EL ALGEBRA DE COHOMOLOGIA DEL GRUPO SIMETRICO DE GRADO p^2

Por Humberto Cárdenas*

Introducción

Como se sabe (ver [3], pág. 224), para cualquier grupo finito y cualquier campo de coeficientes el álgebra de cohomología $H^*(G, K)$ tiene presentación finita, esta presentación ha sido dada explícitamente para algunos grupos sencillos. El propósito de este trabajo es dar con un número finito de generadores y relaciones una presentación simple del álgebra $H^*(S_{p^2}\,;\, Z_p)$ en donde S_{p^2} es el grupo simétrico de grado p^2 y Z_p es el campo de los enteros mod p, con p un número primo impar. Se espera además que este cálculo completo del álgebra de cohomología de un grupo no trivial como S_{p^2} pueda dar una idea de la estructura de $H^*(G; K)$ para grupos finitos en general.

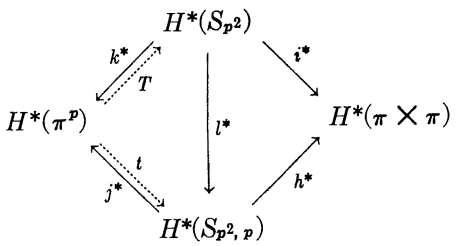
En el caso del grupo simétrico S_p de grado p, la inclusión de π, un p-grupo de Sylow en S_p , induce un monomorfismo

$$H^*(S_p\,;\, Z_p) \to H^*(\pi; Z_p)$$

sobre la subálgebra de $H^*(\pi; Z_p)$ de invariantes bajo los automorfismos inducidos por los elementos del normalizador de π en S_p . Este método para calcular $H^*(S_p\,;\, Z_p)$ se generaliza al caso del grupo simétrico de grado p^2.

En este caso consideramos también un p-grupo de Sylow $S_{p^2,p}$ de S_{p^2} , como se sabe $S_{p^2,p}$ es el producto completo (*wreath product*) $\pi \int \pi$, en donde π es un grupo cíclico de orden p.

Se tiene entonces el siguiente diagrama (con coeficientes en Z_p)



en donde π^p, $\pi \times \pi$ son ciertos subgrupos de $S_{p^2,p}$ (ver el Capítulo I, I.1 Notación), T, t son los homomorfismos de transferencia correspondientes, y los demás homomorfismos están inducidos por inclusión.

Ahora por la teoría general de la cohomología de los grupos finitos (ver [1]) se sabe que la inclusión $G_p \subset G$ de un p-grupo de Sylow G_p en un grupo finito G induce un isomorfismo de la p-componente primaria de $H^*(G; K)$ sobre una

* El autor desea expresar su agradecimiento al Prof. Norman Steenrod bajo cuya dirección se elaboró esta tesis.

subálgebra de $H^*(G_p\ ;\ K)$. Por consiguiente, en el diagrama l^* es un monomorfismo. Además como en el caso de grado p, por el segundo teorema de transferencia [1], la imagen de l^* está formada por elementos que tienen ciertas propiedades de invariancia bajo los automorfismos interiores de S_{p^2}. Además en el Capítulo I (Proposiciones 3.1 y 3.2) se establece que existe una representación como suma directa

$$H^*(S_{p^2,p}\ ;\ Z_p) \cong \operatorname{Im} j^* \oplus \operatorname{Im} h^*.$$

Esta a su vez, Proposición 1.1 y Proposición 2.1 del Capítulo II induce, via l^*, una representación en suma directa

$$H^*(S_{p^2}\ ;\ Z_p) \cong \operatorname{Im} k^*T \oplus \operatorname{Im} i^*,$$

esto nos determina la estructura aditiva del álgebra $H^*(S_{p^2}\ ;\ \mathrm{Z}_p)$.

Ahora, como se sabe,

$$H^*(\pi \times \pi;\ \mathrm{Z}_p) \cong E(u_1\ ,\ u_2\ ;\ 1) \otimes P(v_1\ ,\ v_2\ ;\ 2);$$

los automorfismos interiores de S_{p^2} determinan la acción de $GL(2;\ \mathrm{Z}_p)$, grupo de matrices no singulares de 2×2 con coeficientes en Z_p, en el álgebra $H^*(\pi \times \pi;\ Z_p)$. Estudiando los invariantes bajo esta acción, se obtienen descripciones explícitas de Im h^* y Im i^*.

En particular (Cap. III, Teorema 2), se prueba que Im i^* es la subálgebra de $H^*(\pi \times \pi;\ Z_p)$ de invariantes bajo $GL(2;\ Z_p)$.

Análogamente se sabe que

$$H^p(\pi^p;\ Z_p) \cong E(x_1\ ,\ \cdots\ ,\ x_p\ ;\ 1) \otimes P(y_1\ ,\ \cdots\ ,\ y_p\ ;\ 2),$$

en este caso los elementos del normalizador de π^p en S_{p^2} determinan la acción de S_p grupo simétrico en $H^*(\pi^p;\ Z_p)$, estudiando como antes los invariantes, bajo esta acción, se obtienen descripciones para Im j^*t y Im k^*T. Para obtener una descripición explícita de Im k^*T es necesario generalizar el teorema stándard sobre la estructura de la subálgebra simétrica de $P(y_1\ ,\ \cdots\ ,\ y_p)$ al caso $E(x_1\ ,\ \cdots\ ,\ x_p) \otimes P(y_1\ ,\ \cdots\ ,\ y_p)$ en donde las x_i se permutan simultáneamente con las y_i. Se obtiene una conclusión análoga, es decir (Cap. IV, Teorema 1), la subálgebra simétrica es de la forma $E(X_1\ ,\ \cdots\ ,\ X_p) \otimes P(Y_1\ ,\ \cdots,\ Y_p)$ para $X_i\ ,\ Y_i$ convenientes.

En el Capítulo V se da en el Teorema 1 la descripción de $H^*(S_{p^2}\ ;\ Z_p)$ como subálgebra de $H^*(S_{p^2,p}\ ;\ Z_p)$; el Teorema 2 del mismo capítulo da una descripción directa del álgebra $H^*(S_{p^2}\ ;\ Z_p)$; y, finalmente, las proposiciones 3.1 y 3.2 dan información acerca de la acción de $A(p)$ en las álgebras $H^*(S_{p^2,p}\ ;\ Z_p)$ y $H^*(S_{p^2}\ ;\ Z_p)$.

Capítulo I: Resultados Preliminares

1. Notación

Sea $E = \{1, 2, \cdots, p\}$, con p un número primo distinto de dos. Denotaremos con S_{p^2} el grupo de permutaciones de $E \times E$. Consideremos las siguientes permutaciones:

$$a(i, j) = (i + 1, j), \text{ mod } p,$$
$$b_k(i, j) = (i, j), \text{ si } i \neq k,$$
$$b_k(k, j) = (k, j + 1), \text{ mod } p,$$
$$d(i, j) = (i, j + 1), \text{ mod } p,$$

Denotaremos con

$S_{p^2,p}$ el subgrupo generado por $a, b_1, b_2, \cdots, b_p$;
π^p el subgrupo generado por $b_1, b_2, \cdots, b_p$;
$\pi \times \pi$ el subgrupo generado por a, d.

$S_{p^2,p}$ es un p-grupo de Sylow de S_{p^2} ; π^p es el producto directo de p grupos cíclicos de orden p; y $\pi \times \pi$ es producto directo de dos grupos cíclicos de orden p.

2. Un teorema de transferencia

PROPOSICIÓN 2.1. *Si ρ es un subgrupo propio de π^p, la transferencia de π^p en ρ es cero (coeficientes Z_p).*

Prueba. Ya que ρ es sumando directo de π^p, existen g, f, con g la inclusión de ρ en π^p,

$$\rho \underset{f}{\overset{g}{\rightleftarrows}} \pi^p,$$

y tales que fg = identidad; entonces

$$H^*(\rho, Z_p) \underset{g^*}{\overset{f^*}{\rightleftarrows}} H^*(\pi^p, Z_p),$$

con $(fg)^* = g^*f^*$ = identidad, de donde g^* es epimorfismo.

Consideremos la composición

$$H^*(\pi^p, Z_p) \xrightarrow{g^*} H^*(\rho, Z_p) \xrightarrow{t} H^*(\pi^p, Z_p)$$

en donde t es la transferencia de π^p en ρ. Se sabe (ver [1]) que

$$tg^*u = qu,$$

con q = índice de ρ en π^p; pero si ρ es subgrupo propio $q = pm$, ya que $pu = 0$ para toda u de $H^*(\pi, Z_p)$ y que g^* es epimorfismo, se obtiene $tv = 0$ para toda v de $H^*(\pi^p, Z_p)$.

3. Cohomología de $S_{p^2,p}$

Los resultados que se enuncian en este párrafo están demostrados en |2|.

Sea π grupo cíclico de orden p y W, el complejo stándard acíclico de π y sea también $K = W/\pi$. Consideremos las siguientes transformaciones:

$$(\epsilon \otimes 1)^*: H^*(W \otimes_\pi K^p, Z_p) \to H^*(K^p, Z_p),$$
$$(1 \otimes d)^*: H^*(W \otimes_\pi K^p, Z_p) \to H^*(W/\pi \otimes K, Z_p),$$
$$\tau: H^*(K^p, Z_p) \to H^*(W \otimes_\pi K^p, Z_p),$$
$$P: H^*(K, Z_p) \to H^*(W \otimes_\pi K^p, Z_p).$$

PROPOSICIÓN 3.1. *La sucesión*

$$H^*(K^p, Z_p) \to H^*(W \otimes_\pi K^p, Z_p) \xrightarrow{(1 \otimes d)^*} H^*(W/\pi \otimes K, Z_p)$$

es exacta.

PROPOSICIÓN 3.2. *La restricción de* $(\epsilon \otimes 1)^*$ *a la imagen de* τ *es un monomorfismo.*

PROPOSICIÓN 3.3. *Existe* $u_1, v_1 \in H^*(W/\pi, Z_p)$ $u_2, v_2 \in H^*(K, Z_p)$ *tales que*
(a) $H^*(W/\pi \otimes K, Z_p) \cong E(u_1, 1) \otimes P(v_1, 2) \otimes E(u_2, 1) \otimes P(v_2, 2)$ *y*
(b) Im $(1 \otimes d)^*$ *está generado por*

$$u_1, v_1, (1 \otimes d)^* P u_2 = (v_1 u_2 - u_1 v_2) v_1^{p-3/2} = u,$$
$$(1 \otimes d)^* P v_2 = v_2(v_2^{p-1} - v_1^{p-1}) = v.$$

PROPOSICIÓN 3.4. *Existen* $x_1, x_2, \cdots, x_p, y_1, \cdots, y_p$ *de* $H^*(K^p, Z_p)$, *y* α *endomorfismo del anillo* $H^*(K^p, Z_p)$ *tales que*
(a) $H^*(K^p, Z_p) = E(x_1, x_2, \cdots, x_p, 1) \otimes P(y_1, y_2, \cdots, y_p, 2)$
(b) $\alpha x_i = x_{i+1}$, $\alpha y_i = y_{i+1}$
(c) $(\epsilon \otimes 1)^* \tau z = \sum \alpha^r Z$, $r = 0, 1, \cdots, p-1$.

