Jose Antonio Lorencio Abril

4 Grupos

Clases laterales y teorema de Lagrange

Clases laterales

Sea G un grupo y H un subgrupo de G. Se define la siguiente relación binaria en G:

$$a \equiv_i b \mod H \iff a^{-1}b \in H$$

Esto es una relación de equivalencia:

- Reflexiva: $a^{-1}a \in H \implies a \equiv_i a \mod H$
- Simétrica: $a \equiv_i b \mod H \iff a^{-1}b \in H \implies \left(a^{-1}b\right)^{-1} = b^{-1}a \in H \iff b \equiv_i a \mod H$
- Transitiva: $\begin{cases} a \equiv_i b \mod H \iff a^{-1}b \in H \\ b \equiv_i c \mod H \iff b^{-1}c \in H \end{cases} \implies \left(a^{-1}b\right)\left(b^{-1}c\right) = a^{-1}c \in H \implies a \equiv_i c \mod H$

Y define una partición de G en clases de equivalencia. La clase de equivalencia que contiene a a se denomina **clase lateral de a módulo H por la izquierda** y es

$$aH = \{ah : h \in H\}$$

para ver esto:

'$\subset$' Sea $b \in aH$, entonces $a \equiv_i b \mod H$, entonces $b \equiv_i a \mod H$, lo que quiere decir que $b^{-1}a = h \in H$. O sea, que $b^{-1} = ha^{-1} \implies b = ah^{-1}$, con $h^{-1} \in H$, pues $h \in H$.

'$\supset$' Si $b \in \{ah : h \in H\}$, entonces $b = ag$, con $g \in H$. Y se tiene que $a^{-1}b = a^{-1}ag = g \in H$

Análogamente, se puede definir otra relación de equivalencia

$$a \equiv_d b \mod H \iff ab^{-1} \in H$$

Donde la clase de equivalencia que contiene a a se denomina **clase lateral de a módulo H por la derecha** y es

$$Ha = \{ha : h \in H\}$$

El conjunto de las clases laterales por la izquierda de G módulo H se denota G/H y el de las clases laterales por la derecha $H\backslash G$. Por el lema 4.2 se tiene que las aplicaciones

$$\begin{array}{ccc} H & \to & aH \\ h & \mapsto & ah \end{array} \qquad \begin{array}{ccc} H & \to & Ha \\ h & \mapsto & ha \end{array}$$

son biyectivas, con los que todas las clases laterales tienen el mismo cardinal. Además, la aplicacion

$$\begin{array}{ccc} G/H & \to & H\backslash G \\ aH & \mapsto & Ha^{-1} \end{array}$$

es otra biyección, con lo que también G/H y $H\backslash G$ tienen el mismo cardinal.

En el caso de los grupos el cardinal se denomina **orden de G.**

Para un subgrupo H de G, hemos visto que se verifica:

$$|aH| = |Ha| = |H| \quad y \quad |G/H| = |H\backslash G|$$

El cardinal de G/H y $H\backslash G$ se llama **índice de H en G** y se denota $[G : H]$.

Teorema de Lagrange (4.17)

Si G es un grupo finito y H es un subgrupo de G entonces $|G| = |H|\,|G : H|$.

Demostración

Si G tiene $|G|$ elementos, y G/H tiene $|G/H| = [G : H]$ clases de equivalencia, cada una con $|H|$ elementos, entonces, se tiene que

$$|H| = \frac{|G|}{[G : H]} \implies |G| = |H|\,[G : H]$$

Teorema de la Correspondencia para grupos

Sea N un subgrupo normal de un grupo G. La asignación $H \mapsto H/N$ establece una biyección entre el conjunto de los subgrupos de G que contienen a N y el conjunto de los subgrupos de G/N.

Además, esta biyección conserva las inclusiones y la normalidad. Es decir, dados dos subgrupos H y K de G que contienen a N, se tiene:

1. $H \subset K \iff (H/N) \subset (K/N)$
2. $H \trianglelefteq G \iff (H/N) \trianglelefteq (G/N)$

Demostración

- **Sobreyectividad**

  H/N subgrupo

  Como H subgrupo de G, entonces $1 \in H \implies 1N \in H/N$

  Dados $x, y \in H$, tenemos que $(xN)(yN) = (xy)N \in H/N$, pues $xy \in H$

  Dado $x \in H$, entonces $x^{-1} \in H \implies x^{-1}N \in H/N$. Y se tiene que
  $xNx^{-1}N = xx^{-1}N = 1 = x^{-1}xN = x^{-1}NxN$. Así, vemos que H/N es subgrupo de G/N.

Sea ahora *K subgrupo de G/N* y sea $J = \{a \in G / aN \in K\}$, y definimos

$$\begin{array}{ccccc} G & \xrightarrow{f} & G/N & \xrightarrow{g} & (G/N)/K \\ a & \mapsto & aN & & \\ & & b & \mapsto & bK \end{array}$$

Y sea $h = g \circ f$. Calculemos su núcleo:

$$a \in Ker h \iff f(a)K = g(f(a)) = 1NK \iff f(a) = aN \in K \iff a \in J$$

Es decir, $Ker h = J \overset{lema\ 4.14.7}{\Longrightarrow} J$ *subgrupo de* G.

Además, si $a \in N \implies aN = 1N \in K \implies a \in J$. Es decir, $N \subset J$.

¿$J/N = K$?

'$\subseteq$' $x \in J/N \implies x = aN,\ a \in J \implies x = aN \in K$ (por la definición de J)

'$\supseteq$' $x \in K \subset G/N \implies x = aN \in K,\ a \in G \implies a \in J \implies x = aN \in J/N$

Recapitulando: dado un subgrupo de G/N, podemos escribir este como J/N, donde $I \subset J$ *y este es subgrupo de* A, por lo que nuestra aplicación es suprayectiva.

