1
2
3

MAT35B - ALGÈBRE L3A

Premier Semestre — 2021-2022

Premier Devoir Surveillé

Toute réponse non justifiée ne sera pas validée.

Le barème est donné à titre indicatif et non contractuel.

5pt **1.** Soient G un groupe fini, et a et b deux éléments de G.

(a) Démontrer que a, a^{-1} et bab^{-1} ont tous le même ordre.

(b) Démontrer que ab et ba ont le même ordre.

(c) Soit n un entier, déterminer l'ordre de a^n en fonction de n et de l'ordre de a.

(d) Supposons que $ab = ba$, que $\langle a\rangle \cap \langle b\rangle = \{1_G\}$, et que a et b sont d'ordre fini n et m respectivement. Déterminer l'ordre de ab en fonction de n et m.

(e) Supposons que $ab = ba$, et que a et b sont d'ordre fini n et m respectivement, avec $\mathrm{PGCD}(n, m) = 1$. Déterminer l'ordre de ab en fonction de n et m.

Solution.

(a) Pour tout $k \in \mathbb{N}$, on a $a^k = 1_G$ si et seulement si $a^{-k} = 1_G$, ce qui nous dit que a et a^{-1} ont le même ordre. L'élément bab^{-1} est l'image de a par l'isomorphisme de conjugaison par b, ce qui implique que son ordre coïncide avec celui de a.

(b) De $ab = a(ba)a^{-1}$, on déduit comme précédemment que ab et ba ont le même ordre.

(c) Soient $d = \mathrm{PGCD}(n, \mathrm{ord}(a))$, $n' = n/d$ et $\alpha = \mathrm{ord}(a)/d$. Pour tout $k \in \mathbb{N}$, par définition on a $a^{nk} = 1_G$ si et seulement si $\mathrm{ord}(a) \mid nk$, *i.e.* $nk \equiv 0 \pmod{\mathrm{ord}(a)}$, ce qui équivaut à $n'k \equiv 0 \pmod{\alpha'}$. Comme n' et α' sont premiers entre eux, la condition précédente est équivalente à $k \equiv 0 \pmod{\alpha'}$. En conséquence, l'ordre de a^n est $\mathrm{ord}(a)/d = \mathrm{ord}(a)/\mathrm{PGCD}(\mathrm{ord}(a), n)$.

(d) Soit $k \in \mathbb{N}$. Comme a et b commutent, on voit bien que $1_G = (ab)^k = a^k b^k$ est équivalent à $a^k = b^{-k}$, *i.e.* $a^k = b^{-k} = 1_G$, vu que $\langle a\rangle \cap \langle b\rangle = \{1_G\}$. La dernière condition trouvée est équivalente à $n \mid k$ et $m \mid k$, *i.e.* $\mathrm{PPCM}(n, m) \mid k$. L'ordre de ab est donc égal à $\mathrm{PPCM}(n, m)$.

(e) On pose $q = \mathrm{PPCM}(n, m)$. On a clairement $(ab)^q = 1_G$, ce qui nous dit que $\mathrm{ord}(ab) \mid q$. Réciproquement, si $k \in \mathbb{N}$ est tel que $(ab)^k = 1_G$, alors $a^k = b^{-k}$ et en élevant à l'ordre de a l'égalité on obtient $b^{-nk} = 1_G$, ce qui implique que $m \mid nk$. Comme m et n sont premiers entre eux, on obtient que $m \mid k$. Par symétrie du problème, on a de même $n \mid k$, d'où $q \mid k$. En conclusion l'ordre de ab est égal à $q = \mathrm{PPCM}(n, m)$.

5pt **2.** Soient $(G, \cdot)$ un groupe et $\sim$ une relation d'équivalence sur G.

(a) Soient X un ensemble et $p : G \to X$ une application surjective. Montrer qu'il existe au plus une loi de composition interne $*$ sur X de sorte que $(X, *)$ soit un groupe et p un morphisme de groupes.

(b) On dit que $\sim$ est **compatible avec la structure de groupe de** G s'il existe une structure de groupe sur $G/\sim$ telle que la projection canonique $p : G \to G/\sim$ soit un morphisme de groupes.

(i) Montrer qu'une telle structure de groupe sur $G/\sim$ est unique si elle existe.

