UCBL – L3 Mathématiques Générales et Applications — Automne 2021

UE Groupes et Géométrie

CC1 du 4 novembre 2021

Durée : 1h30

Les calculatrices, ordinateurs, tablettes et téléphones portables sont interdits durant l'épreuve ainsi que les notes de cours et TD.

Question 1. Vrai ou faux? Justifier en moins d'un paragraphe, en donnant un argument cours, évoquant un résultat du cours (ou du TD), ou en donnant un exemple / contre-exemple, selon ce qui convient.

1. Si G est un groupe fini et $x \in G$, alors $\operatorname{ord}(x)$ divise $|G|$.
2. Si G est un groupe fini et $A \subseteq G$ est une partie, alors $|A|$ divise $|G|$.
3. Si G est un groupe fini et $H \leq G$ est un sous-groupe, alors l'indice $[G : H]$ divise $|G|$.
4. Si G et H sont deux groupes non-triviaux (c'est à dire, $G \neq \{e_G\}$ et $H \neq \{e_H\}$), alors il existe un morphisme $\varphi\colon G \to H$ qui n'est pas trivial (n'est pas constamment égal à e_H).

Correction.

1. Vrai. C'est un corollaire du théorème de Lagrange. Plus précisément, $\operatorname{ord}(x) = |\langle x \rangle|$ et $\langle x \rangle \leq G$, et d'après Lagrange, $|\langle x \rangle|$ divise $|G|$.
2. Faux. Il faut donc donner un contre-exemple. Par exemple, $G = \mathbf{Z}/3\mathbf{Z}$, $A = \{\bar{0}, \bar{1}\} = \{0+3\mathbf{Z}, 1+3\mathbf{Z}\}$ (ce qui n'est pas $\mathbf{Z}/2\mathbf{Z} = \{0+2\mathbf{Z}, 1+2\mathbf{Z}\}$!!)
3. Vrai. Suit d'une résultat du cours : $|G| = |H|[G : H]$.
4. Faux. Il faut donc donner un contre exemple. $G = \mathbf{Z}/2\mathbf{Z}$, $H = \mathbf{Z}$. Si $\varphi\colon G \to H$ est un morphisme, alors $\varphi(\bar{1}) + \varphi(\bar{1}) = \varphi(\bar{0}) = 0$, donc $\varphi(\bar{1}) = 0$, et φ est trivial.

Question 2. Soit G un groupe. On note $\operatorname{Aut}(G)$ l'ensemble des automorphismes de G. Montrer que $\operatorname{Aut}(G)$ est un groupe, pour la loi de composition.
Pour cette question, aucun résultat du CM ou du TD n'est autorisé – vous devez tout démontrer.

Correction. On se rappelle : $\operatorname{Aut}(G)$ consiste en les automorphismes de G, c'est à dire les morphismes $\varphi\colon G \to G$ qui sont bijectifs.

- Clôture : Soit $\varphi, \psi \in \operatorname{Aut}(G)$. Alors $\varphi \circ \psi\colon G \to G$, et c'est un application bijective en tant que composition de telles. C'est un morphisme : pour tous $x, y \in G$: $\varphi \circ \psi(xy) = \varphi\big(\psi(xy)\big) = \varphi\big(\psi(x)\psi(y)\big) = \varphi\big(\psi(x)\big)\varphi\big(\psi(y)\big)$. Donc $\psi \circ \psi \in \operatorname{Aut}(G)$.
- Associativité. La composition est associative, ce n'est pas un résultat de ce cours. Ou on démontre directement que pour tout x : $\big((\varphi \circ \psi) \circ \rho\big)(x) = \big(\varphi \circ (\psi \circ \rho)\big)(x)$.
- Neutre. Soit $\mathrm{id}_G\colon G \to G$ l'application identité. Elle est bijective, et elle est un morphisme : $\mathrm{id}_G(xy) = xy = \mathrm{id}_G(x)\,\mathrm{id}_G(y)$. Donc : $\mathrm{id}_G \in \operatorname{Aut}(G)$. C'est le neutre : $\mathrm{id}_G \circ \varphi = \varphi \circ \mathrm{id}_G = \varphi$ pour tout $\varphi \in \operatorname{Aut}(G)$.
- Inverse : Soit $\varphi \in \operatorname{Aut}(G)$. Comme c'est une application bijective, elle admet une application réciproque $\varphi^{-1}\colon G \to G$, également bijective. C'est un morphisme : si $x, y \in G$ et $u = \varphi^{-1}(x)$ et $v = \varphi^{-1}(y)$, alors $\varphi^{-1}(xy) = \varphi^{-1}\big(\varphi(u)\varphi(v)\big) = \varphi^{-1}\big(\varphi(uv)\big) = uv = \varphi^{-1}(x)\varphi^{-1}(y)$.

  Donc $\varphi^{-1} \in \operatorname{Aut}(G)$. Et par définition de l'application réciproque : $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \mathrm{id}_G$.

Soit G, H et K des groupes. On rappelle que $H \times K$ (le *produit direct* des groupes H et K) est un groupe, pour la loi $(h,k)\cdot(h',k') = (hh', kk')$.

Question 3. 1. Soit $\alpha\colon G \to H$ et $\beta\colon G \to K$ deux morphismes de groupes. Montrer que

$$\varphi(g) = \Big(\alpha(g), \beta(g)\Big)$$

définit un morphisme $G \to H \times K$.

2. Réciproquement, montrer que si $\varphi\colon G \to H \times K$ est un morphisme, alors il s'exprime comme plus haut pour une unique paire de morphismes α, β.

