CONTRÔLE CONTINU

CORRECTION

Exercice 1 -

(1) Un groupe est un couple $(G, \times)$ où G est un ensemble et $\times$ est une application de $G \times G$ dans G (l'image d'un couple (g, h) étant notée $g \times h$) tels que
— $(\forall g, h, k \in G) \quad (g \times h) \times k = g \times (h \times k)$,
— $(\exists e \in G)\ (\forall g \in G) \quad g \times e = g = e \times g$,
— $(\forall g \in G)\ (\exists h \in G) \quad g \times h = h \times g = e$.

(2) Un sous groupe de G est un sous-ensemble H de G tel que
— $e \in H$,
— $(\forall g, h \in H) \quad g \times h \in H$,
— $\forall g \in H) \quad g^{-1} \in H$.

(3) Le sous-groupe engendré par A est l'intersection des sous-groupes de G contenant A.

(4) Soit $(H, \times)$ un groupe. Un homomorphisme de groupes de G dans H est une application φ de G dans H telle que

$$(\forall g_1, g_2 \in G) \quad \varphi(g_1 \times g_2) = \varphi(g_1) \times \varphi(g_2)\,.$$

(4) Soit $G = \mathbb{U}_4$. Alors $i, -i \in G$, ils sont d'ordre 4 de G et $i \times i = 1$, c'est un élément d'ordre 1.

Soit $G = \mathbb{U}_4$. Alors $i \in G$, il est d'ordre 4 et $i \times i = -1$, c'est un élément d'ordre 2.

Soit $G = \mathbb{U}_4 \times \mathbb{U}_4$. Alors $(i, 1), (1, i) \in G$, ils sont d'ordre 4 et $(i, 1) \times (1, i) = (i, i)$, c'est un élément d'ordre 4.

Exercice 2 -

(1) D'après la méthode vue en cours pour écrire une permutation comme produit de cycles de longueur au moins 2 et à supports deux-à-deux disjoints on $\sigma = (1\,4\,5)\,(2\,12)\,(3\,6\,11\,8)\,(7\,10\,9)$.

(2) La signature est un homomorphisme de $\mathscr{S}_{12}$ dans $\{-1, 1\}$, sur un cycle de longueur notée ℓ elle prend la valeur $(-1)^{\ell-1}$. Donc

$$\varepsilon(\sigma) = \varepsilon((1\,4\,5))\varepsilon((2\,12))\varepsilon((3\,6\,11\,8))\varepsilon((7\,10\,9)) = (-1)^{2+1+3+2} = 1\,.$$

(3) L'ordre de σ est le ppcm des longueurs des cycles qui apparaissent dans sa décomposition en produit de cycles à supports deux-à-deux disjoints. Donc c'est $\mathrm{ppcm}(3, 2, 4, 3) = 12$.

(4) $\mathscr{A}_{12}$ est l'ensemble des permutations de $\mathscr{S}_{12}$ de signature 1. Donc $\sigma \in \mathscr{A}_{12}$.

(5) Soit $\beta = (1\,7\,3\,9\,5)\,(2\,8\,6)$. Les cycles $(1\,7\,3\,9\,5)$ et $(2\,8\,6)$ commutent parce qu'ils sont à supports disjoints. Donc $\beta^2 = (1\,7\,3\,9\,5)^2\,(2\,8\,6)^2$. Or $(1\,7\,3\,9\,5)^2 = (1\,3\,5\,7\,9)$ et $(2\,8\,6)^2 = (2\,6\,8)$. Donc β répond à la question posée.

Exercice 3 - Soit f l'application de G dans G/H définie par $f(x) = gxH$. Soit $\mathcal{R}$ la relation d'équivalence sur G associée à l'action de H sur G par translation à droite. Donc

$$\begin{array}{rcl}(\forall x, y \in G) \quad x\mathcal{R}y & \Leftrightarrow & (\exists h \in H) \ \ y = xh \\ & \Leftrightarrow & xH = yH\,.\end{array}$$

Soient $x, y \in G$. On suppose que $x\mathcal{R}y$. Donc $xH = yH$. Donc $gxH = gyH$, c'est-à-dire $f(x) = f(y)$. Par passage au quotient par la relation d'équivalence $\mathcal{R}$, il existe donc une application φ_g de G/H ($= G/\mathcal{R}$) dans G/H telle que

$$(\forall x \in G) \ \ \varphi_g(xH) = f(x) = gxH\,.$$

(2) Étant donnés $g \in G$ et $\omega \in G/H$ on note $g \cdot \omega$ pour $\varphi_g(\omega)$.

