Discrete Mathematics 38 (1982) 129–142
North-Holland Publishing Company

CYCLES COMME PRODUIT DE DEUX PERMUTATIONS DE CLASSES DONNÉES

G. BOCCARA
U.E.R. d'Informatique, Université Paris IX Dauphine, 75116 Paris, France

Reçu 16 Janvier 1980
Revisé 24 Novembre 1980

Soit dans le groupe symétrique de degré n, deux classes de conjugaison H et K de partitions respectives $(m_1, \ldots, m_h)$ et $(n_1, \ldots, n_k)$, soit δ le plus grand commun diviseur des entiers $m_1, \ldots, m_h, n_1, \ldots, n_k$, et soit $\lambda = h + k + \varepsilon$ avec $\varepsilon = -1$ ou 1 suivant que $(h+k-1)\delta \leq n$ ou $n < (h+k-1)\delta$. Le résultat principal de cet article est le suivant: pour qu'il existe $\alpha \in H$ et $\beta \in K$ tels que $\alpha\beta$ soit un l-cycle et tels que le groupe $\langle \alpha, \beta \rangle$ soit transitif, il faut et il suffit que $l \equiv \lambda \pmod 2$ et $\lambda \leq l \leq n$. On en déduit une caractérisation de l'ensemble des entiers l pour lesquels un l-cycle peut être décomposé en un produit de deux permutations appartenant respectivement aux classes H et K. Dans le cas où cet ensemble n'est pas vide, c'est l'ensemble des termes d'une progression arithmétique de raison 2.

1. Notations et terminologie

1.1. Dans toute la suite, n désignera un entier positif, $\mathrm{Sym}(n)$ le groupe symétrique de degré n, $\mathrm{Alt}(n)$ le groupe alterné de degré n, A l'ensemble $\{1, \ldots, n\}$ sur lequel opère $\mathrm{Sym}(n)$.

1.2. Si $\alpha \in \mathrm{Sym}(n)$ et si $a \in A$ (resp. $p \subseteqq A$), $a \cdot \alpha$ (resp. $p \cdot \alpha$) désignera l'image de a (resp. p) par α, le produit des permutations etant effectué de gauche à droite.

1.3. Si P et Q sont deux partitions de A, $P \vee Q$ (resp. $P \wedge Q$) désignera la borne supérieure (resp. inférieure) dans le treillis des partitions de A, de (P, Q).

1.4. Si $\alpha \in \mathrm{Sym}(n)$, il existe une partition de A correspondant à la décomposition de α en un produit de cycles disjoints; on la notera $\mathrm{part}(\alpha)$. Les parties de $\mathrm{part}(\alpha)$ sont les orbites du groupe $\langle \alpha \rangle$; on les appellera α-orbites.

1.5. La classe de conjugaison de α dans $\mathrm{Sym}(n)$ sera notée $[\alpha]$. Si $H = [\alpha]$, le nombre de α-orbites est un invariant de H; on le notera $c(\alpha) = c(H)$. Pour tout entier positif μ, le nombre de α-orbites de cardinal μ est un invariant de H; on le notera $c_\mu(\alpha) = c_\mu(H)$. Si $c(H) = h$, la classe H est donc caractérisée par une h-partition $(m_1, \ldots, m_h)$ de l'entier n; on supposera toujours $m_1 \geq \cdots \geq m_h$, et on dira que H est la classe de *partition* $(m_1, \ldots, m_h)$.

0012-365X/82/0000–0000/$02.75

1.6. Si H et K sont deux classes de conjugaison dans $\mathrm{Sym}(n)$, on notera HK l'ensemble des produits $\alpha\beta$ où $\alpha \in H$ et $\beta \in K$. Il est immédiat que $HK = KH$ et que HK est la réunion d'un ensemble de classes de conjugaison.

Soit $(m_1, \ldots, m_h)$ et $(n_1, \ldots, n_k)$ les partitions respectives de H et K, et soit $\alpha \in H$, $\beta \in K$. On définit les invariants suivants du couple (H, K), qui sont indépendants de l'ordre de H et K:

$$D(H, K) = D(\alpha, \beta) = \text{p.g.c.d.}(m_1, \ldots, m_h, n_1, \ldots, n_k),$$

$$E(H, K) = E(\alpha, \beta) = -1 \text{ ou } 1$$

suivant que $(h+k-1)D(H, K) \leqslant n$ ou $n < (h+k-1)D(H, K)$,

$$L(H, K) = L(\alpha, \beta) = c(H) + c(K) + E(H, K).$$

1.7. Si l est un entier supérieur à 1, C_l désignera la classe des l-cycles dans $\mathrm{Sym}(n)$, i.e. la classe H caractérisée par $c_1(H) = n - l$, $c_l(H) = 1$. Si $\gamma \in C_l$, on appellera *support* de γ et on notera $\mathrm{supp}(\gamma)$ l'ensemble des $a \in A$ tels que $a \cdot \gamma \neq a \cdot (a_1, a_2, \ldots, a_l)$ désignera le l-cycle défini par: $a_i \cdot \gamma = a_{i+1}$ pour $1 \leqslant i \leqslant l-1$, $a_l \cdot \gamma = a_1$.

La permutation identique sera appelée 1-cycle, et sa classe dans $\mathrm{Sym}(n)$ sera notée C_1. Si γ est un 1-cycle, on posera $\mathrm{supp}(\gamma) = \{1\}$ $(1 \in A)$.

1.8. Si $f \equiv n \pmod 2$, R_f désignera la classe des réflexions (ou involutions) ayant exactement f points fixes, caractérisée par $c_1(R_f) = f$, $c_2(R_f) = \frac{1}{2}(n-f)$. La classe des involutions sans points fixes sera donc notée R_0.

2. Introduction

Le problème de la recherche des classes de conjugaison H dans $\mathrm{Sym}(n)$ (resp. $\mathrm{Alt}(n)$) pour lesquelles $\mathrm{Alt}(n) \subseteq HH$ est un problème sur lequel un grand nombre de résultats ont été publiés [1–10], mais qui, à notre connaissance, reste encore ouvert.

Dans [6], Brenner énonce une conjecture, qui est une condition suffisante faisant intervenir $c(H)$ et $c_1(H)$, pour que $\mathrm{Alt}(n) \subseteq HH$. Il démontre cette conjecture dans les seuls cas où H a une ou deux orbites essentielles.

Une réponse pourrait être donnée à cette conjecture si l'on connaissait la solution du problème suivant: caractériser les triplets (C, H, K) de classes de conjugaison dans $\mathrm{Sym}(n)$ tels que $C \subseteq HK$. Le cas où deux au moins des classes C, H, K sont des classes de cycles a déjà été résolu dans [2]. Dans cet article on étudie le cas plus général où l'une au moins des classes C, H, K est une classe de cycles.

H et K étant deux classes de conjugaison dans $\mathrm{Sym}(n)$, on détermine dans la Section 3 les entiers l pour lesquels il existe $(\alpha, \beta) \in H \times K$ tel que $\gamma = \alpha\beta$ soit u

l-cycle et tel que $\langle\alpha, \beta\rangle$ soit transitif. Un tel couple (α, β) est appelé *décomposition transitive* (en abrégé d.t.) de γ. Le lemme 3.5 est essentiel pour cette caractérisation; il permet de montrer que si $H \times K$ contient une d.t. d'un l-cycle, alors $L(H, K) \leq l$ (Proposition 3.15), et que si de plus $l \leq n-2$, alors $H \times K$ contient une d.t. d'un $(l+2)$-cycle (Proposition 3.6). Si $\lambda = L(H, K) \leq n$, il se pose alors la question de savoir si $H \times K$ contient une d.t. d'un λ-cycle. Les Propositions 3.9 et 3.12 donnent une réponse affirmative à cette question; on les démontre en raisonnant par récurrence sur $c(H)+c(K)$, et pour cela, on utilise une technique de "suppression" d'orbites dans H ou K (Lemme 3.7), ainsi que des propriétés arithmétiques des partitions de H et K (Lemmes 3.8, 3.10, 3.11).