- **Inyectividad**

  Sean J_1, J_2 subgrupos de A que contienen a N tales que $J_1/N \subseteq J_2/N$. Entonces

  $$x \in J_1 \implies xN \in J_1/N \subset J_2/N \implies xN = yN,\ y \in J_2 \implies$$
  $$\implies y^{-1}x \in N \subset J_2 \implies x = yy^{-1}x \in J_2 \implies J_1 \subseteq J_2$$

  Por tanto, si $J_1/N = J_2/N \implies \begin{cases} J_1/N \subseteq J_2/N \implies J_1 \subseteq J_2 \\ J_2/N \subseteq J_1/N \implies J_2 \subseteq J_1 \end{cases} \implies J_1 = J_2$

  Y la aplicación es inyectiva.

Es decir, que la aplicación del enunciado es biyectiva. Pero esto quiere demuestra también la igualdad de los dos conjuntos de subrupos.

Solo resta ver que conserva la normalidad.

' $\implies$ ' Supongamos que $H \trianglelefteq G$, sean $x \in H/N,\ y \in G/N$, entonces $x = hN,\ h \in H$ e $y = gN,\ g \in G$. Y se tiene que

$$y^{-1}xy = (gN)^{-1}(hN)(gN) = g^{-1}hgN$$

como H es normal en G, entonces $g^{-1}hg \in H$ y tenemos que $y^{-1}xy \in H/N$, por lo que H/N es normal en G/N.

' $\impliedby$ ' Supongamos que $H/N \trianglelefteq G/N$, sean $h \in H$ y $g \in G$, entonces $hN \in H/N$ y $gN \in G/N$, entonces

$$(gN)^{-1}(hN)(gN) = g^{-1}hgN \in H/N$$

esto quiere decir que $\exists k \in H / g^{-1}hgN = kN \iff g^{-1}hgk^{-1} \in N \subset H$. Entonces $g^{-1}hgk^{-1}k = g^{-1}hg \in H$, y H es normal en G.

Teoremas de Isomorfía para grupos

1. Si $f : G \to H$ es un homomorfismo de grupos entonces existe un único isomorfismo de grupos $\overline{f} : G/Kerf \to f$ que hace conmutativo el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/Kerf & \overset{\overline{f}}{\rightarrowtail} & Imf \end{array}$$

   es decir, $i \circ \overline{f} \circ p = f$, donde i es la inclusión y p es la proyección canónica. En particular

$$G/Kerf \simeq Imf$$

2. Sean N, H subgrupos normales de un grupo G con $N \subset H$. Entonces H/N es un subgrupo normal de G/N y se tiene

$$\frac{G/N}{H/N} \simeq G/H$$

3. Sean G un grupo, H un subgrupo de G y N un subgrupo normal de G. Entonces HN es un subgrupo de G que contiene a H, $H \cap N$ es un subgrupo normal de H y se tiene

$$\frac{H}{N \cap H} \simeq \frac{HN}{N}$$

Demostración

1. Veamos que, en caso de existir, debe ser único

   $i \circ \overline{f} \circ p = f \iff i \circ \overline{f} \circ p\,(x) = f\,(x)\,, \forall x \iff i\left(\overline{f}\,(p\,(x))\right) = f\,(x) \iff i\left(\overline{f}\,(xKerf)\right) = f\,(x) \iff \overline{f}\,(xKer$

   es decir, que la única forma que puede tener este isomorfismo es $\overline{f}\,(xKerf) = f\,(x)$. Veamos que, de hecho, es un isomorfismo:

   - **Bien definido:** sean $x, y \in G$ tales que $xKerf = yKerf$, veamos que tienen la misma imagen

     $$xKerf = yKerf \iff xy^{-1} \in Kerf \implies f\,(x)\,f\,(y)^{-1} = f\,(x)\,f\left(y^{-1}\right) = f\left(xy^{-1}\right) = 1 \implies$$

     $$\implies \overline{f}\,(xKerf) = f\,(x) = f\,(y) = \overline{f}\,(yKerf)$$

   - **Homomorfismo:** sean $xKerf, yKerf \in G/Kerf$, entonces

     $$\overline{f}\,(xyKerf) = f\,(xy) = f\,(x)\,f\,(y) = \overline{f}\,(x)\,\overline{f}\,(y)$$

   - **Sobreyectiva:** sea $y \in Imf$, entonces $\exists x \in G / f\,(x) = y \implies \overline{f}\,(xKerf) = f\,(x) = y$
   - **Inyectiva:** si $\overline{f}\,(xKerf) = \overline{f}\,(yKerf) \implies f\,(x) = f\,(y) \implies f\,(x)\,f\,(y)^{-1} = 1 \implies f\left(xy^{-1}\right) = 1 \implies xy^{-1} \in Kerf \implies xKerf = yKerf$

   Y tenemos el resultado.

2. Que H/N es un subgrupo normal de G/N es consecuencia inmediata del teorema de la correspondencia.

   Para ver el isomorfismo, consideramos

$$\begin{array}{ccc} f: G/N & \to & G/H \\ gN & \mapsto & gH \end{array}$$

   que es un homomorfismo:

$$f(xyN) = xyH = xHyH = f(xN)\, f(yN)$$

   Es sobreyectiva: sea $yH \in G/H$, entonces $y \in G$ y $yN \in G/N$, entonces $f(yN) = yH$.

   Por último, calculamos el núcleo

$$xN \in Kerf \iff xH = f(xN) = 1H = H \iff x \in H$$

   es decir, que el núcleo es $Kerf = H/N$. Entonces, por el 1er teorema de isomorfía, tenemos que

$$\frac{G/N}{H/N} \simeq G/H$$

3. Veamos que HN es un subgrupo de G.

   - Como $1 \in H,\ 1 \in N \implies 1 = 1 \cdot 1 \in HN$
   - Dado $x, y \in HN$, entonces $x = h_1 n_1,\ y = h_2 n_2$ y se tiene que

$$xy = h_1 n_1 h_2 n_2 = h_1 h_2 h_2^{-1} n_1 h_2 n_2$$

     y se tiene que $h_1 h_2 \in H$, por ser N normal se tiene que $h_2^{-1} n_1 h_2 \in N$ y así $xy \in HN$
   - Además, $x^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1} h_1 n_1^{-1} h_1^{-1} \in HN$, puesto que $h_1^{-1} \in H$ y $h_1 n_1^{-1} h_1^{-1} \in N$

   Ahora vamos a ver que $H \cap N$ es normal en H. Para ello, tomamos $h \in H,\ x \in H \cap N$, y tenemos que $h^{\cdot 1} x h \in H$ por ser producto de elementos de H y $h^{-1} x h \in N$ porque N es normal. Por tanto, $h^{-1} x h \in H \cap N$ y tenemos que es normal en H.

