EL NORMALIZADOR DEL p-GRUPO DE SYLOW DEL GRUPO SIMETRICO S_{p^n}

POR HUMBERTO CARDENAS Y EMILIO LLUIS

1. Introducción

En [1] se demostró que el normalizador N_2 de un p-grupo de Sylow G_2 del grupo simétrico de permutaciones de p^2 objetos es la extensión inesencial (split extension) $(Z_{p-1})^2 * G_2$ de $(Z_{p-1})^2 = Z_{p-1} \times Z_{p-1}$ por G_2 en donde Z_{p-1} indica un grupo cíclico de orden $p - 1$. Para ello se construyó un homomorfismo $\phi: N_2 \longrightarrow (Z_{p-1})^2$ de tal forma que la sucesión

$$1 \longrightarrow G_2 \xrightarrow{\ \theta\ } N_2 \xrightarrow{\ \phi\ } (Z_{p-1})^2 \longrightarrow 1$$

resulta exacta y escindible (splits) (θ es la inclusión).

En esta nota se demostrará el mismo resultado para los p-grupos de Sylow del grupo de permutaciones de p^n objetos con n arbitraria (ver el teorema del párrafo 5). La demostración es por inducción.

2. Caso $n = 1$

Sea $E_1 = \{0, 1, \cdots, p - 1\}$ el campo de los enteros módulo p y Z_{p-1} el grupo multiplicativo de E_1. Sea S_1 el grupo de permutaciones de E_1 y $d \in S_1$ la permutación definida por

$$d(i) = i + 1 \qquad (i \in E_1)$$

(la operación de sumar es la del campo E_1). El grupo G_1 generado por d en S_1 es un p-grupo de Sylow de S_1.

Sea x un elemento del normalizador N_1 de G_1 en S_1. Tenemos $xdx^{-1} = d^q$ $(q \in Z_{p-1})$. Definimos entonces el homomorfismo $\phi_1: N_1 \longrightarrow Z_{p-1}$ con la fórmula $\phi_1(x) = q$. Si designamos con $\phi_1: G_1 \longrightarrow N_1$ al homomorfismo de inclusión tenemos la sucesión

$$1 \longrightarrow G_1 \xrightarrow{\ \theta_1\ } N_1 \xrightarrow{\ \phi_1\ } Z_{p-1},$$

que resulta exacta: Evidentemente $\phi_1\theta_1 = 1$ pues si $x \in G_1$, $xdx^{-1} = d$. Supongamos ahora que $x \in N_1$ es tal que $xdx^{-1} = d$. Entonces $xd^i = d^ix$, de donde

$$x(i) = xd^i(0) = d^ix(0) = x(0) + i = d^{x(0)}(i),$$

es decir, $x = d^{x(0)}$, o sea que $x \in G_1$, con lo cual queda probada la exactitud.

Definimos ahora un homomorfismo $\psi_1: Z_{p-1} \longrightarrow S_1$ como sigue: $\psi_1(q)(i) = qi$ $(q \in Z_{p-1},\ i \in E_1)$ (operación de multiplicar de E_1). Tenemos entonces

$$\psi_1(q)d(\psi_1(q))^{-1}(i) = \psi_1(q)d(i/q) = \psi_1(q)(i/q + 1) = i + q = d^q(i),$$

lo cual prueba, en primer lugar, que ψ_1 es un homomorfismo de Z_{p-1} en N_1 y, en segundo lugar, que

$$\phi_1 \psi_1 = 1,$$

es decir que la sucesión

$$1 \to G_1 \xrightarrow{\theta_1} N_1 \underset{\psi_1}{\overset{\phi_1}{\rightleftarrows}} Z_{p-1} \to 1$$

es exacta y escindida. Podemos escribir pues $N_1 = Z_{p-1} * G_1$.

3. Notaciones

Con $E_1 = \{0, 1, \cdots, p-1\}$ denotaremos como antes el campo de los enteros módulo p, y con $E_{n-1} = \{0, 1, \cdots, p^{n-1} - 1\}$, un conjunto de p^{n-1} elementos. Z_{p-1} será el grupo multiplicativo de E_1. Sea $E_n = E_{n-1} \times E_1$, producto cartesiano de los dos conjuntos.