Dans la Section 4, on utilise les résultats de la Section 3 pour caractériser les entiers l tels que $C_l \subseteq HK$. Pour cela, on remarque que si $\gamma = \alpha\beta$ est un cycle, et si $\langle\alpha, \beta\rangle$ n'est pas transitif, alors il existe une orbite $\bar{A}$ de $\langle\alpha, \beta\rangle$ telle que si $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ sont les restrictions respectives de α, β, γ à $\bar{A}$, $(\bar{\alpha}, \bar{\beta})$ est une d.t. de $\bar{\gamma}$, et que d'autre part toute orbite de $\langle\alpha, \beta\rangle$ distincte de $\bar{A}$ est à la fois une α-orbite et une β-orbite.

3. Décompositions transitives d'un cycle

3.1. Définition. Soit $\alpha, \beta, \gamma \in \mathrm{Sym}(n)$. (α, β) est une *décomposition transitive* (en abrégé d.t.) de γ, si $\alpha\beta = \gamma$ et si $\langle\alpha, \beta\rangle$ est un groupe transitif.

Comme les orbites du groupe $\langle\alpha, \beta\rangle$ sont les parties de $\mathrm{part}(\alpha) \vee \mathrm{part}(\beta)$, (α, β) est une d.t. de $\gamma = \alpha\beta$ si et seulement si $\mathrm{part}(\alpha) \vee \mathrm{part}(\beta) = \{A\}$.

Comme $\alpha\beta = \beta(\beta^{-1}\alpha\beta)$, si H et K sont deux classes de conjugaison dans $\mathrm{Sym}(n)$, $H \times K$ contient une d.t. de γ si et seulement si $K \times H$ contient une d.t. de γ. De plus, si $H \times K$ contient une d.t. de γ, alors $H \times K$ contient une d.t. de tout conjugué de γ.

Dans cette section, on établit le théorème suivant, qui caractérise les cycles admettant une d.t. dans un couple de classes de conjugaison données dans $\mathrm{Sym}(n)$.

3.2. Théorème. *Soit dans* $\mathrm{Sym}(n)$ *deux classes de conjugaison H et K, et soit $\lambda = L(H, K)$. Alors, l'ensemble des entiers l pour lesquels $H \times K$ contient une d.t. d'un l-cycle est défini par:*

$$\lambda \leq l \leq n \quad \text{et} \quad l \equiv \lambda \pmod 2.$$

Certains des raisonnements utilisés pour prouver ce théorème sont des raisonnements par récurrence, dans lesquels on a besoin des deux notions définies ci-aprés.

3.3. Définition. (α, β) est une *bonne décomposition transitive* (en abrégé b.d.t.) du cycle γ, si (α, β) est une d.t. de γ, et s'il existe $a \in A$ tel que a et $a \cdot \alpha$ appartiennent tous deux à $\operatorname{supp}(\gamma)$.

3.4. Définition. Soit dans $\operatorname{Sym}(n)$ une classe de conjugaison H, et soit μ et ν deux entiers positifs tels que: $c_\mu(H) \neq 0$, $\nu \leq \mu$, $\nu < n$. $\Phi^\nu_\mu(H) = \bar{H}$ désigne la classe de $\operatorname{Sym}(n-\nu)$ définie par: $c_\lambda(\bar{H}) = c_\lambda(H)$ si $\lambda \neq \mu$ et $\lambda \neq \mu - \nu$, $c_\mu(\bar{H}) = c_\mu(H) - 1$, et, dans le cas où $\nu < \mu$, $c_{\mu-\nu}(\bar{H}) = c_{\mu-\nu}(H) + 1$.

3.5. Lemme. *Si* (α, β) *est une d.t. d'une cycle* γ, *alors* $\operatorname{supp}(\gamma)$ *reconte chacune des parties de* $\operatorname{part}(\alpha) \wedge \operatorname{part}(\beta)$.

Preuve. Si $\alpha \in C_n$ et $\beta \in C_n$, alors $\operatorname{part}(\alpha) \wedge \operatorname{part}(\beta) = \{A\}$, et $\operatorname{supp}(\gamma) \cap A \neq \emptyset$.

Si $\alpha \notin C_n$ ou $\beta \notin C_n$, et si r est une partie de $\operatorname{part}(\alpha) \wedge \operatorname{part}(\beta)$, alors $r \neq A$, et $r = p \cap q$, où p est une α-orbite et q une β-orbite. Si on avait $\operatorname{supp}(\gamma) \cap r = \emptyset$, alors γ fixerait tous les points de r, et il en résulterait: $r \cdot \alpha = r \cdot \beta^{-1} = r = p = q$. r serait alors une partie de $\operatorname{part}(\alpha) \vee \operatorname{part}(\beta)$, et (α, β) ne serait pas une d.t. de γ.

3.6. Proposition. *Soit dans* $\operatorname{Sym}(n)$ *deux classes de conjugaison* H *et* K. *Si* $H \times K$ *contient une d.t. d'un l-cycle et si* $1 \leq l \leq n-1$, *alors* $H \times K$ *contient une b.d.t. d'un* $(l+2)$*-cycle.*

Preuve. Soit $\alpha \in H$, $\beta \in K$ tels que (α, β) soit une d.t. d'un l-cycle λ. Si $1 \leq l \leq n-2$, alors il existe au moins deux points a et b qui n'appartiennent pas à $\operatorname{supp}(\gamma)$. Soit $a' = a \cdot \alpha$, $b' = b \cdot \beta$. On distingue les cas suivants.

(1) $a', b' \in \operatorname{supp}(\gamma)$. Soit $\tau = (b, a')$, $\beta' = \tau\beta\tau$. Alors $\beta' \in K$, et $\beta' = \beta(\beta^{-1}\tau\beta)\tau = \beta\tau'\tau$, avec $\tau' = (b \cdot \beta, a' \cdot \beta) = (b', a) \cdot \alpha\beta = \gamma$ implique $\alpha\beta' = \gamma'$, avec $\gamma' = \gamma\tau'\tau$. Il est immédiat que γ' est un $(l+2)$-cycle et que $\operatorname{supp}(\gamma') = \operatorname{supp}(\gamma) \cup \{a, b\}$. Donc $\operatorname{part}(\alpha) \vee \operatorname{part}(\gamma')$ est moins fine que $\operatorname{part}(\alpha) \vee \operatorname{part}(\gamma)$, et (α, β') est une d.t. de γ'. De plus, $\{a, a'\} \subseteq \operatorname{supp}(\gamma')$, donc (α, β') est une b.d.t. de γ'.

(2) $b' \notin \operatorname{supp}(\gamma)$. Soit q la β-orbite contenant b. Il résulte du Lemme 3.5 qu'il existe $c \in \operatorname{supp}(\gamma) \cap q$. Soit $\theta = (b, b', c)$, $\beta' = \beta\theta$. Il est immédiat que $\beta' \in K$. $\alpha\beta = \gamma$ implique $\alpha\beta' = \gamma'$, avec $\gamma' = \gamma\theta$. γ' est un $(l+2)$-cycle et $\operatorname{supp}(\gamma') = \operatorname{sup}(\gamma) \cup \{b, b'\}$. Donc (α, β') est une d.t. de γ'. De plus $b' \cdot \alpha = b' \cdot \beta^{-1} = b$ et $\{b, b'\} \subseteq \operatorname{supp}(\gamma')$. Donc (α, β') est une b.d.t. de γ'.

(3) $a' \notin \operatorname{supp}(\gamma)$. Si p est la α-orbite contenant a, il existe $d \in \operatorname{supp}(\gamma) \cap p$. Soit $\sigma = (a, a', d)$ et $\alpha' = \sigma\alpha$. Alors $\alpha' \in H$ et $\alpha'\beta = \gamma'$, avec $\gamma' = \sigma\gamma$. γ' est un $(l+2)$-cycle et $\operatorname{supp}(\gamma') = \operatorname{supp}(\gamma) \cup \{a, a'\}$. De plus, $d \cdot \alpha' = a \cdot \alpha = a'$, et $\{d, a'\} \subseteq \operatorname{supp}(\gamma')$. Donc (α', β) est une b.d.t. de γ'.

3.7. Lemme. *Soit dans* $\operatorname{Sym}(n)$ *deux classes de conjugaison* H *et* K, μ *et* ν *deux entiers positifs tels que* $c_\mu(H) \neq 0$, $c_\nu(K) \neq 0$, $\nu < n$, $\nu \leq \mu$. *Soit* $\bar{H} = \Phi^\nu_\mu(H)$, $\bar{K} = \Phi^\nu_\nu(K)$.

