SUR UNE GÉNÉRALISATION DU TRANSFERT EN THÉORIE DES GROUPES

par P. CARTIER (Strasbourg)

Dans cette note, nous indiquons une construction générale d'homomorphismes de groupes, dans le cas de deux groupes opérant sur un même ensemble fini. Nous montrons ensuite que cette construction redonne celle du transfert dans un cas particulier, et nous indiquons diverses autres spécialisations, liées à la signature d'une permutation, au symbole de Legendre-Jacobi ou aux systèmes de racines. Cette note a intérêt à être lue en même temps que deux autres notes [2] et [3] qui paraissent dans le même volume.

1. On considère les données suivantes:

a) un ensemble fini X;

b) un groupe G opérant à gauche sur X;

c) un groupe *commutatif* A opérant à droite sur X.

Nous notons indistinctement e l'élément neutre de G ou celui de A. Dire que G opère à gauche sur X signifie qu'à tout élément g de G, et tout élément x de X, on a fait correspondre un élément gx de X et que l'on a $g(g'x) = (gg')x$ et $ex = x$ pour g, g' dans G et x dans X. De manière analogue, on a défini xa pour x dans X et a dans A et l'on a les relations $(xa)a' = x(aa')$ et $xe = x$.

On fait les deux hypothèses suivantes:

(A) *On a* $(gx)a = g(xa)$ *pour* g *dans* G, x *dans* X *et* a *dans* A.

(B) *Pour tout* x *dans* X *et tout* $a \neq e$ *dans* A, *on a* $xa \neq x$.

La propriété (B) entraîne la suivante, d'énoncé plus fort:

(B′) *Si* a *et* a' *sont deux éléments distincts de* A, *on a* $xa \neq xa'$.
En effet, on a $a'^{-1}a \neq e$, d'où $xa = (xa')(a'^{-1}a) \neq xa'$ d'après (B).

Comme il est usuel, on appelle *orbite* de A dans X toute partie de X qui est l'ensemble des transformés x_0a d'un élément fixe x_0 de X par tous les éléments a de A. Nous dirons simplement « orbite » pour « orbite de A dans X ». Il est bien connu que deux orbites distinctes sont disjointes, et

que X est réunion des orbites. Nous appellerons *section* toute partie S de X qui rencontre chaque orbite en un point et un seul.

2. Nous associons maintenant à deux sections S et S' un élément $d(S, S')$ de A qui mesure en quelque sorte leur « distance ». Il est commode de numéroter les orbites sous la forme $P_1, \ldots, P_m$. Une section S est alors de la forme $\{s_1, \ldots, s_m\}$ avec $s_i \in P_i$ pour $1 \leqq i \leqq m$; représentons de même la section S' sous la forme $\{s_1', \ldots, s_m'\}$ avec $s_i' \in P_i$ pour $1 \leqq i \leqq m$. Comme s_i et s_i' appartiennent à la même orbite, il existe un élément a_i de A tel que $s_i' = s_i a_i$ et cet élément est unique d'après (B'). Nous posons alors $d(S, S') = a_1 \ldots a_m$. Comme le groupe A est commutatif, cette définition est indépendante de toute numérotation des orbites.

Voici le formulaire correspondant à cette notion:

$$d(S, S) = e \tag{1}$$

$$d(S', S) = d(S, S')^{-1} \tag{2}$$

$$d(S, S'') = d(S, S')\, d(S', S''). \tag{3}$$

Etablissons par exemple la formule (3). Nous représentons les sections S, S' et S'' sous la forme

$$S = \{s_1, \ldots, s_m\}, \quad S' = \{s_1', \ldots, s_m'\}, \quad S'' = \{s_1'', \ldots, s_m''\},$$

et nous choisissons des éléments a_i et a_i' de A tels que $s_i' = s_i a_i$ et $s_i'' = s_i' a_i'$ pour i compris entre 1 et m. On a alors $s_i'' = s_i (a_i a_i')$, d'où

$$d(S, S') = a_1 \ldots a_m, \quad d(S', S'') = a_1' \ldots a_m', \quad d(S, S'') = (a_1 a_1') \ldots (a_m a_m'),$$

et la formule (3) résulte de la commutativité du groupe A.

