2ej
25

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

EL GENERO DE GRUPOS NILPOTENTES FINITAMENTE GENERADOS

T E S I S

Que para obtener el Título de

MATEMATICO

p r e s e n t a

Alberte Catherine Pierrette SEMERENA MIREMONT

México, D. F. 1987

INDICE

INTRODUCCION

El propósito de este trabajo es estudiar, en el marco de la Teoría de grupos y del Algebra Homológica, el género de un grupo nilpotente finitamente generado, según el artículo "On the Genus of Nilpotent Groups and Spaces" de Peter Hilton, , y establecer algunas de sus propiedades. Definimos la noción de género, introducida por Guido Mislin, utilizando la teoría de localizaciones en grupos nilpotentes de Peter Hilton y Guido Mislin. Así, diremos que dos grupos nilpotentes finitamente generados N y M pertenecen al mismo género si y sólo si, para cada primo p, las localizaciones N_p y M_p son isomorfas. Concretamente, el género G(N) de un grupo nilpotente finitamente generado N es el conjunto de las clases de isomorfismo de grupos nilpotentes finitamente generados M con p-localizaciones tal que $N_p \cong M_p$ para todo primo p.

En el Capitulo I, consideramos un cierto grupo nilpotente N finitamente generado, definido mediante la presentación

$$N = \langle x,y \,;\, x^{p^{n+k}} = 1,\, yxy^{-1} = x^u \rangle ,$$

donde p es primo, $n,k \geq 1$; $u = 1+cp^k$ tal que p no divide a c, excluyendo el caso excepcional de $p=2$, $k=1$ que estudiaremos en el capitulo siguiente.

Demostraremos que el género de N, que es finito, admite una estructura de grupo abeliano, donde la clase de isomorfismo de N es el elemento neutro. Calcularemos el número de elementos "s" de G(N), excluyendo $p=2$, $n=1$, en cuyo caso G(N) contiene solamente un elemento. En los demás casos, $s = p^{n-1}(p-1)/2$, excluyendo $p=2$, $n=2$; $p=3$, $n=1$; por ser casos triviales donde $s=1$.

Construiremos el género total N_0 (= N), N_1 , ...,N_{s-1}; demostraremos que N_1 genera el grupo del género, y si

$$N_i = \langle x,y \,;\, x^{p^{n+k}} = 1,\, yxy^{-1} = x^{u^{m^i}} \rangle ,$$

entonces $N_i = iN_1$.

Más aún, obtendremos una "Escalera de Escher" de encajes normales tal que cada grupo cociente es cíclico de orden ℓ , donde ℓ es semi primitivo módulo p^n (es decir, la mínima potencia q de ℓ^q tal que $\ell^q \equiv \pm 1 \mod p^n$ es $q = s$).

También demostraremos que

$$N_i^k \cong N_j^k \qquad \forall\, i,j$$

donde N^k es el producto directo de k copias de N.

En el Capitulo II discutiremos el caso excepcional cuando

$$p=2,\ k=1 \ \text{ en } N= \langle x, y\ ;\ x^{p^{n+k}}=1,\ yxy^{-1}=x^u \rangle .$$

En el Capitulo III presentaremos una construcción más general de los grupos $N_0, N_1, \ldots N_{s-1}$ desarrollada por Peter Hilton en su artículo "Non-cancelation properties for certain finitely presented groups", que nos permitirá demostrar la propiedad siguiente:

$$N_i \times C \cong N_j \times C \qquad \forall\, i,j$$

donde C es un grupo libre cíclico.

También mencionaremos la existencia de cálculos precisos para determinar el orden, la estructura y el exponente del grupo genérico y así obtener el valor de k tal que

$$N_i^k \cong N_j^k .$$

Para terminar, construiremos espacios nilpotentes X_i que pertenecen a un mismo género y que no son homotópicamente equivalentes dos a dos.

Quiero agradecer al Dr. Emilio Lluis Puebla quien, además de asesorar este trabajo, supo darme, durante mis estudios tardíos, su confianza en los momentos de dudas y el impulso necesario para seguir adelante, con paciencia y generosidad.

I-UN GENERO CICLICO.

I-1 CONSTRUCCION DE UN GRUPO NILPOTENTE FINITAMENTE GENERADO CON SUBGRUPO CONMUTADOR FINITO.

Sean n, k, c enteros con $k \geq 1$, $u = 1 + cp^k$, donde p es un número primo que no divide a c. Sea N el grupo definido mediante la siguiente presentación:

$$N = \langle x, y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^u \rangle .$$

1.1 LEMA. El orden de u módulo p^{n+k} es p^n.

Nota: excluiremos el caso $p=2$, $k=1$ que se estudiará en el Capítulo II.

Demostración.

Tenemos que $(1+cp^k)^{p^n} = 1 + \sum_{r=1}^{p^n} \binom{p^n}{r} c^r p^{kr}$.

Si $r = ap^s$, $0 \leq s \leq n$,

entonces p^{n-s} divide a $\binom{p^n}{r}$ pero p^{n-s+1} no divide a $\binom{p^n}{r}$.

En efecto

$$\binom{p^n}{r} = \binom{p^n}{ap^s} = \frac{p^n!}{ap^s!\,(p^n-ap^s)!} = \frac{p^n(p^n-1)\dots(p^n-i)\dots(p^n-p^n+1)}{ap^s(ap^s-1)\dots(ap^s-i)\dots(ap^s-ap^s+1)(p^n-ap^s)!}.$$

Luego p^{n-s} divide a $\binom{p^n}{ap^s}$ y p^{n-s+1} no divide a $\binom{p^n}{ap^s}$.

Por lo tanto $p^{n-s+kap^s}$ es la máxima potencia de p que divide a $\binom{p^n}{r} c^r p^{kr}$.

Como $k \geq 1$, $a \geq 1$, $p \geq 3$, $0 \leq s \leq n$, entonces $k(ap^s - 1) \geq s$ y $n-s+kap^s \geq n+k$.

De ahí que p^{n+k} divide a $\binom{p^n}{r} c^r p^{kr}$ y, por lo tanto,

$$(1+cp^k)^{p^n} \equiv 1 \pmod{p^{n+k}}.$$

Nos resta por demostrar que $(1+cp^k)^{p^{n-1}}$ no es congruente con 1 módulo p^{n+k}.

Sabemos que $(1+cp^k)^{p^{n-1}} = 1 + cp^{n+k-1} + \sum_{r=2}^{p^{n-1}} \binom{p^{n-1}}{r} c^r p^{kr}$.

y si $r = ap^s$, $0 \leq s \leq n-1$, entonces

$$p^{n-1-s} \text{ divide a } \binom{p^{n-1}}{ap^s} \text{ pero } p^{n-s} \text{ no divide a } \binom{p^{n-1}}{ap^s}.$$

Por lo tanto, $p^{n-1-s+kap^s}$ es la máxima potencia de p que divide a $\binom{p^{n-1}}{r} c^r p^{kr}$. Luego p^{n+k} divide a $\binom{p^{n-1}}{r} c^r p^{kr}$, $r \geq 2$.

En efecto, $n-1-s+kap^s \geq n+k$ ya que

a) si $s=0$ entonces $a \geq 2$

b) hemos excluido el caso $p=2$, $k=1$ para el cual la desigualdad sería falsa cuando $s=1$, $a=1$.

De ahí se sigue que $(1+cp^k)^{p^{n-1}} \equiv 1 + cp^{n+k-1} \pmod{p^{n+k}}$

y $(1+cp^k)^{p^{n-1}}$ no es congruente con 1 módulo p^{n+k}. ///

1.2 DEFINICION DE GRUPO NILPOTENTE.

Consideremos la sucesión central descendente de un grupo cualquiera P

$$\ldots \subseteq \Gamma_{i+1}(P) \subseteq \Gamma_i(P) \subseteq \ldots \subseteq \Gamma_1(P)$$

con $\Gamma_1(P) = P$ y $\Gamma_{i+1}(P) = [P, \Gamma_i(P)]$ donde $[P, \Gamma_i(P)]$ es el subgrupo de P generado por $aba^{-1}b^{-1}$ con $a \in P$ y $b \in \Gamma_i(P)$. Diremos que P es *nilpotente* si $\Gamma_i(P) = \{1\}$ para alguna i suficientemente grande.

1.3 DEFINICION DE ACCION NILPOTENTE. Sea A un grupo abeliano, Q un grupo arbitrario y $\omega : Q \longrightarrow \mathrm{Aut}(A)$ una acción de Q sobre A denotada por $\omega(x)(a) = x.a$.

Definimos la ω -sucesión central descendente de A como la sucesión

$$\ldots \subseteq \Gamma_\omega^{i+1}(A) \subseteq \Gamma_\omega^{i}(A) \subseteq \ldots \subseteq \Gamma_\omega^{1}(A)\text{, donde } \Gamma_\omega^{1}(A) = A \quad \text{y}$$

$$\Gamma_\omega^{i+1}(A) = \text{grupo generado por } \{x.a - a \mid x \in Q,\ a \in \Gamma_\omega^{i}(A),\ i \geq 1\}.$$

Entonces diremos que Q *actúa nilpotentemente* sobre A si $\Gamma_\omega^{j}(A) = \{1\}$ para alguna j suficientemente grande y que ω es una *acción nilpotente*.

1.4 DEFINICION DE PRODUCTO SEMIDIRECTO. Un grupo G es el *producto semidirecto* de K por Q , denotado por $\ltimes$ si G tiene subgrupos K y Q tales que

i) K es normal en G
ii) $KQ = G$
iii) $K \cap Q = \{1\}$.

1.5 PROPOSICION. N es el producto semidirecto de Z/p^{n+k} y C.

Demostración. Sea $C_p n$ el grupo cíclico que actúa sobre Z/p^{n+k} con la acción dada por $\xi.a = ua$ donde ξ genera a $C_p n$ y $Z/p^{n+k} = \langle a \rangle$.

Por el Lema 1.1 esta acción está bién definida. Además, es necesariamente una acción nilpotente. En efecto, sea

$$\ldots \subseteq \Gamma_\omega^{i+1}(Z/p^{n+k}) \subseteq \Gamma_\omega^{i}(Z/p^{n+k}) \subseteq \ldots \subseteq \Gamma_\omega^{1}(Z/p^{n+k})$$

la ω-sucesión central descendente de Z/p^{n+k}, donde $\Gamma_\omega^{1}(Z/p^{n+k}) = Z/p^{n+k}$,

$\Gamma_\omega^{i+1}(Z/p^{n+k})$ = grupo generado por $\{ \xi a - a \mid \xi \in Cp^n, a \in \Gamma_\omega^i(Z/p^{n+k}) \ i \geq 1 \}$

y ω la acción de $C_p n$ sobre Z/p^{n+k} tal que $\xi.a = ua$.

Si ω es una acción nilpotente, entonces $\Gamma_\omega^j(Z/p^{n+k}) = \{1\}$ para alguna j. Supongamos $j = p^{n+1}$. Luego $a = p^n$ y $\xi.a - a = ua - a = acp^k = cp^{n+k}$. Por lo que $\Gamma_\omega^{p^{n+1}}(Z/p^{n+k}) = \{1\}$ y ω es una acción nilpotente.
Si hacemos actuar a C sobre Z/p^{n+k} vía la proyección $C \twoheadrightarrow C_p n$ entonces C actúa también nilpotentemente.