El grupo simétrico S_n que consideraremos será el de las permutaciones de los p^n elementos de E_n. Con S_1 y S_{n-1} denotaremos los grupos de permutaciones de E_1 y E_{n-1} respectivamente. Sean $\bar{\alpha}$: $S_{n-1} \to S_n$ y $\bar{\beta}$: $S_1 \to S_n$ las inclusiones definidas como sigue:

$$\bar{\alpha}(x)(i, j) = (x(i), j), \qquad (i, j) \in E_n, x \in S_{n-1},$$

$$\bar{\beta}(x)(i, j) = (i, x(j)), \qquad (i, j) \in E_n, x \in S_1.$$

Para facilitar las notaciones escribiremos siempre $t = p^{n-1} - 1$.

Sea G_{n-1} un p-grupo de Sylow de S_{n-1}, y sean $h_0, h_1, \cdots, h_t$ los elementos de S_n definidos por

$$h_k(i, j) = (i, j), \qquad \text{para} \quad i \neq k,$$

$$h_k(k, j) = (k, j + 1).$$

Sea G_n el subgrupo de S_n generado por G_{n-1} (o sea por $\bar{\alpha}(G_{n-1})$) y por los elementos $h_0, h_1, \cdots, h_t$. Los elementos de G_n son de la forma

$$x = g h_0^{s_0} h_1^{s_1} \cdots h_t^{s_t}, \qquad (g \in G_{n-1}, 0 \leqslant s_i \leqslant p-1).$$

G_n es un p-grupo de Sylow de S_n pues su orden es $p^{(p^n-1)/(p-1)}$.

$H_0, H_1, \cdots, H_t$ denotan los subgroupos cíclicos generados por $h_0, h_1, \cdots, h_t$ respectivamente y $H = H_0 H_1 \cdots H_t$. Al elemento $h_0 h_1 \cdots h_t$ lo denotaremos por h.

4. Lemas auxiliares

LEMA 1. *Vale la siguiente regla de conmutatividad:*

$$h_k g = g h_{g^{-1}(k)}, \qquad (g \in G_{n-1}, 0 \leqslant k \leqslant t).$$

En efecto, sea $(i, j) \in E_n$. Entonces

$$h_k g(i,j) = h_k(g(i),j) = \begin{cases} (g(i),j) & \text{si } k \neq g(i) \\ (g(i),j+1) & \text{si } k = g(i) \end{cases}$$
$$= \begin{cases} g(i,j) \\ g(i,j+1) \end{cases} = \begin{cases} gh_{g^{-1}(k)}(i,j) \\ gh_i(i,j) \end{cases} = gh_{g^{-1}(k)}(i,j).$$

El siguiente resultado es inmediato:

LEMA 2. $h(i,j) = (i, j+1)$, $((i,j) \in E_n)$.

LEMA 3. *Si* $x \in G_r$ *entonces* $x^{p^{n-1}} = h^q$.

Sea $x = gh_0^{s_0} \cdots h_t^{s_t}$, y supongamos primero que $g \in G_{n-1}$ es de orden p^{n-1}. Entonces g es un ciclo y por lo tanto si $r \not\equiv s \pmod{p^{n-1}}$, $g^r(i) \neq g^s(i)$ para toda $i \in E_{n-1}$. Se tiene que

$$x^{p^{n-1}} = (h_{g^{-t-1}(0)})^{s_0} \cdots (h_{g^{-t-1}(t)})^{s_t} \cdots (h_{g^{-1}(0)})^{s_0} \cdots (h_{g^{-1}(t)})^{s_t} h_0^{s_0} \cdots h_t^{s_t},$$

y por lo arriba mencionado resulta

$$x^{p^{n-1}} = h_0^q h_1^q \cdots h_t^q = h^q, \qquad \text{con} \quad q = s_0 + \cdots + s_t\,.$$

Si g es ahora de orden $\leqslant p^{n-2}$, se tiene

$$x^{p^{n-1}} = (x^{p^{n-2}})^p = (g^{p^{n-2}} h_0^{s_0'} \cdots h_t^{s_t'})^p = 1 = h^0,$$

con lo cual queda probado el lema.