Soit $\omega \in G/H$. Soient $g_1, g_2 \in G$. Il existe $x \in G$ tel que $\omega = xH$. Alors

— $e \cdot \omega = \varphi_e(\omega) = exH = xH = \omega$,

— $g_1 \cdot (g_2 \cdot \omega) = \varphi_{g_1}(\varphi_{g_2}(\omega)) = \varphi_{g_1}(g_2xH) = g_1g_2xH = \varphi_{g_1g_2}(\omega)$.

Donc l'application de $G \times G/H$ dans G/H définie par $(g, \omega) \mapsto \varphi_g(\omega)$ est bien une action de groupe à gauche.

(3) Soient $\omega_1, \omega_2 \in G/H$. Il existe $x_1, x_2 \in G$ tels que $\omega_1 = x_1H$ et $\omega_2 = x_2H$. On pose $g = x_2x_1^{-1}$. Alors $g \cdot \omega_1 = gx_1H = x_2x_1^{-1}x_1H = x_2H = \omega_2$. Donc l'action est transitive.

(4) Soit $g \in G$. On a (avec les notations utilisées en (1))

$$\begin{array}{rcl}g \in \mathrm{Stab}_G(x) & \Leftrightarrow & gxH = xH \\ & \Leftrightarrow & gx\mathcal{R}x \\ & \Leftrightarrow & (\exists h \in H) \ \ gx = xh \\ & \Leftrightarrow & (\exists h \in H) \ \ g = xhx^{-1} \\ & \Leftrightarrow & g \in xHx^{-1}\,.\end{array}$$

Donc $\mathrm{Stab}_G(x) = xHx^{-1}$.

Exercice 4 - On suppose qu'il existe $g_1, \ldots, g_n \in G$ deux-à-deux distincts tels $G = \langle g_1, \ldots, g_n\rangle$ et que G n'est engendré par aucune partie à $n-1$ éléments.

On note f l'application définie par

$$\begin{array}{rcl}\{0,1\}^n & \to & G \\ (x_1, \ldots, x_n) & \mapsto & g_1^{x_1} \cdots g_n^{x_n}\,.\end{array}$$

On démontre par l'absurde que f est injective. Soient $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \{0,1\}^n$ distincts tels que $g_1^{x_1} \cdots g_n^{x_n} = g_1^{y_1} \cdots g_n^{y_n}$. Il existe donc $i \in \{1, \ldots, n\}$ tel que $x_{i+1} = y_{i+1}, x_{i+2} = y_{i+2}, \ldots, x_n = y_n$. Quitte à échanger les rôles de $(x_1, \ldots, x_n)$ et de $(y_1, \ldots, y_n)$ on peut supposer que $y_i = 1$ et $x_i = 0$. Par simplification à droite, on a $g_1^{x_1} \cdots g_{i-1}^{x_{i-1}} = g_1^{y_1} \cdots g_{i-1}^{y_{i-1}} g_i$. Donc $g_i = \left(g_1^{y_1} \cdots g_{i-1}^{y_{i-1}}\right)^{-1} g_1^{x_1} \cdots g_{i-1}^{x_{i-1}}$. Ainsi $g_i \in \langle g_1, \ldots, g_{i-1}\rangle$. Donc G est engendré par les $n-1$ éléments $g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n$. C'est absurde. Donc f est injective. Donc $\mathrm{Card}(G) \geqslant \mathrm{Card}(\{0,1\}^n) = 2^n$.

Exercice 5 - On pose $H = \mathrm{Ker}(\varphi)$. Comme $\varphi(K) \subseteq \mathrm{Im}(\varphi)$ et comme φ est un homomorphisme, on a

$$\begin{array}{rcl}\mathrm{Im}(\varphi) = \varphi(K) & \Leftrightarrow & (\forall g \in G)\ (\exists k \in K) \ \ \varphi(g) = \varphi(k) \\ & \Leftrightarrow & (\forall g \in G)\ (\exists k \in K) \ \ \varphi(gk^{-1}) = e \\ & \Leftrightarrow & (\forall g \in G)\ (\exists k \in K) \ \ gk^{-1} \in \mathrm{Ker}(\varphi) \\ & \Leftrightarrow & (\forall g \in G)\ (\exists k \in K)\ (\exists h \in \mathrm{Ker}(\varphi)) \ \ g = hk \\ & \Leftrightarrow & G = HK\,.\end{array}$$

Pour conclure il suffit de démontrer que $\langle H \cup K\rangle = HK$. Pour cela on démontre successivement que $HK \subseteq \langle H \cup K\rangle$ et que $\langle H \cup K\rangle \subseteq HK$.