3. Jusqu'à présent, le groupe G n'a joué aucun rôle. En utilisant l'hypothèse (A), on voit que tout élément g de G transforme une orbite en une orbite, donc une section en une section. Nous allons déduire de ce fait la relation

$$d(gS, gS') = d(S, S'). \tag{4}$$

Nous conservons les mêmes notations que plus haut, et nous posons $Q_i = gP_i$ pour $1 \leqq i \leqq m$. Il est clair que l'on peut énumérer les orbites sous la forme $Q_1, \ldots, Q_m$ et que l'on a

$$gS = \{gs_1, \ldots, gs_m\}, \qquad gS' = \{gs_1', \ldots, gs_m'\};$$

de plus, gs_i et gs_i' appartiennent à Q_i, et de $s_i' = s_i a_i$, on déduit $gs_i' = (gs_i)\, a_i$ d'après (A). On a donc $d(gS, gS') = a_1 \ldots a_m = d(S, S')$.

Nous en arrivons au point essentiel, à savoir l'*existence d'un homomorphisme Φ de G dans A tel que l'on ait $d(gS, S) = \Phi(g)$ pour tout g dans G et toute section S.* Considérons deux sections S et S'; on a

$$d(gS, S) = d(gS, gS')\, d(gS', S')\, d(S', S)$$

d'après (3), on a $d(gS, gS') = d(S, S')$ d'après (4) et $d(S', S) = d(S, S')^{-1}$ d'après (2). On a donc $d(gS, S) = d(S, S')\, d(gS', S')\, d(S, S')^{-1}$, et comme le groupe A est commutatif, on en conclut $d(gS, S) = d(gS', S')$. Notons $\Phi(g)$ la valeur commune de $d(gS, S)$ pour toutes les sections S. Si g' est un autre élément de G, on a $\Phi(g) = d(gS', S')$ avec $S' = g'S$, d'où

$$\Phi(g)\,\Phi(g') = d(gg'S, g'S)\, d(g'S, S) = d(gg'S, S) = \Phi(gg') \tag{5}$$

d'après (3). On a prouvé que Φ est un homomorphisme de G dans A.

4. Montrons comment la définition usuelle du transfert s'obtient par spécialisation de la construction précédente. On considère [1]) un groupe fini G et un sous-groupe H de G; on note H' le groupe dérivé de H, engendré par les commutateurs $aba^{-1}b^{-1}$ de deux éléments a et b de H. On note A le groupe quotient H/H' et X l'ensemble G/H' des classes de la forme gH' avec g dans G. On fait opérer G à gauche sur X de la manière usuelle. De plus, pour h dans H, on a $hH' = H'h$; par suite, si $x = gH'$ est un élément de X, on a $xh = ghH'$ et le sous-ensemble xh de G ne dépend que de la classe $a = hH'$. On définit donc une action à droite de A sur X en posant $xa = ghH'$ pour $x = gH'$ et $a = hH'$. La vérification des hypothèses (A) et (B) du n° 1 est immédiate.

Pour calculer Φ, on choisit un système de représentants $g_1, \ldots, g_m$ de G modulo H; on pose $s_1 = g_1H', \ldots, s_m = g_mH'$. Alors $S = \{s_1, \ldots, s_m\}$ est une section au sens des n^{os} précédents. Soit g dans G; comme les éléments $gg_1, \ldots, gg_m$ forment un système de représentants de G modulo H, il existe donc une permutation σ de $\{1, 2, \ldots, m\}$ et des éléments $h_1, \ldots, h_m$ de H tels que l'on ait

$$gg_i = g_{\sigma(i)}\, h_i \quad \text{pour} \quad 1 \leqq i \leqq m\,. \tag{6}$$

Posons $a_i = h_iH'$; on a alors $gs_i = s_{\sigma(i)}\, a_i$, d'où

$$gS = \{gs_1, \ldots, gs_m\} = \{s_{\sigma(1)}\, a_1, \ldots, s_{\sigma(m)}\, a_m\} = \{s_1 a_{\sigma^{-1}(1)}, \ldots, s_m a_{\sigma^{-1}(m)}\}.$$

[1]) On remarquera que l'on définit d'habitude le transfert dans le cas d'un groupe G et d'un sous-groupe H d'indice fini de G, alors que notre construction ne semble s'appliquer qu'au cas où G est fini. En fait, nous n'utilisons nulle part le fait que l'ensemble X est fini, mais seulement le fait que A n'a qu'un nombre fini d'orbites dans X. La construction donnée dans ce numéro donne donc le transfert dans le cas le plus général.