En seguida demostraremos que N es el producto semidirecto de Z/p^{n+k} y C.
Primero definamos la ley multiplicativa en N de la siguiente manera:

$(a,g)(a',g') = (a+ga', gg')$ $\quad a \in Z/pn+k \quad g \in C.$

Es claro que dicha multiplicación cumple las siguientes propiedades:

i) es asociativa puesto que

$$\begin{aligned}[(a_1, g_1)(a_2, g_2)](a_3, g_3) &= (a_1 + g_1 a_2, g_1 g_2)(a_3, g_3) \\ &= (a_1 + g_1 a_2 + g_1 g_2 a_3, g_1 g_2 g_3)\end{aligned}$$

$$\begin{aligned}(a_1, g_1)[(a_2, g_2)(a_3, g_3)] &= (a_1, g_1)(a_2 + g_2 a_3, g_2 g_3) \\ &= (a_1 + g_1 a_2 + g_1 g_2 a_3, g_1 g_2 g_3).\end{aligned}$$

ii) Existe un elemento neutro (0, 1), puesto que

$$(a,g)(0,1) = (a,g).$$

iii) Existe un elemento inverso $(-g^{-1}a, g^{-1})$, puesto que

$$(a,g)(-g^{-1}a, g^{-1}) = (a - gg^{-1}a, gg^{-1}) = (0,1).$$

Además existe un monomorfismo de grupos

$$i : Z/pn+k \rightarrowtail N \qquad \text{dado por } i(a) = (a,1), \quad a \in Z/pn+k.$$

También existen un epimorfismo de grupos

$$p: N \longrightarrow\!\!\!\!\rightarrow C \qquad \text{dado por } p(a,g) = g, \ a \in Z/p^{n+k}, g \in C$$

y un homomorfismo de grupos

$$s: C \longrightarrow N \qquad \text{dado por } s(g) = (a,g), \ g \in C, \text{ tal que } ps = 1_C .$$

Entonces $\quad Z/p^{n+k} \stackrel{i}{\rightarrowtail} N \stackrel{p}{\longrightarrow\!\!\!\!\rightarrow} C$

es una extensión escindible y Z/p^{n+k} es normal en N .

Si identificamos a Z/p^{n+k} como el subgrupo de N que consiste de todos los elementos de la forma (a, 1) y a C como el subgrupo de N que consiste de todos los elementos de la forma (0,g), tenemos que $(a,1)(0,g) = (a,g)$.
Luego $N = Z/p^{n+k}\, C$.
Finalmente $Z/p^{n+k} \cap C = (0,1)$.
Por lo tanto N es el producto semidirecto de Z/p^{n+k} y C; también es un grupo nilpotente. ///

1.6 PROPOSICION. El subgrupo conmutador de N es finito.

Demostración. $[N,N] = yxy^{-1}x^{-1} = x^{u-1} = x^{cp^k}$.
Luego $[N,N] = \langle x^{p^k} \rangle$ es finito . ///

1.7 OBSERVACION. Si indexamos la sucesión central descendente por

$$\Gamma_1(N) = N, \qquad \Gamma_{i+1}(N) = [\, N, \Gamma_i(N)\,]$$

y definimos la clase de nilpotencia "c" como el mínimo índice i tal que $\Gamma_i(N) = (1)$; entonces la clase de nilpotencia de N es el mínimo entero j tal que $j \geq (n/k)+1$.

En efecto, $yxy^{-1}x^{-1} = \langle x^{p^k} \rangle$ y si $yxy^{-1}x^{-1} \in \Gamma_j$ entonces $yxy^{-1}x^{-1} = 1 = x^{p^{n+k}}$.

Por lo tanto, $j \geq (n+k)/k$ es decir $j \geq (n/k)+1$. ///

1-2 EL GENERO DE N.

Sea P una colección de primos y P' la colección de primos complementaria. Si el entero n es un producto de primos en P', por abuso de lenguaje escribiremos $n \in P'$.

2.1 DEFINICION. Se dice que un grupo G es *P-local* si $f\colon G \longrightarrow G$ dada por $f\colon x \longmapsto x^n$, $x \in G$, es biyectiva para todo $n \in P'$.

2.2 DEFINICION. Se dice que un homomorfismo $e\colon G \longrightarrow G_p$ es una *P-localización* si G_p es P-local.

2.3 DEFINICION. Un homorfismo de grupos $\phi\colon G \longrightarrow K$ es *P-inyectivo* si Ker ϕ consiste de los elementos de P'-torsión.

2.4 DEFINICION . Un homomorfismo de grupos $\phi\colon G \longrightarrow K$ es *P-suprayectivo* si, dada $y \in K$, existe $n \in P'$ con $y^n \in \operatorname{im} \phi$; es decir, si coker ϕ consiste de los elementos de P'-torsión.

2.5 DEFINICION. Un homomorfismo de grupos $\phi : G \longrightarrow K$ es *P-biyectivo* o un *P-isomorfismo* si es P-inyectivo y P-suprayectivo.

2.6 DEFINICION. El *género* de un grupo nilpotente N finitamente generado, denotado por G(N), es el conjunto de las clases de isomorfismo de grupos nilpotentes M finitamente generados, tales que $M_p \cong N_p$, para todo primo $p \in P$.

2.7 PROPOSICION. Si α es un P-automorfismo de N, entonces $\det \alpha \equiv 1 \mod p^n$.

Demostración. Obsérvese que cada elemento de N se puede expresar como $x^m y^r$, donde m y r son enteros.
Consideremos el subgrupo conmutador $[w,z] = wzw^{-1}z^{-1}$. Por hipótesis, sabemos que $yxy^{-1}x^{-1} = x^u$. Luego

$$[x^m y^r, y] = (x^m y^r) y (y^{-r} x^{-m}) y^{-1} = x^m y x^{-m} y^{-1} = x^m (y x^{-m} y^{-1}) = x^m x^{-mu} = x^{m-um} = x^{mcp^k}.$$

$$[x^m y^r, x] = (x^m y^r) x (y^{-r} x^{-m}) x^{-1} = x^m (y^r x y^{-r}) x^{-m} x^{-1} = x^m x^{u^r} x^{-m} x^{-1} = x^{u^r - 1}.$$

Sea ZN el centro de N: $ZN = \{ z \in N \mid zx = xz, \forall\, x \in N\}$.
Por lo anterior, tenemos que $x^m y^r \in ZN$ si y sólo si:

i) p^{n+k} divide a mp^k, i.e p^n divide a m y

ii) p^{n+k} divide a u^r-1, i.e p^n divide a r, por el Lema 1.1.

De donde $x^m y^r \in ZN$ si y sólo si p^n divide a m y p^n divide a r.
Entonces $ZN = \langle x^{p^n}, y^{p^n} \rangle$.
Ahora consideremos el subgrupo de torsión de ZN

$TZN = \{ z \in ZN$ tal que $\exists\, x \neq 0,\ x \in ZN$ tal que $xz=0\}$.

Como ZN tiene orden p^n y N tiene orden p^{n+k} entonces TZN tiene orden p^k.
Sea $FZN = \{ z \in ZN \mid z = w^n$ para alguna $w \in ZN$, con $n = |TZN|\}$, el centro libre de N. Luego podemos escribir: $FZN = \{ z \in ZN;\ z = w^{p^k},\ w \in ZN \}$, de donde $FZN = \langle y^{p^{n+k}} \rangle$.
Sean $QN = N/FZN$ y $QN_{ab} = (N/[N,N])/FZN$.

Como $[N,N] = \langle x^{p^k} \rangle$ entonces el exponente de QN_{ab} es p^{n+k}. Recordemos que el *exponente* de G es el mínimo $n \in Z$ tal que $nG=0$.
De manera que $QN_{ab} = \langle x,y;\ p^{n+k}x = 0,\ p^{n+k}y = 0,\ cp^k x = 0 \rangle$,

i.e $QN_{ab} = \langle x,y;\ p^k x = 0,\ p^{n+k} y = 0\rangle$.

Estudiaremos el semigrupo de los P-automorfismos de N.
Sea $\alpha : N \longrightarrow N$ un P-automorfismo. Consideremos el siguiente diagrama:

$$\begin{array}{ccccc}
Z/p^{n+k} & \rightarrowtail & N & \xrightarrow{h} & C \\
\downarrow\beta & & \downarrow\alpha & & \downarrow\delta \\
Z/p^{n+k} & \rightarrowtail & N & \xrightarrow{g} & C
\end{array}$$

Como Z/p^{n+k} es libre de torsión, β no puede ser un P-automorfismo; es un automorfismo.
Consideremos δ. Sea $(x,y) \in N$, $x \in Z/p^{n+k}$, $y \in C$. Veamos que δ es un P-automorfismo.

Sea $y^n \in C$, $n \in P'$; como g es suprayectiva existe $(x,y)^n \in N$ tal que $g(x,y)^n = y^n$. Por otra parte α es P-suprayectiva, por lo que existe $n \in P'$ con $(x,y)^n \in \operatorname{Im} \alpha$, $(x,y) \in N$ y $g\alpha(x,y) = g(x,y)^n = \delta h(x,y) = \delta(y)$. Luego $\delta(y) = y^n$, por lo que existe $n \in P'$ tal que $y^n \in \operatorname{Im}\delta$. Por lo tanto δ es P-suprayectiva.

Sea $(x,y) \in N$, $x \in Z/p^{n+k}$, $y \in C$. Como α es P-inyectiva existe $m \in P'$ tal que $\alpha(x,y)^m = 1$. Entonces $g\alpha\ (x,y)^m = g(1) = 1 = \delta g(x,y)^m = \delta(y^m)$, por lo que existe $m \in P'$ tal que $\delta(y^m) = 1$. Por lo tanto δ es P-inyectiva. Entonces δ es un P-automorfismo.

Supongamos que $C = \langle \xi \rangle$ y sea $\delta(\xi) = \xi^t$. Entonces $\alpha\ (y) = x^q y^t$ para alguna q y $\alpha\ (y^{p^{n+k}}) = x^r y^{tp^{n+k}}$ para alguna r. Como α manda FZN en FZN, tenemos que $\alpha\ (y^{p^{n+k}}) = y^{tp^{n+k}}$ y como FZN no tiene P-torsión, entonces tp^{n+k} no divide a p. Así que $\det \alpha = t$ y para esta t, α es un P-automorfismo. En efecto, para $y \in N$:

i) existe $t \in P'$ tal que $y^t \in \operatorname{Im} \alpha$ y α es P-suprayectiva;

ii) existe $t \in P'$ tal que $\alpha\ (y^t) = 1$ y α es P-inyectiva.

En seguida demostraremos que t toma precisamente los valores congruentes con 1 módulo p^n. Por la restricción sobre t, tenemos que $y^t x y^{-t} = y x y^{-1} = x^u$, es decir $u^t \equiv u \pmod{p^{n+k}}$, luego $u^{t-1} \equiv 1 \pmod{p^{n+k}}$. Finalmente, por el Lema 1.1, $t \equiv 1 \mod p^n$. ///

Entonces podemos asociar a α con la clase residual módulo p^{n+k} de t y así obtener la función

$$\Theta : P\text{-Aut}(N) \longrightarrow (Z/p^{n+k})^* / \{\pm 1\}.$$

2.8 PROPOSICION. Θ es multiplicativa y la $\operatorname{Im}\Theta$ es un subgrupo de $(Z/p^{n+k})^*/\{\pm 1\}$.

Demostración. Sean $\alpha, \beta \in P\text{-Aut}(N)$. Entonces $\Theta(\alpha) = u \in (Z/p^{n+k})^*/\{\pm 1\}$, $\Theta(\beta) = u' \in (Z/p^{n+k})^*/\{\pm 1\}$, luego $\Theta(\alpha\beta) = uu' = 1 = \Theta(\alpha)\Theta(\beta)$. Por lo tanto Θ es multiplicativa.

Como $t \equiv 1 \mod p^n$, $\operatorname{Im}\Theta$ es un subgrupo de $(Z/p^{n+k})^*/\{\pm 1\}$ que consiste de las unidades de Z/p^{n+k}, modulo ± 1, que son congruentes con 1 módulo p^n. ///

Observación. Claramente hay p^k de estas unidades y $\operatorname{Im}\Theta$ es un subgrupo de orden p^k.

Definamos una función suprayectiva $\sigma: (Z/p^{n+k})^*/\{\pm 1\} \longrightarrow\!\!\!\!\to G(N)$

como sigue : para $a \in Z$ sea $\bar{a} \in (Z/p^{n+k})^{*}/\{\pm 1\}$ y sea $\delta\bar{a}=M$. Si h es el rango de FZN, tenemos el siguiente diagrama de extensiones de grupos: (recordemos que el rango de un grupo abeliano A es el máximo número de elementos linealmente independientes de A)

$$\begin{array}{ccccc} Z^h & \xrightarrow{f} & N & \longrightarrow\!\!\!\!\rightarrow & N/FZN \\ \downarrow A & & \downarrow \Phi & & \cong\ \downarrow B \\ Z^h & \xrightarrow{g} & M & \longrightarrow\!\!\!\!\rightarrow & M/FZM \end{array} \qquad (2.1)$$

donde $|\det A| = |a|$, $fZ^h = FZN$, $gZ^h = FZM$, $B: N/FZN \cong M/FZM$. Por lo tanto Φ es un P-isomorfismo.