Comme $\langle H \cup K\rangle$ est un sous-groupe de G contenant $H \cup K$, il contient tout élément de le forme hk où $h \in H$ et $k \in K$. Donc $HK \subseteq \langle H \cup K\rangle$.

Comme $\langle H \cup K\rangle$ est le plus petit sous-groupe de G contenant $H \cup K$, il suffit de démontrer que HK est un sous-groupe de G contenant $H \cup K$ pour démontrer que $\langle H \cup K\rangle \subseteq HK$. Or

— si $h \in H$ alors $h = he \in HK$ car $e \in K$, de sorte que $H \subseteq HK$,

— si $k \in K$ alors $k = ek \in HK$ car $e \in H$, de sorte que $K \subseteq HK$.

Donc $H \cup K \subseteq HK$. Par ailleurs

— $e \in H$ et $e \in K$ donc $e = ee \in HK$,

— si $h, h' \in H$ et $k, k' \in K$ alors $(hk)(h'k') \in HK$; en effet

$$(hk)(h'k') = (hkh'k^{-1})(kk')\,;$$

ici $kk' \in K$ parce que K est un sous-groupe de G ; de plus

$$\varphi(kh'k^{-1}) = \varphi(k)\varphi(h')\varphi(k)^{-1} = \varphi(k)e\varphi(k)^{-1} = e$$

en utilisant que φ est un homomorphisme de groupes et que $h' \in \mathrm{Ker}(\varphi)$; donc $kh'k^{-1} \in H$ puis $hkh'k^{-1} \in H$ (parce que H est un sous-groupe de G),

— si $h \in H$ et $k \in K$ alors $(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1}$. Or, suivant les arguments donnés au point précédent, on a $\varphi(k^{-1}h^{-1}k) = e$ de sorte que $k^{-1}h^{-1}k \in H$. Donc $(hk)^{-1} \in HK$.

Donc HK est bien un sous-groupe de G contenant $H \cup K$. Donc $HK = \langle H \cup K\rangle$.

Ainsi $HK = \langle H \cup K\rangle$ de sorte que $\varphi(K) = \mathrm{Im}(\varphi)$ si et seulement si $G = \langle H \cup K\rangle$.

Exercice 6 -

(1) Soit d l'ordre de g. Donc $d = \langle g\rangle$. On a $d|6$ (théorème de Lagrange). Donc $d \in \{1, 2, 3, 6\}$. Comme $\langle g\rangle$ est un sous-groupe commutatif de G, on déduit que $\langle g\rangle \subsetneq G$. Donc $d < 6$. Donc $d \in \{1, 2, 3\}$.

(2) Par l'absurde on suppose que : $(\forall g \in G)\ g^2 = e$. Donc tout élément de G est égal à son inverse. Soient $g, h \in G$. Alors $hg = h^{-1}g^{-1} = (gh)^{-1} = gh$. C'est absurde parce que G n'est pas commutatif. Donc il existe $g \in G$ tel que $g^2 \neq e$.

(3) Le sous-groupe $\langle \rho\rangle$ est d'ordre 3 car ρ est d'ordre 3. Donc tout élément de ce sous-groupe est d'ordre 1 ou 3 (théorème de Lagrange). Seul e est d'ordre 1. Donc $\langle \rho\rangle$ contient deux éléments d'ordre 3.

On note $\mathcal{S}$ l'ensemble des sous-groupes de G de la forme $\langle g\rangle$ pour $g \in G$ d'ordre 3. Vu que tout tel sous-groupe est engendré par n'importe lequel de ses éléments d'ordre 3 (d'après le théorème de Lagrange), deux tels sous-groupes n'ont un élément d'ordre 3 en commun que si ils sont égaux. On a donc une partition

$$\{g \in G \mid g \text{ est d'ordre } 3\} = \coprod_{S \in \mathcal{S}} \{g \in S \mid g \text{ est d'ordre } 3\}$$

où chaque sous-ensemble contient deux éléments. Donc le nombre d'éléments d'ordre 3 de G est pair.