(i) *Si $\nu<\mu$ et si $\bar{H}\times\bar{K}$ contient une d.t. (resp. une b.d.t.) d'un l-cycle, alors $H\times K$ contient une d.t. (resp. une b.d.t.) d'un $(l+1)$-cycle.*

(ii) *Si $2\leq\nu=\mu$, et si $\bar{H}\times\bar{K}$ contient une b.d.t. d'une l-cycle, alors $H\times K$ contient une b.d.t. d'un $(l+2)$-cycle.*

Preuve. Soit $\bar{A}=\{1,\ldots,n-\nu\}$, $A'=A\setminus\bar{A}$, $(\bar{\alpha},\bar{\beta})\in\bar{H}\times\bar{K}$ une d.t. d'un l-cycle $\bar{\gamma}$. Soit α',β',γ' les éléments de $\mathrm{Sym}(n)$ qui fixent tous les points de A' et dont les restrictions respectives à $\bar{A}$ sont $\bar{\alpha},\bar{\beta},\bar{\gamma}$. Soit σ un ν-cycle de support A'. Soit $\alpha''=\alpha'\sigma$, $\beta=\sigma^{-1}\beta'$. Il est clair que $\beta\in K$. $\bar{\alpha}\bar{\beta}=\bar{\gamma}$ implique $\alpha''\beta=\gamma'$. Comme $(\bar{\alpha},\bar{\beta})$ est une d.t. de $\bar{\gamma}$, on a: $\mathrm{part}(\alpha'')\vee\mathrm{part}(\beta)=\mathrm{part}(\beta)\vee\mathrm{part}(\gamma')=\{\bar{A},A'\}$. *Soit $a'\in A'$.*

(i) Si $\nu<\mu$, il existe une α''-orbite $\bar{p}$ de cardinal $\mu-\nu$, incluse dans $\bar{A}$, et, d'après le Lemme 3.5, il existe $\bar{a}\in\mathrm{supp}(\gamma')\cap\bar{p}$. Soit $\tau=(\bar{a},a')$, $\alpha=\tau\alpha''$, $\gamma=\tau\gamma'$. $p=\bar{p}\cup A'$ est une α-orbite de cardinal μ, donc $\alpha\in H$, et $\mathrm{part}(\alpha)\vee\mathrm{part}(\beta)=\{A\}$. $\alpha''\beta=\gamma'$ implique $\alpha\beta=\gamma$. Donc (α,β) est une d.t. de γ, et γ est un $(l+1)$-cycle tel que $\mathrm{supp}(\gamma)=\mathrm{supp}(\gamma')\cup\{a'\}$.

Si l'on suppose que $(\bar{\alpha},\bar{\beta})$ est une b.d.t. de $\bar{\gamma}$, il existe $\bar{b}\in\bar{A}$ tel que $\bar{b}$ et $\bar{b}\cdot\bar{\alpha}=\bar{b}\cdot\alpha''$ appartiennent tous deux *à* $\mathrm{supp}(\bar{\gamma})=\mathrm{supp}(\gamma')\subseteq\mathrm{supp}(\gamma)$. Si $\bar{b}\neq\bar{a}$, alors $\bar{b}\cdot\alpha=\bar{b}\cdot\alpha''$, donc (α,β) est une b.d.t. de γ. Si $\bar{b}=\bar{a}$, alors $a'\cdot\alpha=\bar{a}\cdot\alpha''=\bar{b}\cdot\bar{\alpha}$, et comme a' et $a'\cdot\alpha$ appartiennent tous deux *à* $\mathrm{supp}(\gamma)$, (α,β) est une b.d.t. de γ.

(ii) Si $\nu=\mu$, alors $\alpha''\in H$. Si $(\bar{\alpha},\bar{\beta})$ est une b.d.t. de $\bar{\gamma}$, il existe $\bar{a}\in\bar{A}$ tel que $\bar{a}$ et $\bar{a}\cdot\bar{\alpha}$ appartiennent tous deux *à* $\mathrm{supp}(\bar{\gamma})=\mathrm{supp}(\gamma')$. Soit $\bar{b}=\bar{a}\cdot\bar{\alpha}=a\cdot\alpha''$, $b'=a'\cdot\alpha''$, $\tau=(\bar{b},b')$, $\alpha=\tau\alpha''\tau$. Alors $\alpha\in H$, et $\alpha=\tau(\alpha''\tau\alpha''^{-1})\alpha''=\tau\tau'\alpha''$, avec $\tau'=(\bar{b}\cdot a''^{-1},b'\cdot\alpha''^{-1})=(\bar{a},a')$. $\alpha''\beta=\gamma'$ implique $\alpha\beta=\gamma$, avec $\gamma=\tau\tau'\gamma'$. Si $2\leq\nu$, alors $a'\neq b'$, et γ est un $(l+2)$-cycle tel que $\mathrm{supp}(\gamma)=\mathrm{supp}(\gamma')\cup\{a',b'\}$. Il en résulte $\mathrm{part}(\beta)\vee\mathrm{part}(\gamma)=\{A\}$, donc (α,β) est une d.t. de γ.

Si $\bar{b}\neq\bar{a}$, alors $\bar{a}\cdot\alpha=a'\cdot\alpha''=b'$. Si $\bar{b}=\bar{a}$, alors $b'\cdot\alpha=a'\cdot\alpha''=b'$. Comme $\{\bar{a},b'\}\subseteq\mathrm{supp}(\gamma)$, $(\alpha\ \beta)$ est une b.d.t. de γ.

3.8. Lemme. *Soit dans $\mathrm{Sym}(n)$ deux classes de conjugaison H et K. Si $3\leq c(H)+c(K)$ et $E(H,K)=-1$, alors il existe deux entiers positifs μ et ν tels que $\mu\neq\nu$, $c_\mu(H)\neq0$, $c_\nu(K)\neq0$, et tels que, si $\omega=\min\{\mu,\nu\}$, $\bar{H}=\Phi_\mu^\omega(H)$, $\bar{K}=\Phi_\nu^\omega(K)$, alors $E(\bar{H},\bar{K})=-1$.*

Preuve. Soit $(m_1,\ldots,m_h)$ et $(n_1,\ldots,n_k)$ les partitions respectives de H et K, et soit $\delta=D(H,K)$. Si on avait $m_1=\cdots=m_h=n_1=\cdots=n_k$, on aurait aussi $h\delta=k\delta=n$, ce qui impliquerait soit $h=k=1$, soit $h=k\geq2$ et $(h+k-1)\delta>n$. Ceci contredit l'hypothèse $3\leq h+k$ et $E(H,K)=-1$. On a donc soit $n_k\leq m_h$ et $n_k<m_1$, soit $m_h\leq n_k$ et $m_h<n_1$. La propriété à démontrer étant symétrique par rapport à H et K, on peut supposer $n_k\leq m_h$ et $n_k<m_1$. Soit $\nu=n_k$, $\bar{n}=n-\nu$, $\bar{K}=\Phi_\nu^\nu(K)$. Pour tout i tel que $\nu<m_i$, posons $H_i=\Phi_{m_i}^\nu(H)$, $\delta_i=D(H_i,\bar{K})$. Soit $\bar{\delta}=\min\{\delta_i: 1\leq i\leq h$ et $\nu<m_i\}$, i_0 tel que $\bar{\delta}=\delta_{i_0}$, $\mu=m_{i_0}$, $\bar{H}=\Phi_\mu^\nu(H)$. $\bar{H}$ et $\bar{K}$ sont

dans $\mathrm{Sym}(\bar{n})$ deux classes de conjugaison telles que $c(\bar{H})=h$, $c(\bar{K})=k-1$. Nous allons montrer que $E(\bar{H},\bar{K})=-1$, donc que $(h+k-2)\bar{\delta}\leqslant\bar{n}$. On distingue les cas suivants.

(1) $h=1$. $\bar{\delta}$ divise n_j pour tout j tel que $1\leqslant j\leqslant k-1$. Comme $\bar{n}=\sum_{1\leqslant j\leqslant k-1} n_j$, on a: $(h+k-2)\bar{\delta}=(k-1)\bar{\delta}\leqslant\bar{n}$.

(2) $\bar{\delta}=\delta$.