   Por último, queda ver la isomorfía. Para ello, hacemos

$$\begin{array}{ccccc} f: H & \to & HN & \to & HN/N \\ h & \mapsto & h & \mapsto & hN \end{array}$$

   Veamos que f es suprayectiva: dado $x \in HN/N \implies x = (hn)\, N = hN = f(h)$.

   Y calculemos el núcleo:

$$Kerf = \{h \in H : hN = 1 = N\} = H \cap N$$

   Así, por el primer teorema de isomorfía, tenemos que

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}$$

Teorema chino de los restos para grupos

Si G y H son dos subgrupos cíclicos de órdenes n y m, entonces $G \times H$ es cíclico si y solo si $mcd\,(n,m) = 1$. Más generalmente, si g, h son dos elementos de un grupo G de órdenes coprimos n y m y $gh = hg$, entonces $\langle g, h\rangle = \langle gh\rangle$ es cíclico de orden nm.

Demostración

Por la proposición 4.22, tenemos que $G \simeq (\mathbb{Z}_n, +)\,,\ H \simeq (\mathbb{Z}_m, +)$.

' $\Longleftarrow$ ' Si $mcd\,(n,m) = 1$, entonces, por el teorema chino de los restos para anillos, $\mathbb{Z}_n \times \mathbb{Z}_m$ y $\mathbb{Z}/nm\mathbb{Z}$ son isomorfos como anillos. En particular son isomorfos sus grupos aditivos. Es decir,
$G \times H \simeq (\mathbb{Z}_n, +) \times (\mathbb{Z}_m, +) \simeq (\mathbb{Z}/nm\mathbb{Z}, +)$, que es cíclico.

' $\Longrightarrow$ ' Si n y m no son coprimos y $d = mcd\,(n,m)$, entonces G tiene un subgrupo G_1 de orden d y H tiene otro subgrupo H_1 de orden d. Entonces $G_1 \times 1$ y $1 \times H_1$ son dos subgrupos distintos de $G \times H$ del mismo orden, en contra de la proposición 4.22, por lo que $G \times H$ no puede ser cíclico y el resultado queda demostrado por contrarrecíproco.

Supongamos ahora que $g, h \in G$ tienen órdenes coprimos n y m y que $gh = hg$. Entonces la aplicación

$$\begin{array}{rcl} f : \mathbb{Z}_n \times \mathbb{Z}_m & \to & G \\ (i,j) & \mapsto & g^i h^j \end{array}$$

es un homomorfismo de anillos cuya imagen es $\langle g, h\rangle$, puesto que $gh = hg$.

$$Ker f = \Big\{(a,b) : g^a h^b = 1\Big\}$$

Entonces $g^a = h^{-b} \in \langle g\rangle \cap \langle h\rangle$, que es un subgrupo tanto de $\langle g\rangle$ como de $\langle h\rangle$. Como el primero tiene orden n y el segundo tiene orden m, entonces, por el teorema de Lagrange, el orden de $\langle g\rangle \cap \langle h\rangle$ divide a n y a m. Como son coprimos, el orden debe ser 1.

Entonces los elementos de $Ker f$ son tales que $g^a = 1 = h^b$.

Si $g^a = 1 \implies n|a \implies a \equiv 0 \mod n$ y de igual forma $m|b$ y $b \equiv 0 \mod m$. Pero, esto quiere decir que $Ker f = \{(0,0)\}$. Por tanto, la aplicación es inyectiva y se tiene, por el primer teorema de isomorfía, que

$$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \langle g, h\rangle$$

y así, $\langle g, h\rangle$ es cíclico de orden nm. Falta ver que es generado por gh.

Es claro que $\langle gh\rangle$ es un subgrupo de $\langle g, h\rangle$, si demostramos que tienen el mismo orden, nm, tendremos la igualdad. Calculemos el orden de gh:

$$1 = (gh)^k = g^k h^k \implies g^k = h^{-k} \in \langle g\rangle \cap \langle h\rangle = \{1\}$$

como antes. De esta forma, se tiene que $n = |g|\,|k$ y $m = |h|\,|k$, luego el orden, que es el menor k que verifica esto, es el mcm. Como n y m son coprimos, entonces $k = nm$.

Propiedades y aplicaciones de las acciones de grupos en conjuntos

Proposición 4.26

Sea G un grupo actuando en un conjunto X y sean $x \in X$ y $g \in G$. Entonces:

1. $Estab_G(x)$ es un subgrupo de G
2. $[G : Estab_G(x)] = |G \cdot x|$. En particular, si G es finito, entonces el número de elementos de cada órbita es un divisor del orden de G.
3. Si se trata de una acción por la izquierda entonces $Estab_G(g \cdot x) = Estab_G(x)^{g^{-1}}$. Sin embargo, si se trata de una acción por la derecha entonces $Estab_G(x \cdot g) = Estab_G(x)^g$. En particular, si $x, g \in G$ y H es un subgrupo de G entonces
$$C_G(x^g) = C_G(x)^g \qquad y \qquad N_G(H^g) = N_G(H)^g$$
4. **Ecuación de Órbitas:** si R es un subconjunto de representantes de las órbitas de la acción de G en X, es decir, R contiene exactamente un elemento de cada órbita, entonces
$$|X| = \sum_{r \in R} |G \cdot r| = \sum_{r \in R} [G : Estab_G(r)]$$