(4) Les éléments d'ordre 3 forment avec e un sous-ensemble de G de cardinal impair. Donc ce sous-ensemble ne peut être G. Ceci et (1) implique qu'il existe un élément d'ordre 2 dans G.

(5) Par l'absurde on suppose que X n'a qu'un seul élément τ. On vérifie d'abord que $\rho\tau\rho^{-1}$ est d'ordre 2 : $\rho\tau\rho^{-1} \neq e$ car $\tau \neq e$, et $(\rho\tau\rho^{-1})^2 = \rho\tau^2\rho^{-1} == \rho e\rho^{-1} = e$. Donc $\rho\tau\rho^{-1} = \tau$. Donc $\rho\tau = \tau\rho$. Or, on peut constater que $\rho\tau$ n'est pas d'ordre 1, 2 ou 3 :

- ρ est d'ordre 3 et $\tau = \tau^{-1}$ est d'ordre 2, donc $\rho \neq \tau^{-1}$, donc $\rho\tau \neq e$,
- $\rho \neq e$ donc $\rho\tau \neq \tau$, donc $\rho\tau \notin X$, donc $\rho\tau$ n'est pas d'ordre 2,
- $(\rho\tau)^3 = \rho^3\tau^3$ car $\rho\tau = \tau\rho$, donc $(\rho\tau)^3 = \tau$ parce que $\tau^2 = \rho^3 = e$, donc $\rho\tau$ n'est pas d'ordre 3.

Ceci est en contradiction avec (1). Donc $\mathrm{Card}(X) \geqslant 2$.

(6) La vérification faite en (5) démontre que pour tout $\tau \in X$ et pour tout $g \in G$, l'ordre de $g\tau g^{-1}$ est 2 de sorte que $g\tau g^{-1} \in X$. Autrement dit, la restriction à $G \times X$ de l'application $G \times G \to G$ de l'action de G sur lui-même par conjugaison est à valeurs dans X. L'application $G \times X \to X$ qui en résulte (donc définie par $(g,\tau) \mapsto g\tau g^{-1}$) vérifie les axiomes des actions de groupes parce que l'application $G \times G \to G$ à partir de laquelle elle est définie par restriction à la source et au but les vérifie.

(7) On a $\varphi(g)(x) = gxg^{-1}$.

(8) On a $\mathrm{Stab}_G(\tau) = \{g \in G \mid g\tau g^{-1} = \tau\}$. C'est un sous-groupe de G qui contient un sous-groupe d'ordre 2, à savoir $\langle\tau\rangle$. Si on applique le théorème de Lagrange aux inclusions $\langle\tau\rangle \subseteq \mathrm{Stab}_G(\tau)$ et $\mathrm{Stab}_G(\tau) \subseteq G$ on déduit que $\mathrm{Stab}_G(\tau)$ est d'ordre 2 ou 6. Les arguments présentés en (5) démontrent que $\mathrm{Stab}_G(\tau)$ ne contient pas d'élément d'ordre 3. Donc $\mathrm{Stab}_G(\tau) \neq G$. Donc $\mathrm{Stab}_G(\tau)$ est d'ordre 2. Donc $\mathrm{Stab}_G(\tau) = \langle\tau\rangle$.

(9) Soit $g \in G$. On a

$$\begin{array}{rcl} g \in \mathrm{Ker}(\varphi) & \Leftrightarrow & (\forall \tau \in X) \;\; \varphi_g(\tau) = \tau \\ & \Leftrightarrow & g \in \bigcap_{\tau \in X} \mathrm{Stab}_G(\tau) \\ & \Leftrightarrow & g \in \bigcap_{\tau \in X} \{e, \tau\}\,. \end{array}$$

Comme $\bigcap_{\tau \in X}\{e,\tau\} = \{e\}$, on déduit que φ est injectif.

(10) Ainsi, $\mathrm{Im}(\varphi)$ est un sous-groupe de $\mathscr{S}_3$, et l'application de G dans $\mathrm{Im}(\varphi)$ définie par $g \mapsto \varphi(g)$ est un homomorphisme de groupes qui est injectif (voir (9)) et surjectif par construction. Donc G est isomorphe à un sous-groupe d'ordre 6 de $\mathscr{S}_3$. Comme $\mathscr{S}_3$ est d'ordre 6 on déduit que G et $\mathscr{S}_3$ sont isomorphes.