Si $\nu=\delta$, $(h+k-1)\delta\leqslant n$ implique $(h+k-2)\bar{\delta}\leqslant\bar{n}$.

Si $\nu\neq\delta$, alors $2\delta\leqslant\nu$, d'où $2(k-1)\delta\leqslant\bar{n}$; $\nu\leqslant m_h$ implique $2(h-1)\delta\leqslant\bar{n}$. Il en résulte $(h+k-2)\bar{\delta}\leqslant\bar{n}$.

(3) $2\leqslant h$ et $\bar{\delta}\neq\delta$. δ divise $\nu=n_k$, et pour tout $i\,(1\leqslant i\leqslant h)\delta$ divise m_i, donc divise $m_i-\nu$. Il en résulte que pour tout i tel que $\nu<m_i$, δ divise δ_i. $\bar{\delta}\neq\delta$ implique alors: $2\delta\leqslant\bar{\delta}\leqslant\delta_i$, pour tout i tel que $\nu<m_i$.

δ_1 divise $m_1-\nu$ et m_h. Comme δ_1 ne divise pas δ, on a $m_h\neq\nu$. $\nu\leqslant m_h$ implique alors $\nu<m_i$ pour tout i.

Si $i'\neq i''$, $\delta_{i'}$ divise $m_{i'}-\nu$ et $m_{i''}$. Comme $\delta_{i'}$ ne divise pas δ, on a $m_{i'}\neq m_{i''}$. $\delta_{i'}$ divise $m_{i'}-\nu$ et $\delta_{i''}$ divise $m_{i''}$. Comme $\delta_{i'}$ ne divise pas δ, $\delta_{i'}$ ne divise pas $m_{i''}$, donc $\delta_{i'}\neq\delta_{i''}$.

$\bar{\delta}$ divise $\mu-\nu$ et divise m_i pour tout $i\neq i_0$. Les entiers m_i étant deux à deux distincts, on a:

$$\bar{n}=(\mu-\nu)+\sum_{i\neq i_0} m_i\geqslant\Bigg(1+\sum_{1\leqslant i\leqslant h-1} i\Bigg)\bar{\delta} \tag{3.8.1}$$

$h\geqslant 2$ implique:

$$1+\sum_{1\leqslant i\leqslant h-1} i\geqslant 1+(h-1)+(h-2)=2(h-1) \tag{3.8.2}$$

(3.8.1) et (3.8.2) impliquent alors:

$$\bar{n}\geqslant 2(h-1)\bar{\delta} \tag{3.8.3}$$

Comme $h\geqslant 2$, et que les entiers δ_i sont deux à deux distincts, il existe $i_1\neq i_0$ tel que $\delta_{i_1}>\bar{\delta}$. Pour tout j tel que $1\leqslant j\leqslant k-1$, δ_{i_1} et $\bar{\delta}$ divisent n_j, donc $n_j\geqslant 2\bar{\delta}$. Il en résulte:

$$\bar{n}=\sum_{1\leqslant j\leqslant k-1} n_j\geqslant 2(k-1)\bar{\delta} \tag{3.8.4}$$

(3.8.3) et (3.8.4) impliquent: $(h+k-2)\bar{\delta}\leqslant\bar{n}$.

3.9. Proposition. *Soit dans* $\mathrm{Sym}(n)$ *deux classes de conjugaison* H *et* K, *et soit* $\lambda=L(H,K)$. *Si* $E(H,K)=-1$, *alors* $H\times K$ *contient une d.t. d'un* λ*-cycle.*

Preuve. Soit $h=c(H)$, $k=c(K)$. Si $E(H,K)=-1$, alors $\lambda=h+k-1$. On fait un raisonnement par récurrence sur $h+k$.

Si $h+k=2$, alors $h=k=1$, $H=K=C_n$, $E(H,K)=-1$, $\lambda=1$. Si $\alpha\in H$, alors $\alpha^{-1}\in K$, et (α,α^{-1}) est une d.t. d'un 1-cycle.

Si $3 \leqslant h+k$ et $E(H, K)=-1$, comme la propriété à démontrer est symétrique par rapport à H et K, on peut supposer, en utilisant le Lemme 3.8, qu'il existe deux entiers positifs μ et ν tels que $\nu<\mu$, $c_\mu(H)\neq 0$, $c_\nu(K)\neq 0$, et tels que, si $\bar{H}=\Phi^\nu_\mu(H)$ et $\bar{K}=\Phi^\nu_\nu(K)$, alors $E(\bar{H}, \bar{K})=-1$. On a alors: $\bar{\lambda}=L(\bar{H}, \bar{K})= h+k-2=\lambda-1$. Faisons l'hypothèse de récurrence: $\bar{H}\times\bar{K}$ contient une d.t. d'un $\bar{\lambda}$-cycle. Il résulte alors du Lemme 3.7 que $H\times K$ contient une d.t. d'un λ-cycle.

3.10. Lemme. *Soit dans* Sym(n) *deux classes de conjugaison H et K, et soit $\delta=D(H, K)$. Si $E(H, K)=1$, alors:*

(i) $c(H)\geqslant 2$ *et* $c(K)\geqslant 2$.

(ii) $c_\delta(H)\geqslant 2$ *ou* $c_\delta(K)\geqslant 2$.

Preuve. On raisonne par l'absurde. Soit $h=c(H)$, $k=c(K)$.

Si $h=1$ ou $k=1$, alors $(h+k-1)\delta\leqslant n$, ce qui contredit $E(H, K)=1$.

Si $c_\delta(H)\leqslant 1$ et $c_\delta(K)\leqslant 1$, alors $2(h-1)\delta+\delta\leqslant n$ et $2(k-1)\delta+\delta\leqslant n$, d'où $(h+k-1)\delta\leqslant n$, ce qui contredit $E(H, K)=1$.

3.11. Lemme. *Soit dans* Sym(n) *deux classes de conjugaison H et K. Si $D(H, K)\geqslant 2$ et si ($H\neq R_0$* ou *$K\neq R_0$), alors $c(H)+c(K)\leqslant n-1$.*

Preuve. Soit $h=c(H)$, $k=c(K)$, $\delta=D(H, K)$. La propriété à démontrer étant symétrique par rapport à H et K, on peut supposer $H\neq R_0$. Comme $\delta\geqslant 2$, il existe $\mu\geqslant 3$ tel que $c_\mu(H)\neq 0$. On a alors $2k\leqslant k\delta\leqslant n$ et $2(h-1)+3\leqslant (h-1)\delta+\mu\leqslant n$, d'où $h+k\leqslant n-1$.

3.12. Proposition. *Soit dans* Sym(n) *deux classes de conjugaison H et K, et soit $\lambda=L(H, K)$. Si $E(H, K)=1$, $D(H, K)\geqslant 2$ et ($H\neq R_0$ ou $K\neq R_0$), alors $H\times K$ contient une b.d.t. d'un λ-cycle.*

Preuve. Soit $(m_1, \ldots, m_h)$ et $(n_1, \ldots, n_k)$ les partitions respectives de H et K, et soit $\delta=D(H, K)$. $E(H, K)=1$ implique $\lambda=h+k+1$, et d'après le Lemme 3.10, on a ($h\geqslant 2$ et $k\geqslant 2$) et ($c_\delta(H)\geqslant 2$ ou $c_\delta(K)\geqslant 2$). La propriété à démontrer étant symétrique par rapport à H et K, on peut supposer $n_{k-1}=n_k=\delta$ et $H\neq R_0$. Soit $\mu=m_h$, $\bar{H}=\Phi^\delta_\mu(H)$, $\bar{K}=\Phi^\delta_\delta(K)$, $\bar{n}=n-\delta$. Il est immédiat que $D(\bar{H}, \bar{K})=\delta$. $H\neq R_0$ et $\delta\geqslant 2$ implique $m_1\geqslant 3$, donc $\bar{H}$ n'est pas la classe des involutions sans points fixes dans Sym($\bar{n}$).

Pour démontrer la proposition on fait un raisonnement par récurrence sur $h+k$.

(1) Si $h+k=4$, alors $h=k=2$ et $m_1=m_2=n_1=n_2=\delta\geqslant 3$. Il est immédiat que $\bar{H}\times\bar{K}$ contient une d.t. d'un 1-cycle. Comme $n\geqslant 6$, il résulte de la Proposition 3.6 que $\bar{H}\times\bar{K}$ contient une b.d.t. d'un 3-cycle. D'aprés le Lemme 3.7, $H\times K$ contient alors une b.d.t. d'un 5-cycle, et $\lambda=5$.