Par suite, $\Phi(g) = a_{\sigma^{-1}(1)} \dots a_{\sigma^{-1}(m)} = a_1 \dots a_m$ est la classe de $h_1 \dots h_m$ modulo H'. On reconnaît là la définition du transfert Φ de G dans le groupe $A = H/H'$ (voir par exemple [4], chapitre 14.2).

5. Comme deuxième cas particulier, nous expliciterons celui où le groupe A a deux éléments que nous noterons e et t, e étant bien entendu l'élément neutre. Nous allons prouver que $\Phi(g)$ *est égal à* e *ou* t *selon que la permutation de* X *définie par* g *est paire ou impaire.*

Soit g un élément de G. Selon la définition usuelle, un *cycle* de la permutation de X définie par g est une partie de X qui se compose des transformés $g^n x_0$ d'un élément fixe x_0 de X par les puissances (positives ou négatives) de g. Il est bien connu que les cycles forment une partition de X. De plus, la relation $(g^n x)\, t = g^n (xt)$ montre que t transforme un cycle en un cycle. Comme on a $t^2 = e$, on peut donc énumérer les cycles sous la forme

$$C_1, \dots, C_p, D_1, \dots, D_q, D_1', \dots, D_q'$$

où chaque C_i est invariant par t et où t échange D_j et D_j' pour $1 \leqq j \leqq q$.

Examinons le cas d'un cycle invariant C_i. Notons $n(i)$ le nombre d'éléments de C_i et choisissons un élément x_i de C_i. Alors C_i se compose des éléments distincts $x_i, gx_i, g^2 x_i, \dots, g^{n(i)-1} x_i$; comme C_i est invariant par t et qu'on a $x_i t \neq x_i$, il existe un entier $m(i)$ compris entre 1 et $n(i) - 1$ tel que $x_i t = g^{m(i)} x_i$. On a alors

$$x_i = (x_i t)\, t = (g^{m(i)} x_i)\, t = g^{m(i)}(x_i t) = g^{m(i)}(g^{m(i)} x_i) = g^{2m(i)} x_i ,$$

et par suite, $2m(i)$ est multiple de $n(i)$; comme on a $0 < m(i) < n(i)$, la seule possibilité est $2m(i) = n(i)$. Pour tout entier k compris entre 0 et $m(i) - 1$, on a

$$(g^k x_i)\, t = g^k (x_i t) = g^k (g^{m(i)} x_i) = g^{m(i)+k} x_i ;$$

on peut par suite partager C_i en deux parties C_i^+ et C_i^- selon le schéma

$$\begin{aligned} C_i^+ &= \{ x_i, gx_i, g^2 x_i, \dots, g^{m(i)-1} x_i \} \\ C_i^- &= \{ x_i t, (gx_i)\, t, (g^2 x_i)\, t, \dots, (g^{m(i)-1} x_i)\, t \} . \end{aligned}$$

On a donc $C_i^- = C_i^+ t$ et

$$gC_i^+ = \{ x_i t, gx_i, g^2 x_i, \dots, g^{m(i)-1} x_i \} .$$

Comme t transforme D_j en D_j' pour $1 \leqq j \leqq q$, les résultats précédents montrent que $S = C_1^+ \cup \dots \cup C_p^+ \cup D_1 \cup \dots \cup D_q$ est une section, et que gS ne diffère de S que par le remplacement de $x_1, \dots, x_p$ par $x_1 t, \dots, x_p t$.

On a donc $\Phi(g) = t^p$. Par ailleurs, il est bien connu qu'une permutation circulaire d'ordre n a la parité opposée à celle de n. Il en résulte que la permutation de X définie par g a la même parité que le nombre des cycles de longueur paire. Or $C_1, \ldots, C_p$ sont des cycles de longueur paire, et si l'un des cycles D_j est de longueur paire, il en est de même de D_j' qui a même longueur que D_j. Par suite, la permutation de X définie par g a même parité que p. Comme on a $\Phi(g) = t^p$, on voit que $\Phi(g)$ est bien égal à e ou à t selon que la permutation de X définie par g est paire ou impaire.

