Sur l'itération des opérations de Steenrod.

Autor(en): **Cartan, Henri**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **29 (1955)**

PDF erstellt am: **27.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-23277

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Sur l'itération des opérations de Steenrod

par Henri Cartan, Paris

A Monsieur Heinz Hopf, en témoignage de profonde admiration

Introduction

Le but de cet article est de déterminer explicitement les relations existant entre les opérations de Steenrod itérées. Le cas d'un entier premier p impair se différencie du cas où $p = 2$.

Pour $p = 2$, les relations entre les „carrés" itérés $Sq^a Sq^b$, conjecturées d'abord par Wu Wen-tsün, ont été établies par J. Adem [1]. Plus récemment, J.-P. Serre et R. Thom ([6], [8]) ont indiqué (sans l'expliciter en détail) une méthode commode pour calculer ces relations; elle consiste à connaître d'avance une „base" pour les carrés itérés, grâce à une détermination explicite des groupes d'Eilenberg-MacLane du groupe cyclique d'ordre 2 (cf. [6]), puis à faire les calculs dans un produit d'espaces projectifs réels. Cette méthode montre en outre qu'il n'y a pas d'autre relation entre les $Sq^a Sq^b$ que celles données par Adem.

Une extension de la méthode de Serre et Thom m'a permis de déterminer toutes les relations existant entre puissances de Steenrod itérées $St_p^a St_p^b$ pour p premier impair. Ces relations ont été trouvées indépendamment par J. Adem [2], qui utilise l'homologie des sous-groupes de Sylow du groupe symétrique d'ordre p^2 ; sa démonstration n'a pas encore été publiée, à ma connaissance.

La démonstration que nous donnons ici, dont le principe est différent, a l'inconvénient d'utiliser la détermination explicite des groupes d'Eilenberg-MacLane du groupe cyclique d'ordre p (cf. [3]), mais présente l'avantage de calculs presque mécaniques. Pour la commodité du lecteur, nous avons réuni dans un bref Appendice quelques propriétés (sans doute connues) des coefficients binomiaux réduits modulo p.

1. Les opérations des Steenrod

On note Z l'anneau des entiers naturels, Z_p l'anneau (corps) des entiers mod. p (p premier).

Pour tout espace topologique X, l'*homomorphisme de Bockstein* α_p envoie la cohomologie $H^*(X\,;Z_p)$ dans la cohomologie $H^*(X\,;Z)$ en augmentant le degré d'une unité. Rappelons la définition de α_p, en précisant les conventions de signe adoptées ici : tout cocyle mod. p, de degré q, provient par réduction mod. p d'une cochaine entière x telle que dx ait la forme $(-1)^{q+1}px'$, où x' est un $(q+1)$-cocycle entier. L'image de x' dans $H^{q+1}(X\,;Z)$ ne dépend que de l'image de x dans $H^q(X\,;Z_p)$, et ceci définit l'homomorphisme α_p. Il est, au facteur $(-1)^{q+1}$ près, identique à l'homomorphisme „cobord" de la suite exacte de cohomologie de l'espace X, relativement à la suite exacte de coefficients

$$0 \to Z \xrightarrow{f} Z \to Z_p \to 0$$

où f désigne la multiplication par p.

L'homomorphisme de Bockstein $\beta_p : H^q(X\,;Z_p) \to H^{q+1}(X\,;Z_p)$ sera, par définition, le composé de α_p et de l'homomorphisme naturel

$$H^{q+1}(X\,;Z) \to H^{q+1}(X\,;Z_p)\ .$$

Il est évident que l'homomorphisme composé $\beta_p \circ \beta_p$ est nul.

La définition précédente s'étend au cas de la cohomologie relative $H^q(X, Y\,;Z_p)$, Y désignant un sous-espace de X. Considérons alors l'homomorphisme „cobord"

$$\delta^* : H^q(Y\,;Z_p) \to H^{q+1}(X, Y\,;Z_p)\ ;$$

l'homomorphisme de Bockstein β_p *commute avec* δ^* (vérification immédiate). Il en résulte que β_p *commute avec la suspension* quand celle-ci est définie (cf. [5], Chap. II, § 7 ; et [3], Note 1, § 5).

Relativement au cup-produit, β_p jouit de la propriété :

$$\beta_p(u\cdot v) = u\cdot\beta_p(v) + (-1)^q\beta_p(u)\cdot v \tag{1.1}$$

si v est de degré q.

Soit a un entier $\geqslant 0$, congru à 0 ou 1 mod. $2p-2$. Comme en [3] (Note II, § 4), nous définirons l'homomorphisme

$$St_p^a : H^q(X\,;Z_p) \to H^{q+a}(X\,;Z_p)$$

de la manière suivante : si $p=2$, on pose $St_2^a = Sq^a$, carré de Steenrod.

Si p est premier impair, et $a = 2k(p-1)$, k entier, on pose $St_p^a = \mathscr{P}_p^k$ (opération de Steenrod définie en [7], formule (6.8)). Pour des raisons de commodité, nous écrirons ici P_p^k au lieu de $\mathscr{P}_p^k$, ou même seulement P^k lorsqu'aucune confusion n'est à craindre. Si $a = 2k(p-1)+1$, p premier impair, St_p^a est, par définition, l'homomorphisme composé $\beta_p \circ P_p^k$.

Rappelons les principales propriétés des opérations de Steenrod St_p^a :

(i) soit f une application $X \to Y$, et f^* l'homomorphisme

$$H^*(Y\,;Z_p) \to H^*(X\,;Z_p)$$

défini par f ; alors $f^* \circ St_p^a = St_p^a \circ f^*$ (autrement dit, St_p^a est une *opération cohomologique*).

(ii) l'opération St_p^a commute avec la suspension ;

(iii) St_p^0 est l'identité, $St_p^1 = \beta_p$.

(iv) *pour p premier impair*, on a :

(1.2) $P_p^k(u) = u^p$ si u est de degré $2k$ (u^p désigne la puissance p-ième au sens du cup-produit) ;

(1.3) $P_p^k(u) = 0$ si u est de degré $q < 2k$;

(1.4) $P_p^k(u \cdot v) = \sum_{h=0}^{k} P_p^h(u) \cdot P_p^{k-h}(v)$,

cette dernière formule se généralisant aussitôt au cas du produit d'un nombre quelconque de facteurs.

(iv, a) *pour* $p = 2$, on a :

(1.2a) $Sq^k(u) = u^2$ si u est de degré k ;

(1.3a) $Sq^k(u) = 0$ si u est de degré $q < k$;

(1.4a) $Sq^k(u \cdot v) = \sum_{h=0}^{k} Sq^h(u) \cdot Sq^{k-h}(v)$.

On a en outre $Sq^{2k+1} = Sq^1 \circ Sq^{2k}$, formule qui est en accord avec la formule de définition $St_p^{2k(p-1)+1} = St_p^1 \circ St_p^{2k(p-1)}$ pour p impair.

2. Les opérations de Steenrod itérées

Soit p premier, éventuellement égal à 2. Pour chaque suite $I = (a_1, \ldots, a_k)$ d'entiers $a_i \geqslant 0$, congrus à 0 ou 1 mod. $2p-2$, définissons l'opération composée

$$St_p^I = St_p^{a_1} \circ \ldots \circ St_p^{a_k} \ .$$

Si la suite I est vide, on convient que St_p^I est l'endomorphisme identique.

