Théorie des groupes/*Group Theory*

Relèvements dans $\widetilde{\mathfrak{A}}_n$

Jean-Pierre SERRE

Résumé – Soit $\widetilde{\mathfrak{A}}_n$ ($n \geqslant 4$) l'extension non triviale du groupe alterné $\mathfrak{A}_n$ par $\{\pm 1\}$. Soient $s_1, \ldots, s_k \in \mathfrak{A}_n$ des cycles de longueurs impaires $e_1, \ldots, e_k$ tels que $s_1 \ldots s_k = 1$. Soit $\tilde{s}_i$ le relèvement de s_i dans $\widetilde{\mathfrak{A}}_n$ qui est d'ordre e_i. Le produit $\tilde{s}_1 \ldots \tilde{s}_k$ est égal à ± 1. On donne une formule permettant de calculer ce produit lorsque les s_i engendrent un sous-groupe transitif de $\mathfrak{A}_n$ et que $\Sigma (e_i - 1) = 2n - 2$: on a $\tilde{s}_1 \ldots \tilde{s}_k = 1$ si et seulement si $e_1 \ldots e_k \equiv \pm 1 \pmod 8$.

$\widetilde{\mathfrak{A}}_n$-liftings

Abstract – *Let $\widetilde{\mathfrak{A}}_n$ ($n \geqslant 4$) be the non split extension of the alternating group $\mathfrak{A}_n$ by $\{\pm 1\}$. Let $s_1, \ldots, s_k \in \mathfrak{A}_n$ be cycles of odd order $e_1, \ldots, e_k$ such that $s_1 \ldots s_k = 1$. Let $\tilde{s}_i$ be the unique lifting of s_i in $\widetilde{\mathfrak{A}}_n$ which has order e_i. Assume that the s_i generate a transitive subgroup of $\mathfrak{A}_n$ and that $\Sigma (e_i - 1)$ is equal to $2n - 2$. We then show that $\tilde{s}_1 \ldots \tilde{s}_k = 1$ if and only if $e_1 \ldots e_k \equiv \pm 1 \pmod 8$.*

1. NOTATIONS. – Soit s un élément du groupe symétrique $\mathfrak{S}_n$, produit de cycles à supports disjoints c_α, d'ordres e_α. On pose :

$$v(s) = \Sigma (e_\alpha - 1). \tag{1}$$

Si s est d'ordre impair, on définit $\omega(s) \in \mathbf{Z}/2\,\mathbf{Z}$ par :

$$\omega(s) \equiv \Sigma (e_\alpha^2 - 1)/8 \equiv (\Pi e_\alpha^2 - 1)/8 \pmod 2. \tag{2}$$

On a $\omega(s) = 0$ si et seulement si $\Pi e_\alpha \equiv \pm 1 \pmod 8$.

On note $\widetilde{\mathfrak{S}}_n$ (*cf.* [8]) l'extension de $\mathfrak{S}_n$ par le groupe à deux éléments $\{\pm 1\}$ caractérisée par la propriété suivante : sa restriction au sous-groupe d'ordre 2 (resp. 4) engendré par une transposition (resp. par le produit de deux transpositions à supports disjoints) est triviale (resp. non triviale). On a $\widetilde{\mathfrak{S}}_n = 2^+ \mathrm{S}_n$, avec les notations de l'*Atlas* [2].

L'image réciproque de $\mathfrak{A}_n$ dans $\widetilde{\mathfrak{S}}_n$ est notée $\widetilde{\mathfrak{A}}_n$; si $n \leqslant 3$, on a $\widetilde{\mathfrak{A}}_n \simeq \mathfrak{A}_n \times \{\pm 1\}$; si $n \geqslant 4$, $\widetilde{\mathfrak{A}}_n$ est l'unique extension non triviale de $\mathfrak{A}_n$ par $\{\pm 1\}$.

Si $s \in \mathfrak{A}_n$ est d'ordre impair, on notera $\tilde{s}$ l'unique relèvement de s dans $\widetilde{\mathfrak{A}}_n$ qui a le même ordre que s; l'autre relèvement $-\tilde{s}$ a un ordre double de celui de s. On posera :

$$s' = (-1)^{\omega(s)} \tilde{s}, \tag{3}$$

où $\omega(s)$ est défini par (2) ci-dessus.