Inversamente, un diagrama de la forma (2.1) con B un isomorfismo, $fZ^h = FZN$ y Φ un P-isomorfismo implica que: $M \in G(N)$, $gZ^h = FZM$ y $\delta\bar{a} = M$ donde $\bar{a} = \alpha(\Phi)$, $\alpha \in$ P-Aut (N). (2.2)

De un modo similar, si $\bar{A}$ es una matriz con $|\det \bar{A}| = |\bar{a}|$ representando a $\bar{a}^{-1}$, podemos construir el diagrama conmutativo siguiente

$$\begin{array}{ccccc} Z^h & \xrightarrow{g} & M & \longrightarrow\!\!\!\!\rightarrow & M/FZM \\ \downarrow \bar{A} & & \downarrow \phi & & \downarrow \cong \\ Z^h & \xrightarrow{f} & N & \longrightarrow\!\!\!\!\rightarrow & N/FZN \end{array} \qquad (2.3)$$

Debido a lo anterior, tenemos el siguiente teorema:

2.9 TEOREMA. La sucesión $\text{P-Aut}(N) \xrightarrow{\theta} (Z/p^{n+k})^{*}/\{\pm 1\} \xrightarrow{\delta}\!\!\!\!\rightarrow G(N)$ es exacta, entendiendo que $\delta x=\delta y$ si y sólo si $x= \alpha(y)$ para algún P-Automorfismo $\alpha : N \longrightarrow N$.

Demostración. Sea $\delta x = \delta y = M$. Por (2.1) y (2.3) existe un diagrama conmutativo

$$\begin{tikzcd}
Z^h \arrow[r, tail, "f"] \arrow[d, "X"] & N \arrow[r, two heads] \arrow[d, "\Phi"] & N/FZN \arrow[d, "\cong"] \\
Z^h \arrow[r, tail, "g"] \arrow[d, "Y"] & M \arrow[r, two heads] \arrow[d, "\Psi"] & M/FZM \arrow[d, "\cong"] \\
Z^h \arrow[r, tail, "f"] & N \arrow[r, two heads] & N/FZN
\end{tikzcd}$$

con $fZ^h = FZN$, $gZ^h = FZM$, $|\det X|$ representando a x y $|\det Z|$ representando a y^{-1}. Entonces $\Psi\Phi : N \longrightarrow N$ es un P-Automorfismo y $\Theta(\Psi\Phi) = y^{-1}x$.

Inversamente, sea $\partial y = M$ y sea $\Phi \in$ P-Aut(N). Consideremos el diagrama conmutativo siguiente:

$$\begin{tikzcd}
Z^h \arrow[r, tail, "f"] \arrow[d, "A"] & N \arrow[r, two heads] \arrow[d, "\Phi"] & N/FZN \arrow[d, "\cong"] \\
Z^h \arrow[r, tail, "f"] \arrow[d, "Y"] & N \arrow[r, two heads] \arrow[d, "\Psi"] & N/FZN \arrow[d, "\cong"] \\
Z^h \arrow[r, tail, "g"] & M \arrow[r, two heads] & M/FZM
\end{tikzcd}$$

con $fZ^h = FZN$, $gZ^h = FZM$, $|\det A|$ representando a $\Theta\Phi$ y $|\det Y|$ representando a y. Entonces $\Psi\Phi$ es un P-Isomorfismo y por (2.2) $M = \partial a$, donde $a = \alpha(\Psi\Phi) = \alpha(\Psi)\,\Theta(\Phi) = \Theta\Phi\,(y)$. ///

Utilizaremos el Teorema anterior para dar al conjunto G(N) una estructura de grupo cíclico y calcularemos su orden.

2.10 DEFINICION. Sea N un grupo nilpotente finitamente generado con subgrupo conmutador finito, definido mediante la siguiente presentación:

$$N = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^u \rangle$$

donde el centro libre de N es $FZN = \langle y^{p^k} \rangle$ y exponente $(QN = N/FZN) = p^{n+k}$.

El grupo abeliano (aditivo) G(N) consiste del conjunto G(N) provisto de la única estructura de grupo que hace de $\delta: (Z/p^{n+k})^*/\{\pm 1\} \longrightarrow\!\!\!\!\rightarrow G(N)$ un homomorfismo.

2.11 TEOREMA. G(N) es un grupo cíclico de orden $p^{n-1}(p-1)/2$.

Demostración. Por definición, G(N) es un grupo finito y $N = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^u \rangle$ es su elemento neutro. Podemos deducir del Teorema 2.9 que G(N) es cíclico y calcular su orden.

En efecto, $Z/p^{n+k})^*/\{\pm 1\}$ es cíclico y tenemos que

$$(Z/p^{n+k})^* \begin{cases} Z/(p-1) \times Z/p^{n+k-1} & \text{si } p \text{ es impar} \\ \{\pm 1\} \times Z/2n+k-1 & \text{si } p=2,\ k>1 \\ \{1\} & \text{si } p=2,\ k=1 \end{cases}$$

Como hemos eliminado el caso $p=2,\ k=1$ que se estudiará en el Capítulo II, el

orden de $(Z/p^{n+k})^*/\{\pm 1\}$ es $p^{n+k-1}(p-1)/2$.
Entonces el grupo cociente G(N) es cíclico de orden $p^{n-1}(p-1)/2$. ///

Dado que asignamos a N el papel de elemento neutro de G(N), queda por encontrar un generador del grupo G(N).

2.12 PROPOSICION. N_1 es generador de G(N).

Demostración. Como $(Z/p^{n+k})^*/\{\pm 1\}$ es cíclico, posee un generador ℓ tal que ℓ puede ser considerado como un entero positivo y el mínimo exponente s tal que $\ell^s \equiv \pm 1 \bmod p^n$ es $s = p^{n-1}(p-1)/2$. Ignoramos los casos triviales $p=2,\ n=1$; $p=2,\ n=2$; $p=3,\ n=1$ donde G(N) es el grupo trivial. Sea $\ell m \equiv 1 \pmod{p^n}$ y sea N_1 el grupo dado por

$$N_1 = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^u \rangle.$$

Consideremos el homomorfismo $\Phi : N \longrightarrow N_1$ dado por $\Phi(x) = x,\ \Phi(y) = y^{\ell}$.
Luego Φ induce, por restriccion, $\Phi_F: FZN \longrightarrow FZN_1$ dado por

$\Phi_F(y^{p^{n+k}}) = y^{\ell p^{n+k}}$ con det $\Phi_F = \ell$. Entonces la función inducida de los grupos cocientes $N/FZN = QN \cong QN_1 = N_1/FZN_1$ es un isomorfismo y $\partial: (Z/p^{n+k})^*/\{\pm 1\} \twoheadrightarrow G(N)$ manda la clase de ℓ en N_1. Como ℓ genera $(Z/p^{n+k})^*/\{\pm 1\}$ módulo $\mathrm{Im}\Theta$, entonces N_1 genera $G(N)$. ///

2.13 TEOREMA. N no es isomorfo a N_1.

Demostración. Sean $N = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^u \rangle$,

$$N_1 = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^{u^m} \rangle,$$

donde m no es congruente con $\pm 1 \pmod{p^n}$.
Como vimos en la Proposición 1.5, N es el producto semidirecto de Z/p^{n+k} y C bajo la acción $\xi.a = ua$, $C = \langle \xi \rangle$, $a \in Z/p^{n+k}$.
En N_1, la acción es $\xi.a = u^m a$, $C = \langle \xi \rangle$, $a \in Z/p^{n+k}$.
Entonces existen las siguientes sucesiones exactas cortas (escindibles).

$$Z/p^{n+k} \rightarrowtail N \twoheadrightarrow C$$

y

$$Z/p^{n+k} \rightarrowtail N_1 \twoheadrightarrow C$$

Supongamos que existe un isomorfismo $\Phi : N \cong N_1$. Luego tenemos el siguiente diagrama

$$\begin{tikzcd}
Z/p^{n+k} \arrow[r, tail] \arrow[d, "\cong\ \alpha"] & N \arrow[r, two heads] \arrow[d, "\Phi"] & C = \langle \xi \rangle \arrow[d, "\cong\ \beta"] \\
Z/p^{n+k} \arrow[r, tail] & N_1 \arrow[r, two heads] & C
\end{tikzcd}$$

donde α y β son inducidos por Φ.

Luego $\beta\xi = \xi$ o $\beta\xi = \xi^{-1}$ y $ua = u^m a$ o $ua = u^{-m}a$ donde u^{-m}

es el inverso de u^m (mod p^{n+k}).
Se sigue que $u^{m-1} \equiv 1 \pmod{p^{n+k}}$ o $u^{m+1} \equiv 1 \pmod{p^{n+k}}$.

Por el Lema 1.1, sabemos que $u^{p^n} \equiv 1 \pmod{p^{n+k}}$. Entonces $m \equiv 1 \pmod{p^n}$ o $m \equiv -1 \pmod{p^n}$ y $m \not\equiv \pm 1 \pmod{p^n}$, lo que contradice nuestra hipótesis. Por lo tanto N no es isomorfo a N_1. ///

I-3 RELACIONES ENTRE LOS GRUPOS QUE PERTENECEN A UN GENERO DADO.

3.1 PROPOSICION. En el grupo aditivo $G(N)$, cíclico de orden s, $N_i = iN_1$, $0 \leq i \leq s-1$, $N_0 = N_s$.

Demostración. Sea $N_1 = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^{u^m} \rangle$. Entonces $i(x^{p^{n+k}}) = x^{ip^{n+k}} = 1$ y

$$i(yxy^{-1}) = i(x^{u^m}) = \underbrace{x^{u^m} \cdots x^{u^m}}_{i \text{ veces}} = x^{\overbrace{u^m \cdots u^m}^{i \text{ veces}}} = x^{u^{m^i}}.$$

Por lo tanto $\quad iN_1 = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^{u^{m^i}} \rangle = N_i$. /// $\quad$ (3.1)

3.2 PROPOSICION. Sea $N_i = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^{u^{m^i}} \rangle$.
Entonces Φ_i: $N_i \longrightarrow N_{i+1}$, $0 \leq i \leq s-1$, dado por $\Phi_i(x) = x$, $\Phi_i(y) = y^\ell$ encaja cada N_i como un subgrupo normal de N_{i+1}, con cociente Z_ℓ.

Demostración. Veamos que Φ_i es un homomorfismo, es decir que: $\Phi_i(yxy^{-1}) = \Phi_i(y)\,\Phi_i(x)\,\Phi_i(y^{-1})$, lo que equivale a demostrar que $\Phi_i(yxy^{-1}) = y^\ell xy^{-\ell}$ en N_{i+1}.

i.e $\quad y^\ell xy^{-\ell} = x^{u^{m^i}}$ en N_{i+1}.

En N_{i+1} tenemos que $yxy^{-1} = x^{u^{m^{i+1}}}$, luego $y^\ell xy^{-\ell} = x^{(u^{m^{i+1}\ell})}$.
Por hipótesis $m\ell \equiv 1 \pmod{p^n}$, por lo que $m^{i+1}\ell \equiv m^i \pmod{p^n}$ y $m^{i+1}\ell = m^i + cp^n$ para alguna c. Además, por el Lema 1.1, $u^{cp^n} = 1 + dp^{n+k}$ para alguna d, así que $u^{m^{i+1}\ell} = u^{m^i+cp^n} = u^{m^i}(1+dp^{n+k})$, de donde

$$x^{u^{m^{i+1}\ell}} = x^{u^{m^i}(1+dp^{n+k})} = x^{u^{m^i}}.$$

Por lo tanto Φ_i es un homomorfismo.