Soit q la somme des termes de la suite I, que nous appellerons le *degré* de I ; St_p^I est un endomorphisme de $H^*(X\,;Z_p)$ *de degré* q, c'est-à-dire qui envoie $H^n(X\,;Z_p)$ dans $H^{n+q}(X\,;Z_p)$. Si I et J sont deux suites, et si (I, J) désigne la suite obtenue par juxtaposition des suites I et J, on a évidemment

$$St_p^I \circ St_p^J = St_p^{(I,J)} \ . \tag{2.1}$$

Soit M_p l'algèbre (sur le corps Z_p) ayant pour base l'ensemble des suites finies I d'entiers $\geqslant 0$ congrus à 0 ou 1 mod. $2p-2$. C'est une *algèbre graduée*. Pour tout espace X, la formule (2.1) montre que l'application $I \to St_p^I$ définit un *homomorphisme* de l'algèbre graduée M_p sur une sous-algèbre graduée de l'algèbre des endomorphismes de $H^*(X\,;Z_p)$. Soit $R_p(X)$ le noyau de cet homomorphisme, et soit R_p l'intersection des $R_p(X)$ relatifs à tous les espaces X possibles. L'algèbre quotient $A_p = M_p/R_p$ s'appellera l'*algèbre de Steenrod* relative à l'entier premier p. Pour tout espace X, la cohomologie $H^*(X\,;Z_p)$ est munie d'une structure de *module à gauche sur l'algèbre de Steenrod* A_p ; d'une façon précise, $H^*(X\,;Z_p)$ est un *module gradué sur l'algèbre graduée* A_p.

L'idéal bilatère R_p est somme directe de ses composantes R_p^q des divers degrés q. Chercher R_p^q, c'est chercher les combinaisons linéaires (à coefficients dans Z_p) des St_p^I de degré q, qui donnent zéro dans n'importe quel espace X. Or une telle combinaison définit, pour tout entier n, une *opération cohomologique* $H^n(X\,;Z_p) \to H^{n+q}(X\,;Z_p)$; et l'on sait ([6], § 4, corollaire du théorème 1) que, pour qu'une opération cohomologique $H^n(X\,;Z_p) \to H^{n+q}(X\,;Z_p)$ soit nulle pour tout X, il faut et il suffit qu'elle donne zéro quand on l'applique à la „classe fondamentale" d'un *espace d'Eilenberg-MacLane* $K(Z_p, n)$, c'est-à-dire d'un espace X dont tous les groupes d'homotopie sont nuls, sauf $\pi_n(X)$ qui est cyclique d'ordre p. Comme les St_p^I commutent avec la suspension [4] qui envoie $H^{r+1}(Z_p, n+1\,;Z_p)$ dans $H^r(Z_p, n\,;Z_p)$, une combinaison linéaire des St_p^I de degré q sera nulle dans l'algèbre A_p si et seulement si, appliquée à la classe fondamentale de $H^n(Z_p, n\,;Z_p)$, elle donne zéro *pour n assez grand* (car alors, par suspension, elle donnera zéro pour tout n). Or on a le résultat suivant ([3], Note II, corollaire du théorème 6 ; cf. aussi, pour le cas $p = 2$, [6], § 4, corollaire du théorème 2) :

Soit u_0 la classe fondamentale de $H^n(Z_p, n\,;Z_p)$. Si $q<n$, l'espace vectoriel $H^{n+q}(Z_p, n\,;Z_p)$ a une Z_p-base formée des éléments $St_p^I(u_0)$, où I parcourt l'ensemble des suites $(a_1, \ldots, a_k)$ de degré q telles que

$$a_i \geqslant p a_{i+1} \quad \text{pour} \quad 1 \leqslant i \leqslant k-1 \ . \tag{2.2}$$

Une suite I satisfaisant à (2.2) sera dite *admissible* (cf. [6]). De tout ce qui précède résulte le :

Théorème 1. *Les St_p^I relatifs aux suites admissibles I forment une base*[1]) *de l'algèbre de Steenrod A_p.*

Dans cet énoncé et dans tout ce qui suit, nous adoptons la notation suivante : St_p^I désigne désormais l'élément de l'algèbre A_p, image de $I \in M_p$.

3. Enoncé des résultats

Dans ce travail, nous nous proposons d'exprimer les St_p^I relatifs aux suites I non admissibles, comme combinaisons linéaires des St_p^I admissibles. Cela explicitera l'algèbre de Steenrod A_p ; en même temps, cela déterminera entièrement les opérations de Steenrod dans la cohomologie d'Eilenberg-MacLane $H^*(Z_p, n\,; Z_p)$, en vertu du théorème 6 de [3], Note II.

Il est commode de considérer que chaque suite I est une suite illimitée $(a_1, \ldots, a_i, \ldots)$ telle que les a_i soient nuls pour i assez grand. Une telle suite sera *admissible* si $a_i \geqslant p a_{i+1}$ pour tout i. La suite I sera dite de rang $\leqslant r$ (r entier $\geqslant 0$) si $a_i = 0$ pour $i > r$; le *rang* de I sera le plus petit des r tels que I soit de rang $\leqslant r$.

Dans l'ensemble des suites I, nous considérerons une relation d'ordre : l'*ordre lexicographique* en commençant *par la droite*. Une suite

$$(a_1, \ldots, a_r, 0, 0, \ldots)$$

sera donc *antérieure* à une suite $(b_1, \ldots, b_r, 0, 0, \ldots)$ si $a_r < b_r$, *ou* si $a_r = b_r$ et la suite $(a_1, \ldots, a_{r-1}, 0, 0, \ldots)$ est antérieure à

$$(b_1, \ldots, b_{r-1}, 0, 0, \ldots)\ .$$

Le théorème 1 se trouvera complété par le :

Théorème 2. *Soit J une suite non admissible de degré q ; alors St_p^J est combinaison linéaire des St_p^I relatifs aux suites admissibles I de degré q, qui sont antérieures à J dans l'ordre lexicographique.* En particulier, le *rang* de chaque suite I est au plus égal au rang de J.

Lorsque p est premier *impair*, on peut préciser davantage. Appelons *type* d'une suite $I = (a_1, \ldots, a_i, \ldots)$ le nombre des entiers a_i *impairs*. On prouvera le :

Théorème 2 bis. *Soit p premier impair, et soit J une suite non admissible de degré q et de type τ. Alors St_p^J est combinaison linéaire des St_p^I*

[1]) Cf. [2], theorem 1.5, où malheureusement le sens du mot „base" n'est pas précisé. Dans notre théorème 1, le mot „base" est pris au sens de la théorie des espaces vectoriels; il implique donc l'indépendance linéaire.

relatifs aux suites admissibles I de degré q, de type τ, qui sont antérieures à J dans l'ordre lexicographique.

Le théorème 2bis apporte une précision relative au *type*, qui serait inexacte pour $p = 2$. Par exemple, il est bien connu que $Sq^2 \circ Sq^2 = Sq^3 \circ Sq^1$.

Nous nous proposons, pour chaque suite J non admissible *de rang* 2, d'exprimer explicitement St_p^J comme combinaison linéaire des St_p^I relatifs aux suites admissibles I de rangs 2 et 1. La solution du cas général d'un rang quelconque s'en déduira, au moins théoriquement.