Si s est produit de cycles c_α à supports disjoints, d'ordres e_α, les $\tilde{c}_\alpha$ commutent entre eux et l'on a

$$\tilde{s} = \Pi \tilde{c}_\alpha, \qquad s' = \Pi c'_\alpha. \tag{4}$$

2. ÉNONCÉ DU THÉORÈME. – Soient $s_1, \ldots, s_k \in \mathfrak{S}_n$ tels que :

$$s_1 \ldots s_k = 1, \tag{5}$$

(6) le sous-groupe $\langle s_1, \ldots, s_k \rangle$ de $\mathfrak{S}_n$ engendré par les s_i est transitif.

On sait (*cf.* par exemple [3]) que cela entraîne :

$$\Sigma v(s_i) \geqslant 2n - 2. \tag{7}$$

[Les s_i définissent un revêtement X de degré n de la droite projective $\mathbf{P}_1(\mathbf{C})$, ramifié en k points; d'après (6), ce revêtement est connexe; son genre g est $1 - n + (1/2)\Sigma v(s_i)$; comme g est $\geqslant 0$, on en déduit (7).]

Note présentée par Jean-Pierre SERRE.

0764-4442/90/03110477 $ 2.00

Dans la suite, on s'intéressera au cas où il y a égalité dans (7), autrement dit :

$$\Sigma v(s_i) = 2n-2. \tag{8}$$

(Cela revient à dire que le genre g de la surface de Riemann X est 0.)

Si les s_i sont des éléments de $\mathfrak{A}_n$ d'ordres impairs, (5) entraîne :

$$\tilde{s}_1 \ldots \tilde{s}_k = \pm 1 \quad \text{dans } \tilde{\mathfrak{A}}_n. \tag{9}$$

Lorsque la condition (8) est satisfaite, on peut préciser le signe de (9). On a en effet le résultat suivant, qui sera démontré au n° 7 :

THÉORÈME. — *Soient* $s_1, \ldots, s_k \in \mathfrak{A}_n$ *des éléments d'ordres impairs satisfaisant aux conditions* (5), (6) *et* (8) *ci-dessus. On a* :

$$\tilde{s}_1 \ldots \tilde{s}_k = (-1)^{\omega}, \quad \text{où} \quad \omega = \Sigma \omega(s_i) \in \mathbf{Z}/2\mathbf{Z}. \tag{10}$$

Il revient au même de dire que :

$$s'_1 \ldots s'_k = 1 \quad \text{dans } \tilde{\mathfrak{A}}_n, \tag{11}$$

puisque $s'_i = (-1)^{\omega(s_i)} \tilde{s}_i$, *cf.* (3).

Exemple. — Supposons que les s_i soient des cycles d'ordre 3 engendrant $\mathfrak{A}_n$, auquel cas (8) signifie que $k = n-1$. Comme $\omega(s_i) = 1$ pour tout i, la formule (10) dit que *le produit des* $\tilde{s}_i$ *est égal à* 1 *si et seulement si n est impair.* Ce résultat m'a été suggéré par M. Fried en 1989; depuis, M. Fried en a obtenu une démonstration différente, et qui donne davantage d'informations, *cf.* [4].

3. APPLICATION AUX REVÊTEMENTS RAMIFIÉS DE LA DROITE PROJECTIVE. — Soient $s_1, \ldots, s_k$ des éléments de $\mathfrak{A}_n$ d'ordres impairs satisfaisant à (5) et (6). Soit $G = \langle s_1, \ldots, s_k \rangle$ le sous-groupe de $\mathfrak{A}_n$ engendré par les s_i, et soit $\tilde{G}$ son image réciproque dans $\tilde{\mathfrak{A}}_n$. Soient d'autre part $Q_1, \ldots, Q_k$ des points de $\mathbf{P}_1(\mathbf{C})$, deux à deux distincts. Ces données définissent comme on sait un revêtement galoisien connexe $X^{gal} \to \mathbf{P}_1(\mathbf{C})$, de groupe G, non ramifié en dehors des Q_i (les groupes d'inertie au-dessus des Q_i étant les conjugués des $\langle s_i \rangle$). On peut se demander s'il existe un *revêtement quadratique non ramifié*

$$\varepsilon : \tilde{X}^{gal} \to X^{gal},$$

et une action de $\tilde{G}$ sur $\tilde{X}^{gal}$ telle que :

