CORRIGÉ du Devoir à la maison du 15 décembre 2008

Ce corrigé vous donne le barême et des indications de correction. La rédaction ne prétend pas être parfaite ; elle est parfois concise, car le but est plutôt de commenter les points qui en valent le coup.

Exercice 1 L'essence de cet exercice a été vue en Algèbre Linéaire avec Emmanuel Ferrand.

1 pt Démontrer qu'il s'agit d'une action est facile et n'a pas posé de problèmes. Mais attention : beaucoup confondent l'application $\rho : G \times X \to X$ donné par $\rho(g, M) = g.M$, et l'application $\varphi : G \to S_X$ telle que $\varphi(g)$ est l'application de X dans lui-même qui envoie M sur $g.M$. L'application ρ n'est pas un morphisme de groupes, d'ailleurs, ni sa source ni son but de sont des groupes en général. En revanche, dire qu'on a une action veut dire exactement que φ est un morphisme de groupes.

2 pts Décrire l'ensemble des orbites est moins simple. Vous avez vu qu'on peut choisir des bases B et B' telles que la matrice, dans ces bases, de l'endomorphisme associé à M, est la matrice diagonale J_r dont les r premiers termes diagonaux sont des 1 et les $n - r$ suivants sont des 0, où $r = \mathrm{rg}(M)$ est le rang de M. L'orbite $\mathcal{O}(M)$ de la matrice M est l'ensemble des matrices équivalentes à M. Beaucoup confondent l'orbite de M, $\mathcal{O}(M)$, et l'ensemble des orbites X/G ! En fait, on a une application $X/G \to \{0, 1, \ldots, n\}$ qui associe à une orbite $\mathcal{O}(M)$ le rang $\mathrm{rg}(M)$ de M. C'est bien défini, car toutes les matrices d'une même orbite sont équivalentes, donc ont même rang. Cette application est injective, car si $\mathrm{rg}(M) = \mathrm{rg}(M')$, alors M et M' sont équivalentes et donc $\mathcal{O}(M) = \mathcal{O}(M')$. Cette application est aussi surjective, car un entier $r \in \{0, \ldots, n\}$ est l'image de $\mathcal{O}(J_r)$. Finalement, X/G est en bijection avec $\{0, 1, \ldots, n\}$.

Exercice 2 (1)

0,5 pt Il est clair que $H \subset N_G(H)$, car si $h \in H$, alors comme H est un sous-groupe (donc stable par multiplication et par passage à l'inverse), on a $hHh^{-1} = H$.

1 pt De plus $N_G(H)$ est un sous-groupe puisque :
• de toute évidence $1 \in N_G(H)$.
• si $(g_1, g_2) \in (N_G(H))^2$ alors $(g_1g_2)H(g_1g_2)^{-1} = g_1g_2Hg_2^{-1}g_1^{-1} = g_1(g_2Hg_2^{-1})g_1^{-1} = g_1Hg_1^{-1} = H$ donc $g_1g_2 \in N_G(H)$.
• si $g \in N_G(H)$ alors $gHg^{-1} = H$ donc en multipliant à gauche par g^{-1} et à droite par g on trouve $H = g^{-1}Hg$, donc $g^{-1} \in N_G(H)$.

(2) La formulation de cette question est un exemple très classique où l'on vous demande en fait, en répondant à la question, de montrer qu'*il existe* un plus grand sous-groupe $K \subset G$ tel que $H \lhd K$. Ceci n'a rien d'évident a priori !

0,5 pt Il suffit de démontrer, d'abord, que $H \lhd N_G(H)$, , ce qui est clair car si $h \in H$, on a $hHh^{-1} = H$ par les propriétés de sous-groupe.

1 pt Ensuite, il faut montrer que tout sous-groupe de G tel que $K \subset G$ tel que $H \lhd K$ est inclus dans $N_G(H)$. Or, si K est un tel sous-groupe, pour tout $k \in K$ on a $kHk^{-1} = H$ donc $k \in N_G(H)$. Ainsi $K \subset N_G(H)$ et c'est fini.

1 pt (3) Supposons que $G = S_4$ et $H = \langle (1, 2) \rangle$. Notons $h = (1, 2)$. Soit $g \in G$, alors $gHg^{-1} = H$ ssi $ghg^{-1} = h$, puisque ghg^{-1} ne peut être égal à l'identité. C'est donc équivalent à $gh = hg$, ou encore à $(g(1) = h(g(2))$ et $g(2) = h(g(1)))$. On trouve donc soit $g(1) = 1$ et $g(2) = 2$, soit $g(1) = 2$ et $g(2) = 1$. Dans le premier cas, $g = \mathrm{Id}$ ou $g = (3, 4)$. Dans le deuxième cas, $g = h$ ou $g = h(3, 4)$. Finalement, $N_G(H) = \{\mathrm{Id}; (1, 2); (3, 4); (1, 2)(3, 4)\}$.

0 pt Si $G = A_4$ et $H = \langle (1, 2) \rangle$, alors à strictement parler, $N_G(H)$ n'est pas défini puisqu'il faut en principe que $H \subset G$, or ici $(1, 2)$ n'est pas dans A_4. Cependant, on peut chercher l'ensemble des permutations $g \in A_4$ telles que gHg^{-1}, c.-à-d. $N_{S_4}(H) \cap A_4$. On trouve alors $\{\mathrm{Id}; (1, 2)(3, 4)\}$.

Exercice 3 (1)

1.5 pt On commence par démontrer que c_g est un morphisme de groupes, ce qui est facile. Ensuite on doit démontrer que c_g est bijectif. Le plus simple était d'observer que $c_g \circ c_{g^{-1}} = c_{g^{-1}} \circ c_g = \mathrm{Id}_G$, ceci montre que c_g est bijectif et que sa réciproque est $c_{g^{-1}}$.

