Séminaire Henri Cartan

H. Cartan

Détermination des algèbres $H_*(\pi, n; Z_p)$ et $H^*(\pi, n; Z_p)$, p premier impair

Séminaire Henri Cartan, tome 7, n° 1 (1954-1955), exp. n° 9, p. 1-10
<http://www.numdam.org/item?id=SHC_1954-1955__7_1_A9_0>

DÉTERMINATION DES ALGÈBRES $H_*(\pi,n;Z_p)$ et $H^*(\pi,n;Z_p)$, p premier impair.

(Exposé de H. CARTAN, 17.1.1955)

1.- Mots admissibles ; opérations correspondantes.

Considérons trois symboles σ , γ_p et φ_p . Considérons les mots (suites finies, y compris la suite vide) formés avec ces trois éléments. La hauteur n d'un mot α sera, par définition, le nombre total des lettres du mot α égales à σ ou à φ_p . Le degré d'un mot α se définit par récurrence sur le nombre des lettres de α : le degré du mot vide est 0 ; un mot non vide s'écrit sous l'une des trois formes $\sigma\alpha$, $\gamma_p\alpha$, $\varphi_p\alpha$, où α est un mot ; on pose

$$(1)\quad \begin{cases} \deg(\sigma\alpha) = 1 + \deg(\alpha) \text{ , } \deg(\gamma_p\alpha) = p.\deg(\alpha) \text{ ,} \\ \deg(\varphi_p\alpha) = 2 + p.\deg(\alpha) \text{ .} \end{cases}$$

La différence entre le degré et la hauteur est le degré stable q ; le degré est donc $n + q$.

Un mot α sera dit admissible si : (i) α n'est pas vide, la première et la dernière lettre de α sont σ ou φ_p ; (ii) pour chaque lettre γ_p ou φ_p du mot, le nombre des lettres σ situées à droite est pair.

Proposition 1. - Soit α un mot admissible de hauteur n ; pour qu'un mot $\beta\alpha$ soit admissible de hauteur $n + 1$, il faut et il suffit que le mot β soit réduit à la lettre σ si $\deg(\alpha)$ est impair, et, si $\deg(\alpha)$ est pair, que β soit égal à $\sigma(\gamma_p)^k$ ou à $\varphi_p(\gamma_p)^k$, k entier $\geqslant 0$.

C'est une conséquence immédiate des définitions.

Un mot admissible α est dit de première espèce s'il se termine (à droite) par la lettre σ ; de deuxième espèce s'il se termine par φ_p . A chaque mot admissible α , de première espèce, associons une application $f(\alpha) : \pi/p\pi \longrightarrow H_{n+q}(\pi,n;Z_p)$, où n et q désignent la hauteur et le degré stable de α ; on définit $f(\alpha)$ par récurrence sur la hauteur du mot α , en posant les conditions suivantes : si α est de hauteur 1 (donc $\alpha = \sigma$), $f(\alpha)$ est la suspension $\sigma : \pi \otimes Z_p \longrightarrow H_1(\pi,1;Z_p)$; si $\alpha = \sigma\beta$, le mot admissible β étant de hauteur n et de degré impair $n+q$, $f(\alpha)$ est l'application composée $\pi/p\pi \xrightarrow{f(\beta)} H_{n+q}(\pi,n;Z_p) \xrightarrow{\sigma} H_{n+q+1}(\pi,n+1;Z_p)$; si

$\alpha = \sigma(\gamma_p)^k\beta$, le mot admissible β étant de hauteur n et de degré pair $n+q$, $f(\alpha)$ est l'application composée

$$\pi/p\pi \xrightarrow{f(\beta)} H_{n+q}(\pi,n;Z_p) \xrightarrow{\sigma\circ\gamma_{pk}} H_{pk(n+q)+1}(\pi,n+1;Z_p) \quad ;$$

si $\alpha = \varphi_p(\gamma_p)^k\beta$, le mot admissible β étant de hauteur n et de degré pair $n+q$, $f(\alpha)$ est l'application composée

$$\pi/p\pi \xrightarrow{f(\beta)} H_{n+q}(\pi,n;Z_p) \xrightarrow{\varphi_p\circ\gamma_{pk}} H_{pk+1(n+q)+2}(\pi,n;Z_p) \quad .$$