PROPOSICIÓN 3.5. *El anillo* $H^*(W \otimes_\pi K^p, Z_p)$ *está determinado por los anillos* Im $(1 \otimes d)^*$, *y* Im $(\epsilon \otimes 1)^* \tau$ *como sigue.*
(a) *Como módulo*

$$H^*(W \otimes_\pi K^p, Z_p) \cong \text{Im } (1 \otimes d)^* \oplus \text{Im } (\epsilon \otimes 1)^* \tau.$$

(b) *La multiplicación está determinada por* Im $(1 \otimes d)^*$, *es subanillo y* Im $(\epsilon \otimes 1)^* \tau$ *es ideal. Además:*

$$(z, 0)(0, u_1) = 0,$$
$$(z, 0)(0, v_1) = 0,$$
$$(z, 0)(0, u) = (z(\epsilon \otimes 1)^* P u_2, 0),$$
$$(z, 0)(0, v) = (z(\epsilon \otimes 1)^* P v_2, 0) \text{ y}$$
$$(\epsilon \otimes 1)^* P u_2 = x_1 x_2 \cdots x_p,$$
$$(\epsilon \otimes 1)^* P v_2 = y_1 y_2 \cdots y_p.$$

Se tienen las siguientes identificaciones:

$$H^*(W \otimes_\pi K^p, Z_p) = H^*(S_{p^2,p}, Z_p),$$
$$H^*(K^p, Z_p) = H^*(\pi^p, Z_p), \text{ y}$$
$$H^*(W/\pi \otimes K, Z_p) = H^*(\pi \times \pi, Z_p).$$

Además, si $j: \pi^p \subset S_{p^2,p}$, $h: \pi \times \pi \subset S_{p^2,p}$ y t es la transferencia de $S_{p^2,p}$ a π^p, se tiene

$$j^* = (\epsilon \otimes 1)^*, \qquad h^* = (1 \otimes d)^*, \qquad \tau = t.$$

4. Normalizador de π^p en S_{p^2}

LEMA 1. *Si z es una permutación de renglones, entonces z pertenece a N_1, N_1 es el normalizador de π^p en S_{p^2}.*

Prueba. z es de la forma

$$z(i, j) = (z(i), j).$$

sea h tal que $z^{-1}(h) = k$. Se verifica directamente que

$$zb_kz^{-1} = b_h .$$

LEMA 2. *Sea ρ_k el subgrupo de S_{p^2} generado por las permutaciones*

$$c_k(i, j) = (i, j), \quad si \quad i \neq k, \quad \text{y}$$

$$c_k(k, j) = (k, hj) \ mod\ p, \qquad h = 1, 2, \cdots, p - 1;$$

entonces ρ_k está contenido en N_1.

Prueba. En efecto

$$c_kb_kc_k^{-1} = b_k^h, \quad \text{y}$$

$$c_kb_jc_k^{-1} = b_j, \quad \text{si} \quad j \neq k.$$

Es inmediato que el subgrupo generado por ρ_i, $i = 1, 2, \cdots, p$ es isomorfo al producto directo, $\rho = \rho_1 \times \cdots \times \rho_p$.

Sea N el subgrupo generado por ρ y π^p. Entonces:

PROPOSICIÓN 4.1. *La sucesión*

$$1 \to N \to N_1 \xrightarrow{\phi} S_p \to 1$$

es exacta, y se divide. S_p es el grupo de permutaciones de los renglones de $E \times E$, y ϕ se define como sigue.

Sea $x \in N_1$; entonces,

$$xdx^{-1} = b$$

$$b(i, j) = (i, j + r(i)) \quad \text{y} \quad r(i) \neq p.$$

Sea $x(i, p) = (m(i), n(i))$; se tiene

$$x(i, j) = xd^j(i, p) = b^jx(i, p) = b^j(m(i), n(i)) = (m(i), n(i) + jr(m(i))).$$

Lo anterior prueba que x *transforma el renglón i en el renglón $m(i)$*; es decir, $m(i, j) = (m(i), j)$ es una permutación de renglones. Definimos entonces

$$\phi x(i, j) = (m(i), j),$$

en donde $m(i)$ se define como antes. ϕ *es un homomorfismo*, ya que

$$xx'(i, p) = (m''(i), n''(i) = x(m'(i), n'(i))$$

$$= (m(m'(i)),\ n(m'(i)) + n'(i)r(m(m'(i))));$$

es decir, $m''(i) = m(m'(i))$.

De la definición de ϕ, se verifica directamente la proposición 4.1.

PROPOSICIÓN 4.2. *El subgrupo $S_p\rho$ (generado por S_p y ρ) de N_1 es un sistema de representantes de clases izquierdas de π^p en N_1.*

Prueba. Ya que, si $z \in S_p$, $z\rho z^{-1} = \rho$, se tiene que todo elemento de $S_p\rho$ es de la forma zc con z en S_p y c en ρ. La expresión es única ya que si $zc = z'c'$, entonces $(z')^{-1}z = c'c^{-1}$ de donde

$$(z')^{-1}z \in N \cap S_p = 1;$$

es decir $z = z'$ y $c = c'$ por lo tanto el orden de $S_p\rho$ es $p!(p-1)^p$ igual al índice de π^p en N_1. Además, si $y'c' = ycb$ entonces $(y^{-1})y' \in N$ y por lo anterior, $y = y'$ y $c^{-1}c' = b$ pero $\pi^p \cap \rho = 1$ de donde $c = c'$.

5. Normalizador de $\pi \times \pi$ en S_{p^2}

Sea N_2 el normalizador de $\pi \times \pi$ en S_{p^2}, definiremos un homomorfismo

$$\psi: N_2 \to GL,$$

en donde GL es el grupo de las matrices no singulares de 2×2, con coeficientes en Z_p, el campo de los enteros mod p.

Si $x \in N_2$, entonces

$$xdx^{-1} = d^r a^s \quad \text{y} \quad xax^{-1} = d^{r'}a^{s'}.$$

Definimos

$$\psi(x) = \begin{pmatrix} r & r' \\ s & s' \end{pmatrix}.$$

Evidentemente $\psi(x)$ es no singular.

Sea $c \in \rho$, definida por $c(i, j) = (i, kj)$, $k = 1, 2, \cdots, p-1$; entonces $c \in N_2$ y

$$\psi(c) = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}.$$

En efecto,

$$cdc^{-1}(i, kj) = c(i, j+1) = (i, kj + k) = d^k(i, kj) \quad \text{y}$$

$$cac^{-1}(i, kj) = c(i+1, j) = (i+1, kj) = a(i, kj).$$

Sea $b \in \pi^p$ definida por

$$b(i, j) = (i, j + i - 1);$$

entonces $b \in N_2$ y

$$\psi(b) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

En efecto,

$$bdb^{-1} = d \quad \text{y}$$

$$bab^{-1}(i,j) = b(i+1, j-(i-1)) = (i+1, j+1) = da(i,j).$$

Sea $w \in S_{p^2}$ *definida por*

$$w(i,j) = (j,i);$$

entonces $w \in N_2$ y

$$\psi(w) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

En efecto

$$wdw^{-1}(i,j) = w(j, i+1) = (i+1, j) = a(i,j) \quad \text{y}$$

$$waw^{-1}(i,j) = w(j+1, i) = (i, j+1) = d(i,j).$$

El grupo GL está generado por

$$S = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

ya que

(a) $$\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} r & r' \\ s & s' \end{pmatrix} = \begin{pmatrix} kr & kr' \\ s & s' \end{pmatrix},$$

(b) $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r & r' \\ s & s' \end{pmatrix} = \begin{pmatrix} s & s' \\ r & r' \end{pmatrix},$$

(c) $$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} r & r' \\ s & s' \end{pmatrix} = \begin{pmatrix} r+s & r'+s' \\ s & s' \end{pmatrix}.$$

Un cálculo usual prueba que aplicando (a), (b), (c) toda matriz se puede llevar a la matriz identidad, es decir, que S, T, U generan a GL, lo que implica que ψ es epimorfismo.

PROPOSICIÓN 5.1. *La sucesión*

$$1 \to \pi \times \pi \to N_2 \to GL \to 1$$

es exacta.

En efecto, si $x \in \pi \times \pi$,

$$xax^{-1} = a \quad \text{y} \quad xdx^{-1} = d.$$

Además,

$$si \quad xax^{-1} = a \quad y \quad xdx^{-1} = d, \quad entonces \quad x \in \pi \times \pi$$

Prueba. Se tiene $xa^i = a^i x$. Sea $x(p, j) = (m(j), n(j))$; entonces

$$x(i, j) = xa^i(p, j) = a^i x(p, j) = a^i(m(j), n(j))$$
$$= (m(j) + i, n(j)).$$

Además,

$$x(p, j) = xd^j(p, p) = d^j x(p, p) = d^j(m(p), n(p))$$
$$= (m(p), n(p) + j);$$

es decir,

$$m(j) = m(p), \qquad n(j) = n(p) + j.$$

Finalmente,

$$x(i, j) = (i + m(p), j + n(p)) = a^{m(p)} d^{n(p)}(i, j).$$

Sea $N_2' \subset N_2$ el normalizador de $\pi \times \pi$ en $S_{p^2,p}$; entonces tenemos

PROPOSICIÓN 6.1. *La imagen* Im (ψ/N_2') *es el subgrupo de las matrices de la forma*

$$U^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \qquad r = 0, 1, \cdots, p - 1.$$

Prueba. Si $x \in S_{p^2,p}$, x es de la forma $x = a^n b$; supongamos $x \in N_2'$; entonces

$$(a^n b)\, d(a^n b)^{-1} = d \quad \text{y}$$
$$(a^n b) a (a^n b)^{-1} = a^r d^s,$$

de donde $bab^{-1} = a^r d^s$, por lo tanto $a \cdot (a^{-1} ba) \cdot b^{-1} = a^r d^s$; es decir, $r = 1$, por lo que

$$\psi(a^n b) = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}.$$

CAPÍTULO II: UNA SUCESIÓN EXACTA

1. Exactitud de una sucesión

PROPOSICIÓN 1.1. *La sucesión*

$$\hat{H}^*(\pi^p, Z_p) \xrightarrow{T} \hat{H}^*(S_{p^2}, Z_p) \xrightarrow{i^*} \hat{H}^*(\pi \times \pi, Z_p)$$

es exacta.

$\hat{H}$ denota los elementos de grado mayor que cero; T está inducido por la transferencia de S_{p^2} en π^p; y i^* está inducido por la inclusión de $\pi \times \pi$ en S_{p^2}.