Demostración

1. $Estab_G(x) = \{g \in G : gx = x\}$
   - $1 \in Estab_G(x)$: como $1a = a,\ \forall a \in G \implies 1 \in Estab_G(x)$
   - Dados $a, b \in Estab_G(x) \implies abx = a(bx) = ax = x \implies ab \in Estab_G(x)$
   - Dado $a \in Estab_G(x) \implies ax = x \implies x = a^{-1}x \implies a^{-1} \in Estab_G(x)$

   Y $Estab_G(x)$ es un subgrupo de G.
2. Sea $H = Estab_G(x)$, entonces la aplicación
$$\begin{array}{ccc} h : G/H & \to & G \cdot x \\ gH & \mapsto & gx \end{array}$$
   es biyectiva.
   - Inyectividad, sean aH, bH tales que $ax = bx \implies x = a^{-1}bx \implies a^{-1}b \in H \implies a^{\cdot 1}bH = H \implies bH = aH$
   - Sobreyectividad, sea $yx \in G \cdot x \implies y \in G \implies yH \in G/H \implies h(yH) = yx$
3. $$Estab_G(gx) = \{a \in G : agx = gx\} = \left\{a \in G : g^{-1}agx = x\right\} = \left\{a \in G : g^{-1}ag \in Estab_G\{x\}\right\} =$$
$$= \left\{a \in G : a \in gEstab_G\{x\}g^{-1}\right\} = Estab_G\{x\}^{g^{-1}}$$
   Para verlo por la derecha es exactamente igual.
$$C_G(x^g) = Estab_G(x^g) = Estab_G(xg) = Estab_G(x)^g = C_G(x)^g$$
$$N_G(H^g) = Estab_G(H^g) = Estab_G(Hg) = Estab_G(H)^g = N_G(H)^g$$
4. Como las órbitas forman una partición de X entonces el cardinal de X es la suma de los cardinales de las órbitas. La segunda igualdad es obvia habiendo demostrado 2.

Corolario 4.27

Sea G un grupo y $a \in G$.

1. $\left|a^G\right| = [G : C_G(a)]$. En particular, a^G tiene un único elemento si y solo si a es un elemento del centro $Z(G)$.

2. **Ecuación de Clases:** si G es finito y X es un subconjunto de G que contiene exactamente un elemento de cada clase de conjugación con al menos dos elementos, entonces

$$|G| = |Z(G)| + \sum_{x \in X} [G : C_G(x)]$$

Demostración

1. $C_G(a) = Estab_G(a)$ con la acción de conjugación. Entonces, usando 2. de la proposición anterior, $[G : C_G(a)] = |G \cdot a| = \left|a^G\right|$

2. Es evidente por 3. de la proposición anterior.

Proposición 4.28

Si G es un p-grupo no trivial para p un primo entonces $Z(G) \neq 1$.

Demostración

Por el corolario anterior tenemos que

$$|G| = |Z(G)| + \sum_{x \in X} [G : C_G(x)]$$

entonces $|G|$ y $[G : C_G(x)]$ son potencia de $p, \forall x \in X$, por lo que $|Z(G)|$ es múltiplo de p y, por tanto, debe tener más elementos además del 1.

Teorema 4.29

Si G es un $p-$grupo finito entonces G tiene una cadena de subgrupos normales $1 = G_0 \subset G_1 \subset ... \subset G_n = G$ tales que $[G_i : G_{i-1}] = p$ para todo $i = 1, ..., n$.

Demostración

Razonamos por inducción sobre el orden de G.

El caso de orden 1 es obvio.

Supongamos que $G \neq 1$ y que el teorema se verifica para grupos de orden menor.

Por la proposición anterior, existe $g \in Z(G)$ con $g \neq 1$. Sea $N = \langle g \rangle$. Entonces N es normal en G ya que N está dentro del centro de G.

Si $G = N$, entonces G es cíclico y por la proposición 4.22, deducimos que si $|G| = p^n$ entonces $\forall i = 0, 1, ..., n$, G tiene un único subgrupo G_i de orden p^i y que $G_{i-1} \subset G_i$, con lo que se cumple el enunciado.

En caso contrario, tanto N como G/N son $p-$grupos de orden estrictamente menor que G con lo que por la hipótesis de inducción existe una cadena

$$G_0 = 1 \subset G_1 \subset ... \subset G_k = N$$

de subgrupos normales de N y una cadena

$$H_k = 1 \subset H_{k+1} \subset ... \subset H_n = G/N$$

de subgrupos normales de G/N tales que $[G_i : G_{i-1}] = p,\ \forall i = 1, ..., k$ y
$[H_j : H_{j-1}] = p,\ \forall j = k+1, ..., n.$

Por el teorema de la correspondencia, cada $H_j = G_j/N$ para algún subgrupo normal G_j de G que verifica los contenidos y, por el 2^{o} trm de isomorfía se tiene que si $k < j \leq n$ entonces
$H_j/H_{j-1} = \frac{G_j/N}{G_{j-1}/N} \simeq G_j/G_{j-1}$, por lo que $[G_j : G_{j-1}] = [H_j : H_{j-1}] = p$.

Teorema de Cauchy (4.30)

Si G es un grupo finito cuyo orden es múltiplo de un primo p, entonces G tiene un elemento de orden p.

Demostración

Sea $X = \{(g_1, g_2, ..., g_p) \in G^p : g_1 g_2 \cdot ... \cdot g_p = 1\}$. La aplicación

$$\begin{array}{ccc} G^{p-1} & \to & X \\ (g_1, ..., g_{p-1}) & \mapsto & \left(g_1, ..., g_{p-1}, (g_1 \cdot ... \cdot g_{p-1})^{-1}\right) \end{array}$$

es una biyección, luego $|X| = |G|^{p-1}$.