A chaque mot admissible α , de deuxième espèce, on associe une application $f(\alpha) : {}_p\pi \longrightarrow H_{n+q}(\pi,n;Z_p)$, où n et q désignent la hauteur et le degré stable de α ; on définit $f(\alpha)$ par récurrence sur la hauteur du mot α , en posant les conditions suivantes : si α est de hauteur 1 (donc $\alpha = \varphi_p$) $f(\alpha)$ est l'application $\varphi_p : {}_p\pi \longrightarrow H_2(\pi,1;Z_p)$; la récurrence se fait comme dans le cas d'une suite de première espèce : on pose $f(\sigma\beta) = \sigma \circ f(\beta)$, $f(\sigma(\gamma_p)^k\beta) = \sigma\circ\gamma_{pk}\circ f(\beta)$, $f(\varphi_p(\gamma_p)^k\beta) = \varphi_p\circ\gamma_{pk}\circ f(\beta)$.

Proposition 2.- Les applications $f(\alpha)$ sont linéaires, lorsque l'entier premier p est impair.

En effet, $\sigma : \pi/p\pi \longrightarrow H_1(\pi,1;Z_p)$ et $\varphi_p : {}_p\pi \longrightarrow H_2(\pi,1;Z_p)$ sont linéaires ; la démonstration se fait alors par récurrence sur la hauteur de α , en observant que σ est linéaire sur les éléments de $H_{n+q}(\pi,n;Z_p)$ ($n+q$ impair), et que $\sigma\circ\gamma_{pk}$ et $\varphi_p\circ\gamma_{pk}$ sont linéaires sur les éléments de $H_{n+q}(\pi,n;Z_p)$ ($n+q$ pair). Ce dernier point résulte de la formule (3) de l'Exposé n° 7 (propriétés des puissances divisées) et du fait que σ et φ_p sont des applications linéaires qui s'annulent sur les éléments décomposables (Exposé n° 6, proposition 1 et proposition 3).

2.- Les algèbres $U(M^{(n)})$.

Pour chaque entier $n \geqslant 1$, définissons un Z_p-espace vectoriel gradué $M^{(n)}$, comme suit ; c'est la somme directe d'autant d'exemplaires de $\pi/p\pi$ qu'il y a de mots admissibles α de hauteur n et de première espèce, et d'autant d'exemplaires de ${}_p\pi$ qu'il y a de mots admissibles α de hauteur n et de deuxième espèce. Chaque exemplaire de $\pi/p\pi$ (resp. de ${}_p\pi$) est affecté d'un degré égal au degré du mot α qui l'indexe. Pour chaque α , on a une application linéaire $f(\alpha)$ de la composante d'indice α de $M^{(n)}$ dans $H_*(\pi,n;Z_p)$; cette collection d'applications définit une application linéaire de $M^{(n)p}$ dans $H_*(\pi,n;Z_p)$, qui conserve le degré. Nous noterons $f^{(n)}$ cette application.

Or l'algèbre $H_*(\pi,n;Z_p)$ est une algèbre graduée anticommutative, munie de puissances divisées (pour les éléments de degré pair $\geqslant 2$) satisfaisant aux conditions (1), (2), (3), (4') et (5) de l'Exposé n° 7. On peut donc appliquer à l'application linéaire $f^{(n)} : M^{(n)} \longrightarrow H_*(\pi,n;Z_p)$ le théorème 2 de l'Exposé n° 8 : l'application $f^{(n)}$ se prolonge, d'une seule manière, en un homomorphisme $g^{(n)}$ de l'algèbre universelle $U(M^{(n)})$ dans l'algèbre $H_*(\pi,n;Z_p)$, homomorphisme compatible avec les structures d'algèbres graduées et avec les puissances divisées.

Théorème fondamental : l'homomorphisme $g^{(n)}$ est un isomorphisme de l'algèbre $U(M^{(n)})$ sur l'algèbre $H_*(\pi,n;Z_p)$ (p premier impair).

Ce théorème détermine complètement l'algèbre d'homologie $H_*(\pi,n;Z_p)$ avec ses puissances divisées. Il implique que l'application linéaire $f^{(n)}$ applique biunivoquement $M^{(n)}$ sur un sous-espace vectoriel gradué de $H_*(\pi,n;Z_p)$.