Certains ont prétendu que, comme c_g est une application de G dans lui-même, pour montrer qu'il est bijectif, il suffit de montrer qu'il est injectif. C'est faux, par exemple, le morphisme $f : \mathbb{Z} \to \mathbb{Z}$ tel que $f(n) = 2n$ est injectif mais non surjectif.

Certains ont prétendu que pour montrer que c_g est bijectif, il suffit de montrer qu'il est surjectif. C'est faux, par exemple, le morphisme $f : \mathbb{C}^* \to \mathbb{C}^*$ tel que $f(z) = z^2$ est surjectif mais non injectif.

Certains ont prétendu que pour montrer que c_g est bijectif, il suffit de montrer qu'il existe une application c' telle que $c' \circ c_g = \mathrm{Id}_G$. C'est faux, par exemple, si $G = \mathbb{R}[X]$ est le groupe additif des polynômes à coefficients réels (le neutre est le polynôme nul, et la somme des polynômes est leur somme usuelle), considérons le morphisme de dérivation $D : G \to G$ tel que $D(P) = P'$ et le morphisme $I : G \to G$ tel que $I(P)$ est le polynôme qui est la primitive de P nulle en 0. On vérifie facilement que D et I sont bien des endomorphismes de G, que $D \circ I = \mathrm{Id}_G$, et pourtant D n'est pas injectif, I n'est pas surjectif. Donc ni D ni I n'est bijectif.

Ces contre-exemples doivent vous permettre d'apprécier toute la force du Théorème du Rang en Algèbre Linéaire, qui a pour conséquence bien connue que pour les endomorphismes d'espaces linéaires de dimension finie, bijection = injection = surjection. Un autre cas où ceci fonctionne bien sûr est le cas des groupes finis, mais sorti de ces deux situations particulières, cette équation magique est fausse en général.

1.5 pt (2) Cette question a été bien traitée.

1 pt (3) $\ker(c) = \{g \in G,\ c_g = \mathrm{Id}\} = \{g \in G,\ \forall x \in G,\ gxg^{-1} = x\} = \{g \in G,\ \forall x \in G,\ gx = xg\}$. C'est l'ensemble des éléments de G qui commutent avec tous les éléments de G. Ce sous-groupe est appelé le *centre* de G.

1.5 pt (4) Cette question a été bien traitée. On montrait que $c_g \in \mathrm{Int}(G)$ et $f \in \mathrm{Aut}(G) \Rightarrow f \circ c_g \circ f^{-1} = c_{f(g)}$.

1 pt (5) Si G est un groupe abélien, alors il est égal à son centre, et donc $c_g = \mathrm{Id}$ pour tout g. Ainsi $\mathrm{Int}(G) = \{\mathrm{Id}\}$. Il suffisait donc de donner un groupe abélien qui possède des automorphismes non triviaux, par exemple $G = \mathbb{Z}$, puisque $x \mapsto -x$ est un automorphisme.

2 pt (6) On sait que le centre de S_3 est $\{1\}$, donc $c : S_3 \to \mathrm{Aut}(S_3)$ est injectif, et l'image $\mathrm{Int}(S_3)$ possède 6 éléments. De plus S_3 est engendré par $\tau = (1, 2)$ et $\sigma = (1, 2, 3)$, donc un automorphisme $f : S_3 \to S_3$ est déterminé par $f(\tau)$ et $f(\sigma)$. Or $f(\tau)$ doit être d'ordre 2 donc il y a trois possibilités (trois transpositions dans S_3), $f(\sigma)$ doit être d'ordre 3 donc il y a deux possibilités (deux 3-cycles dans S_3). Finalement il y a $2 \times 3 = 6$ possibilités pour f. Donc $|\mathrm{Aut}(G)| \leq 6$. En conclusion $|\mathrm{Int}(G)| = |\mathrm{Aut}(G)| = 6$.

1.5 pt **Exercice 4** (1) Par définition de l'indice, la partition de G en classes à droite modulo H possède 2 éléments. L'une de ces classes est la classe du neutre H, l'autre est une classe aH, pour un certain $a \in G$.

1.5 pt (2) On commençait par montrer que $aHa^{-1} \cap aH = \emptyset$, ce qui a été bien fait. Comme $G = H \sqcup aH$, il en découle que $aHa^{-1} \subset H$. L'inclusion opposée ne va pas de soi. Cependant, comme $a \notin H$, on a $a^{-1} \in aH$, ou dit autrement, $a^{-1}H = aH$. Donc le même raisonnement que précédemment avec $b = a^{-1}$ montre que $bHb^{-1} \cap bH = \emptyset$ puis $bHb^{-1} \subset H$. Ceci fournit $H \subset aHa^{-1}$.

2 pt (3) Voici une solution qui n'a été proposée par personne. $N_G(H)$ est un sous-groupe de G, qui contient H strictement puisque $a \in N_G(H)$. Donc son indice est strictement inférieur à celui de H, donc c'est 1, i.e. $N_G(H) = G$. Ceci veut dire que $H \lhd G$.

1.5 pt (4) Soit H un sous-groupe de S_n d'indice 2. D'après ce qui précède, c'est un sous-groupe distingué. Il existe donc un groupe quotient S_n/H, qui est un groupe à deux éléments donc isomorphe à $\{\pm 1\}$. On a donc un morphisme surjectif $\nu : S_n \to \{\pm 1\}$. Par théorème, il n'y a qu'un seul tel morphisme, c'est la signature ε, et son noyau est A_n. Donc $H = \ker(\nu) = \ker(\epsilon) = A_n$.