Prueba.

a) No existe $x \in S_{p^2}$ tal que

$$x^{-1}\pi^p x \cap \pi \times \pi = \pi \times \pi.$$

fecto, si

$$a = x^{-1}bx, \qquad d = x^{-1}b'x, \quad \text{y} \quad b \cdot b' \in \pi^p,$$

$(p, p) = (m, n)$; entonces

$$x(i, p) = xa^i(p, p) = b^i x(p, p) = (m, n + ir(m)).$$

nás,

$$x(i, j) = xd^j(i, p) = (b')^j x(i, p) = (m, n + ir(m) + jr'(m))$$

toda (i, j), lo que es imposible.

b) La composición $i^*T = 0$. Sea $x \in S$; por a), $x^{-1}\pi^p{}_x \cap \pi \times \pi$ es un rupo propio de $\pi \times \pi$, (o la identidad). Por consiguiente la transferencia

$$t_x : H^*(x^{-1}\pi^p x \cap \pi \times \pi, Z_p \to H^*(\pi \times \pi; Z_p)$$

ro (ver Prop. 2.1, Cap. I). Aplicando ahora el segundo teorema de trans- ıcia, se obtiene $i^*T = 0$.

c) Si $i^*(u) = 0$, existe $z \in H^*(\pi^p, Z_p)$ tal que $T(z) = u$. Consideremos

$$\begin{array}{ccccc} H^*(\pi^p; Z_p) & & & & H^*(\pi \times \pi; Z_p) \\ \downarrow t & \searrow T & & \nearrow i^* & \uparrow h^* \\ H^*(S_{p^2,p}, Z_p) & \xrightarrow[t']{} & H^*(S_{p^2}, Z_p) & \xrightarrow[l']{} & H^*(S_{p^2,p}, Z_p), \end{array}$$

e $i^* = h^*l^*$ y $T = t't$. $i^*(u) = 0$ implica que $h^*l^*(u) = 0$; es decir, $l^*(u)$ ence a Ker h^*. Pero por Proposición 3.1 del Capítulo I, existe $z \in H^*(\pi^p; Z_p)$ ue $tz = l^*(u)$. Ahora

$$t'tz = t'l^*(u) = ru,$$

nde r es el índice de $S_{p^2,p}$ en S_{p^2}, y, por consiguiente, $r \not\equiv 0 \bmod p$, de e

$$\frac{1}{r} Tz = \frac{1}{r} t'tz = u.$$

2. La imagen de la transferencia

OPOSICIÓN 2.1. *La restricción*

$$k^*/\mathrm{Im}\ T : \mathrm{Im}\ T \to H^*(\pi^p; Z_p)$$

monomorfismo.

nsideremos

$$H^*(S_{p^2}; Z_p) \xrightarrow{l^*} H^*(S_{p^2,p}; Z_p) \xrightarrow{j^*} H^*(\pi^p; Z_p),$$

con $k^* = j^*l^*$; ya que l^* es un monomorfismo (ver [1]) y que $j^*/\mathrm{Im}\ t$, por la Proposición 2.2 del Capítulo I, basta observar que $l^*(\mathrm{Im}\ T) \subset \mathrm{Im}\ t$, es decir que $h^*l^*t't = 0$; pero esto es cierto por la proposición anterior.

PROPOSICIÓN 2.2. *La composición k^*T es tal que $k^*T = \sum ad_x$, con $x \in X$ (X un sistema de representantes de clases laterales de π^p en N_1) y ad_x es el homomorfismo*

$$ad_x : H^*(\pi^p; Z_p) \to H^*(\pi^p; Z_p)$$

inducido por el automorfismo de π^p en π^p definido por xyx^{-1} (y en π^p, x en N_1).

Prueba. Por el segundo teorema de transferencia, $k^*T = \sum t_x i_x ad_x$; pero, por Proposición 2.1, del Capítulo I, $t_x = 0$, si $x \notin N_1$; y si $x \notin N_1$, $t_x i_x ad_x = ad_x$.

Lo anterior podemos resumirlo en el

TEOREMA 1. *La imagen de T en $H^*(S_{p^2}; Z_p)$ es isomorfa al subanillo de $H^*(\pi^p; Z_p)$ imagen de $\sum ad_x$, el isomorfismo está dado por $k^*/\mathrm{Im}\ T$.*

3. El homomorfismo i^*

Sea F el subgrupo de GL generado por las matrices

$$R = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}, \qquad S = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Los elementos de F son de la forma $U^rS^sR^t$ donde $s,\ t = 0, 1, \cdots, p-2$ y $r = 0, 1, \cdots, p-1$; esto es consecuencia de

$$RS = SR, \qquad R^{-1}UR = U^k, \quad \text{y} \quad SUS^{-1} = U^k.$$

Este subgrupo se puede caracterizar como el de las matrices triangulares,

$$\begin{pmatrix} l & m \\ 0 & n \end{pmatrix}.$$

De lo anterior se obtiene que el orden de F es $p(p-1)^2$.

PROPOSICIÓN 3.1. *Un sistema de representantes de clases izquierdas de F en GL está dado por $T, P, P^2, \cdots, P^{p-1}, I$ con*

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Prueba. Ya que el índice de F en GL es $p+1$, basta probar que

$$TP^r \notin F, \qquad P^r \notin F.$$

En efecto,

$$TP^r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} = \begin{pmatrix} r & 1 \\ 1 & 0 \end{pmatrix} \notin F,$$

$$P^r = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \notin F, \quad \text{si} \quad r \neq 0.$$

ea $M \in GL$. Por la Proposición 5.1 del Capítulo I, se sabe que existe N_2 tal que $\psi(x) = M$; entonces el automorfismo $ad_x(y) = xyx^{-1}$ induce $:H^*(\pi \times \pi; Z_p) \to H^*(\pi \times \pi; Z_p)$. Además si $x^{-1}x' \in \pi \times \pi$, entonces $= ad_{x'}$. Definimos entonces, para $u \in H^*(\pi \times \pi; Z_p)$ y $M \in GL$,

$$M \cdot u = ad_x(u),$$

$\psi(x) = M$.

ROPOSICIÓN 3.2. *Si* u_1, u_2, v_1, v_2 *en* $H^*(\pi \times \pi; Z_p)$ *son los de la Proposicion de Capítulo I, entonces*

$$\begin{pmatrix} r & r' \\ s & s' \end{pmatrix} \cdot (nu_1 + mu_2) = (rn + r'm)u_1 + (sn + s'm)u_2,$$

$$\begin{pmatrix} r & r' \\ s & s' \end{pmatrix} \cdot (nv_1 + mv_2) = (rn + r'm)v_1 + (sn + s'm)v_2.$$

ROPOSICIÓN 3.3. *El homomorfismo*

$$\Sigma_F : H^*(\pi \times \pi; Z_p) \to H^*(\pi \times \pi; Z_p)$$

nido por

$$\Sigma_F \cdot z = \sum M \cdot z, \quad con \quad M \in F,$$

ıl que

$$\Sigma_F \cdot {v_2}^{p-1} = -{v_1}^{p-1}.$$

rueba. Sea F_1 el subgrupo de F generado por R, S; entonces

$$F = F_1 \cup UF_1 \cup \cdots \cup U^{p-1}F_1$$

ına descomposición de F en clases laterales izquierdas. Se tiene

$$\Sigma_F = \Sigma_{F_1} + U\Sigma_{F_1} + \cdots + U^{p-1}\Sigma_{F_1} \quad \text{y}$$

$$U^k\Sigma_{F_1} \cdot {v_2}^{p-1} = U^k \cdot {v_2}^{p-1}$$

londe se obtiene

$$\Sigma_F {v_2}^{p-1} = (I + U + \cdots + U^{p-1}){v_2}^{p-1}.$$

ectamente se verifica

$${v_2}^{p-1} + (v_2 + v_1)^{p-1} + \cdots + (v_2 + (p-1)v_1)^{p-1} = -{v_1}^{p-1} \mod p$$

ROPOSICIÓN 3.4. *La composición*

$$H^*(\pi \times \pi; Z_p) \xrightarrow{\tilde{T}} H^*(S_{p^2}; Z_p) \xrightarrow{i^*} H^*(\pi \times \pi; Z_p)$$

ıl que $i^* \tilde{T} = \Sigma_{GL}$.

Prueba. Por el segundo teorema de transferencia, $i^*\tilde{T} = \sum t_x i_x a d_x$; pero, por la Proposición 2.1 del Capítulo I, se tiene que $t_x i_x a d_x = 0$ si $x \in N_2$ y, además, $t_x i_x a d_x = a d_x$, la x recorre un sistema de representantes de $\pi \times \pi$ en GL, de donde

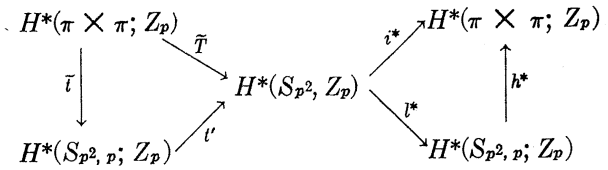
$$i^*\tilde{T} = \Sigma_{GL} .$$

PROPOSICIÓN 3.5. *La composición*

$$H^*(\pi \times \pi; Z_p) \xrightarrow{\tilde{\imath}} H^*(S_{p^2,p} ; Z_p) \xrightarrow{h^*} H^*(\pi \times \pi; Z_p)$$

es tal que $h^*\tilde{\imath} = \sum U^r$, $r = 0, 1, \cdots, p - 1$.

Prueba. La demostración es análoga a la de la Proposición 3.3. Consideremos el diagrama



PROPOSICÍON 3.6. *$h^*\tilde{\imath}z$ es invariante bajo GL si y sólo si $h^*\tilde{\imath}z = i^*\tilde{T}z$.*

Prueba.

$$\begin{aligned}\Sigma_{GL} &= \Sigma_F z + P\Sigma_F z + \cdots + P^{p-1}\Sigma_F z + T\Sigma_F z \\ &= (I + P + \cdots + P^{p-1} + T)\Sigma_F z = \Sigma_F z.\end{aligned}$$

PROPOSICIÓN 3.7. *Si $h^*\tilde{\imath}z = i^*\tilde{T}z$, entonces*

$$i^*\tilde{T}(z \cdot h^*u) = (i^*\tilde{T}z) \cdot (i^*t'u).$$

Prueba. Sea $u' = \tilde{\imath}z - l^*\tilde{T}z$; entonces

$$\begin{aligned}i^*\tilde{T}(z \cdot h^*u) &= i^*t'(\tilde{\imath}z \cdot u), \\ &= i^*t'[(u' + l^*\tilde{T}z) \cdot u], \\ &= i^*t'(u' \cdot u) + i^*t'(l^*\tilde{T}z \cdot u).\end{aligned}$$

Pero, por hipótesis, $u' \cdot u$ pertenece a $\ker h^*$ que es igual a Im t. (Prop. 3.1. Cap. I); además, $i^*t't = i^*T = 0$ (Prop. 1.1, Cap. II), de donde $i^*t(u' \cdot u) = 0$, por lo tanto

$$\begin{aligned}i^*\tilde{T}(z \cdot h^*u) &= i^*t'(l^*\tilde{T}z \cdot u) = i^*(Tz \cdot t'u) \\ &= i^*Tz \cdot i^*t'u.\end{aligned}$$

PROPOSICIÓN 3.8. *Si z y w pertenecen a $E(u_1, u_2 ; 1) \otimes P(v_1, v_2 ; 2)$ y z es un polinomio en v_1, v_2 distinto de cero, entonces $z \cdot w = 0$ implica $w = 0$.*

PROPOSICIÓN 3.9. *El polinomio $C = v_1^{p-1} \cdot v_2^{p-1}(v_2^{p-1} - v_1^{p-1})^{p-1}$ es invariante*

bajo GL y

$$C = h^*tv_2^{p-1}(v_2^{p-1} - v_1^{p-1})^{p-1}.$$

Prueba. Por la Proposición 3.6 del Capítulo I,

$$h^*(v^{p-1}) = v_2^{p-1}(v_2^{p-1} - v_1^{p-1})^{p-1};$$

entonces

$$t(v_2^{p-1}\cdot h^*(v^{p-1})) = tv_2^{p-1}\cdot(v^{p-1}) \quad \text{y}$$

$$h^*t(v_2^{p-1}\cdot h^*(v^{p-1})) = h^*tv_2^{p-1}\cdot h^*(v^{p-1} = -v_1^{p-1}\cdot v_2^{p-1}(v_2^{p-1} - v_1^{p-1})^{p-1}$$

por la Proposición 3.3 del Capítulo II; ya que, por Proposición 3.5 del Capítulo II, $h^*t = I + U + \cdots + U^{p-1}$, se tiene que

$$U\cdot C = C.$$

Además, si

$$S = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

evidentemente $S\cdot C = C$ y $T\cdot C = C$; y, ya que S, T, U son generadores de GL, esto termina la prueba.