(2) Si $h+k\geqslant 5$, posons $\bar{h}=c(\bar{H})$, $\bar{k}=c(\bar{K})$, $\bar{\lambda}=L(\bar{H},\bar{K})$. $E(H,K)=1$ équivaut à:

$$n<(h+k-1)\delta \tag{3.12.1}$$

On distingue deux cas.

(2a) $\delta<\mu$. Alors $\bar{h}=h$. $\bar{k}=k-1$. (3.12.1) implique $\bar{n}<(\bar{h}+\bar{k}-1)\delta$, donc $E(\bar{H},\bar{K})=1$ et $\bar{\lambda}=\bar{h}+\bar{k}+1$. Faisons l'hypothèse de récurrence: $\bar{H}\times\bar{K}$ contient une b.d.t. d'un $\bar{\lambda}$-cycle. Il résulte du Lemme 3.7 que $H\times K$ contient une b.d.t. d'un $(\bar{\lambda}+1)$-cycle, et $\bar{\lambda}+1=\lambda$.

(2b) $\delta=\mu$. Alors $\bar{h}=h-1$, $\bar{k}=k-1$. (3.12.1) implique $\bar{n}-\delta<(\bar{h}+\bar{k}-1)\delta$.

Si $\bar{n}=(\bar{h}+\bar{k}-1)\delta$, alors $E(\bar{H},\bar{K})=-1$, $\bar{\lambda}=\bar{h}+\bar{k}-1$. Il résulte de la Proposition 3.9 que $\bar{H}\times\bar{K}$ contient une d.t. d'un $\bar{\lambda}$-cycle. $\delta\geqslant 2$ et $\bar{H}\neq R_0$ implique, d'après le Lemme 3.11, $\bar{\lambda}\leqslant\bar{n}-2$. Il résulte alors de la Proposition 3.6 que $\bar{H}\times\bar{K}$ contient une b.d.t. d'un $(\bar{\lambda}+2)$-cycle. D'après le Lemme 3.7, $H\times K$ contient alors une b.d.t. d'un $(\bar{\lambda}+4)$-cycle, et $\bar{\lambda}+4=\lambda$.

Si $\bar{n}<(\bar{h}+\bar{k}-1)\delta$, alors $E(\bar{H},\bar{K})=1$, $\bar{\lambda}=\bar{h}+\bar{k}+1$. Faisons l'hypothèse de récurrence: $\bar{H}\times\bar{K}$ contient une b.d.t. d'un $\bar{\lambda}$-cycle. D'après le Lemme 3.7, $H\times K$ contient alors une b.d.t. d'un $(\bar{\lambda}+2)$-cycle, et $\bar{\lambda}+2=\lambda$.

3.13. Lemme. *Soit dans* Sym(n) *deux classes de conjugaison H et K. Si $H\times K$ contient une d.t. d'un l-cycle, alors $c(H)+c(K)-1\leqslant l$.*

Preuve. Soit $h=c(H)$, $k=c(K)$, et $(\alpha,\beta)\in H\times K$ une d.t. d'un l-cycle γ. On fait un raisonnement par récurrence sur k.

Si $k=1$, alors $h+k-1=h$. D'après le Lemme 3.5, supp(γ) rencontre chacune des α-orbites. Donc $h\leqslant l$.

Si $k\geqslant 2$, Comme (α,β) est une d.t. de γ, il existe $a\in\text{supp}(\gamma)$ tel que a et $a'=a\cdot\gamma$ appartiennent à deux β-orbites distinctes q et q'. Soit $\tau=(a,a')$, $\beta'=\beta\tau$, $\gamma'=\gamma\tau$. $\alpha\beta=\gamma$ implique $\alpha\beta'=\gamma'$. $q\cup q'$ est une β'-orbite contenant a et a'. Donc $k'=c(\beta')=k-1$, part$(\beta')\vee$part$(\alpha)=\{A\}$, et (α,β') est une d.t. de γ'. Il est immédiat que γ' est un $(l-1)$-cycle. Faisons l'hypothèse de récurrence: $h+k'-1\leqslant l-1$. Il en résulte: $h+k-1\leqslant l$.

3.14. Lemme. *Soit dans* Sym(n) *deux classes de conjugaison H et K, et soit $\hat{\lambda}=c(H)+c(K)-1$. Si $H\times K$ contient une d.t. d'un $\hat{\lambda}$-cycle, alors $E(H,K)=-1$.*

Preuve. Soit $h=c(H)$, $k=c(K)$, $\delta=D(H,K)$, $(\alpha,\beta)\in H\times K$ une d.t. d'un $\hat{\lambda}$-cycle. D'après le Lemme 3.5, supp(γ) rencontre chacune des α-orbites et chacune des β-orbites. Si toute α-orbite et tout β-orbite avait au moins deux points dans supp(γ), on aurait $\hat{\lambda}\geqslant 2h$ et $\hat{\lambda}\geqslant 2k$, d'où $\hat{\lambda}\geqslant h+k$, ce qui contredit l'hypothèse $\hat{\lambda}=h+k-1$. La propriété à démontrer étant symétrique par rapport à H et K, on peut supposer qu'il existe une α-orbite p telle que supp$(\gamma)\cap p=\{a\}$. D'après le Lemme 3.5, p est nécessairement une partie de part$(\alpha)\wedge$part(β), donc p est incluse dans une β-orbite q.

Pour montrer que $E(H, K) = -1$, donc que $(h+k-1)\delta \leq n$, on fait un raisonnement par récurrence sur $h+k$.

Si $h+k=2$, alors $h=k=1$ et $E(H, K) = -1$.

Si $h+k \geq 3$, alors p est strictement incluse dans q. Soit θ la restriction de α à p, $a' = a \cdot \gamma$, $\tau = (a, a')$, $\alpha' = \alpha\theta^{-1}$, $\beta' = \theta\beta\tau$, $\gamma' = \gamma\tau$. $\alpha\beta = \gamma$ implique $\alpha'\beta' = \gamma'$. On vérifie facilement que tout point de p est en même temps une α'-orbite et une β'-orbite de cardinal 1, que $q \setminus p$ est une β'-orbite, que γ' est un $(\lambda - 1)$-cycle tel que $\operatorname{supp}(\gamma') = \operatorname{supp}(\gamma) \setminus \{a\}$. Soit $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ les restrictions respectives de α', β', γ' à $\bar{A} = A \setminus p$. On vérifie facilement que $\operatorname{part}(\bar{\alpha}) \vee \operatorname{part}(\bar{\beta}) = \{\bar{A}\}$, donc $(\bar{\alpha}, \bar{\beta})$ est une d.t. de $\bar{\gamma}$. On a $\bar{h} = c(\bar{\alpha}) = h - 1$, $\bar{k} = c(\bar{\beta}) = k$, et $\bar{\gamma}$ est un $(\bar{h} + \bar{k} - 1)$-cycle. Soit $\bar{n} = |\bar{A}| = n - |p|$, $\bar{\delta} = D(\bar{\alpha}, \bar{\beta})$. Faisons l'hypothèse de récurrence: $E(\bar{\alpha}, \bar{\beta}) = -1$, i.e. $(\bar{h} + \bar{k} - 1)\bar{\delta} \leq \bar{n}$. δ divise $|p|$ et $|q|$, donc divise $|q| - |p|$, donc divise $\bar{\delta}$. Il en résulte:

$$(h+k-1)\delta = (\bar{h} + \bar{k} - 1)\delta + \delta \leq (\bar{h} + \bar{k} - 1)\bar{\delta} + \delta \leq \bar{n} + |p| = n.$$

3.15. Proposition. *Soit dans* $\operatorname{Sym}(n)$ *deux classes de conjugaison H et K, et soit $\lambda = L(H, K)$. Si $H \times K$ contient une d.t. d'un l-cycle, alors $\lambda \leq l$.*

Preuve. Si $E(H, K) = -1$, alors $\lambda = c(H) + c(K) - 1$, et il résulte du Lemme 3.13 que $\lambda \leq l$.