6. Ce qui précède donne la règle suivante pour calculer la signature d'une permutation. Supposons que g et t soient deux permutations d'un ensemble fini X, que g et t commutent, que t soit d'ordre deux et n'ait pas de point fixe. Soient S une partie de X telle que $\{S, tS\}$ soit une partition de X et p le nombre d'éléments de S dont le transformé par g n'appartient pas à S. Alors, la signature de g est égale à $(-1)^p$.

Comme exemple d'application de cette remarque, considérons un entier positif impair b et un entier a étranger à b. On note Z un groupe cyclique d'ordre b et g la permutation $x \mapsto x^a$ de Z. Nous allons montrer que la *permutation g a une signature égale au symbole de Legendre-Jacobi* $(\frac{a}{b})$; nous renvoyons à une autre note [3] pour un examen plus approfondi de la question.

Posons en effet $b = 2b' + 1$ et choisissons un générateur z de Z; alors Z se compose des éléments

$$e;\ z, z^2, \ldots, z^{b'};\ z^{-1}, z^{-2}, \ldots, z^{-b'}.$$

On a $g(e) = e$, donc g a même signature que sa restriction g' à l'ensemble X des éléments de Z distincts de e. Nous notons t la permutation $x \mapsto x^{-1}$ de X. Il est immédiat que t commute à g, est d'ordre deux et n'a pas de point fixe. Posons $S = \{z, z^2, \ldots, z^{b'}\}$. Avec les notations ci-dessus, p est le nombre des entiers i compris entre 1 et b' tels que ai soit congru modulo b à un entier compris entre $-b'$ et -1, et la signature de g est égale à $(-1)^p$. Or, on a $(-1)^p = (\frac{a}{b})$ d'après une généralisation connue d'un résultat classique de Gauss, et ceci établit notre assertion.

7. Voici un nouveau cas particulier de notre construction générale. On note E un ensemble fini à n éléments, X l'ensemble des couples (i, j) d'éléments distincts de E, G le groupe des permutations de E et A le groupe multiplicatif formé des entiers 1 et -1. On fait opérer les groupes G et A sur X par les règles

$$g(i,j) = (g(i), g(j)), \quad (i,j)(-1) = (j,i). \tag{7}$$

La vérification des hypothèses (A) et (B) du n° 1 est immédiate, d'où un homomorphisme Φ de G dans A. Nous allons montrer que $\Phi(g)$ *n'est autre que la signature de la permutation* g; comme nous le montrons dans une autre note [2], on peut partir de cette remarque pour donner un exposé nouveau des propriétés des permutations.

Nous donnerons trois démonstrations de notre assertion.

a) Il suffit évidemment de prouver que l'on a $\Phi(g) = -1$ si g est la transposition de deux éléments a et b de E. Nous choisirons une section S qui contienne les couples (a, b), (a, i) et (b, i) avec i distinct de a et b; il est immédiat qu'un tel choix est toujours possible et que (a, b) est le seul élément de S que g transforme en un élément n'appartenant pas à S. On a donc $\Phi(g) = -1$.

b) Sans restreindre la généralité, on peut supposer que E se compose des entiers compris entre 1 et n. La permutation g étant quelconque, choisissons pour section l'ensemble S des couples (i, j) avec $i < j$. On a alors $\Phi(g) = (-1)^p$ où p est le nombre des couples (i, j) avec $i < j$ et $g(i) > g(j)$, autrement dit, le nombre d'inversions de g. On retrouve donc une des définitions classiques de la signature.

c) Nous supposons encore que E se compose des entiers compris entre 1 et n. La permutation g de E étant quelconque, nous définissons des permutations $\gamma, g'_1, \ldots, g'_n, g''_1, \ldots, g''_n$ de $E \times E$ par les formules suivantes:

$$\gamma(i,j) = (g(i), g(j)) \tag{8}$$

$$g'_k(i,j) = \begin{cases} (g(i), j) & si \quad j = k \\ (i,j) & si \quad j \neq k \end{cases} \tag{9}$$

$$g''_k(i,j) = \begin{cases} (i, g(j)) & si \quad i = k \\ (i,j) & si \quad i \neq k. \end{cases} \tag{10}$$