- Inyectividad: se tiene por la unicidad del inverso.
- Sobreyectividad: dado $a = (a_1, ..., a_p) \in X \implies a_1 ... a_p = 1 \implies a_p = (a_1 ... a_{p-1})^{-1} \implies a = \left(a_1, ..., a_{p-1}, (a_1 ... a_{p-1})^{-1}\right) = f(a_1, ..., a_{p-1})$

Consideremos la acción de S_p en G^p del ejemplo 4.25.(5):

$$\sigma \cdot (g_1, ..., g_p) = \left(g_{\sigma(1)}, ..., g_{\sigma(p)}\right)$$

Consideremos la permutación $\sigma \in S_p$ dada por

$$\sigma(i) = \begin{cases} i+1, & i \neq p \\ 1, & i = p \end{cases}$$

Si $(x_1, ..., x_p) \in X$ entonces

$$x_p x_1 ... x_{p-1} = x_p (x_1 ... x_p) x_p^{-1} = 1$$

Lo que demuestra que si $x \in X \implies \sigma x \in X$. Esto quiere decir que la acción de S_p en G^p define una acción de $\langle \sigma \rangle$ en X.

Analicemos las órbitas de la acción de $\langle \sigma \rangle$ en X.

Como $|\sigma| = p$, de la proposición 4.26.2 se deduce que cada órbita tiene cardinal 1 ó p.

Sea n el número de órbitas con un elemento y m el número de óritas con p elementos. Como las órbitas forman una partición de X se tiene que

$$|G|^{p-1} = |X| = n + pm$$

Como $p \mid |G|$, se deduce que $p|n$.

Como la órbita de $(1, ..., 1)$ tiene exactamente un elemento se tiene que $n \geq 1$ y como n es múltiplo de p necesariamente $n \geq 2$.

Entonces existe $x = (g_1, ..., g_p) \in X \setminus \{(1, ..., 1)\}$ tal que $|G \cdot x| = 1$.

Por tanto

$$(g_1, ..., g_p) = \sigma x = (g_p, g_1, ..., g_{p-1})$$

Esto implica que todos los g_i son iguales a un elemento $1 \neq g \in G$.

Como $x \in X$ se tiene que $g^p = g_1 \cdot ... \cdot g_p = 1$ y, ya que $g \neq 1$, g tiene orden p.

5 Grupos Abelianos Finitos

Clasificación de grupos abelianos finitos indescomponibles

Proposición 5.10

Sea A un grupo abeliano finito y sean $p_1, ..., p_k$ los divisores primos de $|A|$. Entonces

$$A = t_{p_1}(A) \oplus ... \oplus t_{p_k}(A)$$

con cada $t_{p_i}(A) \neq 0$

Demostración

Sea $a \in A$ y sea $|a| = n = p_1^{a_1} \cdot ... \cdot p_k^{a_k}$ la única descomposición de n en factores primos (recordemos de $\mathbb{Z}$ es un DFU).

Para cada $i = 1, ..., k$ sea $q_i = \frac{n}{p_i^{a_i}}$. Ningún primo divide a la vez a todos los q_i, por lo que $mcd(q_1, ..., q_k) = 1$ y esto quiere decir que existen $m_1, ..., m_k \in \mathbb{Z}$ tales que $m_1 q_1 + ... + m_k q_k = 1$. Como $na = p_i^{a_i} q_i a = 0$, entonces $q_i a \in t_{p_i}(A)$, y entonces

$$a = m_1 q_1 a + ... + m_k q_k a \in t_{p_1}(A) + ... + t_{p_k}(A)$$

Y, por tanto, $A = t_{p_1}(A) + ... + t_{p_k}(A)$.

Para ver que la suma es directa, supongamos que $a_1 + ... + a_k = 0,\ a_i \in t_{p_i}(A)$. Entonces, para cada $i = 1, ..., k$, existe b_i tal que $p_i^{b_i} a_i = 0$. Sea $m = p_1^{b_1} ... p_k^{b_k}$. Para cada i, ponemos $t_i = \frac{m}{p_i^{b_i}}$, de modo que $t_i a_j = \frac{m}{p_i^{b_i}} a_j = 0$ siempre que $i \neq j$, pues el factor $p_j^{b_j}$ multiplica a a_j. Entonces

$$t_1 a_1 + ... + t_k a_k = 0 \implies t_i a_i = -t_i \sum_{j \neq i} a_j = 0$$

entonces $|a_i|$ divide a t_i y a $p_i^{b_i}$, que son coprimos por cómo hemos definido t_i, por lo que $|a_i| = 1$ y se tiene que $a_i = 0$. Así, la familia es independiente.

Queda ver que los $t_{p_i}(A) \neq 0$. Ya hemos visto que $A = t_{p_1}(A) \oplus ... \oplus t_{p_k}(A)$, de donde se deduce que $|A| = |t_{p_1}(A)| ... |t_{p_k}(A)|$. Como el orden de cada $t_{p_i}(A)$ es una potencia de p_i, por el lema 5.9 y cada $p_i \mid |A|$, entonces este orden es mayor que 1 y tenemos el resultado.

Lema 5.13

Sean A un $p-grupo$ finito. Entonces:

1. Existe $a \in A$ tal que $|a| = Exp(A)$
2. Si $B = \langle a \rangle$, siendo a el de 1., entonces todo elemento del cociente A/B tiene un representante con el mismo orden. Es decir, para todo $y \in A/B$ existe $x \in A$ tal que $x + B = y$ y $|x| = |y|$.

Demostración

1. $$\forall x \in A,\ x^{Exp(A)} = 1 \implies |x| \,|Exp(A)\,,\ \forall x \in A$$

   Claramente, el mcm de los órdenes verifica esto, y ningún otro orden que lo verifique puede ser menor que el mcm. Entonces $Exp(A) = mcm\{|x| : x \in A\}$, tomando

   $$a = \prod_{x \in X} x$$

   tenemos el a buscado.

2. Para el segundo apartado, comenzamos eligiendo un representante cualquiera de y y veremos que podemos sustituirlo por otro con la propiedad requerida.

   Sea entonces $z \in A$ tal que $z + B = y$. Supongamos que $|a| = Exp(A) = p^m$, $|z| = p^s$ y $|y| = p^k$.