LEMA 4. *Si* x *está en el normalizador* N_n *de* G_n *en* S_n, *entonces* $xhx^{-1} = h^q$ *con* $1 \leqslant q \leqslant p-1$.

Sea $y = gh_0$ con $g \in G_{n-1}$ de orden p^{n-1}. Por el lema anterior, $y^{p^{n-1}} = h$. Sea $y' = xyx^{-1}$. Entonces $y' \in G_n$. Además $xy^{p^{n-1}}x^{-1} = xhx^{-1} = y'^{p^{n-1}} = h^q$ también por el mismo lema. Además $1 \leqslant q \leqslant p-1$ pues h es un elemento de orden p.

LEMA 5. *Sea* $x \in N_n$ *y sean*

$$x(i,0) = (y(i), v(i))$$
$$x(0,j) = (w(j), z(j)).$$

Entonces las transformaciones $y\colon E_{n-1} \to E_{n-1}$, $z\colon E_1 \to E_1$ *son elementos de* S_{n-1} *y* S_1 *respectivamente. Se tiene además la fórmula*

$$x(i,j) = (y(i), v(i) - v(0) + z(j)).$$

Del Lema 4 resulta $xh^j = h^{qj}x$, o sea que

$$xh^j(i,0) = h^{qj}(y(i), v(i)) = (y(i), v(i) + qj),$$

de donde

$$x(i,j) = (y(i), v(i) + qj).$$

De aquí obtenemos

$$x(0, j) = (y(0), v(0) + qj) = (w(j), z(j)),$$

o sea que $z(j) = v(0) + qj$, de lo cual resulta la fórmula del lema.

Ahora bien, como $q \in Z_{p-1}$, la relación $z(j) = v(0) + qj$ demuestra que $z: E_1 \to E_1$ es biyectiva, o sea, que $z \in S_1$. Por otro lado, si $y: E_{n-1} \to E_{n-1}$ no fuera biyectiva, lo acabado de demostrar, junto con la fórmula del lema implicarían que x no sería una aplicación biyectiva de E_n en E_n, lo cual contradice que $x \in S_n$. O sea que $y \in S_{n-1}$, con lo cual queda probado el lema.

Sean $\lambda: N_n \to S_{n-1}$ y $\mu: N_n \to S_1$ las aplicaciones definidas, según el lema anterior, por las fórmulas

$$\begin{aligned} x(i, 0) &= (\lambda x(i), v(i)) \\ x(0, j) &= (w(j), \mu x(j)) \end{aligned} \qquad (x \in N_n)$$

(o sea $y = \lambda x$, $z = \mu x$ del lema anterior).

Con esta notación, la fórmula del Lema 4 se escribe como sigue:

$$x(i, j) = (\lambda x(i), v(i) - v(0) + \mu x(j)).$$

Denotaremos con $\alpha: N_{n-1} \to N_n$, $\alpha': G_{n-1} \to G_n$, $\beta: N_1 \to N_n$, y $\beta': G_1 \to G_n$ las restricciones de las inclusiones $\bar{\alpha}: S_{n-1} \to S_n$ y $\bar{\beta}: S_1 \to S_n$ respectivamente.

LEMA 6. *λ es un homomorfismo de N_n sobre N_{n-1} y μ un homomorfismo de N_n sobre N_1. Además* $\lambda\alpha =$ ident., $\mu\beta =$ ident., $\mu\alpha = 1$, $\lambda\beta = 1$.

Sean $x, x' \in N_n$. $xx'(i, 0) = (\lambda(xx')(i), v''(i))$; $x(x'(i, 0)) = x(\lambda x'(i), v'(i)) = (\lambda x \lambda x'(i), v(v'(i)))$, de donde $\lambda(xx') = \lambda x \lambda x'$. Sea ahora $x \in N_{n-1}$. Tenemos entonces que $\alpha x(i, j) = (x(i), j)$ y, por otro lado, $\alpha x(i, j) = (\lambda\alpha x(i) v'''(i))$, de donde $\lambda\alpha x = x$, es decir $\lambda\alpha =$ ident. Así pues, en lo que a λ se refiere bastará únicamente probar que $\lambda(N_n) \subset N_{n-1}$. Sea pues $g \in G_{n-1}$ y $x \in N_n$. Se tiene entonces $\lambda x g(\lambda x)^{-1} = \lambda x(\lambda\alpha g)\lambda x^{-1} = \lambda(x(\alpha g)x^{-1}) \in \lambda(G_n)$. La demostración se reduce entonces a probar que $\lambda(G_n) \subset G_{n-1}$, pues entonces $\lambda x \in N_{n-1}$. Para lo último observemos que si $x \in G_n$ y se escribe $x = g h_0^{s_0} \cdots h_t^{s_t}$, con $g \in G_{n-1}$, entonces $x(i, 0) = (g(i), s_i)$, de donde $\lambda x = g$.

