L3 MATHÉMATIQUES, 2020–2021
THÉORIE DES GROUPES
CORRIGÉ DE L'EXAMEN DU 06 JANVIER 2021

PAUL LESCOT

Exercice I

(1) Soit $\sigma = (a_1...a_l)$; par définition $\sigma(a_i) = a_{i+1}$ (les indices étant considérés modulo l) et $\sigma(x) = x$ pour $x \notin \{a_1, ..., a_l\}$.

Alors, pour $x \notin \{a_1, ..., a_l\}$, $\sigma^{'}(x) = \sigma^2(x) = \sigma(\sigma(x)) = \sigma(x) = x$. De plus, pour chaque i, $\sigma^{'}(a_i) = \sigma(\sigma(a_i)) = \sigma(a_{i+1}) = a_{i+2}$. Distinguons donc trois cas :

Cas 1 : l est impair($l = 2k + 1, k \geq 1$)

Alors $\sigma^{'}(a_1) = a_3$, $\sigma^{'}(a_2) = a_4$,..., $\sigma^{'}(a_{2k-1}) = a_{2k+1} = a_l$, $\sigma^{'}(a_l) = \sigma(\sigma(a_l)) = \sigma(a_1) = a_2$, $\sigma^{'}(a_2) = a_4$,..., $\sigma^{'}(a_{2k}) = \sigma(a_{2k+1}) = \sigma(a_l) = a_1$.

$\sigma^{'} = (a_1a_3...a_{2k-1}a_{2k+1}a_2...a_{2k})$ est donc un cycle de longueur l.

Cas 2 : $l = 2$

Alors $\sigma^{'} = \sigma^2 = Id$.

Cas 3 : $l \geq 4$ est pair($l = 2k, k \geq 2$)

Alors $\sigma^{'}(a_1) = a_3$, $\sigma^{'}(a_2) = a_4$,..., $\sigma^{'}(a_{2k-1}) = \sigma(a_{2k}) = a_1$, $\sigma^{'}(a_{2k}) = \sigma(\sigma(a_{2k})) = \sigma(a_1) = a_2$.

On voit que $\sigma^{'} = (a_1a_3...a_{2k-1})(a_2a_4...a_{2k})$ est le produit de deux cycles disjoints de longueur $k = \frac{l}{2}$.

(2) Décomposons σ en cycles à supports disjoints :

$$\sigma = \sigma_1...\sigma_k,$$

et notons l_i la longueur de σ_i. Les σ_i commutent deux à deux, donc

$$\sigma^2 = (\sigma_1...\sigma_k)^2 = \sigma_1^2...\sigma_k^2.$$

Il est clair que

$$\begin{aligned} supp(\sigma_i^2) &= \{x \in \{1, ..., n\} | \sigma_i^2(x) \neq x\} \\ &= \{x \in \{1, ..., n\} | \sigma_i(\sigma_i(x)) \neq x\} \\ &\subset \{x \in \{1, ..., n\} | \sigma_i(x) \neq x\} \\ &= supp(\sigma_i). \end{aligned}$$

Les σ_i^2 sont donc à supports deux à deux disjoints. D'après (1), σ_i^2 est égal à Id si $l_i = 2$, à un cycle de longueur l_i si l_i est impair et au produit de deux cycles de longueur $\frac{l_i}{2}$ si l_i est pair. On obtient ainsi la décomposition en cycles de $\sigma^{'}$ en recollant celles des σ_i^2.

On voit ainsi qu'un cycle de longueur paire $2k$ dans la décomposition de $\sigma^{'}$ en cycles disjoints ne peut que provenir d'un cycle de longueur $4k$ dans l'un des σ_i. Mais alors un autre cycle de même longueur $2k$ est apparu dans σ_i^2, donc dans $\sigma^{'}$. D'où le résultat.

(3) Il suffit de suivre à l'envers le raisonnement de (2). En gros, chaque cycle de longueur impaire est le carré d'un cycle de longueur impaire et le produit de deux cycles de même longueur paire est le carré d'un cycle de longueur double.

Plus précisément, $\sigma^{'} = \sigma_1...\sigma_k$ une décomposition en cycles à supports disjoints, dans laquelle σ_1 et σ_2 sont de même longueur paire l_1, σ_3 et σ_4 sont de même longueur paire l_2, ..., σ_{2u-1} et σ_{2u} sont de même longueur paire l_u, et chaque σ_j pour $2u+1 \leq j \leq v$ est de longueur impaire l_j.