(*a*) l'élément -1 de $\tilde{G}$ agit sur $\tilde{X}^{gal}$ comme l'unique automorphisme non trivial du revêtement ε;

(*b*) si $t \in \tilde{G}$ a pour image $s \in G$, on a $\varepsilon \circ t = s \circ \varepsilon$.

On voit facilement qu'*un tel revêtement* ε *existe si et seulement si* $\Pi \tilde{s}_i = 1$. Si (8) est satisfait, le théorème ci-dessus dit que cela se produit si et seulement si $\Sigma \omega(s_i) = 0$ dans $\mathbf{Z}/2\mathbf{Z}$. Il en est ainsi par exemple pour les extensions à groupe de Galois $\mathfrak{A}_n$, n impair, construites par J.-F. Mestre [5], dans lesquelles les s_i sont des cycles d'ordre 3, *cf.* n° 2. (Pour une autre démonstration de ce résultat, et une construction explicite de $\tilde{X}^{gal}$, *voir* L. Schneps [7].)

4. GÉNÉRALISATION. — On peut se demander ce qui se passe lorsqu'on supprime la condition (8), *i.e.* lorsque le genre g de la surface de Rieman X du n° 2 est >0. Des exemples simples montrent que le produit des s'_i n'est pas toujours 1. On peut toutefois calculer ce produit par la méthode suivante :

Notons π la projection $X \to \mathbf{P}_1(\mathbf{C})$; on a $\deg(\pi) = n$. Si $x \in X$, soit $e(x)$ l'indice de ramification de π en x; les $e(x)$ sont impairs (ce sont les ordres des cycles composant

les s_i). Définissons un diviseur θ de X par :

$$\theta = -\pi^*(a) + \sum_{x \in X} \frac{e(x)-1}{2} x, \tag{12}$$

où a est un point quelconque de $\mathbf{P}_1(\mathbf{C})$. La classe c du diviseur θ ne dépend pas du choix de a, et $2c$ n'est autre que la *classe canonique* de X. Autrement dit, c est une *thêta-caractéristique* de X, *cf.* [1], [6]. Soit $i(c) \in \mathbf{Z}/2\mathbf{Z}$ la *parité* de cette classe (*loc. cit.*). La formule qui généralise (11) est :

$$s'_1 \ldots s'_k = (-1)^{i(c)}, \tag{13}$$

cf. [9], n° 6. [Lorsque $g=0$, X n'a qu'une seule thêta-caractéristique et sa parité est 0; la formule (13) redonne donc bien (11).]

5. PRÉLIMINAIRES À LA DÉMONSTRATION DU THÉORÈME : CALCULS SPINORIELS. — Soit C_n l'algèbre de Clifford de l'espace euclidien $\mathbf{R}^n$. On sait que $\tilde{\mathfrak{S}}_n$ peut être plongé dans le groupe multiplicatif C_n^*. Rappelons comment se fait ce plongement :

L'algèbre C_n est engendrée par des éléments $x_1, \ldots, x_n$ soumis aux relations $x_i^2 = 1$, $x_i x_j = -x_j x_i$ si $i \neq j$. A tout couple ordonné (i, j), $i \neq j$, associons l'élément

$$[ij] = \frac{1}{\sqrt{2}}(x_i - x_j)$$

de C_n^*. On a $[ij]^2 = 1$ et $[ij] = -[ji]$. Le sous-groupe de C_n^* engendré par les $[ij]$ peut être identifié à $\tilde{\mathfrak{S}}_n$; la projection $\tilde{\mathfrak{S}}_n \to \mathfrak{S}_n$ associe à $[ij]$ la transposition (ij).