Cas $p = 2$. On doit exprimer $Sq^k \circ Sq^h$ pour $k < 2h$. Le problème a été résolu par Adem [1]. Nous écrirons la formule comme suit :

$$\boxed{Sq^{2h-1-n} \circ Sq^h = \sum_t (t, n-1-2t)_2 \, Sq^{2h-1-t} \circ Sq^{h-n+t}} \quad , \qquad (3.1)$$

où n désigne un entier $\geqslant 0$, et où l'on fait les conventions suivantes : on convient que Sq^k est nul pour $k < 0$; le symbole (a, b), où a et b sont entiers, désigne le coefficient binomial $\dfrac{(a+b)!}{a!\,b!}$ lorsque a et b sont $\geqslant 0$, et est nul si l'un au moins des entiers a et b est < 0 ; $(a, b)_2$ désigne le nombre (a, b) réduit mod. 2.

Explicitons la formule (3.1) pour $n = 0, 1, 2, 3, 4, 5, 6$:

$$\begin{aligned}
Sq^{2h-1} \circ Sq^h &= 0 \ . \\
Sq^{2h-2} \circ Sq^h &= Sq^{2h-1} \circ Sq^{h-1} \ . \\
Sq^{2h-3} \circ Sq^h &= Sq^{2h-1} \circ Sq^{h-2} \ . \\
Sq^{2h-4} \circ Sq^h &= Sq^{2h-1} \circ Sq^{h-3} + Sq^{2h-2} \circ Sq^{h-2} \ . \\
Sq^{2h-5} \circ Sq^h &= Sq^{2h-1} \circ Sq^{h-4} \ . \\
Sq^{2h-6} \circ Sq^h &= Sq^{2h-1} \circ Sq^{h-5} + Sq^{2h-2} \circ Sq^{h-4} + Sq^{2h-3} \circ Sq^{h-3} \ . \\
Sq^{2h-7} \circ Sq^h &= Sq^{2h-1} \circ Sq^{h-6} + Sq^{2h-3} \circ Sq^{h-4} \ .
\end{aligned}$$

On notera que $Sq^{2h-2^k-1} \circ Sq^h = Sq^{2h-1} \circ Sq^{h-2^k}$.

Cas p premier impair. Le cas où la suite $I = (1, a)$ se résout trivialement par les formules

$$\left.\begin{aligned}
St_p^1 \circ St_p^a &= St_p^{a+1} \quad \text{si} \quad a \equiv 0 \ (\text{mod. } 2p-2) \\
St_p^1 \circ St_p^a &= 0 \quad \text{si} \quad a \equiv 1 \ (\text{mod. } 2p-2)
\end{aligned}\right\} \qquad (3.2)$$

qui résultent des définitions et du fait que $\beta_p \circ \beta_p = 0$. On observera que ces formules sont aussi vraies pour $p = 2$.

Il reste à étudier $St_p^b \circ St_p^a$ lorsque $2p - 2 \leqslant b < pa$. Il suffit de considérer le cas où $b \equiv 0$ (mod. $2p - 2$) ; car, connaissant la formule qui

donne $St_p^b \circ St_p^a$ dans ce cas, on applique β_p aux deux membres pour obtenir la formule donnant $St_p^{b+1} \circ St_p^a$. Il reste donc à exprimer $P_p^k \circ P_p^h$ pour $k < ph$, et $P_p^k \circ \beta_p \circ P_p^h$ pour $k \leqslant ph$. Voici la solution :

$$\boxed{P_p^{ph-1-n} \circ P_p^h = \sum_t (-1)^{t+1} (t, (p-1)n-1-pt)_p \, P_p^{ph-1-t} \circ P_p^{h-n+t}} \tag{3.3}$$

où n désigne un entier $\geqslant 0$, et où l'on convient que $P_p^k = 0$ pour $k < 0$; la notation $(a, b)_p$ désigne le coefficient binomial réduit mod. p, et zéro si $a < 0$ ou $b < 0$. Avec les mêmes conventions, et toujours pour $n \geqslant 0$, on a

$$\boxed{\begin{aligned} P_p^{ph-n} \circ \beta_p \circ P_p^h = & \sum_t (-1)^{t+1} (t, (p-1)n-1-pt)_p \, P_p^{ph-t} \circ \beta_p \circ P_p^{h-n+t} \\ & + \sum_t (-1)^t (t, (p-1)n-pt)_p \, \beta_p \circ P_p^{ph-t} \circ P_p^{h-n+t} . \end{aligned}} \tag{3.4}$$

On observera que, pour $p = 2$, on pourrait déduire la formule (3.1) de la formule (3.3) où l'on conviendrait que P_2^k désigne Sq^k.

Voici ce que donnent (3.3) et (3.4) pour p impair et pour les petites valeurs de n (pour abréger l'écriture, on omet l'indice inférieur p et le signe $\circ$) :

$$\begin{aligned}
P^{ph-1} P^h &= 0 , \qquad P^{ph} \beta P^h = \beta P^{ph} P^h , \\
P^{ph-2} P^h &= - P^{ph-1} P^{h-1} , \\
P^{ph-1} \beta P^h &= - P^{ph} \beta P^{h-1} + \beta P^{ph} P^{h-1} , \\
P^{ph-3} P^h &= - P^{ph-1} P^{h-2} - 2 P^{ph-2} P^{h-1} , \\
P^{ph-2} \beta P^h &= - P^{ph} \beta P^{h-2} - 2 P^{ph-1} \beta P^{h-1} + \beta P^{ph} P^{h-2} + \beta P^{ph-1} P^{h-1} , \\
P^{ph-4} P^h &= - P^{ph-1} P^{h-3} - 3 P^{ph-2} P^{h-2} - 3 P^{ph-3} P^{h-1} .
\end{aligned}$$

On notera que $P^{ph-1-p^k} P^h = - P^{ph-1} P^{h-p^k}$.

On notera encore les formules suivantes, valables pour tout h (elles se déduisent aisément des formules (7.11) et (7.18) ci-dessous, respectivement équivalentes à (3.3) et (3.4)) :

$$\left.\begin{aligned} &(3.5) \quad P^k P^h = (k, h)_p P^{k+h} \\ &(3.6) \quad P^k \beta P^h = (k-1, h)_p P^{k+h} \beta + (k, h-1)_p \beta P^{k+h} \end{aligned}\right\} \text{ pour } 0 \leqslant k \leqslant p-1 .$$

4. Démonstration dans le cas $p = 2$

Pour être complet, nous allons donner ici une démonstration du théorème 2 (pour $p = 2$) et de la formule (3.1) en appliquant une méthode dont le principe est dû à Serre ([6], § 4, n° 33) et à Thom ([8], lemme

II.8). Ce sera d'ailleurs le même principe qui nous permettra de résoudre le cas où p est premier impair.