PROPOSICIÓN 3.10. *Si h^*u es invariante bajo GL, entonces h^*u pertenece a la imagen de i^*.*

Prueba. Sea $z \in H^*(\pi \times \pi; Z_p)$ tal que h^*tz sea invariante bajo GL. Entonces $h^*tz = i^*\tilde{T}z$, por Proposición 3.5 del Capítulo II. Además,

$$i^*\tilde{T}(z\cdot h^*u) = i^*\tilde{T}z\cdot i^*Th^*u = h^*t;$$

pero $h^*\tilde{\imath}(c\cdot h^*u) = h^*(\tilde{\imath}c\cdot u) = h^*\tilde{\imath}c\cdot h^*u$ es invariante bajo GL. Entonces (por Prop. 3.6, Cap. II)

$$i^*\tilde{T}(c\cdot h^*u) = h^*\tilde{\imath}(c\cdot h^*u) = h^*\tilde{\imath}c\cdot h^*u;$$

entonces

$$h^*\tilde{\imath}c\cdot h^*u = h^*\tilde{\imath}c\cdot i^*t'u.$$

Pero $h^*\tilde{\imath}c$ es un polinomio distinto de cero; por lo tanto (Prop. 3.8, Cap. II)

$$h^*u = i^*t'u.$$

CAPÍTULO III: LA SUBÁLGEBRA DE ELEMENTOS INVARIANTES BAJO *GL*

1. Subálgebra invariante bajo *F*

Sea GL como en el capítulo anterior. Denotaremos como antes F el subgrupo generado por

$$R, S, U;$$

y $E(u_1, u_2; 1) \otimes P(v_1, v_2; 2)$ es el álgebra $H^*(\pi \times \pi; Z_p)$.

$$a_0 v_1^{\,n} + a_1 v_1^{\,n-p}(v_2(v_2^{\,p-1} - v_1^{\,p-1})) + \cdots + a_m v_1^{\,r}(v_2(v_2^{\,p-1} - v_1^{\,p-1}))^m = 0.$$

mo polinomio en v_1 y v_2, el coeficiente de $v_1^{\,n}$ es a_0; por lo tanto $a_0 = 0$. Sungamos que $a_0 = a_1 = \cdots = a_{q-1} = 0$, para $q - 1 < m$; el coeficiente de $^{-pq}v_2^{\,q}$, como polinomio en v_1, v_2, es a_q; por lo tanto $a_q = 0$.

PROPOSICIÓN 1.4. *Si z es un polinomio homogéneo en v_1, v_2 y tal que es invariante o F, entonces está generado por*

$$v_1^{\,p-1},\ v_2^{\,p-1}(v_2^{\,p-1} - v_1^{\,p-1})^{p-1}.$$

Prueba. Ya que $U \in F$, se sabe por la Proposición 1.1 de este capítulo que

$$z = \sum a_s v_1^{\,n-s}(v_2(v_2^{\,p-1} - v_1^{\,p-1}))^s.$$

ora

$$z - Rz = \sum a_s(1 - k^s)v_1^{\,n-s}(v_2(v_2^{\,p-1} - v_1^{\,p-1}))^s = 0,$$

or la proposición anterior se obtiene

$$a_s(1 - k^s) = 0.$$

emás

$$z - Sz = \sum a_s(1 - k^{n-s})v_1^{\,n-s}(v_2(v_2^{\,p-1} - v_1^{\,p-1}))^s = 0,$$

donde

$$a_s(1 - k^{n-s}) = 0,$$

que implica que los únicos coeficientes que pueden ser distintos de cero son a_s n $s \equiv 0$ y $n - s \equiv 0 \bmod (p - 1)$.

PROPOSICIÓN 1.5. *Si z es de la forma $z = u_1u_2z'$, con z' polinomio homogéneo en v_2 y tal que es invariante bajo R, entonces z es de la forma*

$$z = u_1u_2v_1^{\,p-2}v_2^{\,p-2}(v_2^{\,p-1} - v_1^{\,p-1})^{p-2}\cdot z'',$$

n z'' *invariante bajo F.*

Prueba. Ya que $z = u_1u_2z' = Uz = u_1u_2\cdot Uz'$, se tiene $z' = Uz'$, de donde $= \sum a_s v_1^{\,n-ps}v_2^{\,s}(v_2^{\,p-1} - v_1^{\,p-1})^s$, con $n = pq + r$, $0 < r < p$, y $s = 0, 1, \cdots, q$. emás,

$$Rz = ku_1u_2\cdot Rz' = u_1u_2z' \quad \text{y} \quad Sz = ku_1u_2\cdot Sz' = u_1u_2z',$$

donde

$$kRz' = z', \qquad kSz' = z',$$

donde

$$kRz' - z' = 0 \quad \text{por lo que} \quad a_s(k^{s+1} - 1) = 0.$$

particular, si $s = 0, 1, \cdots, p - 2$, $a_s = 0$. Además, $kSz' - z' = 0$, de donde

PROPOSICIÓN 1.1. *Si z es un polinomio homogéneo en v_1, v_2 tal que $Uz = z$, entonces z está generado por*

$$v_1,\ v_2(v_2^{p-1} - v_1^{p-1}).$$

Prueba. Si z es de primer grado, se tiene $av_1 + bv_2 = av_1 + b(v_1 + v_2) = (a + b)v_1 + bv_2$ de donde $a + b = a$; es decir, $b = 0$ de donde $z = av_1$.

Supongamos la proposición cierta para polinomios de grado menor que n. Entonces sea $n = mp + r$, con $0 < r < p$.

Primer caso, $(r \neq 0)$: Consideremos

$$z = a_s v_1^{n-s} v_2^{s} \quad \text{y} \quad Uz = \sum a_s v_1^{n-s}(v_1 + v_2)^s.$$

El coeficiente de $v_1 v_2^{n-1}$ en Uz es $na_n + a_{n-1}$. Si $z = Uz$, se tiene $na_n + a_{n-1} = a_{n-1}$, de donde $na_n = 0$ y, por lo tanto, $a_n = 0$; es decir, $z = v_1 z'$. Ahora $Uz = Uv_1 \cdot Uz' = v_1 \cdot Uz' = v_1 \cdot z'$, de donde

$$Uz' = z'.$$

Segundo caso, $(r = 0)$: Sea

$$z' = z - a_n(v_2(v_2^{p-1} - v_1^{p-1}))^m;$$

entonces $Uz' = z'$ y es de la forma $z' = v_1 z''$ con $Uz'' = z''$.

Usando la hipótesis de inducción en cada uno de los casos se obtiene la afirmación de la proposición.

PROPOSICIÓN 1.2. *Si $z = u_1 z_1 + u_2 z_2$, con z_1, z_2 polinomios homogéneos en v_1, v_2, es tal que $Uz = z$, entonces z es de la forma*

$$z = u_1 z_1' + (u_2 v_1 - u_1 v_2) z_2',$$

con $Uz_1' = z_1'$ y $Uz_2' = z_2'$.

Prueba. Se tiene $Uz = u_1 Uz_1 + (u_1 + u_2)Uz_2 = u_1(Uz_1 + Uz_2) + u_2 Uz_2$. Si $Uz = z$, entonces $Uz_2 = z_2$ y $z_1 = U(z_1 + z_2)$ de donde $z_2 = z_1 - Uz_1$. Sea ahora $z_1 = av_2^n + v_1 z_1^*$. Entonces $Uz_1 = a(v_1 + v_2)^n + v_1 Uz_1^*$; por lo tanto,

$$z_2 = z_1 - Uz_1 = v_1 \cdot z_2'$$

y, ya que $Uz_2 = z_2 = v_1 \cdot Uz_2' = v_1 z_2'$, se tiene que $Uz_2' = z_2'$. Tenemos entonces

$$\begin{aligned} z &= u_1 z_1 + u_2 v_1 z_2' - u_1 v_2 z_2' + u_1 v_2 z_2' \\ &= u_1(z_1 + v_2 z_2') + (u_2 v_1 - u_1 v_2) z_2'. \end{aligned}$$

Sea $z_1' = z_1 + v_2 z_2'$. Se tiene, finalmente,

$$Uz_1' = Uz_1 + (v_1 + v_2)Uz_2' = Uz_1 + v_1 z_2' + v_2 z_2' = z_1 + v_2 z_2' = z_1'.$$

PROPOSICIÓN 1.3. *Los monomios de grado n en v_1, $v_2(v_2^{p-1} - v_1^{p-1})$ son linealmente independientes.*

Prueba. Sea $n = mp + r$, con $0 < r < p$, y

$a_s(k^{n-ps+1} - 1) = 0$; en particular, si $s = q$, entonces $a_s(k^{r+1} - 1) = 0$, y si $r \neq p - 2$, $a_s = 0$. En cualquier caso,

$$z' = v_1^{p-2}v_2^{p-2}(v_2^{p-1} - v_1^{p-1})^{p-2} \cdot z'',$$

ya que $u_1u_2v_1^{p-2}v_2^{p-2}(v_2^{p-1} - v_1^{p-1})^{p-2}$ es invariante bajo F, y z'' también lo es.

PROPOSICIÓN 1.6. *Si* $z = u_1z_1 + u_2z_2$, *con* z_1, z_2 *polinomios homogéneos en* v_1, v_2 *y tal que es invariante bajo* F, *entonces* z *es de la forma*

$$z = u_1v_1^{p-2}z_1' + (u_2v_1 - u_1v_2)v_1^{p-2}v_2^{p-2}(v_2^{p-1} - v_1^{p-1})^{p-2}z_2',$$

con z_1', z_2' *invariantes bajo* F.

Prueba. Ya que, en particular, $Uz = z$, se puede expresar z en la forma (Prop. 1.2, Cap. III)

$$z = u_1z_1^* + (u_2v_1 - u_1v_2)z_2^*,$$

con $Uz_1^* = z_1^*$, $Uz_2^* = z_2^*$. Ahora $Sz = ku_1Sz_1^* + k(u_2v_1 - u_1v_2)Sz_2^* = z$, de donde $kSz_1^* = z_1^*$ $kSz_2^* = z_2^*$. Además,

$$Rz = u_1Rz_1^* + k(u_2v_1 - u_1v_2)Rz_2^*$$

que implica

$$Rz_1^* = z_1^*, \qquad kRz_2^* = z_2^*.$$

Como en la proposición anterior, esto implica

$$z_2^* = v_1^{p-2}v_2^{p-2}(v_2^{p-1} - v_1^{p-1})^{p-2} \cdot z_2' \quad \text{y}$$
$$z_1^* = v_1^{p-2}z_1',$$

con z_1' y z_2' invariantes bajo F.