Si $E(H, K) = 1$, alors $\lambda = c(H) + c(K) + 1$. Il résulte du Lemme 3.13 que $\lambda - 2 \leq l$, et il résulte du Lemme 3.14 que $\lambda - 2 \neq l$. Il est immédiat que $l \equiv \lambda \pmod 2$. Donc $\lambda \leq l$.

Nous sommes maitenant en mesure de prouver le théorème.

Preuve du Théorème 3.2. Si $H \times K$ contient une d.t. d'un l-cycle, alors $l \equiv \lambda \pmod 2$, et il résulte de la Proposition 3.15 que $\lambda \leq l \leq n$.

Inversement, si $E(H, K) = -1$, ou si $E(H, K) = 1$ et $D(H, K) \geq 2$ et ($H \neq R_0$ ou $K \neq R_0$), il résulte des Propositions 3.6, 3.9 et 3.12 que pour tout entier l tel que $\lambda \leq l \leq n$ et $l \equiv \lambda \pmod 2$, $H \times K$ contient une d.t. d'un l-cycle.

Si $E(H, K) = D(H, K) = 1$, alors $n < c(H) + c(K) - 1 = \lambda - 2$, et il n'existe pas d'entier l tel que $\lambda \leq l \leq n$.

Si $E(H, K) = 1$ et $H = K = R_0$, alors $c(H) = c(K) = \frac{1}{2}n$, $\lambda = n + 1$, et il n'existe pas d'entier l tel que $\lambda \leq l \leq n$.

4. Cycles appartenant au produit de deux classes de conjugaison

H et K étant deux classes de conjugaison dans $\operatorname{Sym}(n)$, on établit dans cette section un théorème qui caractérise les entiers l pour lesquels $C_l \subseteqq HK$. L'énoncé de ce théorème utilise un invariant du couple (H, K) que nous définissons ci-après.

4.1. Notations et définitions. Soit dans Sym(n) deux classes de conjugaison H et K, et soit $f=\min\{c_1(H), c_1(K)\}$.

Si ($H\neq C_1$ ou $K\neq C_1$), on pose $n^{(0)}=n-f$, et on désigne par $H^{(0)}$ et $K^{(0)}$ les classes de Sym$(n^{(0)})$ définies par: $c_1(H^{(0)})=c_1(H)-f$, $c_1(K^{(0)})=c_1(K)-f$, et pour $\nu\geq 2$, $c_\nu(H^{(0)})=c_\nu(H)$, $c_\nu(K^{(0)})=c_\nu(K)$.

Soit s le nombre de parts communes aux partitions de $H^{(0)}$ et de $K^{(0)}$, et, si $1\leq s$, soit $(\nu_1,\ldots,\nu_s)$ avec $2\leq\nu_1\leq\cdots\leq\nu_s$ la famille de ces parts communes. Si $1\leq s$ et si $H\neq K$, on définit les suites:

$$n^{(0)},\ldots,n^{(s)} \quad \text{par} \quad n^{(t)}=n^{(t-1)}-\nu_t,$$
$$H^{(0)},\ldots,H^{(s)} \quad \text{par} \quad H^{(t)}=\Phi_{\nu_t}^{\nu_t}(H^{(t-1)}),$$
$$K^{(0)},\ldots,K^{(s)} \quad \text{par} \quad K^{(t)}=\Phi_{\nu_t}^{\nu_t}(K^{(t-1)}).$$

Pour tout t tel que $0\leq t\leq s$, soit $\lambda^{(t)}=L(H^{(t)}, K^{(t)})$.

4.2. Définition. Soit H et K deux classes de conjugaison dans Sym(n). $\Lambda=\Lambda(H,K)$ est l'entier défini comme suit:

$$\begin{array}{ll} \text{Si } H=K: & \Lambda=1, \\ \text{Si } H\neq K \text{ et } \lambda^{(0)}>n^{(0)}: & \Lambda=\lambda^{(0)}, \\ \text{Si } H\neq K \text{ et } \lambda^{(0)}\leq n^{(0)}: & \Lambda=\min\{\lambda^{(t)}: 0\leq t\leq s \text{ et } \lambda^{(t)}\leq n^{(t)}\}. \end{array}$$

Il est immédiat que si $t\geq 1$, alors $\lambda^{(t)}\leq\lambda^{(t-1)}$. Donc si $H\neq K$, on a toujours $\Lambda\leq\lambda^{(0)}$.

4.3. Théoreme. *Soit dans* Sym(n) *deux classes de conjugaison H et K, et soit $h=c(H)$, $k=c(K)$, $\Lambda=\Lambda(H,K)$. Si ($H\neq R_0$ ou $K\neq R_0$), alors l'ensemble des entiers l pour lesquels $C_l\subseteqq HK$ est défini par*:

$$\Lambda\leq l\leq\min\{n, 2n-h-k+1\} \quad \text{et} \quad l\equiv\Lambda \pmod 2.$$

Pour établir ce théorème, nous commencerons par prouver les propositions suivantes.

4.4. Lemme. *Si $l=n$ ou $2\leq l=n-1$, alors toute d.t. d'un l-cycle dans* Sym(n) *est une b.d.t.*

Preuve. Soit (α,β) une d.t. d'un l-cycle γ dans Sym(n).

Si $l=n$, alors supp$(\gamma)=A$, et pour tout $a\in A$, a et $a\cdot\alpha$ sont dans supp(γ).

Si $2\leq l=n-1$, alors $|A\setminus\text{supp}(\gamma)|=1$ et $|\text{supp}(\gamma)|\geq 2$. Soit $\{a,b\}\subseteqq\text{supp}(\gamma)$. $a\neq b$ implique $a\cdot\alpha\neq b\cdot\alpha$. Donc $\{a\cdot\alpha, b\cdot\alpha\}\cap\text{supp}(\gamma)\neq\emptyset$.

4.5. Proposition. *Soit dans* Sym(n) *deux classes de conjugaison H et K telles que* $\min\{c_1(H), c_1(K)\}=0$. *Si HK contient un l-cycle et si $2\leq l\leq n-2$, alors HK contient un $(l+2)$-cycle.*

Preuve. Soit $\alpha \in H$, $\beta \in K$ tels que $\gamma = \alpha\beta$ soit un l-cycle. Il existe une partie $\bar{A}$ de $\operatorname{part}(\alpha) \vee \operatorname{part}(\beta)$ telle que si $\bar{\alpha}$, $\bar{\beta}$, $\bar{\gamma}$ sont les restrictions respectives de α, β, γ à $\bar{A}$, alors $(\bar{\alpha}, \bar{\beta})$ est une d.t. de $\bar{\gamma}$. Soit $\bar{n} = |\bar{A}|$, $\bar{H} = [\bar{\alpha}]$, $\bar{K} = [\bar{\beta}]$.

Si $l \leq \bar{n} - 2$, il résulte de la Proposition 3.6 que $\bar{H}\bar{K}$ (donc HK) contient un $(l+2)$-cycle.

Si $\bar{n} - 1 \leq l$, alors $l = \bar{n}$ ou $2 \leq l = \bar{n} - 1$, et il résulte du Lemme 4.4 que $(\bar{\alpha}, \bar{\beta})$ est une b.d.t. de $\bar{\gamma}$. $l \leq n-2$ implique $\bar{n} < n$, donc $\bar{A} \neq A$, $\operatorname{part}(\alpha) \vee \operatorname{part}(\beta)$ a au moins une partie p distincte de $\bar{A}$, et p est à la fois une α-orbite et une β-orbite. Soit $\mu = |p|$, $n' = \bar{n} + \mu$, H' et K' les classes de $\operatorname{Sym}(n')$ définies par $c_\mu(H') = c_\mu(\bar{H}) + 1$, $c_\mu(K') = c_\mu(\bar{K}) + 1$, et pour $\nu \neq \mu$, $c_\nu(H') = c_\nu(\bar{H})$ et $c_\nu(K') = c_\nu(\bar{K})$. On a $\bar{H} = \Phi^\mu_\mu(H')$, $\bar{K} = \Phi^\mu_\mu(K')$, et $\min\{c_1(H), c_1(K)\} = 0$ implique $2 \leq \mu$. Il résulte alors du Lemme 3.7 que $H'K'$ (donc HK) contient un $(l+2)$-cycle

4.6. Proposition. *Soit dans* $\operatorname{Sym}(n)$ *deux classes de conjugaison* H *et* K, *et soit* $\Lambda = \Lambda(H, K)$. *Si* $\min\{c_1(H), c_1(K)\} = 0$ *et si* $(H \neq R_0$ ou $K \neq R_0)$, *alors* HK *contient un* l*-cycle pour tout entier* l *tel que*:

$$\Lambda \leq l \leq n \quad et \quad l \equiv \Lambda \pmod 2.$$

Preuve. Si $H = K$, alors $\Lambda = 1$, et il est immédiat que $C_1 \subseteq HK$. $H \neq R_0$ et $c_1(H) = 0$ implique qu'il existe $\mu \geq 3$ tel que $c_\mu(H) \neq 0$. Soit $\bar{H}$ la classe des μ-cycles dans $\operatorname{Sym}(\mu)$. Il résulte du Théorème 3.2 que $\bar{H}\bar{H}$ (donc HH) contient un 3-cycle. Il résulte alors de la Proposition 4.5 que pour tout entier l tel que $1 \leq l \leq n$ et $l \equiv 1 \pmod 2$, HH contient un l-cycle.