Las demostraciones para la μ son completamente análogas y las dos relaciones restantes se prueban fácilmente.

En la demostración se vió que $\lambda(G_n) \subset G_{n-1}$ y análogamente $\mu(G_n) \subset G_1$. Así pues, podemos denotar con $\lambda': G_n \to G_{n-1}$ y $\mu': G_n \to G_1$ las restricciones respectivas de λ y μ, y se tiene que $\lambda'\alpha' =$ ident. y $\mu'\beta' =$ ident.

LEMA 7. *Si $x \in N_n$, entonces $x' = (\alpha\lambda x)(\beta\mu x)$ está en la misma clase lateral que x de N_n módulo G_n.*

En efecto, tenemos que $x'(i, j) = (\lambda x(i), \mu x(j))$. De aquí, $xx'^{-1}(i, j) = x((\lambda x)^{-1}(i), (\mu x)^{-1}(j)) = (i, v(i) - v(0) + j) = h_i^{v(i)-v(0)}(i, j)$, de donde $xx'^{-1} \in H \subset G_n$. Q.E.D.

5. El normalizador

Consideremos el siguiente diagrama,

$$\begin{tikzcd}
1 \arrow[r] & G_{n-1} \arrow[r, "\theta_{n-1}"] \arrow[d, shift right, "\alpha'"'] & N_{n-1} \arrow[r, shift left, "\phi_{n-1}"] \arrow[d, shift right, "\alpha"'] & (Z_{p-1})^{n-1} \arrow[l, shift left, "\psi_{n-1}"] \arrow[r] \arrow[d, shift right, "\alpha''"'] & 1 \\
1 \arrow[r] & G_n \arrow[r, "\theta_n"] \arrow[u, shift right, "\lambda'"'] \arrow[d, shift left, "\mu'"] & N_n \arrow[r, shift left, "\phi_n"] \arrow[u, shift right, "\lambda"'] \arrow[d, shift left, "\mu"] & (Z_{p-1})^n \arrow[l, shift left, "\psi_n"] \arrow[r] \arrow[u, shift right, "\lambda''"'] \arrow[d, shift left, "\mu''"] & 1 \\
1 \arrow[r] & G_1 \arrow[r, "\theta_1"] \arrow[u, shift left, "\beta'"] & N_1 \arrow[r, shift left, "\phi_1"] \arrow[u, shift left, "\beta"] & Z_{p-1} \arrow[l, shift left, "\psi_1"] \arrow[r] \arrow[u, shift left, "\beta''"] & 1
\end{tikzcd}$$

en donde el primer y el tercer renglón son sucesiones exactas y escindibles mediante las ψ_{n-1} y ψ_1. Las θ_m son inclusiones y las ϕ_1 y ψ_1 se dan explícitamente en el párrafo 2.

Los homomorfismos λ, μ, α, y β y sus restricciones se definieron en el párrafo 4. α'' es la inclusión de $(Z_{p-1})^{n-1}$ en el producto de los primeros $n - 1$ factores de $(Z_{p-1})^n$, y β'', la inclusión de Z_{p-1} en el último factor de $(Z_{p-1})^n$. λ'' y μ'' son las proyecciones correspondientes.

