THÉORIE DES GROUPES
L3 MATHÉMATIQUES
CORRIGÉ DE L'EXAMEN DU 17 JANVIER 2020

PAUL LESCOT

Exercice I

(1) Supposons $m_p(G) \neq 0$; alors il existe un élément x de G tel que $\omega(x) = p$. Mais alors $p = \omega(x)$ divise $|G| = n$.

Par contraposition, on en déduit que, si p ne divise pas n, alors

$$m_p(G) = 0,$$

ce qui est la conclusion demandée.

(2) Vu que $1 \leq k < p$, p ne divise pas k, donc $pgcd(p,k) \neq p$. Mais $pgcd(p,k)$ divise p, donc $pgcd(p,k) = 1$ ou $pgcd(p,k) = p$. On a donc $pgcd(p,k) = 1$, d'où

$$\omega(x^k) = \frac{\omega(x)}{pgcd(\omega(x),k)} = \frac{p}{pgcd(p,k)} = \frac{p}{1} = p.$$

(3) Si $x \in G$ est d'ordre p, le sous–groupe $< x >$ de G engendré par x est égal à

$$\{e, x, ..., x^{p-1}\}.$$

D'aprs (2), chaque élément de $C \setminus \{e\}$ est d'ordre p.

Si C et $C^{'}$ sont deux sous–groupes distincts de G engendrés par un élément d'ordre p, $C \cap C^{'}$ est un sous–groupe strict de C ; son ordre divise donc $|C| = p$ et en est distinct, d'où $|C \cap C^{'}| = 1$ et $C \cap C^{'} = \{e\}$; $C \setminus \{e\}$ et $C^{'} \setminus \{e\}$ sont donc disjoints.

Soient C_1,...,C_r les sous–groupes distincts de G engendrés par un élément d'ordre p ; si x est d'ordre p, x appartient à l'un des $(C_i \setminus \{e\})_{1 \leq i \leq r}$ (car $x \in < x > \setminus \{e\}$) et un seul (car les $(C_i \setminus \{e\})_{1 \leq i \leq r}$ sont deux à deux disjoints). L'ensemble des éléments d'ordre p est donc la réunion disjointe des $(C_i \setminus \{e\})_{1 \leq i \leq r}$, d'où

$$m_p(G) = |\bigcup_{i=1}^{r}(C_i \setminus \{e\})| = \sum_{i=1}^{r}|C_i \setminus \{e\}| = \sum_{i=1}^{r}(p-1) = r(p-1).$$

En particulier, $p-1$ divise $m_p(G)$.

Exercice II

Notons $E = \{1,2,3,4,5\}$.

(1) Il suffit de démontrer que les deux éléments considérés ont le même effet sur chaque $j \in \{1, ..., 5\}$. Si $j \in \{4,5\}$ on a

$$(\tilde{\sigma_1} \circ \tilde{\sigma_2})(j) = \tilde{\sigma_1}(\tilde{\sigma_2}(j)) = \tilde{\sigma_1}(j) = j = \widetilde{\sigma_1 \circ \sigma_2}(j).$$

Si $j \in \{1,2,3\}$, $\tilde{\sigma_2}(j) = \sigma_2(j) \in \{1,2,3\}$ d'où

$$\begin{aligned}(\tilde{\sigma_1} \circ \tilde{\sigma_2})(j) &= \tilde{\sigma_1}(\tilde{\sigma_2}(j)) \\ &= \tilde{\sigma_1}(\sigma_2(j)) \\ &= \sigma_1(\sigma_2(j)) \\ &= (\sigma_1 \circ \sigma_2)(j) \\ &= \widetilde{\sigma_1 \circ \sigma_2}(j).\end{aligned}$$

(2) Supposons $(k,l) \in \mathbf{Z}^2$ et $\bar{k} = \bar{l}$; alors $k - l \in 2\mathbf{Z}$: $k - l = 2u$ pour un $u \in \mathbf{Z}$. Mais alors

$$(45)^k((45)^l)^{-1} = (45)^{k-l} = (45)^{2u} = ((45)^2)^u = (Id_E)^u = Id_E$$

d'où

$$(45)^k = (45)^l$$

et

$$\tilde{\sigma} \circ (45)^k = \tilde{\sigma} \circ (45)^l :$$

ψ est bien défini.