   Nótese que si G es un grupo abeliano y S es un subgrupo. Si $ng = 0,\ n \in \mathbb{N}, g \in G$, entonces, en G/S se tiene $n(g + S) = 0$. Esto implica que el orden de $g + S$ divide al orden de g.

   Retomando lo anterior, esto quiere decir que $k \leq s \leq m$.

   Si $k = s$, tomamos $x = z$ y hemos terminado.

   Supongamos entonces que $k < s$. Como $p^k(z + B) = p^k y = 0$, se tiene que $p^k z \in B = \langle a \rangle \implies p^k y = qa,\ q \in \mathbb{Z}$.

   Dividiendo q por la mayor potencia posible de p, podemos poner $q = rp^t$, con $mcd(p, r) = 1$. Entonces

   $$p^{m+k-t} z = p^{m-t} p^k z = p^{m-t} qa = rp^m a = 0$$

   y, por tanto, $s \leq m + k - t$. Por otro lado

   $$p^{m+k-t-1} z = p^{m-t-1} qa = rp^{m-1} a \neq 0$$

   y, por tanto, $s = m + k - t$.

   Sea ahora $x = z - tp^{m-s} a$, entonces

   $$x + B = z + B = y$$

   por lo que $|y| = p^k |\,|x|$. Pero, además

   $$p^k x = p^k y - rp^{m+k-s} a = p^k y - rp^t a = p^k y - qa = p^k y - p^k y = 0$$

   es decir, que $|x| = p^k = |y|$, como queríamos ver.

Proposición 5.14

Un grupo abeliano finito es indescomponible si y solo si es un $p-$grupo cíclico.

Demostración

' $\Longleftarrow$ ' Supongamos que $G = \langle a \rangle$ es un grupo cíclico de orden p^n con p primo y $n \in \mathbb{N}$. Entonces los subgrupo de G forman una cadena:

$$1 < \left\langle a^{p^{n-1}} \right\rangle_p < \left\langle a^{p^{n-2}} \right\rangle_{p^2} < ... < \left\langle a^{p^2} \right\rangle_{p^{n-2}} < \langle a^p \rangle_{p^{n-1}} < \langle a \rangle_{p^n} = G$$

Por lo que G es indescomponible, ya que no puede expresarse como suma directa de subgrupos suyos.

' $\Longrightarrow$ ' Supongamos que A es indescomponible, por el corolario 5.11, que dice que un grupo finito indescomponible es un p-grupo, tenemos que es un $p-$grupo, y solo resta ver que es cíclico.

Para esto, vamos a hacer inducción sobre n.

Si $n = 1$, entonces A tiene orden primo, por lo que es isomorfo a $\mathbb{Z}_p$ (corolario 4.23) y, por tanto, es cíclico.

En el caso general, por el lema anterior, A contiene un elemento a tal que $|a| = Exp(A)$. Sean $B = \langle a \rangle$ y $C = A/B$. Por la proposición 5.6 (todo grupo abeliano finito y no nulo es una suma directa de subgrupos indescomponibles), se tiene $C = C_1 \oplus ... \oplus C_k$ para ciertos $C_1, ..., C_k$ indescomponibles. Por hipótesis de inducción, cada C_i es cíclico. Es decir, existen $x_1, ..., x_k \in A$ tales que $C_i = \langle x_i + B \rangle$ para cada i, y por el lema anterior podemos suponer que $|x_i| = |x_i + B|$ para cada i.

Entonces se tiene que $A = B + \langle x_1 \rangle + ... + \langle x_k \rangle$. Vamos a ver que esta suma es directa.

Sean $b \in B$ y $m_1, ..., m_k \in \mathbb{Z}$ tales que $b + m_1 x_1 + ... + m_k x_k = 0$. Entonces $0 = m_1 (x_1 + B) + ... + m_k (x_k + B)$ y, por tanto, cada $m_i (x_i + B) = 0$. De aquí se deduce que m_i es múltiplo de $|x_i + B| = |x_i|$ y por tanto $m_i x_i = 0$ y $b = 0$. Como A es indescomponible y $B \neq 0$, se deduce que $A = B = \langle a \rangle$, por lo que A es cíclico y tenemos el resultado.

Teorema de Estructura de Grupos Abelianos Finitos

Teorema 5.20

Todo grupo abeliano finito tiene una descomposición invariante.

Demostración

Sea A un grupo abeliano finito. Añadiendo sumandos triviales a una descomposición primaria suya tenemos

$$\begin{aligned} A = \quad & \langle a_{11} \rangle_{p_1^{\alpha_{11}}} \oplus ... \oplus \langle a_{1m} \rangle_{p_1^{\alpha_{1m}}} \oplus \\ & ... \\ & \langle a_{k1} \rangle_{p_k^{\alpha_{k1}}} \oplus ... \oplus \langle a_{km} \rangle_{p_k^{\alpha_{km}}} \end{aligned}$$

para ciertos primos positivos distintos $p_1 < p_2 < ... < p_k$ y ciertos enteros a_{ij} que satisfacen $\alpha_{i1} \geq ... \geq \alpha_{im} \geq 0, \ \forall i = 1, ..., k$.

Los α_{ij} que valen 0 se corresponden con los sumandos triviales que hemos añadido para que en cada fila de la descomposición de A haya el mismo número de sumandos.

Para obtener la descomposición invariante basta con agrupar los sumandos por columnas. Entonces, tenemos, para cada $j = 1, ..., m$

$$b_j = a_{1j} + a_{2j} + ... + a_{kj} \ y \ d_j = p_1^{\alpha_{1j}} \cdot ... \cdot p_k^{\alpha_{kj}}$$

Entonces, como las potencias de primos usadas son coprimas, tenemos que

$$\langle b_j \rangle_{d_j} = \langle a_{1j} \rangle_{p_1^{\alpha_{1j}}} \oplus ... \oplus \langle a_{kj} \rangle_{p_k^{\alpha_{kj}}}$$

Entonces

$$A = \langle b_1 \rangle_{d_1} \oplus ... \oplus \langle b_k \rangle_{d_k}$$

es una descomposición invariante, ya que se tiene, por la definición de los d_i, que $d_i | d_{i-1}, \ \forall i = 2, ..., k$.

