A,\ ax=-xa\}.$$

Il est facile de vérifier que Z et Z' sont des sous-groupes de $(A,+)$.

Démontrons que $A=Z\cup Z'$. Soit $a\in A$. Par l'absurde, supposons que $a\notin Z\cup Z'$. Comme $a\notin Z$, il existe $x\in A$ tel que $ax\neq xa$, ce qui impose que $ax=-xa$. De même, comme $a\notin Z'$, il existe $y\in A$ tel que $ay\neq -ya$, ce qui impose que $ay=ya$. Dès lors, en additionnant les égalités $ay=ya$ et $ax=-xa$, on obtient $a(y+x)=(y-x)a$. Il s'ensuit que $a(y+x)=\pm a(y-x)$, c'est-à-dire $ax=-ax$ ou $ay=-ay$. Comme $ax=-xa$ et $ay=ya$, cela donne $ax=xa$ et $ay=-ya$. C'est absurde !

On sait qu'un groupe ne peut pas être la réunion de deux sous-groupes stricts. On a donc $A = Z$ ou $A = Z'$.

Si $A = Z$, on crie « youpi ! ».

Si $A = Z'$, on a en particulier $1 \in Z'$, ce qui donne $1.1 = -1.1$, c'est-à-dire $1 = -1$. Dès lors, pour tout $a, b \in A$, on a $ab = -ba = ba$ où la première égalité découle du fait que $a \in Z'$ et la seconde du fait que $1 = -1$. Ainsi, A est commutatif.

En conclusion,

$$\boxed{A \text{ est commutatif.}}$$