Considérons un espace $K(Z_2, 1)$ dont tous les groupes d'homotopie sont nuls, sauf π_1 cyclique d'ordre 2 ; par exemple, l'espace projectif réel à une infinité de dimensions. Son algèbre de cohomologie mod. 2 est une algèbre de polynômes engendrée par un unique générateur x de degré 1 (classe fondamentale). D'après (1.2a) et (1.3a), on a

$$Sq^1(x) = x^2 \ , \qquad Sq^k(x) = 0 \quad \text{pour} \quad k > 1 \ ,$$

d'où l'on déduit facilement, en utilisant (1.4a),

$$Sq^k(x^{2^i}) = 0 \quad \text{si} \quad 1 \leqslant k \neq 2^i \ , \quad Sq^k(x^k) = x^{2k} \quad \text{si} \quad k = 2^i \ . \tag{4.1}$$

Soit X le produit de n exemplaires de $K(Z_2, 1)$; soient $x_1 \ldots, x_n$ leurs classes fondamentales, identifiées à des éléments de $H^1(X ; Z_2)$. Soit u le produit $x_1 \ldots x_n$ (au sens du cup-produit). Compte tenu du théorème 1 (qui est déjà démontré), le théorème 2 (pour $p = 2$) résultera aussitôt de la :

Proposition 4.1. *Les $Sq^I(u)$ relatifs aux suites admissibles I de degré q sont des éléments linéairement indépendants de l'espace vectoriel $H^{n+q}(X ; Z_2)$, pourvu que n soit assez grand* (en fait, $n \geqslant q$). *Pour toute suite non admissible J de degré q, $Sq^J(u)$ est combinaison linéaire des $Sq^I(u)$ relatifs aux suites admissibles I de degré q, qui sont antérieures à J dans l'ordre lexicographique.*

Démonstration : elle ne présente pas de difficulté essentielle, puisque, pour toute suite I, $Sq^I(u)$ peut être calculé à l'aide des formules (4.1). En fait, associons à chaque suite $I = (a_1, \ldots, a_i, \ldots)$ la suite d'entiers

$$\alpha_i = a_i - 2a_{i+1} \ , \tag{4.2}$$

qui sont $\geqslant 0$ si et seulement si I est admissible. A chaque suite admissible I de degré q, on va associer un élément $D^I(u) \in H^{n+q}(X ; Z_2)$ comme suit. Observons d'abord que $H^{n+q}(X ; Z_2)$ est l'espace vectoriel des *polynômes* de degré $n + q$ en $x_1, \ldots, x_n$; considérons les monômes qui contiennent exactement α_i exposants égaux à 2^i (pour $i = 1, 2, \ldots$), et dont tous les autres exposants sont égaux à 1. La somme de tous ces monômes est un polynôme symétrique, qui sera par définition l'élément $D^I(u)$. Si $n \geqslant q$, on a $n \geqslant \sum_i \alpha_i$, donc les $D^I(u)$ relatifs à toutes les suites admissibles I de degré q sont linéairement indépendants. On prouve alors facilement, par récurrence sur le rang r de la suite J :

Proposition 4.2. *Soit J une suite (admissible ou non) de degré q ($q \leqslant n$). Alors $Sq^J(u)$ est combinaison linéaire des $D^I(u)$ relatifs aux suites admissibles I de degré q, qui sont antérieures* (au sens large) *à J dans l'ordre lexicographique. De plus, si J est admissible, le coefficient de $D^J(u)$ dans l'expression de $Sq^J(u)$ est égal à* 1.

La proposition 4.2 entraîne immédiatement :

Corollaire 4.3. *Les $Sq^J(u)$ relatifs aux suites admissibles de degré q sont des éléments linéairement indépendants de $H^{n+q}(X\,;Z_2)$ si $n \geqslant q$. De plus, pour toute suite admissible I de degré q, $D^I(u)$ est combinaison linéaire des $Sq^K(u)$ relatifs aux suites admissibles K de degré q, qui sont antérieures* (au sens large) *à I dans l'ordre lexicographique.*

Si J n'est pas admissible, $Sq^J(u)$ est combinaison linéaire des $D^I(u)$ relatifs aux suites admissibles I, antérieures à J et de même degré (d'après la proposition 4.2). Appliquant alors à chacune de ces suites I le corollaire 4.3, on voit que $Sq^J(u)$ est combinaison linéaire des $Sq^K(u)$ relatifs aux suites admissibles K antérieures à J et de même degré. Ceci achève de démontrer la proposition 4.1.

Ainsi le théorème 2 est établi dans le cas $p = 2$. Il reste à démontrer la formule (3.1), et pour cela on doit calculer $Sq^k Sq^h$ pour $k < 2h$ (nous omettons désormais le signe $\circ$). Il est visible que $Sq^h(u) = D^h(u)$, et que $Sq^k(D^h(u))$ est combinaison linéaire des $D^I(u)$ tels que

$$I = (k + h - t, t) \quad \text{avec} \quad t \leqslant k/2 \ .$$

On peut donc écrire a priori

$$Sq^k Sq^h = \sum_{0 \leqslant t \leqslant k/2} c^t_{k,h}\, Sq^{k+h-t}\, Sq^t \qquad (k < 2h) \ . \tag{4.3}$$

Pour expliciter les coefficients $c^t_{k,h}$, considérons l'espace-produit $K(Z_2, 1) \times X$, et, dans sa cohomologie, l'élément xu (x désignant la classe fondamentale de $K(Z_2, 1)$). Appliquant au produit xu les opérations des deux membres de (4.3), on trouve, à gauche comme à droite, des termes en x, x^2 et x^4. Egalons les termes en x^4 ; on obtient la relation $c^t_{k-2,h-1} = c^{t+1}_{k,h}$ pour $k \geqslant 2$, d'où

$$c^t_{k,h} = c_{k-2t,h-t} \quad (\text{en posant } c_{k,h} = c^0_{k,h}) \ . \tag{4.4}$$

Egalons ensuite les termes en x^2 ; on trouve

$c_{1,1} = 0$, $c_{1,h} = 1 + c_{1,h-1}$ pour $h \geqslant 2$, d'où $c_{1,h} = h + 1$ (à réduire mod. 2). Puis on a

$$\left.\begin{aligned} &c_{k,h} + c_{k-2,h-1} = c_{k-1,h} + c_{k,h-1} \quad \text{pour } h \geqslant 2,\ 2 \leqslant k < 2(h-1)\ , \\ &c_{k,h} + c_{k-2,h-1} = c_{k-1,h} \quad \text{pour } h \geqslant 2,\quad 2(h-1) \leqslant k < 2h. \end{aligned}\right\} \tag{4.5}$$

Les relations (4.5) permettent le calcul de $c_{k,h}$ pour $h \geqslant 2$, $0 \leqslant k < 2h$, par récurrence sur h : les $c_{k,h-1}$ sont déjà connus pour $k < 2(h-1)$, et les $c_{k,h}$ se calculent par récurrence sur k, à partir des valeurs $c_{0,h} = 1$, $c_{1,h} = h + 1$.

Il reste à vérifier que les $c_{k,h}$ ainsi calculés pour $0 \leqslant k < 2h$ satisfont à la relation

$$c_{k,h} = (h-k-1, k)_2 \quad \text{(coefficient binomial réduit mod. 2)} \tag{4.6}$$

Nous ne ferons pas ici cette vérification, car elle sera faite au § 7 pour p premier quelconque. Les formules (4.3), (4.4) et (4.6) donnent :

$$\boxed{Sq^k Sq^h = \sum_t (h-k-1+t, k-2t)_2 Sq^{k+h-t} Sq^t \quad \text{pour} \quad k < 2h} \tag{4.7}$$

En remplaçant k par $2h-1-n$ et t par $h-n+t$, on obtient la formule (3.1) ; mais la formule (4.7) peut aussi être commode.