(ii) Montrer que $\sim$ est compatible avec la structure de groupe de G si et seulement si $x \sim x'$ et $y \sim y'$ impliquent $x \cdot y \sim x' \cdot y'$, pour tout $x, x', y, y' \in G$.

(c) Soit $\sim$ une relation d'équivalence sur G compatible avec la structure de groupe. On note $[x] = \{y \in G : x \sim y\}$ la classe d'équivalence de $x \in G$.

(i) Montrer $H = [1_G]$ est un sous-groupe distingué de G.

(ii) Montrer que $\sim$ coïncide avec la relation d'équivalence $\sim_H$ associée au sous-groupe H.

Solution.

(a) Soient $*$ et $\star$ deux lois de groupes sur X, telles que p est un morphisme de groupes de $(G, \cdot)$ dans $(X, *)$ et dans $(X, \star)$. Soient $x_1, x_2 \in X$. Comme p est surjectif, il existe $g_1, g_2 \in G$ tels que $p(g_i) = x_i$ pour $i \in \{1, 2\}$. Comme p est un morphisme de groupes, alors

$$x_1 * x_2 = p(g_1) * p(g_2) = p(g_1 \cdot g_2) = p(g_1) \star p(g_2) = x_1 \star x_2.$$

Par conséquent, $*$ et $\star$ coïncident.

(b) (i) Il s'agit d'une conséquence directe de l'item précédent.

(ii) On suppose d'abord que $\sim$ est compatible avec la structure de groupe de G. Soient $x, x', y, y' \in G$ tels que $x \sim x'$ et $y \sim y'$, *i.e.* $p(x) = p(x')$ et $p(y) = p(y')$. Comme p est un morphisme de groupes dans ce cas, on conclut que

$$p(x \cdot y) = p(x) * p(y) = p(x') * p(y') = p(x' \cdot y'),$$

i.e. $x \cdot y \sim x' \cdot y'$.

Réciproquement, on suppose que, étant donnés $x, x', y, y' \in G$, $x \sim x'$ et $y \sim y'$ impliquent $x \cdot y \sim x' \cdot y'$. On définit alors une loi de composition sur $G/\sim$ via $[x]*[y] = [x \cdot y]$, pour $x, y \in G$. Cette loi $*$ est bien définie précisément en raison de l'hypothèse sur $\sim$. On voit bien que $*$ est associative, car

$$\begin{aligned}\big([x]*[y]\big)*[z] &= [x \cdot y]*[z] = \big[(x \cdot y) \cdot z\big] = \big[x \cdot (y \cdot z)\big] \\ &= [x]*[y \cdot z] = [x]*\big([y]*[z]\big),\end{aligned}$$

pour tous $x, y, z \in G$. En plus, la définition de la loi $*$ nous dit directement que $[1_G]$ est le neutre de $G/\sim$ et que $[x^{-1}]$ est l'inverse de $[x]$, pour $x \in G$. En conséquence, $(G/\sim, *)$ est un groupe. En outre, comme $p(x) = [x]$, la définition de la loi $*$ nous dit que $p(x) * p(y) = p(x \cdot y)$, *i.e.* p est un morphisme de groupes, ce qui implique que $\sim$ est compatible avec la structure de groupe de G.

(c) (i) Comme $H = [1_G]$ est le noyau du morphisme de groupes $p : G \to G/\sim$, il s'agit d'un sous-groupe normal de G.

(ii) D'après l'item (b), (ii), on voit bien que $x \sim y$ si et seulement si $1_G \sim x^{-1}y$, *i.e.* $x^{-1}y \in H$, qui est précisément la définition de $x \sim_H y$. En conséquence, $\sim$ et $\sim_H$ coïncident.

10pt

3. Soient G un groupe et H un sous-groupe de G. On appelle **normalisateur** de H dans G l'ensemble

$$N_H = \left\{g \in G : gHg^{-1} = H\right\}.$$

(a) Montrer que N_H est un sous-groupe de G contenant H et que c'est le plus grand sous-groupe de G dans lequel H est distingué.

(b) Calculer le normalisateur de $H = \langle(1\,3\,4)\rangle$ dans le groupe $\mathbb{S}_4$.