PROPOSICIÓN 1.7. *La subálgebra de* $E(u_1, u_2; 1) \otimes P(v_1, v_2; 2)$ *de elementos invariantes bajo* F *está generada por*

$$A = u_1v_1^{p-2},$$
$$B = v_1^{p-1},$$
$$C = u_1u_2 \cdot v_1^{p-2}v_2^{p-2}(v_2^{p-1} - v_1^{p-1})^{p-2},$$
$$D = (u_2v_1 - u_1v_2)v_1^{p-2}v_2^{p-2}(v_2^{p-1} - v_1^{p-1})^{p-2}, \quad \text{y}$$
$$E = v_2^{p-1}(v_2^{p-1} - v_1^{p-1})^{p-1}.$$

Prueba. Esta proposición es consecuencia de las proposiciones anteriores, y de que estos elementos son invariantes bajo F. (Esto último se obtiene de la Prop. 3.6, Cap. I.) Ya que los elementos de la imagen de h^* son invariantes bajo U, la invariancia bajo R, S se verifica directamente.

$$A = u_1v_1^{p-2} = h^*(xy^{p-2}),$$
$$B = v_1^{p-1} = h^*(y^{p-1}),$$

$$C = u_1u_2v_1^{p-2}v_2^{p-2}(v_2^{p-1} - v_1^{p-1})^{p-2} = h^*(xy^suv^{p-2}),$$
$$E = v_2^{p-1}(v_2^{p-1} - v_1^{p-1})^{p-1} = h^*(v^{p-1}).$$

2. Subálgebra invariante bajo GL

Combinando la proposición anterior con la Proposición 3.10 del Capítulo II, se obtiene:

TEOREMA 2. *La subálgebra de $H^*(\pi \times \pi; Z_p)$ de elementos invariantes bajo GL es igual a la imagen de i^*.*

3. Generadores del álgebra invariante bajo GL

PROPOSICIÓN 3.1. *Si z es un polinomio invariante bajo GL, entonces z está generado por*

$$B^p + E, BE.$$

Prueba. Por el párrafo anterior, z es de la forma

$$z = a_0B^n + a_1B^{n-p}E + \cdots + a_mB^rE^m,$$

con $n = mp + r$, $0 < r < p$. Si $r \neq 0$, entonces $a_0 = 0$, ya que

$$z = a_0(v_1^{p-1})^n + B\cdot Ez' = a_0v_1^{n(p-1)} + v_1v_2z'',$$

con z'' un polinomio en v_1, v_2. Ahora $Tz = a_0v_2^{n(p-1)} + v_1v_2Tz'' = a_0v_1^{n(p-1)} + v_1v_2Tz''$, lo que implica $a_0 = 0$. Si $r = 0$,

$$z - a_0(B^p + E)^m = B\cdot E\cdot z',$$

ya que $B\cdot E$, $B^p + E$ son invariantes bajo GL. En ambos casos z está generado por $B^p + E$, BE, y polinomios de grado menor invariantes bajo GL. Inductivamente se obtiene la proposición.

PROPOSICIÓN 3.2. *Si z es de la forma*

$$z = u_1z_1 + u_2z_2,$$

con z_1, z_2 polinomios homogéneos en v_1, v_2, entonces z está generada por

$$B^p + E, BE, AE + BD, C, D.$$

Prueba. Por una proposición anterior (Prop. 1.6 de este capítulo), se sabe que $z = Az_1' + Dz_2'$, con z_1', z_2' polinomios homogéneos invariantes bajo F.

$$Bz = B\cdot z_1' + ABz_1' = Bz_1' \quad \text{y}$$
$$T(Bz_1') = Bz_1',$$

de donde $Bz' = BEz''$, por lo que $z_1' = Ez_1''$ y $Tz'' = z''$. Sea ahora

$$z^* = Az_1' + BDz'' = (AE + BD)z''$$

la diferencia

$$z - z^* = Dz_2{}^* - BDz'' = D(z_2{}' - Bz'');$$

pero, ya que $TD = D$ y $Tz^* = z^*$, se tiene $T(z_2{}' - Bz'') = z_2{}' - Bz''$, de donde, por la proposición anterior, queda terminada la demonstración.

PROPOSICIÓN 3.3. *Si z es de la forma $z = u_1u_2z'$, con z' polinomio homogéneo en v_1, v_2, entonces z está generado por*

$$B^p + E, BE, AE + BD, C, D.$$

Prueba. Por la Proposición 1.5 del Capítulo III, $z = Cz''$, con z'' polinomio homogéneo invariante bajo F, y z'' es además invariante bajo T, ya que

$$Tz = TC \cdot Tz'' = C \cdot Tz'' = C \cdot z'',$$

de donde, por una proposición anterior, $Tz'' = z''$.

TEOREMA 3. *La subálgebra de $H^*(\pi \times \pi; Z_p)$ de elementos invariantes bajo GL está generada por*

$$B^p + E, BE, AE + BD, C, D.$$

Esta teorema es consecuencia de las proposiciones anteriores.

CAPÍTULO IV: UN SISTEMA DE GENERADORES PARA LA IMAGEN DE k^*T

1. Sistema de representantes de π^p en N_1

Sean c_i las permutaciones

$$c_i(n, m) = (n, m), \quad \text{si} \quad n \neq \text{i}$$

$$c_i(i, m) = (i, km) \bmod p,$$

en donde K es un generador del grupo multiplicativo de los enteros mod p. Si s es un elemento del grupo simétrico S_p, denotaremos con la misma letra la permutación de renglones

$$s(n, m) = (s(n), m);$$

entonces es fácil verificar que el subconjunto X de elementos de N_1 de la forma

$$s \cdot c_1{}^{r_1} c_2{}^{r_2} \cdots c_p{}^{r_p},$$

con $r_1, r_2, \cdots, r_p = 0, \cdots, p - 2$, forma un subgrupo de N_1 que es un sistema de representantes de π^p en N_1. Es claro que X tiene $p!\,(p-1)^p$ elementos.

Denotaremos con C el subconjunto de X de elementos con $s = 1$. En este capítulo, si $Y \subset N_1$, se designará con Σ_Y un homomorfismo

$$\Sigma_Y : H^*(\pi^p; Z_p) \to H^*(\pi^p; Z_p)$$

definido como sigue: si $y \in Y \subset N_1$, y determina

$$\text{aut}\, y : \pi^p \to \pi^p,$$

con aut $y(x) = yxy^{-1}$. Si $y^*: H^*(\pi^p; Z_p) \to H^*(\pi^p; Z_p)$ denota el inducido, se tiene

$$\Sigma_Y(z) = \Sigma y^*(z), \quad \text{con} \quad y \in Y.$$

2. Acción de X en $H^*(\pi^p; Z_p)$

Se verifica directamente usando el complejo standard para π^p que los homomorfismos inducidos por los elementos de X son como sigue.

PROPOSICIÓN 2.1. *Si* $x_1, x_2, \cdots, x_p$; $y_1, y_2, \cdots, y_p$ *son como en la Proposición* 3.4 *del Capítulo I, entonces*

$$c_i^*(x_j) = x_j, \qquad c_i^*(y_j) = y_j, \quad \text{si} \quad i \neq j,$$
$$c_i^*(x_i) = kx_i, \qquad c_i^*(y_i) = ky_i,$$
$$s^*(x_j) = x_{s(j)}, \qquad s^*(y_j) = y_{s(j)}.$$

PROPOSICIÓN 2.2. *Sea* w *un monomio de* $H^*(\pi^p; Z_p)$,

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_p^{\epsilon_p} y_1^{s_1} y_2^{s_2} \cdots y_p^{s_p};$$

entonces w *es invariante bajo* C ($c^* \cdot w = w$, *toda* $c \in C$), *si y sólo si*

$$\epsilon_i + s_i \equiv 0 \mod (p-1), \quad \textit{para toda} \quad i.$$

Prueba. $c_i^* \cdot w = k^{\epsilon_i + s_i} w = w$, de donde

$$\epsilon_i + s_i \equiv 0 \mod (p-1).$$

Es inmediato que si cumple esa condición, es invariante.

Sea $\mathfrak{M}$ la subálgebra de $H^*(\pi^p; Z_p)$ de elementos invariantes bajo C de la proposición anterior. Se obtiene

PROPOSICIÓN 2.3. $\mathfrak{M}$ *está generada por*

$$x_1 y_1^{p-2}, x_2 y_2^{p-2}, \cdots, x_p y_p^{p-2} \quad y \quad y_1^{p-1}, y_2^{p-1}, \cdots, y_p^{p-1}$$

y, por lo tanto,

$$\mathfrak{M} \cong E(x_1 y_1^{p-2}, x_2 y_2^{p-2}, \cdots, x_p y_p^{p-2}) \otimes P(y_1^{p-1}, y_2^{p-1}, \cdots, y_p^{p-1}).$$

La proposición anterior se puede considerar una generalización del resultado que sigue.

Sea $\pi \subset S_p$; entonces, en

$$H^*(\pi; Z_p) \underset{i^*}{\overset{t}{\rightleftarrows}} H^*(S_p; Z_p),$$

t es epimorfismo y i^* es monomorfismo; además

$$i^* t = \sum (c^*)^q, \qquad q = 0, 1, \cdots, p-2.$$

Si $H^*(\pi, Z_p) = E(x, 1) \otimes P(y, 2)$, entonces

$$c^*(x) = kx \quad \text{y} \quad c^*(y) = ky$$

por consiguiente. i^* es un monomorfismo sobre los elementos invariantes bajo c^*, y un monomio $x^\epsilon y^s$ es invariante si y sólo si $\epsilon + s \equiv 0 \bmod (p-1)$. Por consiguiente,

$$H^*(S_p\,; Z_p) \cong E(xy^{p-2}) \otimes P(y^{p-1}).$$

LEMA 2.1. *Si* $z \in \mathfrak{M}$ *entonces* $\Sigma_c \cdot z = -z$.

Prueba. Ya que z es invariante, $c^* \cdot z = z$. Como C tiene $(p-1)^p$ elementos, inmediatamente se obtiene

$$\Sigma_c \cdot z = (p-1)^p \cdot z = -z \pmod p.$$

LEMA 2.2. *Si* $z \in H^*(\pi^p; Z_p)$ *entonces* $\Sigma_X \cdot z = \Sigma_{S_p} \cdot \Sigma_C z$; *además* $\Sigma_C z \in \mathfrak{M}$.

Prueba. La proposición es evidente ya que

$$X = \bigcup sC, \quad \text{con} \quad s \in S_p\,.$$

De lo anterior se tiene

PROPOSICIÓN 2.4. $\Sigma_X \cdot H^*(\pi^p; Z_p) = \Sigma_{S_p} \cdot \mathfrak{M}$.

3. Funciones simétricas

De lo anterior se deduce que, para calcular $\Sigma_X \cdot H^*(\pi^p; Z_p)$, es suficiente considerar la siguiente situación.