5. Démonstration dans le cas où p est premier impair

On va encore considérer un espace $K(Z_p, 1)$. Cette fois, son algèbre de cohomologie mod. p est, comme bien connu, le produit tensoriel d'une algèbre extérieure à un générateur x de degré 1 par une algèbre de polynômes à un générateur y de degré 2. D'ailleurs x est la classe fondamentale, et

$$y = \beta_p(x) \ , \qquad \text{donc} \qquad \beta_p(y) = 0 \ . \tag{5.1}$$

Les opérations de Steenrod sont déterminées, dans $H^*(Z_p, 1 ; Z_p)$, par les formules (5.1) et

$$P^1(y) = y^p, \quad P^k(y) = 0 \ \text{ pour } \ k > 1, \quad P^k(x) = 0 \ \text{ pour } \ k > 0, \tag{5.2}$$

qui résultent de (1.2) et (1.3). Tenant compte de (1.4), on en déduit facilement

$$P^k(y^{p^i}) = 0 \quad \text{si} \quad 1 \leqslant k \neq p^i, \qquad P^k(y^k) = y^{pk} \quad \text{si} \quad k = p^i \ . \tag{5.3}$$

(La démonstration se fait par récurrence sur i.)

Soit X un espace, produit de $n + n'$ exemplaires de $K(Z_p, 1)$; soient $x_1, \ldots, x_n$ les classes fondamentales des n premiers facteurs, $x'_1, \ldots, x'_{n'}$ celles des n' derniers ; et posons $y_i = \beta_p(x_i)$, $y'_i = \beta_p(x'_i)$. Soit u l'élément de $H^{2n+n'}(X ; Z_p)$ égal au cup-produit

$$y_1 \ldots y_n \, x'_i \ldots x'_{n'} \ .$$

Compte tenu du théorème 1 (qui est déjà démontré), le théorème 2 bis résultera aussitôt de la :

Proposition 5.1. *Les $St_p^I(u)$ relatifs aux suites admissibles I de degré q sont des éléments linéairement indépendants de l'espace vectoriel $H^{2n+n'+q}(X\,;Z_p)$, pourvu que n et n' soient assez grands* (par exemple, il suffit que $2n \geqslant q/(p-1)$, $p^{n'} \geqslant 1 + q/2$). *Pour toute suite non admissible J de degré q et de type τ, $St_p^J(u)$ est combinaison linéaire des $St_p^I(u)$ relatifs aux suites admissibles I, de degré q et de type τ, qui sont antérieures à J dans l'ordre lexicographique.*

Démonstration : en principe, $St_p^I(u)$ peut être calculé pour toute suite I, grâce aux formules (5.1), (5.2), (5.3). En fait, associons à chaque suite $I = (a_1, \ldots, a_i, \ldots)$ la suite des entiers k_i et ε_i définis par

$$a_i = 2k_i(p-1) + \varepsilon_i \qquad (\varepsilon_i = 0 \text{ ou } 1)\ , \tag{5.4}$$

puis la suite des entiers λ_i définis par

$$\lambda_i = k_i - pk_{i+1} - \varepsilon_{i+1}\ . \tag{5.5}$$

On vérifie que la suite I est *admissible* si et seulement si les λ_i sont tous $\geqslant 0$. Inversement, la connaissance des ε_i et des λ_i (nuls pour i assez grand) détermine la suite des a_i, car on a

$$k_i = \sum_{j \geqslant 0} p^j(\lambda_{i+j} + \varepsilon_{i+j+1})\ , \tag{5.6}$$

après quoi a_i est déterminé par (5.4). La suite $(\varepsilon_1, \lambda_1, \ldots, \varepsilon_i, \lambda_i, \ldots)$ sera dite *associée* à la suite I. L'ordre lexicographique des suites I est le même que celui des suites associées (en commençant toujours par la droite).

Soit alors I une suite admissible de degré q, et soient ε_i et λ_i les entiers de la suite associée. On va définir un élément $D^I(u) \in H^{2n+n'+q}(X\,;Z_p)$. Parmi les monômes $y_1^{h_1} \ldots y_n^{h_n}$, considérons ceux qui contiennent exactement λ_i exposants égaux à p^i (pour $i = 1, 2, \ldots$), et dont tous les autres exposants sont égaux à 1 ; soit s la somme de ces monômes. L'élément $D^I(u)$ sera le produit de s par l'élément t que voici : t est une somme alternée de monômes dont chacun s'obtient en enlevant du produit $x'_1 \ldots x'_{n'}$ un nombre de facteurs égal au type $\tau = \sum_i \varepsilon_i$ de la suite I, puis en remplaçant chaque x'_j enlevé par une puissance $(y'_j)^{p^h}$, de manière qu'au total le nombre des facteurs y'_j qui figurent avec l'exposant p^h $(h \geqslant 0)$ soit nul si $\varepsilon_{h+1} = 0$, égal à un si $\varepsilon_{h+1} = 1$. Il reste à fixer le signe dont chaque monôme de t doit être affecté : c'est la signa-

ture de la permutation que l'on doit effectuer sur les indices j $(1 \leqslant j \leqslant n')$ pour que les variables x'_j viennent les premières en commençant par la gauche (rangées par ordre d'indices croissants), et que les variables y'_j se suivent dans l'ordre des exposants croissants.

L'élément $D^I(u)$ est ainsi défini pour chaque suite admissible I. Il est clair que les $D^I(u)$ associés à toutes les suites admissibles de degré donné q sont linéairement indépendants, pourvu que l'on ait $n \geqslant \sum_i \lambda_i$ et $n' \geqslant \tau$ pour toutes les suites admissibles de degré q. On en déduit facilement la limitation de n et n' donnée dans l'énoncé. Avant d'achever la démonstration de la proposition 5.1, énonçons-en une autre :

Proposition 5.2. *Soit J une suite (admissible ou non) de degré q et de type τ. Alors $St_p^J(u)$ est combinaison linéaire des $D^I(u)$ relatifs aux suites admissibles I de degré q et de type τ, qui sont antérieures* (au sens large) *à J dans l'ordre lexicographique. Si de plus n et n' sont assez grands* (comme dans la proposition 5.1), *alors pour toute suite admissible J de degré q, le coefficient de $D^J(u)$ dans l'expression de $St_p^J(u)$ est égal à* 1.

Cette proposition sera démontrée au § 6. Signalons-en tout de suite quelques conséquences immédiates :

Corollaire 5.3. *Les $St_p^J(u)$ relatifs aux suites admissibles de degré q sont des éléments linéairement indépendants de $H^{2n+n'+q}(X\,;Z_p)$ si n et n' sont assez grands. De plus, pour toute suite admissible I, de degré q et de type τ, $D^I(u)$ est combinaison linéaire des $St_p^K(u)$ relatifs aux suites admissibles K, de degré q et de type τ, qui sont antérieures* (au sens large) *à I dans l'ordre lexicographique.*

Si J n'est pas admissible, $St_p^J(u)$ est combinaison linéaire des $D^I(u)$ relatifs aux suites admissibles I, antérieures à J, de même degré et de même type que J (d'après la proposition 5.2). Appliquant alors à chacune de ces suites I le corollaire 5.3, on voit que $St_p^J(u)$ est combinaison linéaire des $St_p^K(u)$ relatifs aux suites admissibles K antérieures à J, de même degré et de même type que J. Ceci achève de démontrer la proposition 5.1, et il ne reste plus qu'à prouver la proposition 5.2.