Il est immédiat que g'_k et g''_k ont même signature que g et que l'on a $\gamma = g'_1 \ldots g'_n g''_1 \ldots g''_n$; par suite, la signature de γ est égale à 1. Par ailleurs, γ transforme en elle-même la partie X de $E \times E$, ainsi que son complémentaire Y; si γ_X et γ_Y désignent respectivement les permutations de X et Y induites par γ, la signature de γ est le produit des signatures de γ_X et γ_Y. Comme la signature de γ vaut 1, on voit donc que γ_X a même signature que γ_Y; or, Y se compose des couples (i, i) avec i dans E, et l'on a $\gamma_Y(i, i) = (g(i), g(i))$, donc γ_Y a même signature que g. On en conclut que

la signature de γ_X est égale à celle de g. Enfin, $\Phi(g)$ est la signature de γ_X d'après le n° 5.

8. Comme dernière spécialisation, nous considérons le cas d'un système de racines réduit; nous renvoyons à la monographie de Bourbaki [1] pour la définition précise des systèmes de racines et pour une étude approfondie de leurs propriétés. Il nous suffira ici de rappeler quelques points de la théorie.

On suppose donné un espace vectoriel réel V de dimension finie l, muni d'une forme bilinéaire symétrique $(x|y)$ telle que $(x|x) > 0$ pour $x \neq 0$, en bref un espace euclidien. Pour tout vecteur a, la symétrie S_a par rapport à l'hyperplan orthogonal à a est donnée par

$$S_a(x) = x - 2\frac{(x \mid a)}{(a \mid a)} \cdot a \; ; \tag{11}$$

c'est une transformation linéaire de déterminant -1 dans V. Un système de racines réduit est une partie finie R de V qui jouit en particulier des propriétés suivantes:

(R) Tout élément de R est non nul; avec r, R contient $-r$, mais aucun autre multiple de r.

(R′) Pour tout r dans R, la symétrie S_r laisse stable R.

(R″) Il existe une base $B = (r_1, ..., r_l)$ de V formée d'éléments de R, telle que tout élément de R soit combinaison linéaire à coefficients tous positifs ou tous négatifs de $r_1, ..., r_l$.

Le groupe de transformations orthogonales de V engendré par les symétries S_r (pour r dans R) se note W et s'appelle le *groupe de Weyl de R*. On peut montrer qu'il est engendré par les symétries $S_{r_1}, ..., S_{r_l}$ et la propriété (R') montre que R est stable par W; comme l'ensemble R est fini et contient une base de V, le groupe W est fini. De plus, la base B étant choisie comme dans (R''), on appelle *racine positive* tout élément de R qui est combinaison linéaire à coefficients positifs de $r_1, ..., r_l$ et l'on note R^+ l'ensemble des racines positives. De manière analogue, on définit l'ensemble R^- des racines négatives.

Comme exemple de système de racines, donnons celui des systèmes de type (A_{n-1}) (pour $n \geqq 2$), qui est lié au groupe des permutations. On considère d'abord un espace euclidien E de dimension n et une base orthonormale $(\varepsilon_1, ..., \varepsilon_n)$ de E; on note V le sous-espace de E formé des vecteurs $t_1\varepsilon_1 + ... + t_n\varepsilon_n$ avec $t_1 + ... + t_n = 0$. Si l'on pose

$e_i = \varepsilon_i - (\varepsilon_1 + \ldots + \varepsilon_n)/n$ pour $1 \leqq i \leqq n$, l'espace V de dimension $n - 1$ est engendré par $e_1, \ldots, e_n$ et l'on a $e_1 + \ldots + e_n = 0$. On note R l'ensemble des vecteurs de la forme $e_i - e_j$ pour i, j distincts compris entre 1 et n. On peut identifier W au groupe des permutations des entiers compris entre 1 et n, la permutation w correspondant à la transformation linéaire de V induite par la permutation $\varepsilon_i \mapsto \varepsilon_{w(i)}$ des vecteurs de base de E. La symétrie $S_{e_i - e_j}$ correspond à la transposition de i et j. Si l'on pose $l = n - 1$ et $r_i = e_i - e_{i+1}$ pour $1 \leqq i \leqq l$, la propriété (R'') est satisfaite; les racines positives (resp. négatives) sont les vecteurs $e_i - e_j$ avec $i < j$ (resp. $i > j$).