(c) Montrer que, étant donnés $a, b \in G$, on a

$$aHa^{-1} = bHb^{-1} \text{ si et seulement si } a^{-1}b \in N_H.$$

(d) Soit $\mathscr{H}$ l'ensemble des conjugués de H dans G, *i.e.*

$$\mathscr{H} = \left\{gHg^{-1} : g \in G\right\},$$

et soit $f : G \to \mathscr{H}$ l'application qui associe gHg^{-1} à $g \in G$. Montrer qu'il existe une bijection $\bar{f} : G/N_H \to \mathscr{H}$ telle que $\bar{f} \circ p = f$, où $p : G \to G/N_H$ est la projection canonique.

(e) Déduire de la question précédente que $\mathscr{H}$ est fini si et seulement si G/N_H est fini et que dans ce cas le nombre de sous-groupes conjugués de H dans G est égal à l'indice $[G : N_H]$ de N_H dans G.

(f) On suppose désormais que G est fini et que $H \subsetneq G$.

(i) Si $[G : N_H] = 1$, à quoi est égal l'ensemble $\bigcup_{g \in G} gHg^{-1}$?

(ii) Démontrer l'inégalité $\left|\bigcup_{g \in G} gHg^{-1}\right| \leq [G : N_H].|H|$

Indication : on pourra introduire un système de représentants de G/N_H.

(iii) Si $[G : N_H] > 1$, justifier que l'inégalité ci-dessus est stricte.

(iv) Déduire des questions précédentes que dans tous les cas, on a l'inclusion stricte $\bigcup_{g \in G} gHg^{-1} \subsetneq G$.

(g) Montrer que la conclusion de la question précédente n'est plus valable lorsque le groupe G est infini.
Indication : on pourra considérer le groupe $G = \mathsf{GL}_n(\mathbb{C})$ des matrices inversibles avec $n \geq 2$ et le sous-groupe H formé des matrices triangulaires supérieures.

Solution.

(a) On notera comme d'habitude 1_G l'élément neutre de G. Montrons d'abord que N_H est un sous-groupe de G. En effet, comme $1_G H 1_G^{-1} = H$, $1_G \in N_H$. En plus, si $a, b \in N_H$, alors $ab^{-1} \in N_H$, car

$$(ab^{-1})H(ab^{-1})^{-1} = ab^{-1}(bHb^{-1})ba^{-1} = aHa^{-1} = H.$$

Par conséquent, N_H est bien un sous-groupe de G. En outre, il est clair que $H \subseteq N_H$, vu que H est un sous-groupe de G, et si l'on prend $h \in H$ et $g \in N_H$, on a $ghg^{-1} \in gHg^{-1} = H$, ce qui nous dit que H est un sous-groupe normal de N_H.

Enfin, si K est un sous-groupe de G contenant H tel que H soit normal dans K, alors, pour tout $k \in K$, on a $kHk^{-1} = H$ donc $k \in N_H$. En particulier $K \subseteq N_H$.

(b) On remarque d'abord que $(1\,3\,4)^2 = (1\,4\,3)$ et $(1\,3\,4)^3 = \mathrm{id}_{[\![1,4]\!]}$, ce qui implique que $H = \{\mathrm{id}_{[\![1,4]\!]}, (1\,3\,4), (1\,4\,3)\}$. Étant donné $\sigma \in \mathbb{S}_4$, la condition $\sigma H \sigma^{-1} = H$ est donc équivalente à $\sigma(1\,3\,4)\sigma^{-1} \in H$. Comme $\sigma(1\,3\,4)\sigma^{-1} = \mathrm{id}_{[\![1,4]\!]}$ est impossible, $\sigma \in N_H$ est équivalent à $\sigma(1\,3\,4)\sigma^{-1} \in \{(1\,3\,4), (1\,4\,3)\}$. En outre, si $\sigma \in \mathbb{S}_4$, on voit bien que $\sigma(i_1\,i_2\,i_3)\sigma^{-1} = (\sigma(i_1)\,\sigma(i_2)\,\sigma(i_3))$, pour $i_1, i_2, i_3 \in [\![1,4]\!]$ différents. Cela nous dit que $\sigma \in N_H$ si et seulement si $(\sigma(1)\,\sigma(3)\,\sigma(4)) = (1\,3\,4)$ ou $(\sigma(1)\,\sigma(3)\,\sigma(4)) = (1\,4\,3)$. Dans le premier cas on trouve $\sigma \in \{\mathrm{id}_{[\![1,4]\!]}, (1\,3\,4), (1\,4\,3)\} = H$ et dans le deuxième $\sigma \in \{(1\,3), (1\,4), (3\,4)\}$, *i.e.* $\sigma \in N_H$ si et seulement si $\sigma \in \mathbb{S}_4$ et $\sigma(2) = 2$.