Veamos que Φ_i es inyectivo. En efecto,

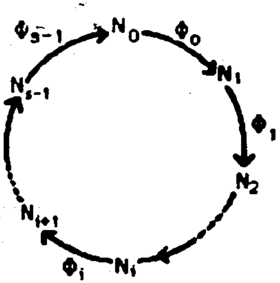
si $\Phi_i(x) = 1 = x^{p^{n+k}}$ entonces $x = x^{p^{n+k}} = 1$, $\forall\, x \in N_i$. Por lo tanto $Ker(\Phi_i)=\{1\}$.

Demostremos que $\Phi_i N_i$ es normal en N_{i+1}.

Sean $x,y \in \Phi_i N_i$, $y^{\ell} \in N_{i+1}$. Como Φ_i es un homomorfismo, entonces $\Phi_i(yxy^{-1}) = y^{\ell}xy^{-\ell} \in \Phi_i N_i$. Por lo tanto $\Phi_i N_i$ es normal en N_{i+1}.

Además $x^{u^{m^{i+1}}\ell} = x^{u^{m^{i}}}$, lo que implica $N_{i+1}/\Phi_i N_i = Z_{\ell}$. ///

Este resultado nos permite construir una "Escalera de Escher" de encajes normales:



tal que cada grupo cociente es cíclico de orden ℓ.

Recordamos que ℓ es un entero positivo y el mínimo exponente tal que $\ell^s \equiv \pm 1 \bmod p^n$ es $s = p^{n-1}(p-1)/2$, donde s es el orden de G(N).

3.3 EJEMPLOS.

A continuación, daremos como ejemplos los dos géneros más simples no triviales:

1) Sean $p=5, n=1, k=1$. Entonces $u = 1+cp^k = 6$ y $s = p^{n-1}(p-1)/2 = 2$

$\ell^s \equiv \pm 1 (\mathrm{mod}\ p^n)$ es decir $\ell = 3$

$\ell m \equiv 1 (\mathrm{mod}\ p^n)$ es decir $m = 2$ y

$N_0 = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^u \rangle$ o sea $N_0 = \langle x,y;\ x^{25} = 1,\ yxy^{-1} = x^6 \rangle$.

$N_1 = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^{u^m} \rangle$ o sea $N_1 = \langle x,y;\ x^{25} = 1,\ yxy^{-1} = x^{11} \rangle$.

2) Sean $p=7$, $n=1$, $k=1$ entonces $u = 1+cp^k = 8$ y $s = p^{n-1}(p-1)/2 = 3$,
$\ell^s \equiv \pm 1\ (\mathrm{mod}\ p^n)$ es decir $\ell = 4$
$\ell m \equiv 1\ (\mathrm{mod}\ p^n)$ es decir $m = 2$ y
$N_0 = \langle x,y;\ x^{49} = 1,\ yxy^{-1} = x^8 \rangle$.
$N_1 = \langle x,y;\ x^{49} = 1,\ yxy^{-1} = x^{15} \rangle$ por lo que $yxy^{-1}x^{-1} = x^{14}$.
$N_2 = \langle x,y;\ x^{49} = 1,\ yxy^{-1} = x^{29} \rangle$ por lo que $yxy^{-1}x^{-1} = x^{28}$.
Así que $N_2 = 2N_1$.
$N_3 = N_s = \langle x,y;\ x^{49} = 1,\ yxy^{-1} = x^8 \rangle = N_0$.

A continuación mostraremos como la estructura del grupo cíclico $G(N)$, dada en la definición 2.10, puede ser descrita de un modo distinto, utilizando las nociones de producto fibrado y de coproducto fibrado en N.

Ya hemos visto en (2.1) y (2.3) que podemos construir P-isomorfismos de $N \longrightarrow M$ y de $M \longrightarrow N$. En seguida demostraremos un resultado más general.

3.4 TEOREMA. Sea $q \in P$ un primo con $q \in (Z/p^{n+k})^*/\{\pm 1\}$ y sea $\delta q = M \in G(N)$. Entonces existe un q'-isomorfismo $\Phi: N \longrightarrow M$, $q' \in P'$.

Demostración. Refiriéndonos a la construcción de (2.1), tenemos $|\det A| = q$, $|\mathrm{coker}\ A| = q$. Ya que Φ encaja N en M como un subgrupo normal y que $\mathrm{coker}\ \Phi = q$, se sigue que Φ es un q'-isomorfismo. ///

3.5 COROLARIO. Sea $M \in G(N)$ y sea P una familia finita de primos. Entonces existen P-isomorfismos $\Phi: N \longrightarrow M$ y $\phi: M \longrightarrow N$.

Demostración. Es suficiente establecer la existencia de Φ. Supongamos que $a \in Z$ es tal que $\delta a = M$ con $a \in (Z/p^{n+k})^{*}/\{\pm 1\}$. Por el Teorema de Dirichlet existe una infinidad de primos p tales que $p \equiv a$. Escogemos $p \in P'$, con $p \equiv a$ y aplicando el Teorema anterior concluimos que $\Phi: N \longrightarrow M$ es un P-isomorfismo. ///

3.6 DEFINICION. Sean $L, M \in G(N)$. Se dice que un par de homomorfismos $\Phi : N \longrightarrow M$ y $\Psi : N \longrightarrow L$ es *un par exhaustivo* si Φ o Ψ es un P-isomorfismo y si, dado cualquier primo $p' \in P'$ entonces Φ o Ψ es un P'-isomorfismo. De una manera similar se habla de un par exhaustivo $\phi : M \longrightarrow N$ y $\psi : L \longrightarrow N$.

3.7 TEOREMA. Existen pares exhaustivos $\Phi : N \longrightarrow M$, $\Psi : N \longrightarrow L$ y pares exhaustivos $\phi : M \longrightarrow N$ y $\psi : L \longrightarrow N$.

Demostración. Sea $\Phi : N \longrightarrow M$ un P-isomorfismo. Entonces el conjunto $P' = \{p' | \Phi$ no es un P'-isomorfismo$\}$ es finito. Como Φ es inyectiva, ΦN es normal en M y coker Φ es finito. Usamos el Corolario 3.5 para construir un P'-isomorfismo $\Psi : N \longrightarrow L$.
Obviamente la demostración es la misma para $\phi : M \longrightarrow N$ y $\psi : L \longrightarrow N$.
///

A continuación, estudiaremos más ampliamente la función α definida en la Proposición 2.7, generalizando primero la Proposición 2.8.

3.8 PROPOSICION. Si $K, L, M \in G(N)$ y $f: M \longrightarrow L$, $g: L \longrightarrow K$ son P-isomorfismos, entonces $\alpha(gf) = \alpha(g)\alpha(f)$ en $(Z/p^{n+k})^{*}/\{\pm 1\}$.

Demostración. Consideremos el diagrama siguiente (ver (2.1)).

$$\begin{array}{ccccc}
Z^n & \rightarrowtail & M & \twoheadrightarrow & M/FZM \\
\downarrow & & \downarrow f & & \downarrow \cong \\
Z^n & \rightarrowtail & L & \twoheadrightarrow & L/FZL \\
\downarrow & & \downarrow g & & \downarrow \cong \\
Z^n & \rightarrowtail & K & \twoheadrightarrow & K/FZK
\end{array}$$

Sean $a, b \in (Z/p^{n+k})^*/(\pm 1)$, δ un homomorfismo. Entonces $\delta(a) = L$ donde $a = \alpha(f)$ y $\delta(ba) = K$ donde $b = \alpha(g)$.
Como $\delta(ba) = \delta(b)\delta(a)$ entonces $\alpha(gf) = \alpha(g)\alpha(f)$. ///

3.9 PROPOSICION. Sean $H, K, L, M \in G(N)$ y $\mathrm{nil}\, N \leq c$. Sea

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\delta"] & L \arrow[d, "\beta"] \\ K \arrow[r, "f'"'] & H \end{tikzcd} \qquad (3.1)$$

un diagrama de coproducto fibrado en N_c (la categoría de grupos nilpotentes con $\mathrm{nil}\, G \leq c$), con f un P-isomorfismo. Entonces
i) f' es un P-isomorfismo,
ii) $\alpha(f) = \alpha(f')$.

Demostración.
i) Por las propiedades de los coproductos fibrados $\ker f \cong \ker f'$. Como f es P-inyectiva, entonces f' también lo es. Sea $y \in M$; por ser f P-suprayectiva, existe $n \in P'$ tal que $y^n \in \mathrm{Im} f$. Entonces $\beta(y^n) \in H$. Como el diagrama conmuta tenemos que $f'(\delta(y)) = \beta(y^n) = (\beta y)^n$, $n \in P'$. Por lo tanto f' es P-suprayectiva. ///
ii) Por las propiedades de los coproductos fibrados $\mathrm{coker}\, f \cong \mathrm{coker}\, f'$ donde el cokernel es tomado en N_c. Sin embargo, el cokernel en N_c es el cokernel habitual. Entonces $\alpha(f) = \alpha(f')$. ///

3.10 TEOREMA. Si $f: M \longrightarrow L$ es un P-automorfismo, entonces $\delta\alpha(f) = L - M$.

Demostración. Sea $g: N \longrightarrow M$ un P-automorfismo. Por (2.2), $\delta\alpha(g) = M$, $\delta\alpha(fg) = L$ y por la Proposición 3.8 (δ siendo un homomorfismo) $\delta\alpha(f) = \delta\alpha(fg) - \delta\alpha(g) = L - M$. ///

3.11 COROLARIO. En el diagrama de coproducto fibrado en N_c (ver 3.1), donde $H, K, L, M \in G(N)$ y $\mathrm{nil}\, N \leq c$, $M + H = L + K$ en $G(N)$.

Demostración. Por la Proposición 3.9 ii) tenemos $\delta\alpha(f) = \delta\alpha(f')$ y por el Teorema 3.10, $\delta\alpha(f) = L - M$, $\delta\alpha(f') = H - K$. Entonces $L - M = H - K$ y $M + H = L + K$. ///

Utilizaremos esos resultados para dar dos interpretaciones de la operación binaria de grupo en $G(N)$.

3.12 TEOREMA. Sea N un grupo nilpotente finitamente generado con subgrupo conmutador finito y sea $G = G(N)$. Definimos las operaciones binarias $b_1, b_2 : G \times G \longrightarrow G$ como sigue:

i) Si $L, M \in G$, escogemos un par exhaustivo $\Phi : N \longrightarrow L$, $\Psi : N \longrightarrow M$ y determinamos $b_1(L,M)$ como el coproducto fibrado en N de (Φ, Ψ).

ii) Si $L, M \in G$, escogemos un par exhaustivo $\phi : L \longrightarrow N$, $\psi : M \longrightarrow N$ y determinamos $b_2(L,M)$ como el producto fibrado en N de (ϕ, ψ).

Entonces b_1, b_2 estan bien definidas y $b_1(L,M) = b_2(L,M) = L + M$.

Demostración. Sean $L, M \in G$, $\Phi : N \longrightarrow L$, $\Psi : N \longrightarrow M$ un par exhaustivo y $b_1(L,M)$ el coproducto fibrado en N de (Φ, Ψ). Supongamos $L = L'$, $M = M'$; sea $\Phi' : N \longrightarrow L'$, $\Psi' : N \longrightarrow M'$ un par exhaustivo. Consideremos los siguientes diagramas:

$$\begin{tikzcd}
N \arrow[r, "\Phi"] \arrow[d, "\Psi"'] & L = L' \arrow[d, "\delta"] \arrow[dd, bend left=60, "\delta'"] \\
M' = M \arrow[r, "\sigma"] \arrow[dr, bend right, "\sigma'"'] & K \arrow[d, "h"] \\
 & K'
\end{tikzcd}
\qquad
\begin{tikzcd}
N \arrow[r, "\Phi'"] \arrow[d, "\Psi'"'] & L' = L \arrow[d, "\delta'"] \arrow[dd, bend left=60, "\delta"] \\
M = M' \arrow[r, "\sigma'"] \arrow[dr, bend right, "\sigma"'] & K' \arrow[d, "h'"] \\
 & K
\end{tikzcd}$$

El coproducto fibrado de (Φ, Ψ), determinado por $b_1(L,M) = (K, \sigma, \delta)$ y el coproducto fibrado de (Φ', Ψ'), determinado por $b_1(L',M') = (K', \sigma', \delta')$. Entonces existen $h : K \longrightarrow K'$ y $h' : K' \longrightarrow K$, únicas, tales que $h\delta = \delta'$, $h'\delta' = \delta$; $h\sigma = \sigma'$, $h'\sigma' = \sigma$. Luego $h'h\delta = \delta$, $hh'\sigma' = \sigma'$ y $h'h = 1_{K'}$, $hh' = 1_K$. Por lo que $\delta = \delta'$, $\sigma = \sigma'$, $(K, \sigma, \delta) = (K', \sigma', \delta')$ y $b_1(L,M) = b_1(L',M')$.