Correction. 1. Soit $g, g' \in G$. Alors

$$\varphi(gg') = \Big(\alpha(gg'), \beta(gg')\Big) = \Big(\alpha(g)\alpha(g'), \beta(g)\beta(g')\Big) = \Big(\alpha(g), \beta(g)\Big)\Big(\alpha(g'), \beta(g')\Big) = \varphi(g)\varphi(g')$$

2. Nous savons déjà que les projections canoniques

$$\pi_1\colon H \times K \to H, \qquad \pi_1(h,k) = h,$$
$$\pi_2\colon H \times K \to H, \qquad \pi_2(h,k) = k,$$

sont des morphismes (et si on ne le sait, on le démontre : $\pi_1\big((h,k)\cdot(h',k')\big) = \pi_1(hh', kk') = hh' = \pi_1(h,k)\pi_1(h',k')$, et pareil pour π_2). D'ailleurs, pour tout $(h,k) \in H \times K$ on a :

$$(h,k) = \Big(\pi_1(h,k), \pi_2(h,k)\Big) \tag{1}$$

Soit $\varphi\colon G \to H \times K$ un morphisme, $\alpha = \pi_1 \circ \varphi$ et $\beta = \pi_2 \circ \varphi$. Alors ce sont des morphismes, en tant que compositions de tels, et pour tout $g \in G$, d'après (1) :

$$\varphi(g) = \Big(\pi_1\big(\varphi(g)\big), \pi_2\big(\varphi(g)\big)\Big) = \Big(\alpha(g), \beta(g)\Big).$$

Unicité : supposons que l'on ait aussi, pour tout $g \in G$:

$$\varphi(g) = \Big(\alpha'(g), \beta'(g)\Big).$$

Alors, pour tout $g \in G$:

$$\Big(\alpha(g), \beta(g)\Big) = \Big(\alpha'(g), \beta'(g)\Big).$$

Ceci équivaut $\alpha(g) = \alpha'(g)$ et $\beta(g) = \beta'(g)$ pour tout $g \in G$, c'est à dire $\alpha = \alpha'$ et $\beta = \beta'$.

Question 4. 1. Soit $\alpha\colon H \to G$ et $\beta\colon K \to G$ deux morphismes de groupes, et supposons de surcroît que

$$\alpha(h)\beta(k) = \beta(k)\alpha(h) \qquad \forall h \in H,\ k \in K \tag{*}$$

Montrer que

$$\varphi(h,k) = \alpha(h)\beta(k)$$

définit un morphisme $H \times K \to G$.

2. Réciproquement, montrer que si $\varphi\colon H \times K \to G$ est un morphisme, alors il s'exprime comme plus haut pour une unique paire de morphismes α, β, et que cette paire vérifie (*).

Correction. 1. Montrons que c'est un morphisme :

$$\begin{aligned}\varphi\big((h,k)\cdot(h',k')\big) &= \varphi(hh',kk') = \alpha(hh')\beta(kk') \\ &= \alpha(h)\alpha(h')\beta(k)\beta(k') \\ &= \alpha(h)\beta(k)\alpha(h')\beta(k') = \varphi(h,k)\varphi(h',k').\end{aligned}$$

2. Réciproquement, soit $\varphi\colon H\times K\to G$ un morphisme. Pour $h\in H$ et $k\in K$ on pose

$$\alpha(h)=\varphi(h,e), \qquad \beta(k)=\varphi(e,k).$$

Ce sont des morphismes : $\alpha(hh')=\varphi\big(hh',e\big)=\varphi\big((h,e)\cdot(h',e)\big)=\varphi(h,e)\varphi(h',e)=\alpha(h)\alpha(h')$, et pareil pour β. On a bien, pour tout $h\in H$ et $k\in K$:

$$(h,k)=(h,e)\cdot(e,k) \qquad \varphi(h,k)=\varphi(h,e)\varphi(e,k)=\alpha(h)\beta(k).$$

Aussi,

$$(h,k)=(e,k)(h,e) \qquad \varphi(h,k)=\varphi(e,k)\varphi(h,e)=\beta(k)\alpha(h).$$

d'où $(*)$. Unicité : Supposons que l'on ait aussi $\varphi(h,k)=\alpha'(h)\beta'(k)$ pour tout $h\in H$, $k\in K$, où $\alpha'\colon H\to G$ et $\beta'\colon K\to G$ sont des morphismes. Alors pour tout $h\in H$: $\alpha(h)=\varphi(h,e)=\alpha'(h)\beta'(e)=\alpha'(h)e=\alpha'(h)$. Donc $\alpha=\alpha'$, et pareil, $\beta=\beta'$

Question 5. Soit G un groupe et soit H et K deux sous-groupes de G tels que $HK=G$, et

$$hkh^{-1}k^{-1}=e \qquad \forall h\in H,\ k\in K.$$

Montrer que H et K sont des sous-groupes distingués de G.

Correction. D'abord, la condition $hkh^{-1}k^{-1}=e$ est équivalente à $hk=kh$, pour tous $h\in H$ et $k\in K$ [ATTENTION : ceci ne préjuge pas que les membres de H commutent entre eux, ni ceux de K, et G pourrait être non abélien].

Pour montrer que H est distingué, il suffit de montrer que pour tout $h\in H$ et $g\in G$: $ghg^{-1}\in H$. Puisque $G=HK$, on peut écrire $g=h'k$ où $h'\in H$ et $k\in K$. Puisque les membres de H commutent avec ceux de K :

$$ghg^{-1}=h'khk^{-1}h'^{-1}=h'hkk^{-1}h'^{-1}=h'hh'^{-1}\in H.$$

Un argument similaire marche pour K.