Siendo $(Z_{p-1})^n$ el producto directo de $(Z_{p-1})^{n-1}$ y Z_{p-1} mediante λ'' y μ'', sea ϕ_n el (único) homomorfismo que existe tal que

$$\phi_{n-1}\lambda = \lambda''\phi_n, \qquad \phi_1\mu = \mu''\phi_n. \tag{1}$$

Analogamente, ya que $(Z_{p-1})^n$ es la suma directa de los mismos grupos mediante las inclusiones α'' y β'', sea ψ_n el (único) homomorfismo que existe tal que

$$\alpha\psi_{n-1} = \psi_n\alpha'', \qquad \beta\psi_1 = \psi_n\beta''. \tag{2}$$

TEOREMA. *La sucesión*

$$\begin{tikzcd}
1 \arrow[r] & G_n \arrow[r, "\theta_n"] & N_n \arrow[r, shift left, "\phi_n"] & (Z_{p-1})^n \arrow[l, shift left, "\psi_n"] \arrow[r] & 1
\end{tikzcd}$$

es exacta y escindida. Es decir, $N_n = (Z_{p-1})^n * G_n$.

θ_n es monomorfismo por construcción. Demostraremos ahora que $\phi_n\psi_n =$ ident. En efecto, usando las relaciones del Lema 6, las fórmulas (1) y (2), y las relaciones

$$\alpha''\lambda''\cdot\beta''\mu'' = \text{ident.}, \qquad \phi_{n-1}\psi_{n-1} = \text{ident.}, \qquad \phi_1\psi_1 = \text{ident.},$$

obtenemos

$$\begin{aligned}
\phi_n\psi_n &= \phi_n\psi_n\alpha''\lambda''\cdot\phi_n\psi_n\beta''\mu'' \\
&= (\alpha''\lambda''\cdot\beta''\mu'')(\phi_n\alpha\psi_{n-1}\lambda''\cdot\phi_n\beta\psi_1\mu'') \\
&= \alpha''\lambda''\phi_n\alpha\psi_{n-1}\lambda''\cdot\alpha''\lambda''\phi_n\beta\psi_1\mu''\cdot\beta''\mu''\phi_n\alpha\psi_{n-1}\lambda''\cdot\beta''\mu''\phi_n\beta\psi_1\mu'' \\
&= \alpha''\phi_{n-1}\lambda\alpha\psi_{n-1}\lambda''\cdot\alpha''\phi_{n-1}\lambda\beta\psi_1\mu''\cdot\beta''\phi_1\mu\alpha\psi_{n-1}\lambda''\cdot\beta''\phi_1\mu\beta\psi_1\mu'' \\
&= \alpha''\lambda''\cdot\beta''\mu'' = \text{ident.}
\end{aligned}$$

Queda únicamente por probar la exactitud en N_n. Sea $x \in G_n$. Tenemos que $\phi_n\theta_n(x) = 1$ si y sólo si $\phi_{n-1}\lambda\theta_n(x) = 1$ y $\phi_1\mu\theta_n(x) = 1$. Estas dos relaciones son válidas ya que

$$\phi_{n-1}\lambda\theta_n(x) = \phi_{n-1}\theta_{n-1}\lambda'(x) = 1,$$

$$\phi_1\mu\theta_n(x) = \phi_1\theta_1\mu'(x) = 1.$$

Finalmente, si $\phi_n(y) = 1$ y $y \in N_n$, se tiene

$$\lambda''\phi_n(y) = \phi_{n-1}\lambda(y) = 1,$$

$$\mu''\phi_n(y) = \phi_1\mu(y) = 1,$$

de donde existen $x' \in G_{n-1}$ y $x'' \in G_1$ tales que

$$\lambda(y) = \theta_{n-1}(x'), \qquad \mu(y) = \theta_1(x'').$$

Por consiguiente,

$$\theta_n(\alpha'(x')\cdot\beta'(x'')) = \theta_n\alpha'(x')\cdot\theta_n\beta'(x'') = \alpha\theta_{n-1}(x')\cdot\beta\theta_1(x'')$$
$$= \alpha\lambda(y)\cdot\beta\mu(y) \in \theta_n(G_n),$$

y por el Lema 7, $y \in \theta_n(G_n)$. Q.E.D.

Instituto de Matemáticas,
Universidad Nacional Autónoma de México

Referencias

[1] H. Cárdenas y E. Lluis. *El normalizador del p-grupo de Sylow del grupo simétrico* S_{p^2}, Anales del Instituto de Matemáticas, U.N.A.M., **2** (1962), 1–8.