Por lo tanto el coproducto fibrado de (Φ,Ψ) no depende de la elección de (L,M) y b_1 está bien definida. De la misma manera, se demuestra que b_2 está bien definida. Por el Corolario anterior, $K = L + M$. ///

Utilizando estos resultados , vamos a establecer el producto fibrado y el coproducto fibrado en N de los grupos N_i y N_k que pertenecen a $G(N)$.

Por el Corolario 3.5, sabemos que existe para cada i,k un ℓ-isomorfismo $\Psi : N_i \longrightarrow N_k$ (ℓ está definida como en la Proposición 2.12, es decir ℓ es un entero positivo y $\ell^s \equiv \pm 1 \bmod p^n$, $s = p^{n-1}(p-1)/2$, donde s es el orden de $G(N)$).

Sea $\Phi: N_j \longrightarrow N_k$ dado por $\Phi(x) = x$, $\Phi(y) = y^{\ell^{k-j}}$ con $k \equiv j \pmod s$.
El Teorema 3.12 implica:

3.13 TEOREMA. Para cada ℓ-isomorfismo $\Psi : N_i \longrightarrow N_k$ el producto fibrado de $\Psi : N_i \longrightarrow N_k$ y $\Phi : N_j \longrightarrow N_k$ es N_t donde $k+t \equiv i+j \pmod s$.

Demostración. Consideremos el siguiente diagrama del producto fibrado de (Ψ, Φ)

$$\begin{tikzcd} N_t \arrow[r, "\sigma"] \arrow[d, "\delta"'] & N_i \arrow[d, "\Psi"] \\ N_j \arrow[r, "\Phi"'] & N_k \end{tikzcd}$$

Por el Teorema 3.12, $N_t = N_i + N_j$ y por el Corolario 3.11, $N_k + N_t = N_i + N_j$ donde $k+t \equiv i+j \bmod s$. ///

3.14 TEOREMA. Para cada ℓ-isomorfismo $\Psi : N_j \longrightarrow N_i$, el coproducto fibrado de $\Psi : N_j \longrightarrow N_i$ y $\Phi : N_j \longrightarrow N_k$ es N_t donde $j+t \equiv i+k \pmod s$.

Demostración. Consideremos el siguiente diagrama del coproducto fibrado de (Φ,Ψ)

$$\begin{tikzcd} N_j \arrow[r, "\Psi"] \arrow[d, "\Phi"'] & N_i \arrow[d, "\rho"] \\ N_k \arrow[r, "\sigma"'] & N_t \end{tikzcd}$$

Por el Teorema 3.12, $N_t = N_i \cdot N_k$ donde $j+t \equiv i+k \pmod{s}$. ///

Recordemos la Proposición 3.1: $N_i = iN_1$, $0 \le i \le s-1$, $N_0 = N_s$ que utilizaremos en seguida, para obtener un resultado importante.

3.15 TEOREMA. Sea N un grupo nilpotente finitamente generado con subgrupo conmutador finito y sea $\Phi: G(N)^k \longrightarrow G(N^k)$ dado por $\Phi(M_1, M_2, \ldots, M_k) = M_1 \times M_2 \times \ldots \times M_k$. Entonces Φ es un homomorfismo.

Demostración. Sean $M_1, M_2, \ldots, M_k$, $L_1, L_2, \ldots L_k$ que pertenecen a $G(N)$. Escojamos P-isomorfismos $\Phi_i: N \longrightarrow M_i$ y sea $P_i = \{p \mid \Phi_i$ no es un p-isomorfismo $\}$ $i = 1,2,\ldots,k$. Entonces P_i es un conjunto finito.
Sea $P = P_1 \cup \ldots \cup P_k$ y escojamos P-isomorfismos $\Psi_i: N \longrightarrow L_i$, $i = 1,2,\ldots,k$. Si $Q = P'$ entonces cada Φ_i es un Q-isomorfismo y $P \cup Q = \Pi$, el conjunto de todos los primos. Se sigue que, si

$$\Phi = \Phi_1 \times \ldots \times \Phi_k: N^k \longrightarrow M_1 \times \ldots \times M_k \quad \text{y}$$
$$\Psi = \Psi_1 \times \ldots \times \Psi_k: N^k \longrightarrow L_1 \times \ldots \times L_k$$

entonces (Φ, Ψ) es un par exhaustivo. Luego el diagrama

$$\begin{tikzcd} N^k \arrow[r, "\Phi"] \arrow[d, "\Psi"'] & M_1 \times \ldots \times M_k \arrow[d, "\rho"] \\ L_1 \times \ldots \times L_k \arrow[r, "\sigma"'] & K_1 \times \ldots \times K_k \end{tikzcd} \tag{3.2}$$

con $\sigma = \sigma_1 \times \ldots \times \sigma_k$, $\rho = \rho_1 \times \ldots \times \rho_k$, es un producto fibrado en N, si cada diagrama para i

$$\begin{array}{ccc} N & \xrightarrow{\Phi_i} & M_i \\ \downarrow\Psi_i & & \downarrow p_i \\ L_i & \xrightarrow[\sigma_i]{} & K_i \end{array} \qquad (3.3)$$

es un producto fibrado en N. Sin embargo, (3.3) es un producto fibrado si y sólo si es un coproducto fibrado e igualmente para (3.2). Entonces si (3.3) es un coproducto fibrado para cada i, por el teorema 3.12 $K_i = M_i + L_i$ en G(N) y $K_1 \times \ldots \times K_k = (M_1 \times \ldots \times M_k) + (L_1 \times \ldots \times L_k)$ en $G(N^k)$. Así hemos probado que Φ es un homomorfismo. ///

Observemos que Φ: $G(N)^k \longrightarrow G(N^k)$ está determinado por sus componentes Φ_i: $G(N) \longrightarrow G(N^k)$, $i = 1,\ldots,k$ y como $\Phi_i(M) = M \times N^{k-1}$ entonces Φ_i es independiente de i.
Para simplificar las notaciones escribamos $\Phi_i = \lambda$: $G(N) \longrightarrow G(N^k)$. Entonces

$$M_1 \times \ldots \times M_k = \Phi(M_1,\ldots,M_k) = \sum_{i=1}^{k} \lambda(M_i) = \lambda(\sum_{i=1}^{k} Mi) = (\sum_{i=1}^{k} M_i) \times N^{k-1}.$$

De este resultado podemos deducir el siguiente teorema.

3.16 TEOREMA. Sea N un grupo nilpotente finitamente generado con subgrupo conmutador finito y sean M_i, $L_i \in G(N)$, $i=1,2,\ldots k$. Entonces si

$$\sum_{i=1}^{k} M_i = \sum_{i=1}^{k} L_i \quad \text{en } G(N) \quad \text{entonces} \quad \Pi M_i \cong \Pi L_i. \qquad ///$$

3.17 TEOREMA. Sea $N_i = \langle x,y;\ x^{p^{n+k}} = 1,\ yxy^{-1} = x^{u^{m^i}} \rangle$ y sean $(i_1, i_2,\ldots, i_t)$, $(j_1, j_2,\ldots, j_t)$ listas de enteros en el intervalo $[0,\ s-1]$, tal que

$$\sum_{m=1}^{t} i_m \equiv \sum_{m=1}^{t} j_m \pmod s,\quad s = p^{n-1}(p-1)/2. \text{ Entonces } \prod_{m=1}^{t} N_{i_m} \cong \prod_{m=1}^{t} N_{j_m}. \quad ///$$

II- EL CASO EXCEPCIONAL.

En el Capítulo I, al estudiar el grupo $N = \langle x,y \,;\, x^{p^{n+k}} = 1,\ yxy^{-1} = x^u \rangle$, donde $u = 1+cp^k$, eliminamos el caso $p = 2$, $k = 1$. Ahora nos ocuparemos de este caso.

En efecto, el Lema I-1.1 es falso para $p = 2$, $k = 1$. Por ejemplo, si $u = 1 + cp^k = 7$, $p = 2$, $k = 1$, $n = 2$, entonces el orden de u módulo 2^3 es 2 y no 2^2.

Con el fin de establecer un Lema para el caso excepcional de $p = 2$, $k = 1$, consideraremos enteros positivos u de la forma $1 + 2c$ con c impar; en otras palabras, enteros positivos que son congruentes con 3 módulo 4.

1.1 PROPOSICION. Si $u \equiv 3 \pmod 4$ entonces existe una m única tal que $u \equiv 2^m - 1 \pmod{2^{m+1}}$, $m \geq 2$

Demostración. Empezaremos por demostrar la existencia de m. Como $u \equiv 3 \pmod 4$, $u \equiv 2^2-1 \pmod{2^2}$, $u + 1 = 2^2 v$ con $v = 1, 2, \ldots$

i) Sea v impar, es decir $v = 2n+1$ con $n = 0, 1, \ldots$

Luego $u + 1 = 2^2(2n+1) = 2^3 n + 2^2$; $u + 1 \equiv 2^2 \pmod{2^3}$, $u \equiv 2^2 - 1 \pmod{2^3}$. Entonces $u \equiv 2^m - 1 \pmod{2^{m+1}}$ y $m = 2$.

ii) Sea v par, es decir v se puede escribir como

$v = 2(2^{\alpha} p_1^{\beta_1} \ldots p_n^{\beta_n})$ con $\alpha = 0,1,\ldots$ $\beta = 0,1,\ldots$ y $p_1,\ldots,p_n$ números primos $\neq 2$.

Luego $u + 1 = 2^3(2^{\alpha} p_1^{\beta_1} \ldots p_n^{\beta_n})$. Entonces $u \equiv 2^m - 1 \pmod{2^{m+1}}$ y $m = 3 + \alpha$.

Observemos que m es única ya que en i) $m = 2$ y en ii) m es la potencia del número primo 2 en la descomposición en primos de u. ///

1.2 OBSERVACION. Si u se escribe en base 2, entonces m es el número de los dígitos 1 que hay, empezando por la derecha, antes de encontrar el primer cero. Como en la Proposición anterior $u = 2^2 v - 1$, $v = 1, 2, \ldots$.

a) si v es impar, es de la forma $v = 2n+1$, $n = 0,1,\ldots$. De donde $u = 2^2 v - 1 = 2^3 n + 3 = 2^3 n + 2^1 + 2^0$.

Así que u, en base 2, es de la forma ...011, porque no existe el término 2^2 en su descomposición. Por lo tanto hay 2 dígitos 1 a la derecha antes del cero y $m = 2$, lo que corrobora el inciso i) de la demostración anterior.

b) v es par, es decir u es de la forma $u = (2^3 2^{\alpha} p_1^{\beta_1} \ldots p_n^{\beta_n}) - 1$ con $\alpha = 0, 1, \ldots \beta = 0, 1, \ldots$ y $p_1, \ldots p_n$ primos $\neq 2$. Luego $u = 2^3 + [2^3(2^{\alpha} p_1^{\beta_1} \ldots p_n^{\beta_n} - 1)] - 1$, $u = 7 + 2^3(2^{\alpha} p_1^{\beta_1} \ldots p_n^{\beta_n} - 1)$.