(3) On a, pour tout $(k,l,\sigma,\sigma^{'}) \in \dfrac{\mathbf{Z}}{2\mathbf{Z}} \times \dfrac{\mathbf{Z}}{2\mathbf{Z}} \times \Sigma_3 \times \Sigma_3$:

$$\begin{aligned}\psi((\sigma,\bar{k}),(\sigma^{'},\bar{l})) &= \psi(\sigma \circ \sigma^{'}, \bar{k} + \bar{l}) \\ &= \psi(\sigma \circ \sigma^{'}, \overline{k+l}) \\ &= (\sigma \circ \sigma^{'}) \circ (45)^{k+l} \\ &= \sigma \circ \sigma^{'} \circ (45)^k \circ (45)^l.\end{aligned}$$

Mais les permutations $\sigma^{'}$ et $(45)^k$ sont à supports disjoints, car le support de la première est contenu dans $\{1,2,3\}$ et celui de la seconde dans $\{4,5\}$; on a donc

$$\begin{aligned}\psi((\sigma,\bar{k}),(\sigma^{'},\bar{l})) &= \sigma \circ \sigma^{'} \circ (45)^k \circ (45)^l \\ &= \sigma \circ (45)^k \circ \sigma^{'} \circ (45)^l \\ &= \psi(\sigma,\bar{k})\psi(\sigma^{'},\bar{l}).\end{aligned}$$

(4) Soit $(\sigma,\bar{k}) \in \ker(\psi)$; alors $\psi(\sigma,\bar{k}) = Id_E$ soit $\tilde{\sigma} \circ (45)^k = Id_E$, et $(45)^k = \tilde{\sigma}^{-1}$.

Mais alors $(45)^k$ laisse fixes 4 et 5, donc k est pair (sans quoi on aurait $(45)^k = (45)$). On a donc $\bar{k} = \bar{0} = 0_{\frac{\mathbf{Z}}{2\mathbf{Z}}}$. Il en résulte que $(45)^k = Id_E$, d'où $\tilde{\sigma}^{-1} = Id_E$ et $\tilde{\sigma} = Id_E$. Mais alors $\sigma = \tilde{\sigma}|_{\{1,2,3\}} = Id_{\{1,2,3\}}$. On a donc

$$(\sigma,\bar{k}) = (Id_{\{1,2,3\}}, 0_{\frac{\mathbf{Z}}{2\mathbf{Z}}}) = e_{\Sigma_3 \times \frac{\mathbf{Z}}{2\mathbf{Z}}}$$

et

$$\ker(\psi) = \{e_{\Sigma_3 \times \frac{\mathbf{Z}}{2\mathbf{Z}}}\}.$$

(5) On a, d'après le Théorème d'Isomorphisme

$$\mathrm{Im}(\psi) \simeq \frac{\Sigma_3 \times \dfrac{\mathbf{Z}}{2\mathbf{Z}}}{\ker(\psi)} = \frac{\Sigma_3 \times \dfrac{\mathbf{Z}}{2\mathbf{Z}}}{\{e_{\Sigma_3 \times \frac{\mathbf{Z}}{2\mathbf{Z}}}\}} \simeq \Sigma_3 \times \frac{\mathbf{Z}}{2\mathbf{Z}}.$$

Σ_5 contient donc un sous–groupe isomorphe à $\Sigma_3 \times \dfrac{\mathbf{Z}}{2\mathbf{Z}}$, donc à $D_6 \times \dfrac{\mathbf{Z}}{2\mathbf{Z}}$ (car $\Sigma_3 \simeq D_6$). Mais, en vertu d'un résultat du cours, pour m impair, $D_{2m} \times \dfrac{\mathbf{Z}}{2\mathbf{Z}}$ est isomorphe à D_{4m}. Prenant $m = 3$, il apparaît que le sous–groupe en question est isomorphe à D_{12}.