Si $H \neq K$, soit s le nombre de parts communes aux partitions de H et K. D'après la définition de Λ, il existe t $(0 \leq t \leq s)$ tel que $\Lambda = \lambda^{(t)}$. Si $\lambda^{(0)} > n^{(0)} = n$, alors $\Lambda = \lambda^{(0)}$, et il n'existe pas d'entier l tel $\Lambda \leq l \leq n$. Si $\lambda^{(0)} \leq n^{(0)}$, alors $2 \leq \Lambda = \lambda^{(t)} \leq n^{(t)}$, et il résulte du Théorème 3.2 que $H^{(t)}K^{(t)}$ (donc HK) contient un Λ-cycle; il résulte alors de la Proposition 4.5 que pour tout entier l tel que $\Lambda \leq l \leq n$ et $l \equiv \Lambda \pmod 2$, HK contient un l-cycle.

4.7. Proposition. *Soit* $n \geq 3$, *et dans* $\operatorname{Sym}(n)$, R_1 *la classe des involutions ayant exactement un point fixe. Alors* R_1R_1 *contient un* l*-cycle pour tout entier* l *impair tel que* $1 \leq l \leq n$.

Preuve. On raisonne par récurrence sur n.

Si $n = 3$, R_1R_1 contient évidemment un 1-cycle, et il résulte du Théorème 3.2 que R_1R_1 contient un 3-cycle.

Si $n \geq 5$, soit $\bar{H} = \Phi^2_2(R_1)$. $\bar{H}$ est dans $\operatorname{Sym}(n-2)$ la classe des involutions ayant exactement un point fixe. Faisons l'hypothèse de récurrence: pour tout entier l impair tel que $1 \leq l \leq n-2$, $\bar{H}\bar{H}$ contient un l-cycle. Il résulte alors du Lemme 4.4 que $\bar{H} \times \bar{H}$ contient une b.d.t. d'un $(n-2)$-cycle, et il résulte du Lemme 3.7 que R_1R_1 contient un n-cycle.

4.8. Lemme. *Soit dans* Sym(n) *deux classes de conjugaison H et K, soit $h = c(H)$, $k = c(K)$. Si $h + k - 1 \leq n$ et $h + k - 1 \equiv n$* (mod 2), *alors HK contient un n-cycle.*

Preuve. $h + k - 1 \equiv n$ (mod 2) implique ($H \neq R_0$ ou $K \neq R_0$).

Si $E(H, K) = -1$, alors $L(H, K) = h + k = 1$, et le lemme résulte du Théorème 3.2. Si $E(H, K) = 1$, alors $n < (h + k - 1)\delta$, où $\delta = D(H, K)$; si de plus, $h + k - 1 \leq n$, alors $\delta \geq 2$, et il résulte du Lemme 3.11 que $h + k \leq n - 1$, i.e. que $L(H, K) \leq n$; le lemme résulte alors du Théoréme 3.2.

4.9. Proposition. *Soit dans* Sym(n) *deux classes de conjugaison H et K, et soit $h = c(H)$, $k = c(K)$, $f = \min\{c_1(H), c_1(K)\}$, $n^{(0)} = n - f$. Si ($H \neq C_1$ ou $K \neq C_1$), alors HK contient un l-cycle pour tout entier l tel que*:

$$n^{(0)} \leq l \leq \min\{n, 2n - h - k + 1\} \quad et \quad l \equiv h + k - 1 \ (\text{mod } 2).$$

Preuve. On raisonne par récurrence sur f.

Si $f = 0$, alors $n^{(0)} = n$. L'ensemble des l tels que $l \equiv h + k - 1$ (mod 2) et $n \leq l \leq \min\{n, 2n - h - k + 1\}$ est non vide si et seulement si $h + k - 1 \leq n$ et $n \equiv h + k - 1$ (mod 2); il est alors égal à $\{n\}$, et dans ce cas, il résulte du Lemme 4.8 que HK contient un n-cycle.

Si $f \geq 1$, et si ($H \neq C_1$ ou $K \neq C_1$). Soit $\bar{H} = \Phi_1^1(H)$, $\bar{K} = \Phi_1^1(K)$, $\bar{n} = n - 1$. On a: $\bar{h} = c(\bar{H}) = h - 1$, $\bar{k} = c(\bar{K}) = k - 1$, $\bar{f} = \min\{c_1(\bar{H}), c_1(\bar{K})\} = f - 1$, $\bar{n} - \bar{f} = n^{(0)}$, $2\bar{n} - \bar{h} - \bar{k} + 1 = 2n - h - k + 1$. Faisons l'hypothèse de récurrence: pour tout l tel que $n^{(0)} \leq l \leq \min\{\bar{n}, 2n - h - k + 1\}$ et $l \equiv h + k - 1$ (mod 2), $\bar{H}\bar{K}$ (donc HK) contient un l-cycle. Si $h + k - 1 \geq n + 1$, alors $\min\{\bar{n}, 2n - h - k + 1\} = \min\{n, 2n - h - k + 1\}$ et la démonstration est terminée. Si $h + k - 1 \leq n$, alors $\min\{\bar{n}, 2n - h - k + 1\} = n - 1$ et $\min\{n, 2n - h - k + 1\} = n$; si $n \equiv h + k$ (mod 2), la démonstration est terminée; si $n \equiv h + k - 1$ (mod 2), il résulte du Lemme 4.8 que HK contient un n-cycle, ce qui achève la démonstration.

4.10. Proposition. *Soit dans Sym(n) deux classes de conjugaison H et K, et soit $h = c(H)$, $k = c(K)$, $\Lambda = \Lambda(H, K)$. Si HK contient un l-cycle, alors*

$$\Lambda \leq l \leq 2n - h - k + 1.$$

Preuve. Soit $\alpha \in H$, $\beta \in K$, tels que $\gamma = \alpha\beta$ soit un l-cycle. Il existe une partie $\bar{A}$ de part$(\alpha) \vee$ part(β) telle que si $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ sont les restrictions respectives de α, β, γ à $\bar{A}$, alors $(\bar{\alpha}, \bar{\beta})$ est une d.t. de $\bar{\gamma}$. Soit $\bar{h} = c(\bar{\alpha})$, $\bar{k} = c(\bar{\beta})$, $\bar{\varepsilon} = E(\bar{\alpha}, \bar{\beta})$, $\bar{n} = |\bar{A}|$. Il résulte du Théorème 3.2:

$$L(\bar{\alpha}, \bar{\beta}) = \bar{h} + \bar{k} + \bar{\varepsilon} \leq l \leq \bar{n}. \tag{4.10.1}$$

Si $\bar{A} \neq A$, tout partie de part$(\alpha) \vee$ part(β) distincte de $\bar{A}$ est à la fois une α-orbite et une β-orbite. Soit u $(0 \leq u)$ le nombre de ces parties. On a : $\bar{h} = h - u$, $\bar{k} = k - u$.

(1) Montrons que $l \leq 2n - h - k + 1$.