En base 2 podemos escribir $u = 2^0 + 2^1 + 2^2 + 2^{\delta_0} + 2^{\delta_1} + \ldots + 2^{\delta_n}$ donde $\delta_0 = 3$, $\delta_1 = 4$, $\delta_2 = 5, \ldots$, $\delta_n = n+3$ y $2^{\delta_i} = 0$ para alguna i, $0 \leq i \leq n$. Así que en base 2, u es de la forma $\ldots 1 \ldots 001 \ldots 111$ y $u \equiv 2^m - 1 \pmod{2^{m+1}}$ con $m = 3 + x$, donde $x = i$ en δ_i tal que $2^{\delta_i} = 0$ por primera vez en la suma de potencias de 2 de u. Es decir, en base 2, m es igual a la cantidad de dígitos 1 que se escriben, empezando por la derecha, antes de encontrar el primer cero.

Ejemplo. Sea $u = 39 = 7 + 32 = 2^0 + 2^1 + 2^2 + 2^3 + 2^3 + 2^3 + 2^3$. Según nuestra descomposición se escribe $u = 39 = 1 + 2 + 4 + 32 = 2^0 + 2^1 + 2^2 + 2^5$. Así que el primer $2^{\delta_i} = 0$ es $2^3 = 2^{\delta_0}$ y $x = 0$, $m = 3$. En efecto, en base 2 $39 = 100111$.

1.3 LEMA. El orden de u módulo 2^{n+1} es 2^{n+1-m}, con $n \geq m$.

Demostración. A lo largo de este argumento, v es una variable entera arbitraria. Por la proposición 1.1, sabemos que $u = 2^m - 1 + v2^{m+1}$.
Elevando al cuadrado tenemos $u^2 = (2^m - 1 + v2^{m+1})^2 = [(2^m - 1 + v2^{m+1})]^2 = 2^{2m} - 2^{m+1} + 1 + 2[(2^m - 1)(v2^{m+1})] + v^2 2^{2m+2} = 1 - 2^{m+1} + 2^{2m} + v2^{2m+2} - v2^{m+2} + v^2 2^{2m+2} = 1 - 2^{m+1} + v'2^{m+2}$, (1.1)

con v' calculada como sigue:
$v'2^{m+2} = 2^{2m} + v2^{2m+2} - v2^{m+2} + v^2 2^{2m+2}$; $v' = 2^{2m}(2v+1)^2 - v2^{m+2}/2^{m+2} = (2^m(2v+1)^2/2^{m+2}) - v = (2^m(2v+1)^2/2^2) - v = 2^{m-2}(2v+1)^2 - v$.
Si $m = 2$, $v' = (2v+1)^2 - v$. Si $m = 3 + x$, $v' = 2^{x+1}(2v+1)^2 - v$.

En seguida probaremos, por inducción, que $u^{2^r} = 1 - 2^{m+r} + v2^{m+r+1}$ con $r \geq 1$. (1.2)

Demostración: (inducción sobre r).

i) para $r = 1$, $u^2 = 1 - 2^{m+1} + v2^{m+2}$, ver (1.1).

ii) Supongamos que (1.2) es válido para $r - 1$, entonces $u^{2^{r-1}} = 1 - 2^{m+r-1} + v2^{m+r}$.

iii) Demostraremos que para r se cumple (1.2).

$u^{2^r} = u^{2^{r-1}}u^{2^{r-1}} = (1-2^{m+r-1}+v2^{m+r})^2 = 1-2^{m+r-1}+v2^{m+r}-2^{m+r-1}+$
$(2^{m+r-1})^2-v2^{m+r}2^{m+r-1}+v2^{m+r}-v2^{m+r}2^{m+r-1}+v^2 2^{2m+2r}$
$= 1-2^{m+r}+v2^{m+r+1}-v2^{2m+2r}+v^2 2^{2m+2r}+2^{2m+2r-2} = 1-2^{m+r}+v'2^{m+r+1}$,
con v' calculado como sigue: $v'2^{m+r+1} = v2^{m+r+1}+(v-1/2)^2(2^{2m+2r})$;
$v' = v+[(v-1/2)^2(2^{m+r})]/2 = v+(v-1/2)^2(2^{m+r-1})$.
Si $m=2$, $v' = v+(v-1/2)^2(2^{r+1})$. Si $m=3+x$, $v' = v+(v-1/2)^2(2^{r+x+2})$.
Como $u^{2^r} = 1-2^{m+r}+v'2^{m+r+1} = 1+(2v'-1)(2^{m+r})$, entonces
$u^{2^r} \equiv 1 \pmod{2^{m+r}}$, con $r \geq 1$. Si $n+1-m = r$ i.e $n+1 = r+m$, entonces
$u^{2^{n+1-m}} \equiv 1 \pmod{2^{n+1}}$, $n \geq m$.
Precisamos que el caso $r=1$ requiere de la observación que $m \geq 2$. ///

1.4 OBSERVACION. Podemos ver este resultado de un modo distinto. Sea $u = 1+c2^k$, c impar, $k \geq 2$. Entonces el Lema I-1.1 nos dice que el orden de u módulo 2^{n+k} es 2^n. El Lema 1.3 implica que, aunque tengamos que excluir $p=2$, $k=1$ de nuestra consideración, podemos considerar $u = -1+c2^k$, c impar, $k \geq 2$, cuando $p=2$ y concluir que el orden de u módulo 2^{n+k} es 2^n.

EJEMPLOS.

i) Sea $u = 13 = 1+c2^k$ $c=3$, $k=2$. En base 2: $13 = 2^0 2^2 2^3 = 1101$ y $m=1$. Por el Lema 1.3 tenemos que $u^{2^{n+1-m}} \equiv 1 \pmod{2^{n+1}}$, i.e $13^2 \equiv 1 \pmod{16}$.

ii) Sea $u = 7 = -1+c2^k$ $c=1$, $k=3$, $n=1$.

Por el Lema I-1.1

$u^{2^n} \equiv 1 \pmod{2^{n+k}}$ y
$7^2 \equiv 1 \pmod{16}$.

III- APLICACIONES

En este capítulo, presentaremos una construcción más general de los grupos que estudiamos en el Capítulo I, a partir de la cual, además de los teoremas que ya demostramos, obtendremos unos resultados muy importantes. Tambien mencionaremos la construcción de espacios nilpotentes X_i que pertenecen a un mismo género y que no son homotópicamente equivalentes dos a dos.

III.1 CONSTRUCCION GENERAL

Mientras que en el primer capítulo al grupo nilpotente finitamente generado N lo definíamos mediante la siguiente presentación:

$$N = \langle x,y;\ x^{p^{n+k}} = 1\ ,\ yxy^{-1} = x^{u} \rangle$$

y, a partir de él, construíamos su género G(N), procederemos ahora de un modo distinto.

Sea C un grupo cíclico infinito generado por ξ y sea A_0 un C-módulo, cuya estructura fundamental de grupo abeliano es Z/n, con C actuando por $\xi.a = ua$, $a \in A_0$, donde u es un entero positivo primo de n y t el orden de u módulo n. Sea A_1 un C-módulo con la misma estructura fundamental de grupo abeliano que A_0, pero con C actuando por $\xi.a = u^m a$, $a \in A_1$, donde m es un entero positivo primo de t tal que m no es congruente con ± 1 módulo t. Tomando los productos semidirectos $A_0 \rtimes C = N_0$, $A_1 \rtimes C = N_1$, podemos expresar N_0 y N_1 en términos de generadores y de relaciones de la manera siguiente:

$$N_0 = \langle x,y;\ x^{n} = 1, yxy^{-1} = x^{u} \rangle,$$

$$N_1 = \langle x,y;\ x^{n} = 1, yxy^{-1} = x^{u^m} \rangle.$$

A partir de esta construcción se demuestran los teoremas que ya vimos en el Capítulo I y se define el género completo de N_i. Además, se obtiene la siguiente propiedad.

1.1 TEOREMA. $C \times N_0 \cong C \times N_1$

Demostración. Supongamos que N es un G-grupo y sea $G{\times}H$ que actúa sobre N por la proyección $G{\times}H \twoheadrightarrow G$. Entonces $N \ltimes (G{\times}H) \cong (N \ltimes G) \times H$. (1.1)
El isomorfismo Φ es tal que $\Phi(x, (g,h)) = ((x,g),h)$, $x \in N$, $g \in G$, $h \in H$.
Sea $C{\times}C = \langle \xi, \eta \rangle$ que actúa en A_0 y A_1 por la proyección sobre el primer factor como en (1.1).

Sea $M = \begin{vmatrix} m & t \\ r & s \end{vmatrix}$ una matriz unimodular, es decir una matriz que satisface $|M| = \pm 1$. Esta matriz existe porque m y t son mutuamente primos. Consideremos la función $\Psi : C{\times}C \longrightarrow C{\times}C$ dada por

$$\xi \longmapsto \xi^m \eta^r,$$
$$\eta \longmapsto \xi^t \eta^s.$$

Entonces Ψ es un automorfismo.

Consideremos el siguiente diagrama:

$$\begin{array}{ccccc}
A_1 & \rightarrowtail & N_1 \times C & \twoheadrightarrow & C{\times}C = \langle \xi, \eta \rangle \\
\downarrow & & \downarrow & & \downarrow\cong \\
A_0 & \rightarrowtail & N_0 \times C & \twoheadrightarrow & C{\times}C = \langle \xi, \eta \rangle
\end{array}$$

En A_1, $\xi.a = u^m a$ mientras en A_0, $\xi^m \eta^r.a = \xi^m.a = u^m a$. Igualmente en A_1, $\eta.a = a$ mientras en A_0, $\xi^t \eta^s.a = \xi^t.a = u^t a = a$. Entonces Ψ es compatible con la función $1: A_1 \longrightarrow A_0$ y Ψ: $C{\times}C \cong C{\times}C$ con $1: A_1 \longrightarrow A_0$, determinan juntas un isomorfismo de $A_1 \ltimes (C{\times}C) \cong A_0 \ltimes (C{\times}C)$. Por (1.1), $A_i \ltimes (C{\times}C) \cong (A_i \ltimes C){\times}C = N_i{\times}C$, $i=0, 1$. Entonces $N_0 \times C \cong N_1 \times C$. ///

En el Capítulo I demostramos que $N_i^s \cong N_j^s$ para todo i, j, donde $s = p^{n-1}(p-1)/2$ es el orden de G(N), y N^s es el producto directo de s copias de N. A continuación, vamos a calcular de una manera más precisa el exponente k para el cual $N_i^k \cong N_j^k$ para todo i, j.
Regresando a la construcción general podemos escribir:
$n = p_1^{m_1} p_2^{m_2} \ldots p_\lambda^{m_\lambda}$, $m_i \geq 1$
$u = 1 + c p_1^{k_1} p_2^{k_2} \ldots p_\lambda^{k_\lambda}$ donde p_i no divide a c, $k_i \geq 1$, $i = 1, 2, \ldots \lambda$.

Supongamos que $m_i \geq k_i$. (a pesar de representar una pequeña pérdida de generalidad, esta suposición no tiene ninguna consecuencia esencial).
Asumimos también que el orden de $p_1, p_2, \ldots, p_\lambda$ es creciente.
Sea $m_i = n_i + k_i$, $i = 1, 2, \ldots \lambda$. Luego, nuestras restricciones son: $n_i \geq 0$, $k_i \geq 1$, $i = 1, 2, \ldots, \lambda$ donde $n_i = m_i - k_i$.
Con esta nueva notación:

a) El orden de u módulo n es $p_1^{n_1} p_2^{n_2} \ldots p_\lambda^{n_\lambda}$ excluyendo $p_1 = 2$, $n_1 \geq 1$, $k_1 = 1$.

b) Si $p_1 = 2$, $n_1 \geq 1$, $k_1 = 1$, escribimos $u = -1 + 2^k c'$ con c' impar y el orden de u módulo 2^{m_1} es $2^{m_1 - k}$. Entonces el orden de u módulo n es $p_1^{n_1 - k} p_2^{n_2} \ldots p_\lambda^{n_\lambda}$.