Exercice III

(1) Par définition, chaque élément $x \in H$ est de la forme

$$x = \lambda_1 g_1 + ... + \lambda_n g_n$$

avec $n \in \mathbf{N}$ et $\lambda_i \in \mathbf{Z}$. Chaque g_i est rationnel, et peut donc être exprimé comme

$$g_i = \frac{a_i}{b_i}$$

avec a_i et b_i entiers et $b_i \geq 1$. Soit $N = b_1...b_n$; alors, pour chaque i, $\dfrac{N}{b_i} = \displaystyle\prod_{j=1;j\neq i}^{n} b_j$ est entier ; donc, pour tout $x \in H$,

$$Nx = N\sum_{i=1}^{n} \lambda_i g_i = N\sum_{i=1}^{n} \lambda_i \frac{a_i}{b_i} = \sum_{i=1}^{n} \lambda_i a_i \frac{N}{b_i} \in \mathbf{Z}.$$

(2) $\dfrac{0}{N} = 0 \in H$, car H est un sous–groupe de $\mathbf{Q}$, donc $0 \in I$.

Soit $(x, y) \in I^2$; alors

$$\frac{x-y}{N} = \frac{x}{N} - \frac{y}{N} \in H$$

car $x \in I$ et $y \in I$, d'où $\dfrac{x}{N} \in H$ et $\dfrac{y}{N} \in H$; on a donc $x - y \in I$.

I est donc bien un sous-groupe de $\mathbf{Z}$.

(3) D'après un théorème du cours, il existe $a \in \mathbf{N}$ tel que $I = a\mathbf{Z}$. On a donc $a = a.1 \in a\mathbf{Z} \in I$, donc $u := \dfrac{a}{N} \in H$. Alors, pour chaque $\lambda \in \mathbf{Z}$, $\lambda u \in H$.

Réciproquement, soit $h \in H$; alors $Nh \in \mathbf{Z}$ (d'près (1)) et $\dfrac{Nh}{N} = h \in H$, donc $Nh \in I = a\mathbf{Z}$; il existe donc $\lambda \in \mathbf{Z}$ tel que $Nh = \lambda a$. Il en résulte que $h = \lambda \dfrac{a}{N} = \lambda u$.

On a donc

$$H = \{\lambda u | \lambda \in \mathbf{Z}\} =< u >:$$

H est monogène.

(4) Soit $g \in G$; alors il existe $x \in \mathbf{Q}$ tel que $g = p(x)$. On peut alors écrire $x = \dfrac{a}{b}$ avec a et b entiers et $b \geq 1$. Alors

$$\begin{aligned} bx &= bp(g) \\ &= p(bg) \\ &= p(a) \\ &= 0_{\frac{\mathbf{Q}}{\mathbf{Z}}} \\ &\quad (\text{car } a \in \mathbf{Z} = \ker(p)) \\ &= 0_G; \end{aligned}$$

g est donc d'ordre fini diviseur de b.

(5) Par hypothèse J est engendré par une famille finie $(j_1, ..., j_n)$ d'éléments de J. Pour chaque i, il existe $h_i \in H$ tel que $j_i = p(h_i)$; soit H le sous–groupe de $\mathbf{Q}$ engendré par $h_1, ..., h_n$.

Pour chaque $i \in \{1, ..., n\}$ on a $h_i \in H$, donc $j_i = p(h_i) \in p(H)$ et

$$J =< j_1, ..., j_n > \subset p(H).$$

Réciproquement, soit $h \in H$; vu que H est engendré par $h_1, ..., h_n$, on peut exprimer h sous la forme

$$h = \sum_{i=1}^{n} \lambda_i h_i$$

avec $(\lambda_1, ..., \lambda_n) \in \mathbf{Z}^n$, d'où

$$p(h) = p(\sum_{i=1}^{n} \lambda_i h_i) = \sum_{i=1}^{n} \lambda_i p(h_i) = \sum_{i=1}^{n} \lambda_i j_i \in J.$$

On a donc $p(H) \subset J$, d'où $p(H) = J$.

(6) D'après (5), H est monogène : il existe $u \in \mathbf{Q}$ tel que $H =< u >$. Mais alors

$$\begin{aligned} J &= p(H) \\ &= p(< u >) \\ &= \{p(y) | y \in < u >\} \\ &= \{p(\lambda u) | \lambda \in \mathbf{Z}\} \\ &= \{\lambda p(u) | \lambda \in \mathbf{Z}\} \\ &= < p(u) > . \end{aligned}$$

J est donc engendré par $p(u)$, donc monogène ; du fait que $p(u)$ est d'ordre fini d'après (4), J est fini.