6. Démonstration de la proposition 5.2 (p premier impair)

La démonstration se fait par récurrence sur le *rang* r de J, la proposition étant triviale pour le rang 0. Supposons-la donc démontrée pour les J de rang $\leqslant r$, et prouvons-la pour J de rang $r+1$. On est aussitôt ramené à prouver ceci :

Lemme. *Soit a un entier $\equiv 0$ ou 1 (mod. $2p-2$). Si J est une suite admissible et si n et n' sont assez grands pour que $D^J(u)$ existe, $St_p^a(D^J(u))$ est combinaison linéaire d'éléments $D^I(u)$, où I parcourt l'ensemble des suites admissibles antérieures à la suite (a, J), de même degré et de même type que (a, J). Si de plus (n et n' étant assez grands) la suite (a, J) est admissible, alors le coefficient de $D^{(a,J)}(u)$ dans l'expression de $St_p^a(D^J(u))$ est égal à 1.*

Il reste à prouver ce lemme. Il est bon d'examiner d'abord le cas où la suite J est vide. On a alors $St_p^a(u) = D^a(u)$: vérification immédiate, en utilisant (5.1) et (5.2).

Soit maintenant J une suite admissible non vide, et soit un entier $a = 2k(p-1) + \varepsilon$, $\varepsilon = 0$ ou 1. On se propose d'étudier l'élément $P^k(D^J(u))$ si $\varepsilon = 0$, resp. $\beta\, P^k(D^J(u))$ si $\varepsilon = 1$. Dans les deux cas, il faut d'abord chercher $P^k(D^J(u))$; nous supposerons donc d'abord que $a = 2k(p-1)$, et chercherons l'effet de P^k sur chacun des monômes m de l'élément $D^J(u)$; $P^k(m)$ est une somme de monômes, dans chacun desquels les facteurs x'_j du monôme m restent inchangés ; chaque facteur $(y_j)^{ph}$ $(h \geqslant 0)$ de m reste inchangé ou est remplacé par $(y_j)^{ph+1}$. De même chaque facteur $(y'_j)^{ph}$ reste inchangé ou est remplacé par $(y'_j)^{ph+1}$. Dans la somme $\sum_m P^k(m)$ étendue à tous les monômes m de $D^J(u)$, seuls subsistent les monômes qui contiennent *au plus une* variable y'_j d'exposant donné (ceci résulte de la convention de signe faite dans la définition de $D^J(u)$). Ainsi $P^k(D^J(u))$ est une somme de polynômes dont chacun a la forme $D^I(u)$, I ayant même degré que la suite (a, J), et même type que J (car le nombre des variables y'_j figurant dans chaque monôme n'a pas changé). Il reste à montrer que chacune de ces suites I est *antérieure* (au sens large) à la suite (a, J). Soit $(\varepsilon'_1, \lambda'_1, \varepsilon'_2, \lambda'_2, \ldots)$ la suite associée à une telle suite I (d'ailleurs $\varepsilon'_1 = 0$) ; et soit $(\varepsilon_1, \lambda_1, \varepsilon_2, \lambda_2, \ldots)$ la suite associée à J. La suite associée à (a, J) a la forme $(0, \lambda, \varepsilon_1, \lambda_1, \varepsilon_2, \lambda_2, \ldots)$. Pour montrer que I est antérieure à (a, J), on prouve ceci : r désignant le rang de J, on a $\lambda'_{r+1} \leqslant \lambda_r$; de même $\varepsilon'_{r+1} \leqslant \varepsilon_r$; si $\lambda'_{r+1} = \lambda_r$, on a $\lambda'_r \leqslant \lambda_{r-1}$; si $\varepsilon'_{r+1} = \varepsilon_r$, on a $\varepsilon'_r \leqslant \varepsilon_{r-1}$; etc.... Si enfin on a les égalités $\lambda'_{i+1} = \lambda_i$ et $\varepsilon'_{i+1} = \varepsilon_i$ pour $1 \leqslant i \leqslant r$, alors les suites I et (a, J) sont identiques. Or ces assertions se prouvent très facilement.

Supposons de plus que la suite (a, J) soit *admissible*. Prenons un monôme m de $D^J(u)$; il y a une façon et une seule de multiplier par p tous les exposants des y_j qui sont $\geqslant p$, et tous les exposants des y'_j qui sont $\geqslant 1$. Donc, si n est assez grand pour que $D^{(a,J)}(u)$ existe,

chaque monôme de $D^{(a,J)}(u)$ figure une fois et une seule dans $P^k(D^J(u))$. Ceci achève de démontrer le lemme dans le cas où $a \equiv 0$ (mod. $2p-2$).

Le cas où $a \equiv 1$ (mod. $2p-2$) s'y ramène aussitôt. En effet, si $J = (a_1, a_2, \ldots, a_i, \ldots)$ est une suite admissible et si $a_1 \equiv 0$ (mod. $2p-2$), on a $\beta_p(D^J(u)) = D^I(u)$, I désignant la suite

$$(a_1 + 1, a_2, \ldots, a_i, \ldots) .$$

7. Formules explicites (p premier impair)

On va établir les formules (3.3) et (3.4). Etudions d'abord $P^k P^h$ pour $k < ph$; on a $P^h(u) = D^h(u)$, et $P^k(D^h(u))$ est évidemment combinaison linéaire des $D^I(u)$ tels que $I = (k+h-t, t)$, $t \leqslant k/p$. On peut donc écrire a priori :

$$P^k P^h = \sum_{0 \leqslant t \leqslant k/p} c^t_{k,h} P^{k+h-t} P^t \qquad (k < ph) . \tag{7.1}$$

Les constantes $c^t_{k,h}$ étant ainsi définies pour $0 \leqslant k < ph$ et $0 \leqslant t \leqslant k/p$, il sera commode d'étendre cette définition à d'autres cas, en posant

$$c^t_{k,h} = 0 \quad \text{pour} \quad 0 \leqslant k < ph , \quad t > k/p ,$$

$$\text{si } t \geqslant 0 \text{ et } k \geqslant ph \geqslant 0, \; c^t_{k,h} = 0 \text{ pour } t \neq h, \; c^h_{k,h} = 1 .$$

De plus, on convient que, pour $k < 0$, $P^k = 0$, d'où la convention

$$c^t_{k,h} = 0 \quad \text{pour} \quad k < 0 \quad \text{ou} \quad h < 0 .$$

Alors $c^t_{k,h}$ est défini pour toutes les valeurs de l'entier $t \geqslant 0$ et toutes les valeurs entières de h et k, $\geqslant 0$ ou $\leqslant 0$; on a toujours

$$P^k P^h = \sum_{t \geqslant 0} c^t_{k,h} P^{k+h-t} P^t . \tag{7.2}$$

Désignons par X le même espace qu'aux §§ 5 et 6, et soit

$$u \in H^{2n+n'}(X, Z_p)$$

comme ci-dessus. Considérons l'espace-produit $K(Z_p, 1) \times X$, et la classe de cohomologie yu de ce produit (y désigne $\beta_p(x)$, x étant la classe fondamentale de $K(Z_p, 1)$). Appliquons au produit yu les opérations des deux membres de (7.2) ; chaque membre donne des termes en y, en y^p et en y^{p^2}. Egalons les coefficients de y^{p^2} et y^p ; on obtient :

$$\sum_{t \geqslant 0} (c^t_{k-p,h-1} - c^{t+1}_{k,h}) P^{k+h-p-1-t} P^t = 0 \tag{7.3}$$

$$\sum_{t \geqslant 0} (c^t_{k-1,h} + c^t_{k,h-1} - c^t_{k,h} - c^{t+1}_{k,h}) P^{k+h-t-1} P^t = 0 . \tag{7.4}$$