Ecrivons, pour $1 \leq i \leq u$,

$$\sigma_{2i-1} = (a_1...a_{l_i})$$

et

$$\sigma_{2i} = (b_1...b_{l_i}),$$

et posons $\rho_i = (a_1 b_1 a_2 b_2 ... a_{l_i} b_{l_i})$; alors le calcul de (2) montre que $\rho_i^2 = \sigma_i$.

Si $2u+1 \leq i \leq v$, l_i est impaire ($l_i = 2k_i + 1$).

Soit ρ_i défini par $\rho_i(a_l) := (a_l a_{l+k_i+1})$ (les indices étant pris modulo l_i). Alors ρ_i est un cycle de longueur l_i et $\rho_i^2 = \sigma_{2i-1}\sigma_{2i}$.

Par construction les ρ_i sont à supports deux à deux disjoints (car ceux des σ_i le sont) ; ils commutent donc et

$$(\rho_1..\rho_u\rho_{2u+1}...\rho_v)^2 = \rho_1^2...\rho_u^2\rho_{2u+1}^2...\rho_v^2 = \sigma_1\sigma_2...\sigma_{2u-1}\sigma_{2u}\sigma_{2u+1}...\sigma_v = \sigma^{'}$$

et $\sigma^{'}$ est un carré.

(4) D'après (2) et (3), un élément de Σ_5 est un carré si et seulement si, dans sa décomposition en produits de cycles disjoints, le nombre de cycles de longueur 2 et le nombre de cycles de longueur 4 sont pairs. Mais il ne saurait exister deux cycles disjoints de longueur 4 car $4+4 = 8 > 5$; le nombre de cycles de longueur 4 doit être nul. Le nombre de cycles de longueur 2 doit, lui, être égal à 0 ou 2.

Les carrés de Σ_5 sont donc les permutations ayant l'une de ces formes :

$$(abcde)$$

$$(abc)$$

$$(ab)(cd)$$

$$Id.$$

Il y en a donc $24 + 10.2 + 5.3 + 1 = 60$.

Exercice II

(1) Soient $g \in G$ et $h \in A_k$; alors $h = (x^k)^m = x^{km}$ pour un m entier. Si $g \in < x >$, $g = x^r$ pour un $r \in \mathbf{Z}$ et $ghg^{-1} = x^r x^{km}(x^r)^{-1} = x^{km} = h \in H$. Si $g \in t < x >$, $g = tx^s$ pour un $s \in \mathbf{Z}$ et

$$ghg^{-1} = tx^s x^{km} x^{-s} t^{-1} = tx^{km}t^{-1} = (txt^{-1})^{km} = (x^{-1})^{km} = x^{-km} = (x^k)^{-m} \in A_k.$$

Donc, dans tous les cas, $ghg^{-1} \in A_k$: $A_k \triangleleft G$.

Pour $g \in G$, notons $\bar{g}$ sa classe modulo A_k. Alors $\bar{x}^l = \bar{e_G}$ si et seulement si $\bar{x}^l = \overline{e_G}$, soit $x^l \in A_k =< x^k >$; cela veut dire qu'existe $m \in \mathbf{Z}$ tel que $x^l = x^k)^m$, ou $x^l = x^{km}$, soit $x^{l-km} = e_G$, ou n divise $l - km$. Cela entraîne que k divise $l - km$, soit $k \mid l$.

Réciproquement, $\bar{x}^k = \bar{x^k} = \overline{e_G}$ car $x^k \in A_k$. Nous venons de montrer que $\bar{x}$ est d'ordre k.

On a $(\bar{y})^2 = \overline{y^2} = \overline{e_G} = e_{\frac{G}{A_k}}$, donc $\bar{y}$ est d'ordre 1 ou 2. Mais il ne peut pas être d'ordre 1 car on aurait alors $y \in A_k =< x^k > \subset < x >$, d'où $y \in < x >$, une contradiction.

De plus $\bar{y}^{-1}\bar{x}\bar{y} = \overline{y^{-1}xy} = \overline{x^{-1}} = (\bar{x})^{-1}$. Vu que $G =< x, y >$, on a $\dfrac{G}{A_k} =< \bar{x}, \bar{y} > \simeq D_{2k}$.