Sea $\mathfrak{M} = E(X_1, \cdots, X_p\,; n) \otimes P(Y_1, y_2, \cdots, Y_p\,; n+1)$, con coeficientes en Z_p, donde n es entero positivo impar. El grupo S_p opera en $\mathfrak{M}$ como sigue:

$$S(X_i) = X_{S(i)}\,, \qquad S(Y_i) = Y_{S(i)}\,.$$

Se puede considerar como álgebra diferencial definiendo

$$dY_i = X_i\,, \qquad dX_i = 0.$$

Entonces la imagen de Σ_X estará dada por las siguiente proposición.

PROPOSICIÓN 3.1. *La imagen de* Σ_{S_p} *está generada por* $\Sigma_{S_p} \cdot X_1^\epsilon Y_1^s$, $\epsilon = 0, 1$, $s > 0$.

La demostración depende de los siguientes lemas.

LEMA 3.1. *Si* S_{p-q} *es el subgrupo de* S_p *que deja* $1, 2, \cdots, q$ *fijos, entonces un sistema de representantes de* S_{p-q} *en* S_p *es*

$$(1i_1)(2i_2) \cdots (qi_q), \quad \text{con} \quad i_k = k, k+1, \cdots, p.$$

La demostración es evidente.

Sea ahora $z_i(\epsilon, s) = X_i^\epsilon Y_i^s$. Con esta notación una base de los elementos homogéneos de grado q está dada por los monomios

$$z = z_1(\epsilon_1, s_1)\cdot z_2(\epsilon_2, s_2)\cdots z_p(\epsilon_p, s_p)$$

en donde $\sum \epsilon_i + 2s_i = q$. Sea $S \in Z(S_p)$ definida con $S = \sum s$, $s \in S_p$.

LEMA 3.2. *Si* $z = z_1(\epsilon_1, s_1)z_2(\epsilon_2, s_2)\cdots z_q(\epsilon_q, s_q)$, *con* $\epsilon_i + 2s_i \neq 0$, *entonces*

$$S\cdot z = (p-q)!\sum z_{i_1}(\epsilon_1, s_1)\cdots z_{i_q}(\epsilon_q, s_q),$$

con $(i_1, i_2, \cdots, i_q)$, *recorriendo las ordenaciones sin repetición de* $1, 2, \cdots p$.

Para la demonstración del lema, probaremos primero inductivamente la fórmula

$$\sum (1i_1)(2i_2)\cdots(qi_q)\cdot z = \sum z_{i_1}(\epsilon_1, s_1)\cdots z_{i_q}(\epsilon_q, S_q\}.$$

En la primera parte de la igualdad, $i_k = k, k+1, \cdots, p$; en la segunda, $(i_1, i_2, \cdots, i_q)$ recorre las ordenaciones sin repetición de $1, 2, \cdots, p$. z es como en el enunciado del lema.

1) $\sum (1i)z_1(\epsilon, s) = \sum z_i(\epsilon, s) i = 1, \cdots, p.$

2) $\sum (1i_1)(2i_2)\cdots(qi_q)z = \sum (1i_1)\sum z_1(\epsilon_1, s_1)z_{i_2}(\epsilon_2, s_2)\cdots z_{i_q}(\epsilon_q, s_q),$

con $i_2, i_3, \cdots, i_q$ recorriendo todas las ordenaciones sin repetición de $2, 3, \cdots, p$.

Sea $z' = z_{i_1}(\epsilon_1, s_1)z_{i_2}(\epsilon_2, s_2)\cdots z_{i_q}(\epsilon_q, s_q)$, con $i_1, i_2, \cdots, i_q$ ordenación de $1, 2, \cdots, p$.

Primer caso. En la ordenación anterior $i_2, \cdots, i_q > 1$; en este caso

$$z' = (1i_1)z_1(\epsilon_1, s_1)z_{i_2}(\epsilon_2, s_2)\cdots z_{i_q}(\epsilon_q, s_q).$$

Segundo caso. $i_k = 1$ para alguna $k > 2$; entonces $i_1 > 2$ y

$$z' = (1i_1)z_1(\epsilon_1, s_1)z_{i_2}(\epsilon_2, s_2\cdots z_{i_1}(\epsilon_{k_1}s_k)\cdots z_{i_q}(\epsilon_q, s_q).$$

En cualquier caso z' aparece en el desarrollo de la suma. Como el número de términos en la suma es $p(p-1)\cdots(p-q+1) = 0_{p,q}$, se obtiene el resultado. Finalmente, el lema se obtiene considerando la descomposición

$$S_p = \bigcup (1i_1)(1i_2)\cdots(1i_q)S_{p-q}$$

y observando que z es invariante bajo S_{p-q}.

LEMA 3.3. *Si* $z = z_1(\epsilon_1, s_1)z_2(\epsilon_2, s_2)\cdots z_q(\epsilon_q, s_q)$ *con* $\epsilon_i + 2s_i \neq 0$ *entonces*

$$qS(z\cdot z_{q+1}(\epsilon, s)) = S(z)\cdot S(z_{q+1}(\epsilon, s)) + \sum_{k=1}^{q} S(z\cdot z_k(\epsilon, s)).$$

Caso $q = 1$.

$$\begin{aligned} S(z_1(\epsilon_1, s_1))\cdot S(z_2(\epsilon, s)) &= (p-1)!\,(p-1)!\sum_{i=1}^{p} z_i(\epsilon_1, s_1)\sum_{j=1}^{p} z_j(\epsilon, s) \\ &= (p-1)!\,((p-1)(p-2)!\sum_{i\neq j} z_i(\epsilon_1, s_1)\cdot z_j(\epsilon, s) \\ &\quad + (p-1)!\sum_{i=1}^{p} z_i(\epsilon_1, s_1)z_1(\epsilon, s)) \\ &= (p-\mathrm{i})!\,((p-1)S(z_1(\epsilon_1, s_1)\cdot z_2(\epsilon, s)) \\ &\quad + S(z_1(\epsilon_1, s_1)z_1(\epsilon, s)). \end{aligned}$$

Caso $q > 1$.

$$S(z)\cdot S(z_{q+1}(\epsilon, s)) = (p-1)!(p-q)!\Big(\sum z_{i_1}(\epsilon_i, s_1)\cdots z_{i_q}(\epsilon_q, s_q)\Big)\cdot\sum z_i(\epsilon, s)$$
$$= (p-1)!(p-q)!\Big(\sum z_{i_1}(\epsilon_1, s_1)\cdots z_{i_q}(\epsilon_q, s_q)\Big)z_i(\epsilon, s),$$

con $i_1, \cdots, i_q$ ordenación sin repetición de $1, 2, \cdots, p$ y $i = 1, \cdots, p$.

Sea $I = 0_q \times 0_1$ el conjunto de índices de la suma anterior; éste se puede descomponer como sigue:

$$I_k = \{(i_1, \cdots, i_q) \times i \quad \text{tales que} \quad i_k = i\}, \quad \text{si} \quad k < q;$$
$$I_{q+1} = \{(i_1, \cdots, i_q) \times i, \qquad i \neq i_k, k = 1, \cdots, q\}.$$

Evidentemente

$$I_k \cap I = \emptyset \quad \text{si} \quad k \neq l, \qquad \bigcup I_k = 0_q \times 0_1$$

además para $i = 1, \cdots, q$

$$(p-q)!\sum z_{i_1}(\epsilon_1, s_1)\cdots z_{i_q}(\epsilon_q, s_q)z_i(\epsilon, s) = S(z_1(\epsilon_1, s_1)\cdots z_q(\epsilon_q, s_q), z_i(\epsilon, s))$$

y si $i = q + 1$,

$$(p-q-1)!\sum z_1(\epsilon_1, s_1)\cdots z_q(\epsilon_q, s_q)z_{q+1}(\epsilon, s) = S(z_1(\epsilon_1, s_1)\cdots z_q(\epsilon_q, s_q)z_{q+1}(\epsilon, s)).$$

Esto concluye la demostración del lema. Finalmente, la fórmula del Lema 3.3 implica la proposición.

PROPOSICIÓN 3.2. *La imagen de* Σ_{S_p} *es subálgebra del álgebra generada por* $S\cdot z_1(\epsilon, s)$, *con* $\epsilon = 0, 1$, $s = 0, 1, \cdots, p-1$, *y* $Y_1\cdot Y_2\cdots Y_p$.

Con coeficientes enteros, se tiene la igualdad

$$S\cdot Y_1^{\,r} = \sum a(s_1, s_2, \cdots, s_p)\sigma_i^{\,s_1}\sigma_2^{\,s_2}\cdots\sigma_p^{\,s_p},$$

con $s_1 + 2s_2 + \cdots + ps_p = r$, $\sigma_1, \sigma_2, \cdots, \sigma_p$ definidas por

$$S(Y_1Y_2\cdots Y_q) = (p-q)!\,\sigma_q,$$
$$a(s_1, s_2, \cdots, s_p) = \pm r(s_1 + s_2 + \cdots + s_p^{-1})!/(s_1!\,s_2!\cdots s_p!).$$

$a(s_1, s_2, \cdots, s_p)$ es un entero; ya que $\sigma_q \in S\cdot Y_2^{\,r}$, cuando $q = 1, 2, \cdots, p-1$, y el grado de σ_q es $q(n+1)$, se tiene que σ_q se puede expresar con $S\cdot z_1(\epsilon, s)$, con $s < p - 1$. Ahora

$$d(S\cdot Y_1^{\,r}) = rSx_1y_1^{\,r-1}$$
$$= \sum a(s_1, \cdots, s_p)(s_1\sigma_1'(s_1)\sigma_2^{\,s_2}\cdots\sigma_p^{\,s_p} + \cdots + s_p\sigma_1^{\,s_1}\cdots\sigma_p'(s_p));$$

entonces r divide a $s_ia(s_1, \cdots, s_p)$. Por consiguiente

$$s_i a(s_1, \cdots, s_p) = r a'(s_1, \cdots, s_p),$$

ı $a'(s_1, \cdots, s_p)$ entero; entonces

$$y_1^{r-1} = \sum a'(s_1, \cdots, s_p)(\sigma_1'(s_1)\sigma_2^{s_2} \cdots \sigma_p^{s_p} + \cdots + \sigma_1^{s_1} \cdots \sigma_p'(s_p)).$$

·o $dS = Sd$, de donde

$$\sigma_i'(s_i) \in S \cdot \mathfrak{M}, \qquad i = 1, \cdots, p-1, \quad \text{y}$$

$$\sigma_p'(s_p) = d(Y_1 \cdot Y_2 \cdots Y_p) = \sum Y_1 \cdot Y_2 \cdots X_k \cdots Y_p$$

tenece a $S \cdot \mathfrak{M}$.

)e lo anterior se concluye la proposición.

'EOREMA. *Sea* $\mathfrak{L} = E(A_1, A_2, \cdots, A_p) \otimes P(B_1, B_2, \cdots, B_p)$, *con coientes en* Z_p, *con*

$$\text{grado } (A_k) = kn + 1 \quad y$$

$$\text{grado } (B_k) = k(n+1).$$

'onces el homomorfismo inducido por

$$\phi(A_k) = X_1 Y_1^{k-1} + \cdots + X_p Y_p^{k-1}, \qquad k = 1, \cdots, p,$$

$$\phi(B_k) = Y_1^k + \cdots + Y_p^k, \qquad k = 1, \cdots, p-1,$$

$$\phi(B_p) = Y_1 \cdot Y_2 \cdots Y_p$$

ın monomorfismo sobre la subálgebra de elementos invariantes bajo S_p.