Dans la relation (7.3), les coefficients sont nuls pour $t+1>\inf(k/p,h)$; pour $t+1\leqslant\inf(k/p,h)$, l'opérateur $P^{k+h-p-1-t}P^t$ est admissible, donc (7.3) implique que tous les coefficients sont nuls : $c^t_{k-p,h-1}=c^{t+1}_{k,h}$. Par récurrence sur t, on a

$$c^t_{k,h}=c_{k-pt,h-t}\quad(\text{en posant}\quad c_{k,h}=c^0_{k,h})\ . \tag{7.5}$$

Il reste à calculer les $c_{k,h}$. Pour cela, utilisons (7.4) : le coefficient de $P^{k+h-t-1}P^t$ est nul si $t>k/p$; si $t\leqslant k/p$, l'opérateur $P^{k+h-t-1}P^t$ est admissible, pourvu que $0\leqslant k<ph$; donc, si $0\leqslant k<ph$, tous les coefficients de (7.4) sont nuls, ce qui donne, pour $t=0$ (et en tenant compte de la relation $c^1_{k,h}=c_{k-p,h-1}$) :

$$c_{k,h}+c_{k-p,h-1}=c_{k-1,h}+c_{k,h-1}\qquad\text{pour}\qquad 0\leqslant k<ph\ . \tag{7.6}$$

Or cette relation, compte tenu du fait que $c_{k,h}$ est déjà connu pour $k<0$ ou $k\geqslant ph$, permet de calculer de proche en proche $c_{k,h}$ pour tous les couples de valeurs de k et h tels que $0\leqslant k<ph$. On procède par double récurrence : récurrence sur h à partir de $h=1$; et, pour chaque h, récurrence sur k à partir de $k=0$. Précisons : si on fait $h=1$ dans (7.6), on trouve (en tenant compte du fait que $c_{k,0}=0$ pour $k<0$, $c_{k,0}=1$ pour $k\geqslant 0$) :

$c_{k,1}=c_{k-1,1}+1$ pour $0\leqslant k<p$, d'où, par récurrence sur k,

$$c_{k,1}=k+1\qquad\text{pour}\qquad 0\leqslant k\leqslant p-1\ . \tag{7.7}$$

Ensuite, utilisant (7.6) pour tout $h\geqslant 2$, puis (7.7) et enfin

$$\text{pour } h\geqslant 1,\ \text{on a } c_{k,h}=0 \text{ si } k<0 \text{ ou } k\geqslant ph\ , \tag{7.8}$$

on calcule tous les $c_{k,h}$ pour $h\geqslant 2$, $0\leqslant k<ph$.

Nous allons montrer que le résultat de ce calcul est

$$c_{k,h}=(-1)^k((p-1)h-k-1,k)_p\qquad\text{pour}\qquad 0\leqslant k<ph\ , \tag{7.9}$$

en désignant toujours par $(a,b)_p$ le nombre (a,b) réduit mod. p, et par (a,b) le coefficient binomial si $a\geqslant 0$, et $b\geqslant 0$, zéro si $a<0$ ou $b<0$. En effet, posons provisoirement

$$\gamma_{k,h}=(-1)^k((p-1)h-k-1,k)_p\qquad\text{quels que soient } k \text{ et } h.$$

Pour prouver que $c_{k,h}=\gamma_{k,h}$ pour $0\leqslant k<ph$, il suffit de montrer

$$\gamma_{k,h}+\gamma_{k-p,h-1}=\gamma_{k-1,h}+\gamma_{k,h-1}\qquad\text{pour}\qquad h\geqslant 2\ , \tag{7.6$'$}$$

$$\gamma_{k,1}=k+1\qquad\text{pour}\qquad 0\leqslant k\leqslant p-1\ , \tag{7.7$'$}$$

pour $h \geqslant 1$, on a $\gamma_{k,h} = 0$ si $k < 0$ ou $k \geqslant ph$. (7.8)'

La vérification de (7.7)' et de (7.8)' est immédiate. Celle de (7.6)' revient à

$$((p-1)h-k-p, k)_p + ((p-1)h-k, k-p)_p$$
$$= ((p-1)h-k-1, k)_p + ((p-1)h-k, k-1)_p \ . \qquad (7.10)$$

(Observer que ce calcul vaut aussi quand $p = 2$). Or, d'après l'*Appendice* ci-dessous (prop. 2), le premier membre est égal à $((p-1)h-k, k)_p$ parce que $(p-1)h - p \geqslant 0$ (h étant $\geqslant 2$), et le second membre est égal aussi à $((p-1)h-k, k)_p$, parce que $(p-1)h - 1 \geqslant 0$. Ceci prouve (7.10), et par suite (7.9) est démontrée.

Les formules (7.1), (7.5) et (7.9) donnent finalement :

$$\boxed{P^k P^h = \sum_t (-1)^{k+t}((p-1)h-k-1+t, k-pt)_p P^{k+h-t} P^t \text{ pour } k < ph} \qquad (7.11)$$

En remplaçant k par $ph - 1 - n$ et t par $h - n + t$, on obtient la formule (3.3) ; mais la formule (7.11) peut aussi être utile. On la comparera à (4.7).

Il reste encore à démontrer (3.4). En considérant $P^k \beta P^h(u)$, on voit tout de suite qu'on a, a priori,

$$P^k \beta P^h = \sum_{0 \leqslant t \leqslant (k-1)/p} a^t_{k,h} P^{k+h-t} \beta P^t + \sum_{0 \leqslant t \leqslant k/p} b^t_{k,h} \beta P^{k+h-t} P^t \ (k \leqslant ph) \ . \qquad (7.12)$$

Considérons la classe de cohomologie xu de l'espace-produit $K(Z_p, 1) \times X$, et soit toujours $y = \beta(x)$. Appliquons à xu les opérations des deux membres de (7.12) ; chacun donne des termes en y et y^p. Egalons les termes en y^p ; il vient

$$P^{k-1} P^h = \sum_{0 \leqslant t \leqslant (k-1)/p} a^t_{k,h} P^{k-1+h-t} P^t \ ;$$

puisque $0 \leqslant k - 1 < ph$, on peut appliquer au premier membre la formule (7.1) où k serait remplacé par $k - 1$, d'où

$$a^t_{k,h} = c^t_{k-1,h} \quad \text{pour} \quad 0 \leqslant t \leqslant (k-1)/p, \quad k \leqslant ph \ .$$

Ceci détermine les coefficients $a^t_{k,h}$:

$$a^t_{k,h} = (-1)^{k-1+t}((p-1)h-k+t, k-1-pt)_p \text{ pour } 0 \leqslant t \leqslant (k-1)/p, k \leqslant ph \ . \qquad (7.13)$$

Egalons maintenant les termes en y ; on obtient

$$P^k P^h = \sum_{0 \leqslant t \leqslant k/p} (b^t_{k,h} + c_{k-1-pt,h-t}) P^{k+h-t} P^t \ , \qquad (7.14)$$

compte tenu du fait que $c_{k-1-pt,h-t} = 0$ pour $t > (k-1)/p$. Tous les opérateurs du second membre de (7.14) sont admissibles. Il y a alors deux cas à distinguer :

Premier cas : $k = ph$. — Le second membre de (7.14) doit se réduire à $P^{ph}P^h$, ce qui donne, en tenant compte de $c_{ph-1-pt,h-t} = 0$,

$$b^t_{ph,h} = 0 \quad \text{pour} \quad 0 \leqslant t \leqslant h-1 \ , \qquad b^h_{ph,h} = 1 \ . \tag{7.15}$$