3.- Démonstration du théorème fondamental.

Pour plus de clarté, écrivons $M^{(n)}(\pi)$ au lieu de $M^{(n)}$, et $g^{(n)}(\pi)$ au lieu de $g^{(n)}$. Il est clair que $M^{(n)}(\pi)$ et $U(M^{(n)}(\pi))$ sont des foncteurs covariants du groupe abélien π , ainsi que $H_*(\pi,n;Z_p)$; et que $g^{(n)}(\pi) : U(M^{(n)}(\pi)) \longrightarrow H_*(\pi,n;Z_p)$ est une application naturelle de foncteurs. Chacun des foncteurs $U(M^{(n)}(\pi))$ et $H_*(\pi,n;Z_p)$ commute avec les limites directes; donc, il suffit de prouver que $g^{(n)}(\pi)$ est un isomorphisme, lorsque π est un groupe de type fini. Alors π est somme directe d'un nombre fini de groupes cycliques dont l'ordre est infini ou une puissance d'un nombre premier q . Or si π est une somme directe $\pi' + \pi''$, les injections $\pi' \longrightarrow \pi$ et $\pi'' \longrightarrow \pi$ identifient $U(M^{(n)}(\pi))$ au produit tensoriel $U(M^{(n)}(\pi')) \underset{Z_p}{\otimes} U(M^{(n)}(\pi''))$, et $H_*(\pi,n;Z_p)$ au produit tensoriel $H_*(\pi',n;Z_p) \underset{Z_p}{\otimes} H_*(\pi'',n;Z_p)$. Il suffira donc de prouver que $g^{(n)}(\pi)$ est un isomorphisme, lorsque π est cyclique infini ou cyclique d'ordre q^f (q premier).

Supposons d'abord que π soit cyclique d'ordre q^f , q premier $\neq p$. Alors $M^{(n)} = 0$ pour $n \geqslant 1$ et $U(M^{(n)})$ est réduit aux scalaires ; or il en est de même de $H_*(\pi,n;Z_p)$: il suffit de montrer que l'algèbre $H_*(\pi,1;Z_p)$ est réduite aux scalaires, car alors une application répétée du théorème 2 de l'Exposé n° 2 entraînera que l'algèbre $H_*(\pi,n;Z_p)$ est réduite aux scalaires, pour tout n . Pour étudier $H_*(\pi,1;Z_p)$, nous utiliserons la construction

acyclique classique, ayant pour algèbre initiale $Z(\pi)$ l'algèbre d'un groupe cyclique π d'ordre h (h entier quelconque) ; il s'agit d'une construction à coefficients entiers, déjà utilisée à la fin de l'Exposé n° 6, et que nous réduirons ensuite modulo p .

On pose $A = Z(\pi)$ avec l'augmentation ϵ égale à 1 sur chaque élément de π ; on choisit un générateur a du groupe cyclique π d'ordre h , et on pose $N = E(x,1) \otimes P(y,2)$ (produit tensoriel d'algèbres graduées munies de puissances divisées) ; sur $M = A \otimes N$, on considère la différentielle d définie par

(2) $dx = a - 1$, $d\gamma_k(y) = (1 + a + \ldots + a^{h-1}) x \gamma_{k-1}(y)$, pour $k \geqslant 1$.

On a donc $d(x\gamma_k(y)) = (a - 1)\gamma_k(y)$, et il est immédiat que M est acyclique. Par passage au quotient, on obtient la différentielle $\bar{d}$ de l'algèbre finale $N = E(x,1) \otimes P(y,2)$:

(3) $\bar{d}x = 0$, $\bar{d}\gamma_k(y) = hx\gamma_{k-1}(y)$ pour $k \geqslant 1$.

Revenons maintenant au cas où $h = q^f$, q premier $\neq p$. Si on réduit modulo p , on obtient $\bar{d}x = 0$, $\bar{d}\gamma_k(y) = hx\gamma_{k-1}(y)$, où h est un élément inversible du corps Z_p . Donc N est acyclique, comme annoncé ; le théorème fondamental est ainsi démontré dans le cas où π est cyclique d'ordre q^f , q premier $\neq p$.