LEMME 1. — *Soit $s = (i_1 i_2 \ldots i_e)$ un cycle d'ordre impair e. On a :*

$$s' = [i_1 i_e][i_1 i_{e-1}] \ldots [i_1 i_2] \quad \textit{dans} \quad \tilde{\mathfrak{S}}_n. \tag{14}$$

Posons $t = [i_1 i_e][i_1 i_{e-1}] \ldots [i_1 i_2]$. L'image de t dans $\mathfrak{S}_n$ est $(i_1 i_e)(i_1 i_{e-1}) \ldots (i_1 i_2)$, c'est-à-dire s. On a donc $t = \varepsilon \tilde{s}$, avec $\varepsilon = \pm 1$, et tout revient à voir que $\varepsilon = 1$ si $e \equiv \pm 1 \pmod 8$ et $\varepsilon = -1$ si $e \equiv \pm 3 \pmod 8$, *cf.* [2], p. 236.

On peut pour cela supposer que $i_1 = 1$, $i_2 = 2, \ldots, i_e = e$, et que $e = n$. Écrivons n sous la forme $n = 1 + 2m$. On a

$$t = 2^{-m}(x_1 - x_n)(x_1 - x_{n-1}) \ldots (x_1 - x_2) \quad \text{dans } C_n.$$

Le terme constant de t est $2^{-m}(x_1 x_1)^m = 2^{-m}$. Sa trace dans la représentation spinorielle de $\tilde{\mathfrak{A}}_n$, qui est de dimension 2^m, est donc 1. D'autre part, il est facile de voir que la trace de $\tilde{s}$ est $\prod_{j=1}^{j=m} (2\cos(2\pi j/n))$, c'est-à-dire 1 si $m \equiv 0,3 \pmod 4$ et -1 si $m \equiv 1,2 \pmod 4$. En comparant, on obtient le résultat cherché.

LEMME 2. — *Soient s un cycle d'ordre impair e, et soit u un cycle d'ordre 3. Supposons que l'intersection des supports de s et de u ait un seul élément. Le produit su est alors un cycle d'ordre $e+2$ et l'on a :*

$$(su)' = s'u' \quad \textit{dans} \quad \tilde{\mathfrak{A}}_n. \tag{15}$$

Soit i_1 le point d'intersection des supports des cycles s et u.

On peut écrire ces cycles sous la forme :

$$s = (i_1 i_e) \ldots (i_1 i_2), \qquad u = (i_1 j)(i_1 k),$$

où $i_1, i_2, \ldots, i_e, j, k$ sont deux à deux distincts. On a :

$$su = (i_1 i_e) \ldots (i_1 i_2)(i_1 j)(i_1 k) = (i_1 k j i_2 \ldots i_e),$$

ce qui montre que su est un cycle de longueur $e+2$. D'après le lemme 1 appliqué à s, u et su, on a :

$$s' = [i_1\, i_e] \ldots [i_1\, i_2], \qquad u' = [i_1\, j]\,[i_1\, k],$$
$$(su)' = [i_1\, i_e] \ldots [i_1\, i_2]\,[i_1\, j]\,[i_1\, k],$$

d'où (15).

LEMME 3. — *Soient s un cycle d'ordre impair e, et soit u un cycle d'ordre* 3. *Supposons que l'intersection des supports de s et de u ait deux éléments. Le produit su est alors produit de deux cycles w_1 et w_2, à supports disjoints, d'ordres e_1 et e_2 tels que $e_1 + e_2 = e+1$. Si e_1 et e_2 sont impairs, on a* :

$$(su)' = w_1' w_2' = s' u' \quad \textit{dans } \mathfrak{A}_n. \tag{16}$$

Soient i_1 et j les deux points d'intersection des supports de s et de u, choisis de telle sorte que $u(i_1) = j$. On peut écrire s et u sous la forme :

$$s = (i_1\, i_e) \ldots (i_1\, i_2), \qquad u = (i_1\, k)\,(i_1\, j),$$

avec $j = i_r$ pour un indice r tel que $2 \leqslant r \leqslant e$. Supposons r distinct de 2 et e (les cas $r=2$ et $r=e$ se traitent de façon analogue). On a alors :

$$su = (i_1\, i_e) \ldots (i_1\, i_{r+1})\,(i_1\, j)\,(i_1\, i_{r-1}) \ldots (i_1\, i_2)\,(i_1\, k)\,(i_1\, j).$$