Deuxième cas : $k < ph$. — Alors (7.14) doit se réduire à (7.1), d'où

$$b^t_{k,h} = c_{k-pt,h-t} - c_{k-1-pt,h-t} \quad \text{pour} \quad 0 \leqslant t \leqslant k/p < h \ . \tag{7.16}$$

On a donc $b^t_{k,h} = b_{k-pt,h-t}$, avec $b_{k,h} = c_{k,h} - c_{k-1,h}$, d'où

$$\begin{aligned}(-1)^k b_{k,h} &= ((p-1)h-k-1, k)_p + ((p-1)h-k, k-1)_p \\ &= ((p-1)h-k, k)_p \ .\end{aligned}$$

Finalement, on a, pour $k < ph$,

$$b^t_{k,h} = (-1)^{k+t}((p-1)h-k+t, k-pt)_p \ , \qquad 0 \leqslant t \leqslant k/p \ . \tag{7.17}$$

Observons que (7.17) vaut aussi pour $k = ph$, d'après (7.15). Finalement, les relations (7.12), (7.13) et (7.17) donnent la formule

$$\boxed{\begin{aligned}P^k \beta P^h = &\sum_t (-1)^{k-1+t}((p-1)h-k+t, k-1-pt)_p P^{k+h-t}\beta P^t \\ &+ \sum_t (-1)^{k+t}((p-1)h-k+t, k-pt)_p \beta P^{k+h-t} P^t \ (k \leqslant ph)\end{aligned}} \ . \tag{7.18}$$

C'est exactement la formule donnée par J. Adem [2] pour $k < ph$.

En remplaçant, dans (7.18), k par $ph - n$ et t par $h - n + t$, on obtient (3.4).

Appendice. *Propriétés des coefficients binomiaux réduits modulo p.*

Pour h et k entiers $\geqslant 0$, nous notons (h, k) le coefficient binomial

$$(h, k) = \frac{(h+k)!}{h!\,k!} = \frac{(h+1)(h+2)\ldots(h+k)}{1.2\ldots k} \ . \tag{1}$$

On note $(h, k)_p$ cet entier réduit modulo p (p premier).

Proposition 1. *Si* $h = h_0 + ph_1$, $k = k_0 + pk_1$ $(0 \leqslant h_0 < p$, $0 \leqslant k_0 < p)$, *on a*

$$(h, k)_p = (h_0, k_0)_p \cdot (h_1, k_1)_p \ ; \tag{2}$$

$(h_0, k_0)_p$ *est nul si et seulement si* $h_0 + k_0 \geqslant p$.

Démonstration : la dernière assertion est évidente. Pour prouver (2), distinguons deux cas : si $h_0 + k_0 \geqslant p$, on va montrer que (h, k) est divisible par p ; dans le dernier membre de (1), enlevons les facteurs (du numérateur et du dénominateur) premiers à p ; il reste

$$\frac{(p(h_1+1))(p(h_1+2))\dots(p(h_1+k_1+1))}{(p)(2p)\dots(k_1 p)} = p(h_1+k_1+1)\,.\,(h_1, k_1)\,,$$

ce qui prouve l'assertion. Le deuxième cas est celui où $h_0 + k_0 < p$; dans le dernier membre de (1), enlevons les facteurs divisibles par p ; il reste une fraction qui, mod. p, est congrue à (h_0, k_0) ; donc (h, k) est congru (mod. p) au produit

$$(h_0, k_0) \cdot \frac{(p(h_1+1))\dots(p(h_1+k_1))}{(p)\dots(k_1 p)} = (h_0, k_0)(h_1, k_1)\,.$$

Corollaire. *Si h et k ont pour développements p-adiques*

$$h = \sum_{i \geqslant 0} p^i h_i\,, \qquad k = \sum_{i \geqslant 0} p^i k_i\,,$$

on a $(h, k)_p = \prod_{i \geqslant 0} (h_i, k_i)_p$. *En particulier, pour que* $(h, k)_p = 0$, *il faut et il suffit que l'on ait* $h_i + k_i \geqslant p$ *pour au moins un* i.

Convenons maintenant de poser $(h, k) = 0$ si $h < 0$ ou $k < 0$. L'identité classique

$$(h+1, k) + (h, k+1) = (h+1, k+1) \tag{3}$$

valable pour $h \geqslant 0$, $k \geqslant 0$, subsiste pour $h + k + 1 \geqslant 0$ (c'est immédiat).

Proposition 2. *Si* $h + k + p \geqslant 0$, *on a*

$$(h+p, k)_p + (h, k+p)_p = (h+p, k+p)_p\,. \tag{4}$$

Démonstration : supposons d'abord h et $k \geqslant 0$, et soit

$$h = h_0 + p h_1\,, \qquad k = k_0 + p k_1 \qquad (0 \leqslant h_0 < p, \quad 0 \leqslant k_0 < p)\,.$$

Puisque $h_1 \geqslant 0$, $k_1 \geqslant 0$, on a, d'après (3),

$$(h_1+1, k_1) + (h_1, k_1+1) = (h_1+1, k_1+1)\,.$$

Réduisons mod. p, puis multiplions par $(h_0, k_0)_p$: on obtient (4). Si maintenant h et $h + p$ sont < 0, (4) est trivialement vérifiée. Reste le cas où $h + p = h_0$, $0 \leqslant h_0 < p$. On est ramené à vérifier le

Lemme. *Si* $0 \leqslant h_0 < p$, *et* $h_0 + k \geqslant 0$, *on a*

$$(h_0, k)_p = (h_0, k + p)_p \ . \tag{5}$$

En effet, distinguons deux cas: si $k \geqslant 0$, soit $k = k_0 + pk_1$ $(0 \leqslant k_0 < p)$; les deux membres de (5) sont égaux à $(h_0, k_0)_p$ d'après la proposition 1. Si $k < 0$, posons $k + p = k_0$ $(0 < k_0 < p)$; le premier membre de (5) est nul, le second est égal à $(h_0, k_0)_p$, et comme $h_0 + k_0 \geqslant p$ par hypothèse, on a bien $(h_0, k_0)_p = 0$.

BIBLIOGRAPHIE

[1] *J. Adem*, The iteration of the Steenrod squares in algebraic topology. Proc. Nat. Acad. Sci. U. S. A. **38**, 1952, p. 720–726.

[2] *J. Adem*, Relations on iterated reduced powers. Proc. Nat. Acad. Sci. U. S. A. **39**, 1953, p. 636–638.

[3] *H. Cartan*, Sur les groupes d'Eilenberg-MacLane, I et II. Proc. Nat. Acad. Sci. U. S. A. **40**, 1954, p. 467—471 et p. 704—707.

[4] *S. Eilenberg* and *S. MacLane*, Cohomology theory of abelian groups and homotopy theory, I. Proc. Nat. Acad. Sci. U. S. A. **36**, 1950, p. 443–447.

[5] *J. P. Serre*, Homologie singulière des espaces fibrés. Ann. Math. **54**, 3, 1951, p. 425–505.

[6] *J. P. Serre*, Cohomologie modulo 2 des complexes d'Eilenberg-MacLane. Comment. Math. Helv. **27**, 1953, p. 198–232.

[7] *N. Steenrod*, Cyclic reduced powers of cohomology classes. Proc. Nat. Acad. Sci. U. S. A. **39**, 1953, p. 217–223.

[8] *R. Thom*, Quelques propriétés globales des variétés différentiables. Comment. Math. Helv. **28**, 1954, p. 17–86.

(Reçu le 12 juillet 1954.)