Examinons maintenant le cas où π est cyclique infini, ou cyclique d'ordre p^f . On choisit un générateur a de π ; si π est infini, ${}_p\pi = 0$; si π est d'ordre p^f , on choisit $a^{p^{f-1}}$ comme générateur de ${}_p\pi$. Alors l'espace vectoriel $M^{(n)}(\pi)$ a une <u>base</u> bien définie, indexée par les mots admissibles de première espèce (si π infini), resp. par tous les mots admissibles (si π fini).

<u>Lemme 1</u>.- sous ces hypothèses, il existe un homomorphisme de $U(M^{(1)}(\pi))$ dans la bar construction $\overline{B}(Z_p(\pi))$, compatible avec les puissances divisées, et qui, par passage à l'homologie, donne $g^{(1)}(\pi)$ qui est un <u>isomorphisme.</u>

<u>Démonstration du lemme 1</u>.: nous devons examiner successivement le cas où π est cyclique infini et celui où π est cyclique d'ordre p^f . Dans le premier cas, il existe une construction acyclique $A \otimes_{Z_p} N$, où $A = Z_p(\pi)$, $N = E_p(x,1)$ (algèbre extérieure à un générateur x de degré 1 et à coefficients dans Z_p), avec la différentielle $dx = a - 1$ (a désignant toujours le générateur de π). Soit $\lambda : E_p(x,1) \longrightarrow \overline{B}(Z_p(\pi))$ l'unique homomorphisme spécial (théorème 5, Exposé n° 4) ; il est compatible avec les puissances

divisées (théorème 3, Exposé n° 7) et définit un isomorphisme $\lambda_* : E_p(x,1) \approx H_*(\overline{\mathcal{B}}(Z_p(\pi)))$ (en vertu du théorème 2, Exposé n° 2). Considérons l'isomorphisme $\mu : U(M^{(1)}) \longrightarrow E_p(x,1)$ qui envoie l'unique élément de base de $M^{(1)}$ dans l'élément x. Considérons l'application composée $\lambda \circ \mu : U(M^{(1)}) \longrightarrow \overline{\mathcal{B}}(Z_p(\pi))$; par passage à l'homologie, on trouve un isomorphisme, d'après ce qui précède. Or cet isomorphisme est $g^{(1)}$, car il coïncide avec $f^{(1)}$ sur l'élément de base de $M^{(1)}$; cela résulte du fait que x est la suspension de a. Ceci prouve le lemme 1 dans le cas où π est cyclique infini.

Supposons maintenant que π soit cyclique d'ordre p^f. Prenons la construction acyclique décrite ci-dessus ; on a donc $N = E_p(x,1) \otimes P_p(y,2)$, avec $\bar{d} = 0$ sur N. La classe d'homologie x est la suspension de a, celle de y est la transpotence de $a^{p^{f-1}}$, en vertu du calcul fait à la fin de l'Exposé n° 6. Soit λ l'unique homomorphisme spécial $N \to \overline{\mathcal{B}}(Z_p(\pi))$; il est compatible avec les puissances divisées, donc est déterminé par la connaissance de $\lambda(x)$ et $\lambda(y)$; par passage à l'homologie, il définit un isomorphisme $\lambda_* : N \approx H_*(\overline{\mathcal{B}}(Z_p(\pi)))$. Considérons l'isomorphisme $\mu : U(M^{(1)}) \to N$ qui envoie le générateur a de $\pi/p\pi$ dans x, et le générateur $a^{p^{f-1}}$ de $p\pi$ dans y. L'application composée $\lambda \circ \mu : U(M^{(1)}) \to \overline{\mathcal{B}}(Z_p(\pi))$ est compatible avec les puissances divisées, et, par passage à l'homologie, définit un isomorphisme. Cet isomorphisme coïncide avec $f^{(1)}$ sur chacun des deux éléments de base de $M^{(1)}$, donc c'est $g^{(1)}$.

4.- Démonstration du théorème fondamental (Suite).