(2) $B_{k,l}$ est engendré par $u := x^k$ et $v := yx^l$. Du fait que k divise $n = \omega(x)$, on a $\omega(x^k) = \dfrac{\omega(x)}{k} = \dfrac{n}{k}$. Comme vu en cours, v est d'ordre 2 ; en outre $vuv^{-1} = yx^l x^k x^{-l} y^{-1} = yx^k y^{-1} = (yxy^{-1})^k = (x^{-1})^k = x^{-k} = (x^k)^{-1} = u^{-1}$.

On a donc bien $G =< u, v > \simeq D_{2\frac{n}{k}}$.

(3) $< x >$ est d'ordre n, donc $\dfrac{G}{< x >}$ est d'ordre $\dfrac{2n}{n} = 2$. Mais $H < x >$ est un sous–groupe de G (car $< x > \triangleleft G$), donc $\dfrac{H < x >}{< x >}$ est un sous–groupe de $\dfrac{G}{< x >}$. Donc soit

$$\frac{H < x >}{< x >}$$

est d'ordre 1, c'est–à–dire que $H < x > \subset < x >$ et $H \subset < x >$, soit

$$\frac{H < x >}{< x >} = \frac{G}{< x >}.$$

Dans ce dernier cas,

$$[H : H \cap < x >]| = |\frac{H}{H \cap < x >}| = |\frac{H < x >}{< x >}| = |\frac{G}{< x >}| = 2.$$

Comme vu en cours, H, sous–groupe du groupe monogène $< x >$, est lui-même monogène ; soit d son ordre, et soit $k := \dfrac{n}{d}$ (d divise n). On a vu que $< x^k >$ était l'unique sous–groupe de $< x >$ d'ordre $\frac{n}{k} = d$, d'où $H =< x^k >= A_k$.

(4) Appliquant le résultat de (4) à $H \cap < x >$, on obtient que $H \cap < x >= A_k =< x^k >$ pour un diviseur k de n. Alors $|H| = 2|H \cap < x > | = 2\frac{n}{k}$.

Soit $u \in H$, $u \notin < x >$; alors $u = yx^m$ pour un $m \in \mathbf{Z}$. Divisons m par k ; on obtient $m = kq + l$ avec $0 \leq l \leq k-1$. Alors $yx^l = yx^{m-kq} = yx^m(x^k)^{-q} = u(x^k)^{-q} \in H$ et

$$B_{k,l} =< x^k, yx^l > \subset H$$

Mais $B_{k,l}$ est d'ordre $2\frac{n}{k} = |H|$, d'où en effet $H = B_{k,l}$.

Remarque 0.1. Des arguments du même type permettent de déterminer les sous–groupes du groupe diédral infini D_∞.

Remarque 0.2. Il est facile de voir que les A_k et les $B_{k,l}$ sont deux à deux distincts ; le nombre de sous–groupes de D_{2n} est donc $\sigma(n) + d(n)$.

Exercice III

(1) S est cyclique, engendré par un élément x d'ordre p. Un morphisme $\alpha : S \to S$ doit vérifier

$$\alpha(x^k) = (\alpha(x))^k \ (*)$$

pour chaque $k \in \mathbf{Z}$; réciproquement, pour chaque choix de $\alpha(x) \in S$, la formule $(*)$ définit un morphisme de S dans S.

Ce morphisme est bijectif si et seulement s'il est injectif, c'est–à–dire si $\alpha(x^k) = e_S$ entraîne

$$x^k = e_S,$$

en d'autres termes que $(\alpha(x))^k = e_S$ entraıne $p \mid k$.

Cela revient à dire que $\alpha(x)$ est d'ordre divisible par p, c'est–à–dire d'ordre p. Mais les éléments d'ordre p de S sont exactement les éléments différents de e_G ; il y en a donc $p-1$, d'où le résultat.

(2) On a

$$539 = 49.11 = 7^2.11$$

Le nombre n_7 de 7–sous–groupes de Sylow de G divise 11 (donc vaut 1 ou 11), et il est congru à 1 modulo 7 ; il vaut donc 1. Il existe donc un unique 7–sous–groupe de Sylow T de G.

De même le nombre n_{11} de 11–sous–groupes de Sylow de G divise 7 (donc vaut 1, 7 ou 7^2), et il est congru à 1 modulo 11 ; il vaut donc 1. Il existe donc un unique 11–sous–groupe de Sylow S de G.