Si l'on pose :

$$w_1 = (i_1\, i_e) \ldots (i_1\, i_{r+1}) = (i_1\, i_{r+1} \ldots i_e),$$
$$z = (i_1\, i_{r-1}) \ldots (i_1\, i_2)\,(i_1\, k) = (i_1\, k i_2 \ldots i_{r-1}),$$
$$w_2 = (i_1\, j)\, z\, (i_1\, j) = (j k i_2 \ldots i_{r-1}),$$

on a $su = w_1 w_2$; de plus w_1 et w_2 sont des cycles à supports disjoints d'ordres $e_1 = e+1-r$ et $e_2 = r$. Si r est impair, le lemme 1, appliqué à s, u, w_1, w_2, donne :

$$s' = [i_1\, i_e] \ldots [i_1\, i_2], \qquad u' = [i_1\, k]\,[i_1\, j],$$
$$w_1' = [i_1\, i_e] \ldots [i_1\, i_{r+1}], \qquad z' = [i_1\, i_{r-1}] \ldots [i_1\, i_2]\,[i_1\, i_k],$$
$$w_2' = [i_1\, j]\, z'\, [i_1\, j] \;=\; [i_1\, j]\,[i_1\, i_{r-1}] \ldots [i_1\, i_2]\,[i_1\, i_k]\,[i_1\, j],$$

d'où aussitôt la formule (16).

6. PRÉLIMINAIRES À LA DÉMONSTRATION DU THÉORÈME : ACTION DU GROUPE DES TRESSES. — Soit $\boldsymbol{s} = (s_1, \ldots, s_k)$ une suite d'éléments d'un groupe G. Si $1 \leqslant i < k$, soit $T_i \boldsymbol{s}$ la suite obtenue en remplaçant (s_i, s_{i+1}) par $(s_{i+1}, s_{i+1}^{-1} s_i s_{i+1})$:

$$T_i \boldsymbol{s} = (s_1, \ldots, s_{i-1}, s_{i+1}, s_{i+1}^{-1} s_i s_{i+1}, s_{i+2}, \ldots, s_k). \tag{17}$$

Si l'on pose $P(\boldsymbol{s}) = s_1 \ldots s_k$, on a évidemment $P(T_i \boldsymbol{s}) = P(\boldsymbol{s})$.

Si les s_i sont des éléments d'ordres impairs de $\mathfrak{A}_n$, et si l'on note $P'(\boldsymbol{s})$ le produit $s_1' \ldots s_k'$ dans $\mathfrak{A}_n$, on a :

$$P'(T_i \boldsymbol{s}) = P'(\boldsymbol{s}); \tag{18}$$

cela résulte de la formule $(yxy^{-1})' = y' x' y'^{-1}$, appliquée à $y = s_{i+1}^{-1}$ et $x = s_i$.

En utilisant (18), on voit que, *si la formule* (11) *est vraie pour* $\boldsymbol{s}$, *elle l'est aussi pour* $T_i \boldsymbol{s}$, et inversement.

Remarque. — Les T_i définissent une action du « groupe des tresses colorées à k brins » sur l'ensemble des suites $\boldsymbol{s}$ à k éléments. Je dois à M. Fried l'idée d'utiliser cette action pour démontrer le théorème du n° 2.

7. DÉMONSTRATION DU THÉORÈME. — Il s'agit de prouver la formule (11). On raisonne par récurrence sur n; le cas $n \leqslant 3$ est immédiat; on peut donc supposer $n \geqslant 4$. Vu (4), on peut aussi supposer que les s_i sont des *cycles*, dont les ordres e_i sont >1. On a $3 \leqslant e_i \leqslant n$.