Lemme 2 : π étant cyclique infini ou d'ordre p^f, engendré par a, il existe, pour chaque entier $n \geqslant 1$, une construction acyclique (sur le corps Z_p) ayant $U(M^{(n)}(\pi))$ comme algèbre initiale (avec différentielle nulle), et $U(M^{(n+1)}(\pi))$ comme algèbre finale (avec différentielle nulle) ; et cette construction satisfait à la condition (Γ) que voici : les éléments de la base de $M^{(n+1)}(\pi)$ se déduisent des éléments de la base de $M^{(n)}(\pi)$ par les opérations suivantes (dans la construction acyclique) :

σ appliquée à chaque élément de degré impair de la base de $M^{(n)}(\pi)$;

$\sigma\gamma_{pk}$ $(k \geqslant 0)$ et $\varphi_p\gamma_{pk}$ $(k \geqslant 0)$ appliquées à chaque élément de degré pair de la base de $M^{(n)}(\pi)$.

Il est clair qu'une fois ce lemme prouvé, une application répétée du théorème 5 de l'Exposé n° 4 fournira, compte tenu du lemme 1, des homomorphismes $U(M^{(n)}) \to \overline{\mathcal{B}}^{(n)}(Z_p(\pi))$, compatibles avec les puissances divisées, et qui,

par passage à l'homologie, donneront des isomorphismes compatibles avec les opérations σ , γ_p et φ_p ; et, à cause de la condition (Γ) du Lemme 2, on verra de proche en proche que ces isomorphismes sont précisément les homomorphismes $g^{(n)}$, puisqu'ils coïncident avec $f^{(n)}$ sur la base de $M^{(n)}$. Ceci achèvera de prouver le théorème fondamental.

Démonstration du lemme 2 : l'algèbre $U(M^{(n)})$ est le produit tensoriel des algèbres universelles des sous-espaces de dimension 1 de $M^{(n)}$ engendrés par les éléments de la base de $M^{(n)}$. Soit x un élément de la base de $M^{(n)}$; si x est de degré impair $2q-1$, l'algèbre universelle du sous-espace engendré par x est $E_p(x,2q-1)$ (algèbre extérieure à coefficients dans Z_p) , si x est de degré pair $2q$, l'algèbre universelle du sous-espace engendré par x est $P_p(x,2q)$ (algèbre des polynômes divisée à coefficients dans Z_p). On va montrer les deux propositions suivantes :

Proposition 3.- Si x est de degré $2q-1$, il existe une construction acyclique ayant $E_p(x,2q-1)$ comme algèbre initiale (différentielle nulle), et $P_p(y,2q)$ comme algèbre finale (différentielle nulle) ; y se déduit de x par la suspension σ .

Proposition 4.- Si x est de degré $2q$, il existe une construction acyclique ayant $P_p(x,2q)$ comme algèbre initiale (différentielle nulle), et dont l'algèbre finale (à différentielle nulle) est un produit tensoriel infini

$$E_p(y_o,2q+1) \otimes \dots \otimes E_p(y_k,2p^k q+1) \otimes \dots \otimes P_p(z_o,2pq+2) \otimes \dots \otimes P_p(z_k,2p^{k+1}q+2) \otimes \dots \otimes \dots ,$$

où $y_k = \sigma \gamma_{pk}(x)$ et $z_k = \varphi_p \gamma_{pk}(x)$.

Une fois ces propositions démontrées, un produit tensoriel de constructions acycliques donnera la construction acyclique du lemme 2, qui sera ainsi prouvé.

La proposition 3 est évidente : sur le produit tensoriel $E_p(x,2q-1) \otimes P_p(y,2q)$, on met la différentielle d que voici :

$$dx = 0 \quad , \quad d\gamma_k(y) = x\gamma_{k-1}(y) \quad \text{pour} \quad k \geqslant 1 .$$

Ceci est bien une construction acyclique, et la différentielle $\bar{d}$ est nulle ; la relation $dy = x$ montre que y est la suspension de x .