.a demostración del teorema se obtiene de la Proposición 3.2 y de los lemas iientes.

.EMMA 3.4. *Si* w *es un monomio invariante bajo* S_p, *entonces*

$$w = a(Y_1 \cdot Y_2 \cdots Y_p)^s.$$

'ste lema es evidente.

.EMA 3.5. *Si* $z = \sum w_i$ *es un elemento de* $\mathfrak{M}$, *homogéneo invariante bajo y* w_i *son monomios no invariantes bajo* S_p *entonces* $z \in S \cdot \mathfrak{M}$.

'a que S_p transforma monomios en monomios, S_p opera en $\{w_1, w_2, \cdots, w_m\}$. $\{w_1, w_2, \cdots, w_e\}$ la clase de intransitividad de w_1 y H, el subgrupo de S_p deja fijo a w_1. Es claro que $S \cdot w_1 = h(w_1 + w_2 + \cdots + w_e)$, en donde h l orden de H, ya que H es distinto de S_p, $h \neq 0 \bmod p$. Por consiguiente

$$\frac{1}{h} S \cdot w_1 = w_1 + w_2 + \cdots + w.$$

.EMA 3.6. *Los monomios distintos de cero, en* $\bar{A}_k = \phi(A_k)$ *y* $\bar{B}_k = \phi(B_k)$, = 1, $\cdots$, p, *son linealmente independientes.*

Consideremos los siguientes resultados.

1) Los monomios en $\bar{B}_k$ son linealmente independientes. Este es el caso conocido de polinomios simétricos.

2) $\bar{A}_1 \cdot \bar{A}_2 \cdots \bar{A}_p P(\bar{B}_1, \cdots, \bar{B}_p) = 0$ implica $P(\bar{B}_1, \cdots, \bar{B}_p) = 0$; $P(\bar{B}_1, \cdots, \bar{B}_p)$ es un polinomio en $\bar{B}_1, \bar{B}_2, \cdots, \bar{B}_p$. Esto es consecuencia de

$$\bar{A}_1\bar{A}_2 \cdots \bar{A}_p = X_1 \cdot X_2 \cdots X_p Q(Y_1, \cdots, Y_p)$$

con $Q \neq 0$.

Sea $M \subset E = \{1, 2, \cdots, p\}$ y $\bar{A}_M = \bar{A}_{i_1}\bar{A}_{i_2} \cdots \bar{A}_{i_m}$, con $i_1 < i_2 < \cdots < i_m$ y $M = \{i_1, i_2, \cdots, i_m\}$, y $P_s = P_s(\bar{B}_1, \cdots, \bar{B}_p)$ un polinomio homogéneo en $\bar{B}_1, \bar{B}_2, \cdots, \bar{B}_p$; el Lema 3.6 es consecuencia.

LEMMA 3.7. *Si* $\sum \bar{A}_M \cdot P_{E-M} = 0$ *cuando* M *recorre los subconjuntos de* E, *entonces*

$$P_{E-M} = 0, \quad \textit{toda} \quad M \subset E.$$

Consideremos

$$\bar{A}_1 \cdot \bar{A}_2 \cdots \bar{A}_p \cdot (\sum \bar{A}_M \cdot P_{E-M}) = P_{E-n} = 0,$$
$$\bar{A}_2 \cdot \bar{A}_3 \cdots \bar{A}_p \cdot (\sum \bar{A}_M \cdot P_{E-M}) = P_E + \bar{A}_1 P_{E-\{1\}},$$

de donde $P_{E-\{1\}}$. Inductivamente se obtiene el resultado. De lo anterior se obtiene

TEOREMA. *La imagen de* k^*T *es isomorfa a el álgebra sobre* Z_p *siguiente*:

$$[E(A_1, A_2, \cdots, A_p) \otimes P(B_1, B_2, \cdots, B_{p-1})]^+ \otimes P(B_p),$$
$$\textit{grado}\ (A_k) = k(2p - 3),$$
$$\textit{grado}\ (B_k) = k(2(p - 1) = 2k(p - 1).$$

CAPÍTULO V: EL ALGEBRA $H^*(S_{p^2}; Z_p)$

1. El álgebra $H^*(S_{p^2}; Z_p)$ como subálgebra de $H^*(S_{p^2,p}; Z_p)$

Consideremos $H^*(S_{p^2,p}; Z_p)$ como en el párrafo 3 del Capítulo I; es decir, si $j: \pi^p \subset S_{p^2,p}$ y $h: \pi \times \pi \subset S_{p^2,p}$, la sucesión

$$H^*(\pi^p; Z_p) \xrightarrow{t} H^*(S_{p^2,p}; Z_p) \to H^*(\pi \times \pi; Z_p)$$

es exacta, con t la transferencia, además j^* restringido a Im t es un monomorfismo. Si

$$H^*(\pi^p; Z_p) = E(x_1, x_2, \cdots, x_p) \otimes P(y_1, y_2, \cdots, y_p) \text{ y}$$
$$H^*(\pi \times \pi; Z_p) = E(u_1, u_2) \otimes P(v_1, v_2),$$

con grado $(x_i) = 1$, grado $(y_i) = 2$, grado $(u_i) = 1$, y grado $(v_i) = 2$, entonces Im j^*t es el subanillo de elementos invariantes bajo la permutación cíclica de

las variables, y Im h^* es el subanillo generado por

$$u_1\,,\ v_1\,,\ u\ =\ (u_1v_2\ -\ u_2v_1){v_1}^{p-3/2},\qquad v\ =\ v_2({v_2}^{p-1}\ -\ {v_1}^{p-1}).$$

Si consideramos a $H^*(S_{p^2,p}\,;\,Z_p)$ como módulo, es la suma directa (en grados mayores que cero)

$$\text{Im}\ j^*t\ \oplus\ \text{Im}\ h^*.$$

El producto está determinado por

$$\begin{aligned}(z,\,0)(z',\,0)\ &=\ (zz',0)\\ (0,\,z)(0,\,z')\ &=\ (0,\,zz')\\ (z,\,0)(0,\,u_1)\ &=\ (0,\,0)\\ (z,\,0)(0,\,v_1)\ &=\ (0,\,0)\\ (z,\,0)(0,\,u)\ &=\ (z\cdot x_1x_2\ \cdots\ x_p\,,\,0)\\ (z,\,0)(0,\,v)\ &=\ (z\cdot y_1y_2\ \cdots\ y_p\,,\,0).\end{aligned}$$

Además,

$$h^*(z,\,z')\ =\ z';$$

$$j^*(z,\,0)\ =\ z;\qquad j^*(0,\,u_1)\ =\ 0;\qquad j^*(0,\,v_1)\ =\ 0;$$

$$j^*(0,\,u)\ =\ x_1x_2\ \cdots\ x_p\ ;\qquad j^*(0,\,v)\ =\ y_1y_2\ \cdots\ y_p\,.$$

Sean ahora en Im j^*t

$$\begin{aligned}A_1\ &=\ x_1{y_1}^{p-2}\ +\ \cdots\ +\ x_p{y_p}^{p-2},\qquad & B_1\ &=\ {y_1}^{p-1}\ +\ \cdots\ +\ {y_p}^{p-1},\\ A_2\ &=\ x_1{y_1}^{2(p-1)-1}\ +\ \cdots\ +\ x_p{y_p}^{2(p-1)-1},\qquad & B_2\ &=\ {y_1}^{2(p-1)}\ +\ \cdots\ +\ {t_p}^{2(p-1)},\\ &\cdots\cdots\cdots\cdots\cdots\cdots, & B_{p-1}\ &=\ {y_1}^{(p-1)(p-1)}\ +\ \cdots\ +\ {y_p}^{p-1)(p-1)},\\ A_p\ &=\ x_1{y_1}^{p(p-1)-1}\ +\ \cdots\ +\ x_p{y_p}^{p(p-1)-1},\qquad & B_p\ &=\ y_1y_2\ \cdots\ y_p\,,\end{aligned}$$

y en Im h^*

$$\begin{aligned}A\ &=\ u_1{v_1}^{p-2},\\ B\ &=\ {v_1}^{p-1},\\ C\ &=\ u_1u_2{v_1}^{p-2}{v_2}^{p-2}({v_2}^{p-1}\ -\ {v_1}^{p-1})^{p-2},\\ D\ &=\ (u_2v_1\ -\ u_1v_2){v_1}^{p-2}{v_2}^{p-2}({v_2}^{p-1}\ -\ {v_1}^{p-1})^{p-2},\\ E\ &=\ {v_2}^{p-1}({v_2}^{p-1}\ -\ {v_1}^{p-1}).\end{aligned}$$

Teorema. *El álgebra* $H^*(S_{p^2}\,;\,Z_p)$ *es isomorfa a la subálgebra de* $H^*(S_{p^2,p}\,;\,Z_p)$ *generada por*

$$A_1{}^{\epsilon_1}A_2{}^{\epsilon_2}\ \cdots\ A_p{}^{\epsilon_p}\cdot B_1{}^{s_1}B_2{}^{s_2}\ \cdots\ B_p{}^{s_p},$$

con $\epsilon_1\ +\ \epsilon_2\ +\ \cdots\ +\ \epsilon_p\ +\ s_1\ +\ s_2\ +\ \cdots\ +\ s_{p-1}\ \neq\ 0$ *si* $s_p\ \neq\ 0$ *y los monomios en*

$$B^p\ +\ E,\quad BE,\quad AE\ +\ BD,\quad C,\quad D.$$

2. Otra descripción de $H^*(S_{p^2}\,;Z_p)$

Considérense las álgebras sobre Z_p,

$$E(u_1\,,u_2)\otimes P(v_1\,,v_2),$$

con grado $(u_i)=2$ y grado $(v_i)=2$, y

$$E(A_1\,,A_2\,,\cdots,A_p)\otimes P(B_1\,,B_2\,,\cdots,B_p),$$

con grado $(A_k)=2k(p-1)-1$ y grado $(B_k)=2k(p-1)$.

Denotemos con

$$[E(u_1\,,u_2)\otimes P(v_1\,,v_2)\,]^{GL}$$

la subálgebra de elementos invariantes bajo el grupo lineal de matrices no singulares de 2×2, con coeficientes en Z_p y con

$$[E(A_1\,,\cdots,A_p)\otimes P(B_1\,,\cdots,B_{p-1})]^{+}$$

los elementos de grado mayor que cero.