(3) Du fait que $S \lhd G$, on a bien $\theta(t)(s) = tst^{-1} \in S$. $\theta(t)$ est donc une application de S dans S ; elle est injective et un morphisme car il s'agit de la restriction à T de l'automorphisme intérieur $i(t)$ de G associé à t. Etant un morphisme injectif de S dans S, elle est bijective et $\theta(t) \in Aut(S)$: θ est bien défini.

Soit $(t, t') \in T^2$ et $s \in S$; on a

$$\begin{aligned}
(\theta(t) \circ \theta(t'))(s) &= \theta(t)(\theta(t')(s)) \\
&= \theta(t)(t's(t')^{-1}) \\
&= t(t's(t')^{-1})t^{-1} \\
&= tt's(tt')^{-1} \\
&= \theta(tt')(s).
\end{aligned}$$

Cela vaut pour tout $s \in S$; on a donc

$$\theta(t) \circ \theta(t^{'}) = \theta(tt^{'}) :$$

$\theta : T \to Aut(S)$ est un morphisme.

(4) $\mathrm{Im}(\theta)$ est un sous–groupe de $Aut(S)$, lequel est d'ordre 10 d'après (1). Mais

$$\mathrm{Im}(\theta) \simeq \frac{T}{\ker(\theta)}$$

donc

$$|\,\mathrm{Im}(\theta)| = |\frac{T}{\ker(\theta)}| = \frac{|T|}{|\ker(\theta)|}$$

divise $|T| = 49$. Or 10 et 49 sont premiers entre eux, donc $|\,\mathrm{Im}(\theta)| = 1$: $|\,\mathrm{Im}(\theta)| = \{Id_S\}$.

Vu que $\theta(t) \in \mathrm{Im}(\theta)$, $\theta(t) = Id_S$.

(5) Pour chaque $s \in S$ et chaque $t \in T$, $tst^{-1} = \theta(t)(s) = Id_S(s) = s$ d'après (4) : $st = ts$.

Il est alors facile de voir que l'application

$$\begin{array}{rcl} \psi & : & S \times T \to G \\ & & (s,t) \mapsto st. \end{array}$$

est un morphisme, injectif car $S \cap T = \{e_G\}$. Mais

$$|S \times T| = |S||T| = 11.49 = 539 = |G| :$$

et

$$G \simeq S \times T.$$

(6) S est abélien car d'ordre premier, et T est abélien car d'ordre le carré d'un nombre premier, donc $G \simeq S \times T$ est abélien.

(7) On a $S \simeq \dfrac{\mathbf{Z}}{11\mathbf{Z}}$; vu que $|T| = 7^2$ et que 7 est premier, T est isomorphe soit à $\dfrac{\mathbf{Z}}{49\mathbf{Z}}$ soit à $\dfrac{\mathbf{Z}}{7\mathbf{Z}} \times \dfrac{\mathbf{Z}}{7\mathbf{Z}}$.

Dans le premier cas

$$G \simeq S \times T \simeq \frac{\mathbf{Z}}{11\mathbf{Z}} \times \frac{\mathbf{Z}}{49\mathbf{Z}} \simeq \frac{\mathbf{Z}}{539\mathbf{Z}}$$

car 11 et 49 sont premiers entre eux.

Dans le second cas,

$$\begin{array}{rcl} G & \simeq & S \times T \\ & \simeq & \dfrac{\mathbf{Z}}{11\mathbf{Z}} \times (\dfrac{\mathbf{Z}}{7\mathbf{Z}} \times \dfrac{\mathbf{Z}}{7\mathbf{Z}}) \\ & \simeq & \dfrac{\mathbf{Z}}{7\mathbf{Z}} \times (\dfrac{\mathbf{Z}}{7\mathbf{Z}} \times \dfrac{\mathbf{Z}}{11\mathbf{Z}}) \\ & \simeq & \dfrac{\mathbf{Z}}{7\mathbf{Z}} \times \dfrac{\mathbf{Z}}{77\mathbf{Z}} \end{array}$$

car 7 et 11 sont premiers entre eux.

L'autre groupe possible est donc $\dfrac{\mathbf{Z}}{7\mathbf{Z}} \times \dfrac{\mathbf{Z}}{77\mathbf{Z}}$.

Dans ce dernier question, il était également possible d'utiliser la classification des groupes abéliens finis.