Démontrons la proposition 4. L'algèbre $P_p(x,2q)$ est, d'après l'Exposé n° 7, paragraphe 7, un produit tensoriel

$$Q_p(x,2q) \otimes Q_p(\gamma_p(x),2pq) \otimes \dots \otimes Q_p(\gamma_{p^k}(x),2p^k q) \otimes \dots ,$$

où $Q_p(x,2q)$ désigne l'algèbre des polynômes <u>tronquée</u> à un générateur x de degré $2q$ (quotient de l'algèbre des polynômes ordinaires, à une lettre x, par l'idéal engendré par x^p). Il suffit de faire une construction acyclique ayant comme algèbre initiale chacune des algèbres de ce produit tensoriel ; puis on fera le produit tensoriel de ces constructions. Ainsi la proposition 4 va résulter du fait suivant : <u>il existe une construction acyclique ayant comme algèbre initiale</u> $Q_p(x,2q)$ (<u>différentielle nulle</u>) <u>et comme algèbre finale</u> $E_p(y,2q+1) \otimes P_p(z,2pq+2)$ (<u>différentielle nulle</u>), <u>avec</u> $y = \sigma(x)$, $z = \varphi_p(x)$. C'est ce qu'on va montrer.

On définit, sur $Q_p(x,2q) \otimes E_p(y,2q+1) \otimes P_p(z,2pq+2)$, la différentielle d que voici :

$$(4) \qquad dx = 0 \ , \quad dy = x \ , \quad d\,\gamma_k(z) = x^{p-1}\, y\, \gamma_{k-1}(z) \quad \text{pour} \quad k \geqslant 1 \ .$$

On vérifie que, en ce qui concerne les éléments de degré > 0 , le noyau de d et l'image de d sont identiques : chacun d'eux est engendré par les éléments $x^h \gamma_k(z)$ $(1 \leqslant h \leqslant p-1 \ , \ k \geqslant 0)$ et $x^{p-1}\, y\, \gamma_k(z)$ $(k \geqslant 0)$. Par passage au quotient, $\bar{d} = 0$ sur l'algèbre finale. La relation $dy = x$ montre que $y = \sigma(x)$, et la relation $dz = x^{p-1}\, y$ montre que $z = \varphi_p(x)$.

La démonstration du théorème fondamental est ainsi terminée.

5.- <u>Structure de l'algèbre de cohomologie</u> $H^*(\pi,n;Z_p)$, p <u>impair</u>.

L'application diagonale $a \to (a,a)$ de π dans $\pi + \pi$ définit un diagramme commutatif

$$\begin{array}{ccccc} U(M^{(n)}(\pi)) & \longrightarrow & U(M^{(n)}(\pi+\pi)) & \approx & U(M^{(n)}(\pi)) \otimes U(M^{(n)}(\pi)) \\ \downarrow & & \downarrow & & \downarrow \\ H_*(\pi,n;Z_p) & \longrightarrow & H_*(\pi+\pi,n;Z_p) & \approx & H_*(\pi,n;Z_p) \otimes H_*(\pi,n;Z_p) \end{array}$$

dans lequel les flèches verticales désignent les isomorphismes $g^{(n)}$ du théorème fondamental. On observe que $M^{(n)}(\pi+\pi)$ est naturellement la somme directe $M^{(n)}(\pi) + M^{(n)}(\pi)$. L'application diagonale $M^{(n)}(\pi) \to M^{(n)}(\pi) + M^{(n)}(\pi)$ s'écrit, avec la notation du produit tensoriel, $x \to x \otimes 1 + 1 \otimes x$. Ainsi, si on identifie $H_*(\pi,n;Z_p)$ à l'algèbre universelle $U(M^{(n)}(\pi))$ au moyen de $g^{(n)}$, la structure multiplicative de la cohomologie $H^*(\pi,n;Z_p)$ est celle qui est définie, sur le <u>dual gradué</u> $\mathrm{Hom}'(U(M^{(n)}),Z_p)$, par l'homomorphisme $\Delta : U(M^{(n)}) \longrightarrow U(M^{(n)}) \otimes U(M^{(n)})$ (homomorphisme d'algèbres graduées, compatible avec les puissances divisées) qui envoie chaque $x \in M^{(n)}$ dans l'élément $x \otimes 1 + 1 \otimes x$.