Teorema 5.24

Sea A un grupo abeliano finito. Entonces

1. Todas las descomposiciones primarias de A son semejantes
2. Todas las descomposiciones invariantes de A son semejantes

Demostración

Hemos visto en la demostración anterior cómo pasar de una descomposición primaria a una invariante. El proceso inverso es similar, basta tomar los órdenes, descomponerlos en factores potencia de primo, ver el generador de cada subgrupo de estos órdenes y agrupar adecuadamente.

Por tanto, para demostrar el teorema basta demostrar una de las afirmaciones. Vamos a ver la primera.

Sea

$$A = \left(\oplus_{j=1}^{m_1} A_{1j} \right) \oplus ... \oplus \left(\oplus_{j=1}^{m_k} A_{kj} \right)$$

una descomposición primaria de A con $|A_{ij}| = p_i^{\alpha_{kj}}$ para ciertos enteros primos positivos $p_1 < p_2 < ... < p_k$ y ciertos enteros positivos α_{ij} con $\alpha_{i1} \geq ... \geq \alpha_{im_i} \geq 1$ para cada $i = 1, ..., k$.

Obsérvese que para cada $i = 1, ..., k$ se tiene

$$\oplus_{j=1}^{m_i} A_{ij} = t_{p_i}(A)$$

por lo que estos subgrupos también están determinados por A.

Por lo tanto, podemos limitarnos a demostrar la unicidad asumiendo que A es un p-grupo finito.

En esta situación, dos descomposiciones primarias de A serán de la forma

$$A = A_1 \oplus ... \oplus A_n = B_1 \oplus ... \oplus B_m$$

donde cada sumando es cíclico. Si ponemos $|A_i| = p^{\alpha_i}$ y $|B_i| = p^{\beta_i}$, se tiene $\alpha_1 \geq ... \geq \alpha_n$ y $\beta_1 \geq ... \geq \beta_m$. Vamos a ver, por inducción en i, que $\alpha_i = \beta_i, \ \forall i$.

Obsérvese que $p^{\alpha_1} = Exp(A) = p^{\beta_1}$, por lo que tenemos el caso $i = 1$.

Supongamos entonces que $\alpha_j = \beta_j,\ \forall j = 1, ..., i-1$ y veamos que $\alpha_i = \beta_i$. Podemos suponer sin perder generalidad que $\alpha_i \leq \beta_i$.

Observamos ahora que: si C es un grupo cíclico de orden p^r y $s \in \mathbb{N}$, entonces se tiene $p^s C = 0 \iff s \geq r$. Si $s \leq r$, entonces $p^s C$ es cíclico de orden p^{r-s}.

Por tanto, si ponemos $q = p^{\alpha i}$, se tiene

$$\begin{array}{rc} qA \simeq & qA_1 \oplus ... \oplus qA_{i-1} \\ \simeq & (qB_1 \oplus ... \oplus qB_{i-1}) \oplus (qB_i \oplus ... \oplus qB_m) \end{array}$$

como $qA_1 \oplus ... \oplus qA_{i-1}$ y $qB_1 \oplus ... \oplus qB_{i-1}$ tienen el miso cardinal, deducimos que $qB_i \oplus ... \oplus qB_m = 0$. Esto quiere decir que $0 = qB_i = p^{\alpha_i} B_i$, por lo que $\alpha_i \geq \beta_i$ y, así, $\alpha_i = \beta_i$.

Teorema 5.27

1. Todo grupo abeliano finito tiene una descomposición primaria y una descomposición invariante
2. Las siguientes condiciones son equivalentes para dos grupos abelianos finitos
   (a) Son isomorfos
   (b) Tienen descomposiciones primarias semejantes
   (c) Tienen descomposiciones invariantes semejantes
   (d) Tienen la misma lista de divisores elementales
   (e) Tienen la misma lista de factores invariantes

Demostración

Esto es practicamente un corolario de lo ya visto.

1. Todo grupo tiene una descomposición primaria y toda descomposición primaria puede dar lugar a una descomposición invariante.
2. $a \implies b$ Evidente

   $b \implies a$ Si
   $A = \left(\oplus_{j=1}^{m_1} A_{1j}\right) \oplus ... \oplus \left(\oplus_{j=1}^{m_k} A_{kj}\right) \simeq \left(\oplus_{j=1}^{m_1} B_{1j}\right) \oplus ... \oplus \left(\oplus_{j=1}^{m_k} B_{kj}\right) = B \implies A \simeq B$

   $b \iff c$ Es obvio porque una composición primaria nos determina una invariante salvo isomorfismos y viceversa

   $d \iff e$ Es también obvio, ya que los factores invariantes vienen unívocamente determinados por los divisores elementales y los divisores elementales no son más que la factorización en potencia de primos de los factores invariantes

   $c \iff e$ Muy fácil también teniendo en cuenta que $\langle a \rangle_{p^k} \simeq \left(\mathbb{Z}_{p^k}, +\right)$

6 Grupos de Permutaciones

Tipo de una permutación y sus propiedades

Teorema 6.5

Toda permutación $\sigma \neq 1$ de S_n se puede expresar de forma única (salvo el orden) como producto de ciclos disjuntos.

Demostración

Razonamos por inducción en $|M(\sigma)|$. Como $\sigma \neq 1$, tenemos que $|M(\sigma)| \geq 2$, con lo que el primer caso $M(\sigma) = \{i, j\}$ lo que implica que $\sigma = (1\ 2)$.

Si $\sigma = \tau_1 ... \tau_k$, con $\tau_1, ..., \tau_k$ ciclos disjuntos, entonces $M(\sigma) = \cup_{i=1}^{k} M(\tau_i) = \{i, j\}$, de donde $k = 1$, y tenemos la unicidad.