Pour n fixé, on raisonne par *récurrence descendante sur* $N = e_1 + e_k$. On a $N \leqslant 2n$. D'après (8), on ne peut avoir $N = 2n$ que si $k = 2$ et si s_1 et s_2 sont des cycles d'ordre n avec $s_1 s_2 = 1$; il est alors clair que $s'_1 s'_2 = 1$, ce qui démontre le théorème dans ce cas. On peut donc supposer que $N < 2n$, donc que e_1 ou e_k est $<n$; quitte à remplacer $(s_1, \ldots, s_k)$ par $(s_k^{-1}, \ldots, s_1^{-1})$, on peut même supposer que $e_1 < n$.

On peut aussi supposer que *les cycles* $s_2, \ldots, s_{k-1}$ *sont d'ordre* 3. En effet, si l'un de ces cycles s_i est d'ordre $e_i > 3$, on peut l'écrire comme produit $s_i = su$, où s est un cycle d'ordre $e_i - 2$ et u un cycle d'ordre 3, l'intersection des supports de ces cycles ayant un seul élément [*e.g.* $(12 \ldots 7) = (12 \ldots 5)(567)$]. D'après (15), on a $s'_i = s' u'$. On peut donc remplacer $(s_1, \ldots, s_k)$ par $(s_1, \ldots, s_{i-1}, s, u, s_{i+1}, \ldots, s_k)$ sans changer la formule à démontrer. En itérant ce procédé, on se ramène bien au cas où $e_i = 3$ pour $1 < i < k$.

Soit S_1 le support du cycle s_1. Comme $\mathrm{Card}(S_1) = e_1 < n$, S_1 n'est pas stable par le groupe $G = \langle s_1, \ldots, s_k \rangle$ puisque ce groupe est supposé transitif. Mais G est engendré par $s_1, \ldots, s_{k-1}$ et s_1 stabilise S_1. Il existe donc un indice i, compris entre 2 et $k-1$, tel que s_i ne stabilise pas S_1. Après application successive des opérateurs $T_{i-1}, T_{i-2}, \ldots, T_2$ (*cf.* n° 6) on peut supposer que $i = 2$. Le support S_2 de s_2 a trois éléments. Comme s_2 ne stabilise pas S_1 on a $\mathrm{Card}(S_1 \cap S_2) = 1$ ou 2.

Distinguons alors deux cas :

(*a*) *L'ensemble* $S_1 \cap S_2$ *a un seul élément.* — Le produit $w = s_1 s_2$ est alors un cycle d'ordre $e_1 + 2$, *cf.* lemme 2. On peut appliquer l'hypothèse de récurrence à la suite $(w, s_3, \ldots, s_k)$. En effet :

le produit $w s_3 \ldots s_k$ est égal à 1;

on a $v(w) + v(s_3) + \ldots + v(s_k) = 2n - 2$ puisque $v(w) = e_1 + 1 = v(s_1) + v(s_2)$;

le groupe $\langle w, s_3, \ldots, s_k \rangle$ est transitif (toute partie de $[1, n]$ stable par w l'est aussi par s_1 et s_2);

la somme de l'ordre de w et de l'ordre de s_k est égale à $N + 2$, où $N = e_1 + e_k$.

On a donc $w' s'_3 \ldots s'_k = 1$. Comme $w' = s'_1 s'_2$ d'après (15), on a bien $s'_1 s'_2 \ldots s'_k = 1$, ce qui démontre le théorème dans le cas considéré.

(*b*) *L'ensemble* $S_1 \cap S_2$ *a deux éléments.* — Dans ce cas $s_1 s_2$ est produit de deux cycles w_1 et w_2, à supports disjoints W_1 et W_2 tels que $W_1 \cup W_2 = S_1 \cup S_2$, *cf.* lemme 3. On a $w_1 w_2 s_3 \ldots s_k = 1$, et $v(w_1) + v(w_2) = v(s_1) + v(s_2) - 2$, d'où :