Sin embargo, a partir de este momento, excluiremos el caso excepcional. Así tendremos las siguientes notaciones:

$$t = p_1^{n_1} p_2^{n_2} \ldots p_\lambda^{n_\lambda}, \qquad p_1 < p_2 < \ldots < p_\lambda,$$
$$d = \operatorname{mcd}(n, u-1) = p_1^{k_1} p_2^{k_2} \ldots p_\lambda^{k_\lambda},$$
$$e = td = n.$$

Sea $T = \{p_1, p_2, \ldots, p_\lambda\}$ y $\Theta : T\text{-Aut}\, N \longrightarrow (Z/e)^*/\{\pm 1\}$. Entonces la imagen de Θ consiste de las unidades módulo ± 1 que son congruentes con 1 módulo t. Claramente hay d de esas unidades. Además el cokernel de Θ, es decir $G(N)$, tiene la estructura de grupo de $(Z/t)^*/\{\pm 1\}$. Por lo que el género completo de N es el grupo abeliano (aditivo) que consiste de todos los grupos del tipo $N(m) = \langle x, y ;\ x^n = 1,\ yxy^{-1} = x^{u^m} \rangle$ con m no congruente con $\pm t$.
Como esos $\frac{1}{2}\Phi(t)$ grupos, donde Φ es la función de Euler, tienen todas las propiedades estudiadas en el Capitulo I, podemos tomar $k = \frac{1}{2}\Phi(t)$ en $N_i^k \cong N_j^k$, lo que es equivalente al valor de s en la construcción particular del primer capitulo. Sin embargo, podemos llegar a más precisión en el cálculo de k.
Para ello, estudiaremos la estructura de grupo de $(Z/t)^*/\{\pm 1\}$.
Supongamos t impar y $n_i \geq 1$ (si $n_i = 0$, $p_i = 1$).Podemos escribir $(Z/t)^*/\{\pm 1\}$ como el producto directo de grupos cíclicos de orden $\Phi(p_i^{n_i}) = p_i^{n_i - 1}(p_i - 1)$ (Φ es la función de Euler), y nos queda por localizar el elemento -1 en este producto directo, para t impar, $t = 2t'$, $t = 2^n t'$.

1.2 PROPOSICION. Sea t impar y sea a_i el generador del factor cíclico de orden $\Phi(p_i^{n_i})$ en $(Z/t)^*$, donde t es impar y sea $b_i = a_i^{*\Phi(p_i^{n_i})}$.

Entonces $\prod_{i=1}^{\lambda} b_i = -1$.

Demostración. $(Z/t)^* = \Phi(p_i^{n_i}) = 2[\Phi(p_i^{n_i})/2]$. Entonces

$(Z/t)^* = \prod_{i=1}^{\lambda} Z/2 \times \prod_{i=1}^{\lambda} Z/*\Phi(p_i^{n_i})$, donde $Z/2$ es generado por $a_i^{*\Phi(p_i^{n_i})} = b_i$

y $Z/*\Phi(p_i^{n_i})$ es generado por a_i^2. Como $Z/2$ es generado por ± 1, entonces

$\prod_{i=1} b_i = -1$. ///

1.3 PROPOSICION. Sea $t = 2t'$ con t' impar. Entonces $(Z/t)^* \cong (Z/t')^*$.

Demostración. Sabemos que si $p>1$ entonces $\Phi(p) = p \prod_{q|p} (1-1/q)$, donde $\prod_{q|p}$ es el producto del conjunto de todos los primos que dividen a p.

Entonces $\Phi(t') = t' \prod_{q|t'} (1-1/q)$, $\Phi(2t') = 2t'(1-*) \prod_{q|t'} (1-1/q) = t' \prod_{q|t'} (1-1/q)$.

Por lo tanto $\Phi(t') = \Phi(2t') = \Phi(t)$ y $(Z/t)^* \cong (Z/t')^*$. ///

1.4 PROPOSICION. Sea $t = 2^n t'$ con t' impar y $n \geq 2$. Entonces $(Z/t)^* \cong Z/2 \times Z/2^{n-2} \times (Z/t')^*$.

Demostración. Sabemos que si $(m,n) = 1$, entonces $\Phi(mn) = \Phi(m)\Phi(n)$. De donde $\Phi(2^n t') = \Phi(2^n)\Phi(t')$. Pero $\Phi(2^n) = 2^{n-1} = 2.2^{n-2}$. Entonces $(Z/t)^* \cong Z/2 \times Z/2^{n-2} \times (Z/t')^*$. ///

En este caso, escogemos a -1 como el generador de $Z/2$.

Utilizando los tres resultados anteriores, encontramos la siguiente estructura del grupo $(Z/t)/\{\pm 1\})^*$ para toda $t \geq 3$.

1.5 TEOREMA. Sea $t = p_1^{n_1} p_2^{n_2} \ldots p_\lambda^{n_\lambda}$ donde cada p_i es impar y $n_i \geq 1$. Sea p_j tal que el 2-factor de $(p_j - 1)$ es minimal entre los enteros $(p_1 - 1) \ldots (p_\lambda - 1)$.
Entonces

$$\text{i)} \quad (Z/t)/\{\pm 1\})^* \cong \prod_{i=1}^{\lambda} Z/k_i \quad \text{donde } k_i = \begin{cases} \Phi(p_i^{n_i}) & i \neq j \\ \varkappa\Phi(p_j^{n_j}) & i = j \end{cases}$$

$$\text{ii)} \quad (Z/2t)^*/\{\pm 1\} \cong (Z/t)^*/\{\pm 1\}$$

$$\text{iii)} \quad \text{Si } n \geq 2 \quad (Z/2^n t)^*/\{\pm 1\} \cong Z/2^{n-2} \times (Z/t)^*$$

Demostración. Por los resultados de las proposiciones 1.3 y 1.4 es suficiente demostrar i).
Sea $\Phi(p_i^{n_i}) = 2^{q_i} d_i$ con d_i impar. En efecto $\Phi(p_i^{n_i}) = p_i^{n_i - 1}(p_i - 1)$ con p_i impar es siempre par.

Entonces $(Z/t)^* = \prod_{i=1}^{\lambda} Z/2^{q_i} \times \prod_{i=1}^{\lambda} Z/d_i$ donde $Z/2^{q_i}$ es generado por $a_i^{d_i} = a_{1i}$

y Z/d_i es generado por $a_i^{2^{q_i}} = a_{2i}$. (1.2)

Sea $b_i = a_{1i}^{2^{q_i - 1}}$. Por la Proposición 1.2, $\prod^{\lambda} a_{1i}^{2^{q_i - 1}} = -1$.
Ahora j es tal que $q_j \leq q_i$ para toda i. Consideremos el elemento

$$a'_{1j} = \prod_{i=1}^{\lambda} a_{1i}^{2^{q_i - q_j}}$$

Luego el orden de a'_{1j} es 2^{q_j} y podemos reemplazar el factor $Z/2^{q_j}$ en (1.2) por un factor isomorfo generado por a'_{1j}, sin afectar la estructura de $(Z/t)^*$.

Así tenemos $-1 = a'_{1j}{}^{2^{q_j - 1}}$. Entonces si reducimos el orden de a'_{1j} a $2^{q_j - 1}$ factorizamos -1, y $k_j = \varkappa\Phi(p_j^{n_j})$, si $i = j$. ///

Utilizando éstos cálculos, podemos encontrar una mejor evaluación para k en $N_i^k \cong N_j^k$. Para ello es suficiente tomar k como el exponente del grupo G(N).

1.6 DEFINICION. Para simplificar la notación en la expresión del exponente de G(N), vamos a definir una función M(t) como sigue: sea t impar, t≥3, (unicamente necesitamos t=5 o t=7 para eliminar los casos triviales); $t = p_1^{n_1} p_2^{n_2} \ldots p_\lambda^{n_\lambda}$, con p_i impar y $n_i \geq 1$. Entonces

$$M(t) = \begin{cases} \varkappa\Phi(p_1^{n_1}) & \text{si } \lambda = 1 \\ Lt_0 & \text{si } \lambda > 1 \end{cases}$$

donde $L = \text{mcm}(p_i - 1)$ y $t_0 = t/(p_1 p_2 \ldots p_\lambda)$.

1.7 TEOREMA. Sea t como lo definimos en esta sección. Entonces

i) Si t es impar, $\exp G(N) = M(t)$,

ii) Si $p_1 = 2$, $n_1 = 1$, $\lambda > 1$, $\exp G(N) = M(\varkappa t)$,

iii) Si $p_1 = 2$, $n_1 \geq 2$, $\lambda = 1$, $\exp G(N) = 2^{n_1 - 2}$,

iv) Si $p_1 = 2$, $n_1 \geq 2$, $\lambda = 2$, $\exp G(N) = \text{mcm}(2^{n_1 - 2}, \Phi p_2^{n_2})$,

v) Si $p_1 = 2$, $n_1 \geq 2$, $\lambda > 2$, $\exp G(N) = \text{mcm}(2^{n_1 - 2}, M(t/2^{n_1}))$.

1.8 EJEMPLOS.

i) Si t es impar entonces $k = M(t)$.

a) $\lambda = 1$, $t = p_1^{n_1} = 5^2 = 25$.

Primera estimación: $k = \varkappa\Phi(t) = 5.4/2 = \underline{10}$.

Nueva estimación: $k = M(t) = \varkappa\Phi(t) = \underline{10}$.

b) $\lambda > 1$, $t = p_1^{n_1} p_2^{n_2} \ldots p_\lambda^{n_\lambda}$. Sea $t = 3^2.5.7 = 315$

Primera estimación: $k = \varkappa\Phi(t) = (3.2)(4)(6)/2 = \underline{72}$.

Nueva estimación: $k = M(t) = Lt_0$, $L = mcm(2,4,6,) = 12$,
$t_0 = 3^2.5.7/3.5.7 = 3$, $k = \underline{36}$.

ii) $p_1 = 2$, $n_1 = 1$, $\lambda > 1$. Sea $t = 2.3^3.5^2 = 1350$.
Primera estimación: $k = \varkappa\Phi(t) = (32.2)(5.4) = \underline{180}$.
Nueva estimación: $k = M(\varkappa t) = M(3^3.5^2)$, $L = mcm\ (2,4) = 4$,
$t_0 = 3^3.5^2/3.5 = 45$, $k = \underline{180}$.

iii) $p_1 = 2$, $n_1 \geq 2$, $\lambda = 1$. Sea $t = 2^5 = 32$.
Primera estimación: $k = \varkappa\Phi(t) = 2^4/2 = 2^3 = \underline{8}$.
Nueva estimación: $k = 2^{5-2} = 2^3 = \underline{8}$.

iv) $p_1 = 2$, $n_1 \geq 2$, $\lambda = 2$. Sea $t = 2^3.5^2 = 200$.
Primera estimación : $k = \varkappa\Phi(t) = \varkappa(2^2.5.4) = \underline{40}$.
Nueva estimación: $k = mcm(2,20) = \underline{20}$.

v) $p_1 = 2$, $n_1 \geq 2$, $\lambda > 2$. Sea $t = 2^4.3.5 = 240$.
Primera estimación: $k = \varkappa\Phi(t) = \varkappa(2^3.2.4) = \underline{32}$.
Nueva estimación: $k = mcm\ (2^{n_1-2}, M(t/2^{n_1}))$.
$M(t/2^{n_1}) = Lt_0$, $L = mcm(2,4) = 4$, $t_0 = 3.5/3.5$, $k = \underline{4}$

III.2 APLICACION EN ESPACIOS NILPOTENTES.

Mencionaremos, sin demostrarlo, que se pueden construir los módulos A_i como grupos homotópicos de poliedros nilpotentes $X_0, X_1, \ldots, X_{s-1}$ y aplicaciones de cubiertas de ℓ-hojas regulares $f_0, f_1, \ldots f_{s-1}$.

$$X_0 \xrightarrow{f_0} X_1 \xrightarrow{f_1} \ldots \longrightarrow X_{s-1} \xrightarrow{f_{s-1}} X_0 \qquad (2.1)$$

tal que:

i) $\Pi_1 X_i = C = \langle \xi \rangle$.

ii) $\Pi_2 X_i = Z/p^{n+k}$.

iii) $\Pi_1 X_i$ actua sobre $\Pi_2 X_i$ por $\xi.a = u^{m^i} a$; $0 \leq i \leq s-1$.

iv) f_i induce una inyección f_{*i} de $\Pi_1 X_i$ en $\Pi_1 X_{i+1}$.

v) Todos los X_i están en el mismo género.

vi) $X_0, X_1, \ldots X_{s-1}$ no son homotópicamente equivalentes dos a dos.