TEOREMA.

$$H^*(S_{p^2}\,;Z_p)=(E(A_i)\otimes P(B_j))^{+}\otimes P(B_p)\oplus(E(u_k)\otimes P(v_h))^{GL}$$

con $i=1,2,\cdots,p$, $j=1,\cdots,p-1$, $k=1,2$, *y* $h=1,2$. *Además, la multiplicación está determinada como sigue:*

$$(E(A_i)\otimes P(B_j))^{+}\otimes P(B_p)\quad \textit{es ideal de}\quad H^*(S_{p^2}\,;Z_p),$$

$$(E(u_k)\otimes P(v_h))^{GL}\quad \textit{es subálgebra de}\quad H^*(S_{p^2}\,;Z_p).$$

Además, si

$$A=u_1{v_1}^{p-2},$$
$$B={v_1}^{p-1},$$
$$C=u_1u_2{v_1}^{p-2}{v_2}^{p-2}({v_2}^{p-1}-{v_1}^{p-1})^{p-2},$$
$$D=(u_2v_1-v_1v_2){v_1}^{p-2}{v_2}^{p-2}({v_2}^{p-1}-{v_1}^{p-1})^{p-2},$$
$$E={v_2}^{p-1}({v_2}^{p-1}-{v_1}^{p-1})^{p-1},$$

entonces B^p+E, BE, $AE+BD$, C, D *generan* $(E(u_k)\otimes P(v_h))^{GL}$, *y*

$$(z,0)(0,B^p+E)=(z\cdot B_p\,,0),$$
$$(z,0)(0,BE)=(0,0),$$
$$(z,0)(0,AE+BD)=(0,0),$$
$$(z,0)(0,C)=0,\quad y$$
$$(z,0)(0,D)=0.$$

3. Potencias reducidas en $H^*(S_{p^2,p}\,;Z_p)$ y $H^*(S_{p^2}\,,Z_p)$

Usando la notación del párrafo 1 de este capítulo, se tienen las siguientes proposiciones.

PROPOSICIÓN 3.1.

$$P^i(z, 0) = (P^i z, 0).$$

Ya que $j^*/\mathrm{Ker}\, h^*$ es un monomorfismo, es sufficiente probar que

$$h^*P^i(z, 0) = h^*(P^i z, 0),$$
$$j^*P^i(z, 0) = j^*(P^i z, 0).$$

Pero esto es inmediato por el párrafo 1 de este capítulo, ya que

$$h^*P^i(z, 0) = P^i h^*(z, 0) = 0,$$
$$h^*(P^i z, 0) = 0,$$
$$j^*P^i(z, 0) = P^i j^*(z, 0) = P^i z,$$
$$j^*(P^i z, 0) = P^i_z.$$

PROPOSICIÓN 3.2.

$$P^i(0, u_1) = (0, P^i u_1) = (0, 0); P^i(0, v_1) = (0, P^i v_1);$$

si $i > 0$, *entonces*

$$P^i(0, u) = (0, P^i u),$$
$$P^i(0, v) = (P^i(y_1 y_2 \cdots y_p), P^i v).$$

Prueba. Sea $i > 0$ y $P^i(0, u) = (z, z')$; entonces

$$h^*(P^i(0, u)) = P^i h^*(0, u) = P^i u = z' = h^*(z, z'),$$
$$j^*(P^i(0, u)) = P^i j^*(0, u) = P^i x_1 \cdot x_2 \cdots x_p, \quad \text{y}$$
$$j^*(z, z') = j^*(z, 0) + j^*(0, z').$$

Ahora

$$P^i u = P^i((u_1 v_2 - u_2 v_1) v_1^q), \quad q = \tfrac{1}{2}(p - 3);$$

por lo tanto,

$$P^i u = P^1(u_1 v_2 - u_2 v_1) \cdot P^{i-1} v_1^q + (u_1 v_2 - u_2 v_1) P^i v_1^q$$
$$= \binom{q}{i-1} (u_1 v_2^p - v_2 v_1^p) v_1^{q+(i-1)(p-1)} + \binom{q}{i} (u_1 v_2 - u_2 v_1) v_1^{q+i(p-1)}.$$

Pero

$$u_1 v_2^p - u_2 v_1^p = u_1 v - u v_1^r,$$

de donde

$$P^i u = \binom{q}{i-1} (u_1 v - u v_1^r) v_1^s + \binom{q}{i} u \cdot v_1^t;$$

por lo tanto, ya que $z' = P^i u$ y que Im h^* es un subanillo de $H^*(S_{p^2,p}\,;\, Z_p)$, se concluye que

$$j^*(0, z') = 0.$$

Por consiguiente $j^*(z, z') = j^*(z, 0) = z$; es decir,

$$z = P^i x_1 x_2 \cdots x_p = 0 \quad \text{y} \quad z' = P^i u.$$

Consideremos ahora

$$P^i(0, v) = (z, z'), \quad \text{como antes} \quad z' = P^i v;$$

además

$$j^*(P^i(0, v)) = P^i(j^*(0, v)) = P^i y_1 \cdot y_2 \cdots y_p \text{ y}$$

$$P^i v = P^i(v_2(v_2^{p-1} - v_1^{p-1})) = v_2^p P^{i-1}(v_2^{p-1} - v_1^{p-1})$$

$$+ v_2 P^i(v_2^{p-1} - v_1^{p-1}) = \binom{p-1}{i-1} \cdot v_2^p (v_2^{i(p-1)} - v_1^{i(p-1)})$$

$$+ \binom{p-1}{i} v_2 (v_2^{(i+1)(p-1)} - v_1^{(i+1)(p-1)}),$$

pero $\binom{p-1}{i-1} + \binom{p-1}{i} = 0$, mod p, de donde

$$P^i v = \binom{p-1}{i} v_2 (v_2^{p-1} - v_1^{p-1}) \cdot v_1^{i(p-1)}.$$

Por consiguiente, si $i > 0$,

$$j^*(0, P^i v) = 0,$$

de donde

$$j^*(z, z') = j^*(z, 0) = z = P^i y_1 y_2 \cdots y_p\,,$$

ya que en el párrafo 1 de este capítulo se ha descrito $H^*(S_{p^2}\,;\, Z_p)$ como un subanillo de $H^*(S_{p^2 p}\,;\, Z_p)$; lo anterior nos determina implícitamente las potencias reducidas en $H^*(S_{p^2}\,,\, Z_p)$.

Apéndice

En este apéndice se hacen algunas aclaraciones referentes a las demostraciones de las proposiciones del párrafo 3 del Capítulo I. La notación es como en el Capítulo I.

1. Proposición 3.1. Por el Lema 4.1 del capítulo VII de [2], se sabe que $d^* \tau = 0$. Ahora, por la Proposición 3.6 del capítulo VIII de [2] (ver la primera parte de la demostración), se sabe que todo elemento z de $H^*(W \times_\pi K^2)$ es de la forma

$$z = \tau z_1 + z_2 \cdot P z_3\,,$$

n z_1 en $H^*(K^p)$, z_2 en $H^*(W/\pi)$, y z_3 en $H^*(K)$. Pero d^* es $H^*(\pi)$-homo-
orfismo; por consiguiente

$$0 = d^*z = d^*\tau z_1 + z_2 \cdot d^*Pz_3 = z_2 \cdot d^*Pz_3 .$$

lemás, ya que

$$H^*(W/\pi) = E(u_1) \otimes P(v_1) \quad \text{y}$$
$$H^*(K) = E(u_2) \otimes P(v_2),$$

r la definición 3.2 del capítulo VII de [2]

$$d^*Pz_3 = \sum w_k \times D_k z_3 ,$$

r lo tanto, como

$$H^*(W/\pi \times K) = H^*(W/\pi) \otimes H^*(K),$$

que las potencias reducidas se conocen en $K = W/\pi$, es fácil ver que

$$d^*Pu_2 = (v_1u_2 - u_1v_2){v_1}^{p-3/2} = u,$$
$$d^*Pv_2 = v_2({v_2}^{p-1} - {v_1}^{p-1}) = v.$$

or consiguiente d^*P es un isomorfismo sobre la subálgebra de $H^*(W/\pi \times K)$ nerada por u, v. Por lo anterior el núcleo de d^* es Im τ.

2. Proposición 3.3, b). Por la Proposición 3.6 del capítulo VIII de [2], la agen de d^* es el $H^*(\pi)$ submódulo generado por Im (d^*P). u_1, v_1 son los neradores de la imagen de

$$H^*(W/\pi) \to H^*(W/\pi \times K)$$

por la parte anterior, u, v son los generadores de Im (d^*P).

3. Proposición 3.4 b), c). Ya que π es un subgrupo normal de $S_{p^2,p}$, se tiene r el segundo teorema de transferencia ([1] pág. 257), que

$$j^*\tau = a\, {d_x}^*,$$

donde x recorre un sistema de representantes de π^p en $S_{p^2,p}$. Si a es la permuta-ón definida en I. 1, Capítulo I, entonces $1, a, \cdots, a^{p-1}$ es un sistema de repre-ntantes. Es fácil ver que, si α denota el homomorfismo inducido por a, se tiene

$$\alpha x_i = x_{i+1} , \qquad \alpha y_i = y_{i+1} ;$$

emás, por la fórmula anterior,

$$j^*\tau = \sum \alpha^r.$$

4. Proposición 3.2. En $H^q(\pi^p; Z_p)$ los monomios son de dos tipos posibles
(a) $x_1^{\epsilon} y_1^{s} \cdot x_2^{\epsilon} y_2^{s} \cdots x_p^{\epsilon} y_p^{s}$;
(b) no son invariantes bajo α.

or consiguiente

$$H^q(\pi^p; Z_p) = I_q \oplus F_q ,$$

con I_q generado por (a) y F_q generado por (b). Ahora, por el Lema 2.3 (pág. 100) del capítulo VII de [2], I_q está contenido en Im j^*. Además directamente se verifica que F_q es π-libre (π generado por α). Por consiguiente, ya que por el primer teorema de transferencia $\tau j^* = 0$ (el índice de π^p en $S_{p^2,p}$ es p), se tiene

$$j^*\tau z = j^*\tau z_1 + j^*\tau z_2 = j^*\tau z_2 = 0,$$

con z_2 en F_q ; pero

$$j^*\tau z_2 = \sum \alpha z_2 = 0$$

de donde, ya que F_q es libre, $z_2 = (1 - \alpha)z_2'$ y

$$\tau z_2 = \tau z_2' - \tau\alpha x_2' = 0,$$

por fórmula (10) de la página 256 de [1]. Es decir, si $j^*\tau z = 0$, entonces $\tau z = 0$.

5. Proposición 3.5, b).

Como en la Proposición 3.1 del Capítulo V de este trabajo, se tiene que $j^*/\text{Ker } d^*$ es un monomorfismo; por lo tanto, si z, z' en $H^*(S_{p^2,p}\ ; Z_p)$ son tales que $j^*(z) = {}^*(z')$, entonces $d^*(z) = d^*(z')$; se tiene $z = z'$. Por consiguiente, basta observar que $j^*(u_1) = j^*(v_1) = 0$ para obtener que, si z está en Im τ,

$$z \cdot u_1 = 0, \qquad z \cdot v_1 = 0.$$

Además, ya que $j^*(u) = x_1x_2 \cdots x_p$ y $j^*(v) = y_1y_2 \cdots y_p$ (ver el Lema 2.3, cap VII de [2]),

$$\begin{aligned} j^*(z \cdot u) &= j^*z \cdot x_1x_2 \cdots x_p\,, \\ d^*(z \cdot u) &= 0, \\ j^*(z \cdot v) &= j^*z \cdot y_1y_2 \cdots y_p\,, \\ d^*(z \cdot v) &= 0. \end{aligned}$$

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

REFERENCIAS

[1] H. CARTAN y S. EILENBERG, Homological algebra. Princeton University Press, 1956.

[2] N. E. STEENROD, Cohomology operations. Annals of Mathematics Studies, No. 50, Princeton University Press, 1962.

[3] LEONARD EVANS, *The cohomology ring of a finite group*, Trans. Amer. Math. Soc., **101** (1961) 224–39.