$$v(w_1) + v(w_2) + v(s_3) + \ldots + v(s_k) \quad = \quad 2n - 4. \tag{19}$$

Vu (7), cela montre que *le groupe* $H = \langle w_1, w_2, s_3, \ldots, s_k \rangle$ *n'est pas transitif* : il a au moins deux orbites. Mais, si X est une orbite de H dans $[1, n]$, il est clair que X rencontre $W_1 \cup W_2$ (sinon, X serait stable par s_1 et s_2, donc par G, ce qui est impossible). Il résulte de là que *l'action de* H *sur* $[1, n]$ *a deux orbites* X_1 *et* X_2, *avec* $W_1 \subset X_1$ *et* $W_2 \subset X_2$. Soit I_1 (resp. I_2) l'ensemble des i, avec $3 \leqslant i \leqslant k$, tels que le support de s_i soit contenu dans X_1 (resp. X_2). Munissons I_1 et I_2 de la relation d'ordre induite par celle de $[3, k]$; cela donne un sens aux produits $\prod_{i \in I_1} s_i$ et $\prod_{i \in I_2} s_i$. On a :

$$w_1 \prod_{i \in I_1} s_i = 1 \qquad \text{et} \qquad w_2 \prod_{i \in I_2} s_i = 1. \tag{20}$$

Si $\mathrm{Card}(X_1)=n_1$ et $\mathrm{Card}(X_2)=n_2$, on a, d'après (7) appliqué aux groupes symétriques $\mathfrak{S}_{n_1}$ et $\mathfrak{S}_{n_2}$:

$$v(w_1)+\sum_{i\in I_1} v(s_i) \geqslant 2n_1-2 \tag{21}$$

et

$$v(w_2)+\sum_{i\in I_2} v(s_i) \geqslant 2n_2-2. \tag{22}$$

En comparant à (19), et en tenant compte de $n=n_1+n_2$, on voit qu'il y a *égalité* dans (21) et (22). Cela montre en particulier que $v(w_1)$ et $v(w_2)$ sont pairs, *i.e.* que w_1 et w_2 sont d'ordres impairs [ce qui résulte aussi de (20)]. D'après (16), on a

$$w'_1 w'_2 = s'_1 s'_2. \tag{23}$$

D'autre part, le fait qu'il y ait égalité dans (21), joint à l'hypothèse de récurrence sur n, montre que :

$$w'_1 \prod_{i\in I_1} s'_i = 1, \tag{24}$$

cette égalité ayant lieu dans $\mathfrak{A}_{n_1}$, donc aussi dans $\mathfrak{A}_n$. De même :

$$w'_2 \prod_{i\in I_2} s'_i = 1 \quad \text{dans } \mathfrak{A}_n. \tag{25}$$

De plus, tous les facteurs de (24) commutent à ceux de (25). En faisant le produit de (24) et (25), et en réarrangeant les termes, on obtient

$$w'_1 w'_2 s'_3 \ldots s'_k = 1,$$

d'où d'après (23) :

$$s'_1 s'_2 s'_3 \ldots s'_k = 1,$$

ce qui achève la démonstration.

Note remise et acceptée le 28 août 1990.

Références bibliographiques

[1] M. F. Atiyah, Riemann surfaces and spin structures, *Ann. E.N.S.* (4), 4, 1971, p. 47-62 (= *Coll. Works*, III, n° 75).

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker et R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[3] W. Feit, R. Lyndon et L. Scott, A remark about permutations, *J. Comb. Theory*, 18, 1975, p. 234-235.

[4] M. Fried, *Alternating groups and lifting invariants*, prépublication, Irvine, 1989.

[5] J.-F. Mestre, Extensions régulières de **Q** (T) de groupe de Galois $\mathfrak{A}_n$, *J. Algebra*, 131, 1990, p. 483-495.

[6] D. Mumford, Theta-characteristics of an algebraic curve, *Ann. E.N.S.* (4), 4, 1971, p. 181-192.

[7] L. Schneps, Explicit construction of extensions of $K(t)$ of Galois group $\mathfrak{A}_n$ for n odd, *J. Algebra* (à paraître).

[8] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helv.* 59, 1984, p. 651-676 (= *Oe.* 131).

[9] J.-P. Serre, Revêtements à ramification impaire et thêta-caractéristiques, *C. R. Acad. Sci. Paris*, 311, série I, 1990 (à paraître).

Collège de France, 75231 *Paris Cedex* 05.