Empezaremos dando algunas definiciones que nos serán necesarias para el desarrollo de esta sección.

Una pareja (X,A) de espacios topológicos está constituida por un espacio topológico X y un subespacio A (que puede ser vacío). Una función entre parejas $f: (X,A) \longrightarrow (Y,B)$ es una función continua si $f: X \longrightarrow Y$ es tal que $f(A)$ es un subconjunto de B. Si (X,A) es una pareja, entonces $(X,A) \times I$ es la pareja $(X \times I, A \times I)$.

2.1 DEFINICION. Sean $f_0, f_1: (X,A) \longrightarrow (Y,B)$ dos funciones continuas. Una *homotopía* de f_0 a f_1 es una función continua $h: (X,A)\times I \longrightarrow (Y,B)$ tal que $h(x,0) = f_0(x)$ y $h(x,1) = f_1(x)$. h se denota por $f_0 \overset{h}{\simeq} f_1$. La relación $\overset{h}{\simeq}$ es de equivalencia y $[f]$ es la clase de homotopía de f.

2.2 DEFINICION. Sea $x \in X$, un espacio topológico arbitrario. El grupoide fundamental de X en x es la colección de clases de homotopía, con los extremos fijos, de las trayectorias de x, junto con la multiplicación $*$. Se denota por $G(X) = \{[f], *\}$. Sea $\Pi_1(X,x) = \{[f] \in G(X) \mid f(0) = f(1) = x\}$. Π_1 es el *grupo fundamental de X en x*.

2.3 DEFINICION. Sea $C\mathcal{G}^*$ la categoría de espacios compactos de Hausdorff junto con sus funciones continuas y punto básico y $\mathcal{G}$ la categoría de Grupos junto con sus homomorfismos. Entonces Π_n es *un functor de dos variables de* $C\mathcal{G}^*$ *a* $\mathcal{G}$ para $n \geq 1$.

2.4 DEFINICION. Un *poliedro* es un espacio homeomorfo a la unión de una colección finita de simplejos en R^m para alguna m, tal que la intersección de dos simplejos es una cara de cada uno y cada cara es un simplejo. Un simplejo Δ^n de dimensión n se define como sigue:
$\Delta^n = \{(x_1,\dots, x_{n+1}) \in R^{n+1} \mid 0 \leq x_i \leq 1,\ \Sigma x_i = 1\}$.

2.5 DEFINICION. Un poliedro conexo es *nilpotente* si su grupo fundamental $\Pi_1 X$ es nilpotente y actúa nilpotentemente sobre los grupos de homotopía $\Pi_n X$, $n \geq 2$, que son abelianos.

2.6 PROPOSICION. Sea $Z \xrightarrow{\mu} Z \xrightarrow{\xi} Z/r$ una presentación proyectiva donde μ es la multiplicación por r. Tenemos la siguiente sucesión exacta:

$$\begin{array}{ccccccc} \mathrm{Hom}(Z/r,Z) & \rightarrowtail & \mathrm{Hom}(Z,Z) & \xrightarrow{\mu^*} & \mathrm{Hom}(Z,Z) & \twoheadrightarrow & \mathrm{Ext}(Z/r,Z) \\ \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\ 0 & \rightarrowtail & Z & \xrightarrow{\mu} & Z & & \end{array}$$

Como μ^* es también la multiplicación por r, tenemos
$$\mathrm{Ext}(Z/r,Z) = \mathrm{coker}\,\mu^* \cong Z/r.$$

2.7 DEFINICION. Un *espacio de Eilenberg-Mac Lane* es un espacio con un solo grupo de homotopía Π de dimensión n, denotado por $K(\Pi,n)$.

2.8 DEFINICION. Un *grupo topológico* G es un conjunto G con una estructura de grupo y una topología sobre G tal que $(s,t) \longmapsto st^{-1}$ es una función continua de $G \times G \longrightarrow G$.

2.9 DEFINICION. Para un grupo topológico G, un G-*espacio* es un espacio X con una función de $X \times G \longrightarrow X$, tal que para todo $x \in X$, $s,t \in G$ entonces $x(st) = (xs)t$ y para todo $x \in X$, $x.1 = x$, donde 1 es la identidad en G.

2.10 DEFINICION. Un G-espacio X es llamado *efectivo* si $xs = x$ implica $s = 1$, $x \in X$, $s \in G$.

2.11 DEFINICION. Sea X^* el subespacio de todos los $(x,xs) \in X \times X$, con $x \in X$, $s \in G$ de un G-espacio efectivo X. La función $\tau : X^* \longrightarrow G$ tal que $x\tau(x,x') = x'$, para todo $(x,x') \in X^*$, se llama *de translación*.

2.12 DEFINICION. Un G-espacio X se llama *principal* si X es un G-espacio efectivo con una función de translación continua $\tau: X^* \longrightarrow G$.

2.13 DEFINICION. Un G-*haz principal* es un G-haz (X,p,B) donde X es un G-espacio principal.

2.14 DEFINICION. Un *haz circular principal* es un G-haz principal donde $G = S^1$.

Habiendo establecido las definiciones y los resultados anteriores, procederemos a la construcción de los módulos A_i.
Sea M un poliedro conexo con $\Pi_1 M$ cíclico de orden k_0. Entonces $H^2(M;Z)$ contiene el sumando $\mathrm{Ext}(Z/k_0, Z) = Z/k_0$. Sea g un generador de este grupo. Podemos representar a g por una función, que llamaremos también g, de M a K(Z,2), el espacio de Eilenberg-Mac Lane de dimensión 2. Utilizamos a g para inducir un haz circular principal X *sobre* M. Entonces, tenemos la sucesión siguiente:

$$S^1 \longrightarrow X \xrightarrow{h} M \xrightarrow{g} K(Z,2). \qquad (2.2)$$

Luego (2.2) induce en homología de dimensión 1, la sucesión exacta corta

$$Z \rightarrowtail H_1 X \twoheadrightarrow Z/k_0 . \qquad (2.3)$$

Esta extensión representa el elemento $g \in \mathrm{Ext}(Z/k_0, Z)$. Si aplicamos Π_1 a

(2.2) utilizando la notación multiplicativa (y, por ende, C, C_{k_0}) para el grupo fundamental solamente donde es conmutativo, obtenemos la extensión central

$$C \rightarrowtail \Pi_1 X \twoheadrightarrow C_{k_0} \qquad (2.4)$$

donde C es un subgrupo de $Z(\Pi_1 X)$ el centro de $\Pi_1 X$.
Entonces Π_1 debe ser abeliano, así que (2.3) y (2.4) coinciden efectivamente.
Más aun, como g genera $Ext(Z/k_0, Z)$, sabemos que $H_1 X = Z$, de donde $\Pi_1 X = C$.
Sea ℓ primo con k_0. Podemos considerar a ℓ como una función de $K(Z,2) \longrightarrow K(Z,2)$ y entonces obtenemos el siguiente diagrama

$$\begin{array}{ccccccc}
S^1 & \longrightarrow & X & \xrightarrow{h} & M & \xrightarrow{g} & K(Z,2) \\
\downarrow \ell & & \downarrow f & & \downarrow = & & \downarrow \ell \\
S^1 & \longrightarrow & X_1 & \xrightarrow{h_1} & M & \xrightarrow{\ell g} & K(Z,2).
\end{array} \qquad (2.5)$$

Este diagrama tiene las propiedades siguientes:

i) $f\colon X \longrightarrow X_1$ es homotópicamente una aplicación de cubiertas regulares y $f_* \Pi_1 X$ es normal en $\Pi_1 X_1$ con cociente C_ℓ.

ii) Si M es nilpotente también lo serán X, X_1 y X, X_1 están en el mismo género.

iii) Si $\Pi_1 M = C_{p^n}$ y $\Pi_2 M = Z/p^{n+k}$, (excluyendo el caso p=2, k=1) y si $\Pi_1 M = \langle\eta\rangle$ actúa sobre $\Pi_2 M$ por $\eta.a = ua$, donde $u = 1+cp^k$, p no divide a c, entonces en (2.5) X y X_1 tienen diferentes tipos de homotopía siempre que ℓ no es congruente con ± 1 módulo p^n.
Si escogemos ℓ como en el Capítulo I, para representar un generador de $(Z/p^n)^*/\{\pm 1\}$ entonces $f\colon X \longrightarrow X_1$ en (2.5) es precisamente la función

$f_0 : X_0 \longrightarrow X_1$ que vimos en (2.1); así obtenemos el ciclo completo de (2.1), utilizando repetidamente $\ell : K(Z,2) \longrightarrow K(Z,2)$ como en (2.5).
El diagrama general es el siguiente.

$$\begin{tikzcd}
S^1 \arrow[r] \arrow[d, "\ell"] & X_i \arrow[r, "h_i"] \arrow[d, "f_i"] & M \arrow[r, "\ell^i g"] \arrow[d, "="] & K(Z,2) \arrow[d, "\ell"] \\
S^1 \arrow[r] & X_{i+1} \arrow[r, "h_{i+1}"] & M \arrow[r, "\ell^{i+1} g"] & K(Z,2).
\end{tikzcd}$$

Entonces el C-módulo $\Pi_2 X_i$ es exactamente A_i y el producto semidirecto de Z/p^{n+k} y C por esta acción es precisamente el grupo N_i del primer capítulo.

BIBLIOGRAFIA.

BIRKHOFF, Garrett and MAC LANE, Saunders; A survey of Modern Algebra, Mac Millan, 4th edition, New York, 1977.

GRAY, Brayton; Homotopy Theory; an Introduction to Algebraic Topology, Academic Press, New York, 1975.

HERSTEIN, I.N; Topics in Algebra, John Wiley & Sons, 2nd Edition, New York, 1975.

HILTON, Peter; "On the Genus of Nilpotent Groups and Spaces". Israel Journal of Mathematics; mimeo.

HILTON, Peter; "Non-Cancellation Properties for Certain Finitely Presented Groups"; mimeo.

HILTON, Peter and MISLIN, Guido; "On the Genus of a Nilpotent Group with Finite Commutator Subgroups". Mathematische Zeitschrift, Vol. 146, 1976.

HILTON, Peter, MISLIN, Guido and ROITBERG, Joseph; "Localization of nilpotent Groups and Spaces", Amsterdam, North Holland, Mathematics Studies Vol. 15,1975.

HILTON, Peter and STAMMBACH, Urs; A course in Homological Algebra, Springer-Verlag, New York, 1971.

HUSEMOLLER, Dale; Fibre Bundles, Springer, New York, 1975.

LANG, Serge; Algebra, Addisson Wesley, 2nd. Edition, Menlo Park, 1984.

NIVEN, I. y ZUCKERMAN, H.S; Introducción a la Teoría de los Números, Limusa, Mexico D.F., 1976.

INDICE DE SIMBOLOS.

Además de los símbolos de uso general, hacemos uso de la siguiente notación:

N_p	localización de N en p, p es primo.
$\binom{p}{n}$	combinaciones de p en n.
$[N,N]$	subgrupo conmutador de N.
$K \rtimes Q$	producto semi directo de K por Q.
ZN	centro de N.
TZN	grupo de torsión de ZN.
FZN	centro libre de N.
$QN = N/FZN$.	
$QN_{ab} = (N/[N,N])/FZN$	
$(Z/p)^{*}$	grupo de las unidades de Z/p.
$\mathcal{N}_c$	categoría de grupos nilpotentes con nilpotencia $G \leq c$.
$\Phi(m)$	función de Euler.
$\overset{h}{\simeq}$	relación de homotopía.
$[f]$	clase de homotopía de f.
$G(X)$	grupoide fundamental de X en x.

$\Pi_1(X,x)$ grupo fundamental de X en x.

$C\mathcal{G}^*$ categoria de espacios topológicos de Hausdorff con punto básico y funciones continuas.

$\mathcal{G}$ categoria de los Grupos con sus homomorfismos.

Π_n functor de $C\mathcal{G}^*$ a $\mathcal{G}$.

Δ^n simplejo de dimensión n.

$K(\Pi,n)$ espacio de Eilenberg-Mac Lane de dimensión n.

S^1 círculo.