(4.10.1) implique:

$$h+k-2u-1=\bar{h}+\bar{k}-1\leq \bar{h}+\bar{k}+\bar{\varepsilon}\leq l\leq \bar{n}\leq n-u \tag{4.10.2}$$

Il en résulte: $u\geq h+k-n-1$, d'où:

$$l\leq n-u\leq n-(h+k-n+1)=2n-h-k+1$$

(2) Montrons que $\Lambda\leq l$.
Si $H=K$, alors $\Lambda=1\leq l$. Si $H\neq K$ et si $\lambda^{(0)}\leq l$, alors $\Lambda\leq\lambda^{(0)}\leq l$. Si $H\neq K$ et si $l<\lambda^{(0)}$, comme $\lambda^{(0)}=L(H^{(0)},K^{(0)})\leq h+k-2f+1$, il résulte de (4.10.2): $h+k-2u-1<h+k-2f+1$, d'où $u\geq f$. Soit $t=u-f$. Soit $(\nu_1,\ldots,\nu_s)$ avec $2\leq \nu_1\leq\cdots\leq\nu_s$, la famille des parties de cardinal supérieur à 1, communes aux partitions de H et K. On a évidemment $u\leq f+s$, donc $t\leq s$. Soit $\rho_1,\ldots,\rho_u$ avec $\rho_1\leq\cdots\leq\rho_u$, les carbinaux respectifs des u parties de $\operatorname{part}(\alpha)\vee\operatorname{part}(\beta)$ distinctes de $\bar{A}$. On a:

$$\begin{aligned}\bar{n}=n-\sum_{1\leq i\leq u}\rho_i&\leq n-f-\sum_{1\leq i\leq t}\rho_{f+i}\\ &\leq n-f-\sum_{1\leq i\leq t}\nu_i=n^{(t)}.\end{aligned}\tag{4.10.3}$$

Soit $\varepsilon^{(t)}=E(H^{(t)},K^{(t)})$.

Si $\varepsilon^{(t)}=-1$, il résulte de (4.10.2) et (4.10.3):

$$\lambda^{(t)}=h+k-2u-1\leq l\leq n^{(t)}.$$

D'aprés la définition de Λ, on a nécessairement $\Lambda\leq\lambda^{(t)}$, donc $\Lambda\leq l$.

Si $\varepsilon^{(t)}=1$, on a: $n^{(t)}<(h+k-2u-1)\delta^{(t)}$, où $\delta^{(t)}=D(H^{(t)},K^{(t)})$. Il résulte de (4.10.2) et (4.10.3): $h+k-2u-1\leq n^{(t)}$. Donc, $\delta^{(t)}\geq 2$. Comme $t\leq s$, $\delta^{(t)}$ divise $\delta^{(s)}=D(H^{(s)},K^{(s)})$, donc $\delta^{(s)}\geq 2$. Comme $H\neq K$, il résulte du Lemme 3.11 que $c(H^{(s)})+c(K^{(s)})\leq n^{(s)}-1$, donc $\lambda^{(s)}\leq n^{(s)}$, et d'après la définition de Λ, $\Lambda\leq\lambda^{(s)}$. Si $t<s$, alors $\lambda^{(s)}\leq h+k-2u-1\leq l$, donc $\Lambda\leq l$. Si $t=s$, alors $[\bar{\alpha}]=H^{(s)}$, $[\bar{\beta}]=K^{(s)}$, et d'après le Théorème 3.2 on a $\lambda^{(s)}\leq l$, donc $\Lambda\leq l$.

Preuve du Théorème 4.3. Si HK contient un l-cycle, on a évidemment $l\equiv\Lambda$ (mod 2), et il résulte de la Proposition 4.10:

$$\Lambda\leq l\leq\min\{n,2n-h-k+1\}.$$

Inversement, si ($H\neq C_1$ ou $K\neq C_1$), alors $\Lambda(H,K)=\Lambda(H^{(0)},K^{(0)})$; si de plus ($H\neq R_f$ ou $K\neq R_f$), alors ($H^{(0)}\neq R_0$ ou $K^{(0)}\neq R_0$), et il résulte des Propositions 4.6. et 4.9 que pour tout l tel que $\Lambda\leq l\leq\min\{n,2n-h-k+1\}$ et $l\equiv\Lambda$ (mod 2), HK contient un l-cycle. Si $H=K=R_f$ avec $f\geq 1$, alors $h=k=\frac{1}{2}(n+f)$, $\min\{n,2n-h-k+1\}=n-f+1$, et il résulte de la Proposition 4.7 que pour tout l tel que $1=\Lambda\leq l\leq n-f+1$ et $l\equiv 1$ (mod 2), R_fR_f contient un l-cycle. Si $H=K=C_1$, alors $2n-h-k+1=1=\Lambda$, et C_1C_1 contient un 1-cycle.

4.11. Corollaire. *Soit dans* Sym(n) *deux classes de conjugaison H et K, et soit $h=c(H)$, $h=c(K)$, $f=\min\{c_1(H), c_1(K)\}$. Pour que HK contienne des cycles, il faut et il suffit que*: $h+k-1 \leqslant n+f$.

Preuve. (1) Si $H=K$, on a toujours $C_1 \subseteqq HH$, et $2(h-f) \leqslant n-f$, donc $2h-1 < n+f$.

(2) Supposons $H \neq K$.

Si $h+k-1 \leqslant n+f$, alors:

$$h+k-2f-1 \leqslant n^{(0)} \leqslant \min\{n, 2n-h-k+1\}. \tag{4.11.1}$$

Soit $\varepsilon^{(0)}=E(H^{(0)}, K^{(0)})$, $\delta^{(0)}=D(H^{(0)}, K^{(0)})$. Si $\varepsilon^{(0)}=-1$, alors $\lambda^{(0)}=h+k-2f-1$ et il résulte de (4.11.1) et du Théorème 4.3 que HK contient des cycles. Si $\varepsilon^{(0)}=1$, alors $n^{(0)} < (h+k-2f-1)\delta^{(0)}$, et il résulte de (4.11.1) que $\delta^{(0)} \geqslant 2$; il résulte alors du Lemme 3.11 que $\lambda^{(0)} \leqslant n^{(0)}$; donc d'après (4.11.1) et le Théorème 4.3, HK contient des cycles.

Si $h+k-1 > n+f$, alors:

$$2n-h-k+1 < n^{(0)} < h+k-2f-1 \leqslant \lambda^{(0)} = \Lambda$$

et il résulte du Théorème 4.3 que HK ne contient pas de cycles.

4.12. Remarque. Soit dans Sym(n) une classe de conjugaison $H \neq R_0$, et soit $h=c(H)$. D'après le Théorème 4.3, une condition nécessaire et suffisante pour que HH contienne tous les cycles de longueur impaire est que: $2n-2h+1 \geqslant n$, i.e. $n-2h \geqslant -1$. $n-2h$ est appelé par Brenner excès orbital (orbital excess) de la classe H. On généralise ainsi un résultat de Brenner [7].

Il est facile de vérifier que les seuls cycles appartenant à R_0R_0 sont les 1-cycles.

Références

[1] E. Bertram, Even permutations as a product of two conjugate cycles, J. Combin. Theory 12 (3) (1972) 368–380.

[2] G. Boccara, Décompositions d'une permutation d'une ensemble fini en produit de deux cycles, Discrete Math. 23 (1978) 189–205.

[3] J.L. Brenner, Covering theorems for nonabelian simple groups II, J. Combin. Theory 14 (1973) 264–269.

[4] J.L. Brenner, R.M. Cranwell, and J. Ridell, Covering theorems for finite nonabelian simple groups V, Pacific J. Math. 58 (1975)55–60.

[5] J.L. Brenner and J. Ridell, Covering theorems for finite nonabelian simple groups VII Asymptotics in the alternating groups, Ars Combinatoria 1 (1976) 77–108.

[6] J.L. Brenner, Covering theorems for finite nonabelian simple groups IX, Ars Combinatoria 4 (1977) 151–176.

[7] J.L. Brenner, Covering theorems for finasigs VIII, Almost all conjugacy classes in A_n have exponent ≤4, J. Austral. Math. Soc. 25(A) (1978) 210–214.

[8] N. Ito, A theorem on the alternating group A_n ($n \geqslant 5$), Math. Japon. 2 (1950–52) 59–60.

[9] O. Ore, Some remarks on commutators, Proc. Amer. Math. Soc 2 (1951) 307–314

[10] Xu, The commutators of the alternating group, Scientia Sinica 14 (1965) 339–342.