Revenons au cas général et notons A le groupe des homothéties de rapport 1 ou -1 dans V; d'après (R), le groupe A opère sans point fixe sur R et il est clair que les actions de W et A sur R commutent. Conformément à notre construction générale, on définit donc un homomorphisme Φ de W dans A. On peut décrire Φ de trois manières distinctes:

a) *$\Phi(w)$ est la signature de la permutation de R induite par w;*

b) *on a $\Phi(w) = (-1)^{N(w)}$ où $N(w)$ est le nombre des racines positives r telles que $w(r)$ soit négative;*

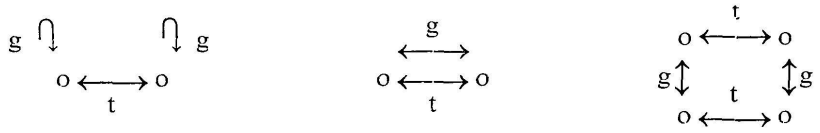
c) *$\Phi(w)$ est le déterminant de la transformation linéaire w de V.*

De ces trois descriptions, la première ne semble pas avoir été remarquée jusqu'ici. Le lecteur est invité à spécialiser la situation au cas des systèmes de type (A_{n-1}).

L'assertion a) résulte immédiatement du n° 5, et b) résulte de ce que R^+ est une section pour l'action du groupe A. Pour prouver c), il suffit de montrer que l'on a $\Phi(S_{r_i}) = -1$ pour $1 \leqq i \leqq l$, puisque le groupe W est engendré par $S_{r_1}, \ldots, S_{r_l}$. Or, si $r = m_1 r_1 + \ldots + m_l r_l$ est une racine positive, $S_{r_i}\, r$ est de la forme $r - a \,.\, r_i$ et ne peut être négative que si l'on a $m_1 = \ldots = m_{i-1} = m_{i+1} = \ldots = m_l = 0$, c'est-à-dire si r est multiple de r_i; d'après (R), ceci ne peut se produire que si $r = r_i$. Autrement dit, r_i est la seule racine positive que S_{r_i} transforme en une racine négative, et l'on a $N(S_{r_i}) = 1$; d'après b), on a donc $\Phi(S_{r_i}) = -1$.

9. Le lecteur qui désire un peu d'exercice pourra résoudre lui-même, ou faire résoudre par ses étudiants, le problème suivant:

a) Soient X un ensemble fini, et g, t deux permutations de X. On suppose que g et t sont d'ordre deux, que t est sans point fixe, et que g et t commutent. Montrer que les schémas suivants représentent toutes les situations élémentaires



et en déduire que la signature de g est égale à $(-1)^{n/2}$ où n est le nombre des $x \in X$ tels que $gx = tx$.

b) Soit E un espace euclidien de dimension finie. Tout hyperplan H de E définit une symétrie orthogonale s_H et deux demi-espaces (ouverts) qui sont dits opposés. Montrer que les deux demi-espaces limités par H sont les seuls demi-espaces que s_H transforme en leur opposé.

c) On note W un groupe fini de transformations orthogonales dans E, engendré par des symétries par rapport à des hyperplans. On note $\mathcal{H}$ l'ensemble des hyperplans H tels que s_H appartienne à W et R l'ensemble des demi-espaces limités par un hyperplan appartenant à $\mathcal{H}$. Soit w dans W; montrer que le déterminant de la transformation linéaire w dans E est égal à la signature de la permutation de R induite par w (on se ramènera au cas $w = s_H$; on définira la permutation t de R qui associe à tout demi-espace le demi-espace opposé, et l'on appliquera les résultats de a) et b)).

BIBLIOGRAPHIE

[1] Bourbaki, N., *Groupes et algèbres de Lie*, Chapitres IV à VI. Actualités Scientifiques et Industrielles, n° 1337, Hermann, Paris 1968.

[2] Cartier, P., Remarques sur la signature d'une permutation, ce même volume, pp. 7-19.

[3] —— Sur une généralisation des symboles de Legendre-Jacobi, ce même volume, pp. 31-48.

[4] Hall, M., The theory of groups. Mac Millan, New York 1959.

(Reçu le 1er novembre 1969)

Institut de recherche mathématique avancée
Rue René-Descartes, 67
Strasbourg