On est ramené à un problème d'algèbre pure : soit M un module libre gradué (sur un anneau commutatif Λ), et soit Δ l'homomorphisme $U(M) \longrightarrow U(M) \otimes_\Lambda U(M)$, compatible avec les puissances divisées, qui envoie x dans $x \otimes 1 + 1 \otimes x$, pour tout $x \in M$. On cherche la structure multiplicative définie par Δ sur le dual $\mathrm{Hom}'_\Lambda(U(M),\Lambda)$. Soit $M = M^- + M^+$, où M^- désigne le sous-module des éléments de degré impair, et M^+ le sous-module des éléments de degré pair. On a

$$\Delta^- : E(M^-) \to E(M^-) \otimes E(M^-) \quad , \quad \Delta^+ : S(M^+) \longrightarrow S(M^+) \otimes S(M^+) \quad .$$

Δ^- est bien connu, et définit sur $\mathrm{Hom}'(E(M^-),\Lambda)$ la structure multiplicative de l'algèbre extérieure $E(M'^-)$ du dual $M'^- = \mathrm{Hom}'(M,\Lambda)$. Si $x \in M^+$, on a $\Delta^+\gamma_k(x) = \gamma_k(x \otimes 1 + 1 \otimes x) = \sum_{i+j=k} \gamma_i(x) \otimes \gamma_j(x)$. Dans le cas où M^+ possède une base formée d'un seul élément x , $S(M^+)$ possède une base formée des $\gamma_k(x)$ $(k \geqslant 0)$; soient x'^k les éléments de la base duale ; on trouve la loi de multiplication $x'^i.x'^j = x'^{i+j}$, donc le dual de $S(M^+)$ est l'algèbre des polynômes (ordinaire) à un générateur x' . Le cas général se ramène à celui-là par produit tensoriel, lorsque la base est finie en toute dimension : l'algèbre duale de $S(M^+)$ est l'algèbre symétrique $\Sigma(M'^+)$, quotient de l'algèbre tensorielle $T(M'^+)$ par l'idéal bilatère engendré par les éléments $x' \otimes y' - y' \otimes x'$, $x' \in M'^+$, $y' \in M'^+$.

Finalement, si M est un module gradué ayant une base finie en toute dimension, l'algèbre duale de $U(M)$ (pour l'application Δ) est l'algèbre $L(M') = E(M'^-) \otimes \Sigma(M'^+)$, qu'on appelle l'algèbre anticommutative libre du module M' dual de M (i.e. : $M' = \mathrm{Hom}'(M,\Lambda)$).

Revenons à l'algèbre de cohomologie $H^*(\pi,n;Z_p)$. On a prouvé :

Théorème 2. Soit, pour p premier impair, $M'^{(n)}$ le Z_p-espace vectoriel gradué, somme directe d'autant d'exemplaires de $\mathrm{Hom}(\pi,Z_p)$ qu'il y a de mots admissibles de première espèce et de hauteur n , et d'autant d'exemplaires de $\mathrm{Hom}({}_p\pi,Z_p)$ qu'il y a de mots admissibles de deuxième espèce et de hauteur n ; chaque sous-espace $\mathrm{Hom}(\pi,Z_p)$, resp. $\mathrm{Hom}({}_p\pi,Z_p)$, est affecté d'un degré égal au degré du mot α qui l'indexe. L'isomorphisme $g^{(n)}$ du théorème fondamental définit alors, par dualité, un isomorphisme de l'algèbre de cohomologie $H^*(\pi,n;Z_p)$ sur l'algèbre anticommutative libre $L(M'^{(n)})$.

L'isomorphisme précédent est un isomorphisme naturel de foncteurs contravariants du groupe abélien π . On observera que l'algèbre $L(M'^{(n)})$ est universelle vis-à-vis des applications linéaires (de degré 0) de l'espace vectoriel gradué $M'^{(n)}$ dans les algèbres graduées anticommutatives.

6.- Schémas décrivant les mots admissibles.