(c) Soient $a, b \in G$. Alors $aHa^{-1} = bHb^{-1}$ si et seulement si $H = a^{-1}bHb^{-1}a$, ce qui équivaut à $a^{-1}b \in N_H$.

(d) Par définition de $\mathscr{H}$, l'application f est surjective. De plus, si g et g' sont deux éléments de G tels que $g' = ga$ pour un certain $a \in N_H$, alors $gaHa^{-1}g^{-1} = gHg^{-1}$, ce qui nous dit que $f(g) = f(g')$, *i.e.* f est constante sur chaque classe d'équivalence. En conséquence, il existe une application $\bar{f} : G/N_H \to \mathscr{H}$ telle que $\bar{f} \circ p = f$, et $\bar{f}$ est également surjective. L'injectivité de $\bar{f}$ provient directement de l'item précédent.

(e) La bijection $\bar{f} : G/N_H \to \mathscr{H}$ permet de voir que $\mathscr{H}$ est fini si et seulement si G/N_H est fini et qu'alors $[G : N_H] = |\mathscr{H}|$.

(f)
(i) Si $[G : N_H] = 1$, alors $N_H = G$, donc H est distingué dans G, ce qui entraîne que $\cup_{g \in G} gHg^{-1} = H$.

(ii) Soit S un système de représentants des classes à gauche de G modulo N_H, *i.e.* S contient un élément et un seul dans chaque classe d'équivalence. En particulier, $|S| = |\mathscr{H}| = [G : N_H]$. D'après l'item (c), on a alors $\bigcup_{g \in G} gHg^{-1} = \bigcup_{g \in S} gHg^{-1}$, d'où

$$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq \sum_{g \in S} \left| gHg^{-1} \right|.$$

Or pour tout $g \in G$, l'application $H \mapsto gHg^{-1}$ est une bijection, donc $|gHg^{-1}| = |H|$, et finalement

$$\left|\bigcup_{g\in G} gHg^{-1}\right| \leq |S|.|H| = [G : N_H].|H|.$$

(iii) Si $[G : N_H] > 1$, alors l'union $\bigcup_{g\in S} gHg^{-1}$ n'est pas disjointe. En effet, 1_G appartient à tous les gHg^{-1}. Par conséquent,

$$\left|\bigcup_{g\in S} gHg^{-1}\right| < \sum_{g\in S} \left|gHg^{-1}\right|,$$

ce qui implique que

$$\left|\bigcup_{g\in G} gHg^{-1}\right| < [G : N_H].|H|$$

(*cf.* item précédent) .

(iv) Si $[G : N_H] = 1$, on a vu que $\bigcup_{g\in G} gHg^{-1} = H$, qui est bien inclus strictement dans G. Sinon, comme l'inclusion $H \subseteq N_H$ implique l'inégalité $[G : N_H] \leq [G : H]$, on a

$$\left|\bigcup_{g\in G} gHg^{-1}\right| < [G : N_H].|H| \leq [G : H].|H| = |G|,$$

d'où $\bigcup_{g\in G} gHg^{-1} \subsetneq G$.

(*g*) Comme toute matrice M de $\mathsf{GL}_n(\mathbb{C})$ est trigonalisable, elle peut être écrite sous la forme $M = PTP^{-1}$ avec $P \in \mathsf{GL}_n(\mathbb{C})$ et $T \in \mathsf{GL}_n(\mathbb{C})$ triangulaire supérieure. En notant $\mathscr{T}$ le sous-groupe des matrices triangulaires supérieures inversibles, on a donc

$$\mathsf{GL}_n(\mathbb{C}) = \bigcup_{P\in\mathsf{GL}_n(\mathbb{C})} P\mathscr{T}P^{-1}.$$