Soit α un mot admissible. Considérons la suite (éventuellement vide) des lettres du mot α qui sont distinctes de la lettre σ. Numérotons-les, de gauche à droite, par les entiers 1, 2, ... Si α_i désigne la i-ième de ces lettres, soit $2k_i$ le degré du mot β_i obtenu en enlevant du mot α la lettre α_i et toutes celles qui sont à gauche de α_i. Alors le mot $\alpha_i \beta_i$ est de degré $2k_i p$ si $\alpha_i = \gamma_p$, et de degré $2k_i p + 2$ si $\alpha_i = \varphi_p$. Soit a_i la différence des degrés stables des mots $\alpha_i \beta_i$ et β_i ; on a

(5) $\quad a_i = 2k_i(p-1) + u_i$, avec $u_i = 0$ si $\alpha_i = \gamma_p$, $u_i = 1$ si $\alpha_i = \varphi_p$

Il est commode de définir l'entier a_i pour tout $i \geqslant 1$, en convenant que $a_i = 0$ si i est plus grand que le nombre des lettres du mot α distinctes de σ. Un mot qui ne contient que σ définit donc la suite $a_1 = 0$, $a_2 = 0$, ...

Théorème 3.- La suite $(a_1, \ldots, a_i, \ldots)$ associée à un mot admissible de hauteur n et de degré stable q satisfait aux conditions :

(i) $\quad a_i \equiv 0$ ou $1 \pmod{2p-2}$ pour tout i ,

(ii) $\quad a_i \geqslant p\, a_{i+1}$ pour tout i ,

(iii) $\quad \sum_i a_i = q$,

(iv) $\quad p\, a_1 < (p-1)(n+q)$.

Réciproquement, étant donnés n et q, toute suite (a_i) satisfaisant à (i), (ii), (iii) et (iv) est associée à un mot admissible de hauteur n et de degré stable q, et ce mot est unique.

Démonstration : (i) résulte de (5). Puisque le mot $\alpha_i \beta_i$ est de degré $2k_i p + 2u_i$, on a $2k_i p + 2u_i \leqslant 2k_{i-1}$ pour $i \geqslant 2$, d'où (ii). La relation (iii) est évidente puisque a_i est le saut du degré stable dans l'opération définie par α_i (et que le degré stable ne change pas par suspension). Enfin, si $a_1 \neq 0$, le mot α a l'une des formes $\sigma^h \gamma_p \beta$ $(h \geqslant 1)$ ou $\sigma^h \varphi_p \beta$ $(h \geqslant 0)$, le mot β étant de degré $2k_1$. Donc le degré $n+q$ du mot α est $> 2pk_1 + u_1 - \ldots$, d'où facilement l'inégalité (iv).

Réciproquement, soient des a_i vérifiant (i), (ii) et (iv). Définissons, pour chaque i, les entiers k_i et u_i au moyen de (5), ce qui est possible grâce à (i). Alors (ii) entraîne $k_i - p\, k_{i+1} - u_{i+1} \geqslant 0$. Posons $h_{i+1} = k_i - p\, k_{i+1} - u_{i+1}$. S'il existe un mot admissible α donnant naissance

à la suite (a_i) , le nombre des lettres σ situées entre α_i et α_{i+1} dans ce mot est nécessairement égal à $2\,h_{i+1}$, et on a $\alpha_i = \gamma_p$ si $u_i = 0$, $\alpha_i = \varphi_p$ si $u_i = 1$. Ceci détermine le mot α , sauf qu'il faut encore connaître le nombre h_1 des lettres σ venant à gauche de α_1 dans le mot α . On doit avoir $n + q = h_1 + 2k_1p + 2u_1$, et ceci détermine un entier h_1 qui est bien $\geqslant 1$ si $u_1 = 0$, et est $\geqslant 0$ si $u_1 = 1$, grâce à la condition (iv) Le degré stable q du mot α satisfait à (iii). Le théorème est entièrement prouvé.

Remarque : la connaissance des entiers h_{i+1} $(i \geqslant 1)$, qui sont $\geqslant 0$, et celle des entiers u_i (égaux à 0 ou 1) détermine entièrement la suite des a_i , par les formules

$$(6) \qquad k_i = \sum_{j \geqslant 0} p^j \,(h_{i+j+1} + u_{i+j+1}) \,, \quad a_i = 2k_i(p-1)+u_i \,.$$

Autre remarque : pour que le mot α associé à une suite (a_i) soit de deuxième espèce, il faut et il suffit que le dernier des a_i non nuls soit égal à 1 .

Dernière remarque : les résultats précédents valent aussi pour $p = 2$ lorsque Π est cyclique, car alors les applications $f(\alpha)$ sont encore additives.