Supongamos que la propiedad se verifica para toda permutación que mueve menos elementos que σ.

Fijemos $i \in M(\sigma)$ y definamos recursivamente $i_0 = i,\ i_j = \sigma(i_{j-1})$.

Como los i_j toman valores en un conjunto finito existirán $0 \leq j < k$ con $i_j = i_k$ y tomamos el menor j para el que existe un k con estas condiciones. Para este j tomamos el menor k que verifica $i_j = i_k$.

De hecho, $j = 0$, pues, en caso contrario, $i_{j-1} = \sigma^{-1}(i_k) = i_{k-1}$.

Entonces $i_0, ..., i_{k-1}$ son distintos y $i_0 = i_k = \sigma(i_{k-1})$.

Por tanto, $\tau = (i_0\ i_1\ ...\ i_{k-1})$ es un $k-$ciclo.

Definimos $\rho \in S_n$ poniendo

$$\rho(j) = \begin{cases} j, & si\ j \in (i_0\ i_1 ... i_{k-1}) \\ \sigma(j) & en\ otro\ caso \end{cases}$$

Entonces ρ y τ son disjuntas, pues si τ mueve a j, entonces $j \in (i_0\ i_1 ... i_{k-1})$ y ρ no lo mueve. Y si ρ mueve a j, entonces ocurre al contrario y τ no lo mueve.

Es evidente, entonces, que ρ mueve tantos elementos como σ, menos los que mueve τ. Es decir

$$|M(\rho)| = |M(\sigma)| - |M(\tau)| = |M(\sigma)| - k < |M(\sigma)|$$

Y, además, se tiene que

$$\tau\rho(j) = \begin{cases} \tau(j) & j \in (i_0\ i_1 ... i_{k-1}) \\ \tau(\sigma(j)) & otro\ caso \end{cases} = \sigma(j)$$

Es decir, que $\sigma = \tau\rho$.

Aplicando la hipótesis de inducción deducimos que $\rho = \rho_1 ... \rho_l$, con $\rho_1, ..., \rho_l$ ciclos disjuntos dos a dos. Además, son disjuntos con τ, pues, de no ser así, no lo sería ρ.

Entonces $\sigma = \tau\rho_1 ... \rho_l$ es un producto de ciclos disjuntos.

Si fuera $\sigma = \tau_1 ... \tau_m$ con $\tau_1, ..., \tau_m$ ciclos disjuntos, entonces $i \in M(\tau_j)$ para un único $j = 1, ..., m$. Como los τ_j conmutan por ser disjuntos, podemos suponer $j = 1$. Entonces

$$\tau(i) = \sigma(i) = \tau_1(i)$$

por lo que $\tau = \tau_1$. Por lo que $\rho = \tau_2 ... \tau_m$. Usando de nuevo la hipótesis de inducción, tenemos la unicidad de la factorización de ρ como producto de ciclos disjuntos, y deducimos la unicidad de la factorización como producto de ciclos disjuntos de σ.

Proposición 6.8

El orden de una permutación es el mcm de las componentes de su tipo.

Demostración

Sea $\sigma = \tau_1 ... \tau_k$ la factorización de una permutación σ como producto de ciclos disjuntos y sea s_i la longitud del ciclo τ_i.

Sea $m \in \mathbb{N}$. Como los τ_i conmutan entre sí por ser disjuntos, se tiene

$$\sigma^m = \tau_1^m ... \tau_k^m$$

Por otra parte, para cada i se tiene $M(\tau_i^m) \subset M(\tau_i)$ y por tanto los τ_i^m son disjuntos.

Eso implica que $\sigma^m = 1$ precisamente si $\tau_i^m = 1,\ \forall i$, por la unicidad de la factorización, pero esto sucede si, y solo si, $s_i | m,\ \forall i$ o, lo que es lo mismo, si $mcm(s_1, ..., s_m) | m$.

Teorema 6.9

Dos elementos de S_n son conjugados si tienen el mismo tipo. En consecuencia, cada clase de conjugación de S_n está formada por todos los elementos de un mismo tipo.

Demostración

' $\Longrightarrow$ '

Sea una permutación α. Para un s-ciclo $\tau = (i_1\ i_2 ... i_s)$, se tiene que

$$\alpha\tau\alpha^{-1}(j) = \alpha\tau\left(\alpha^{-1}(j)\right) = \begin{cases} \alpha(i_k) & si\ \alpha^{-1}(j) = i_{k-1} \\ \alpha\left(\alpha^{-1}(j)\right) = j & si\ \alpha^{-1}(j) \notin (i_1\ i_2 ... i_s) \end{cases}$$

es decir, que

$$\alpha\tau\alpha^{-1} = (\alpha(i_1)\ \ \alpha(i_2) ... \alpha(i_s))$$

y es un s-ciclo.

Si τ_1, τ_2 son disjuntos, entonces también lo son $\alpha\tau_1\alpha^{-1}$ y $\alpha\tau_2\alpha^{-1}$, pues

$$\alpha\tau_1\alpha^{-1}(j) = \alpha\tau_2\alpha^{-1}(j) \iff \alpha(i_{1n}) = \alpha(i_{2m}) \iff i_{1n} = i_{2m} \implies \tau_1,\ \tau_2 \text{ no son disjuntos}$$

Entonces, como se tiene, en general, que

$$\sigma(\tau_1 ... \tau_k)\alpha^{-1} = \left(\alpha\tau_1\alpha^{-1}\right) ... \left(\alpha\tau_k\alpha^{-1}\right)$$

esto quiere decir que dos elementos conjugados de S_n tendrán el mismo tipo.

' $\Longleftarrow$ ' Supongamos que σ, σ' tienen el mismo tipo. Entonces las descomposiciones de σ, σ' en producto de ciclos disjuntos son de la forma $\sigma = \tau_1 ... \tau_k$ y $\sigma' = \tau_1' ... \tau_k'$ donde $\tau_i,\ \tau_i'$ tienen la misma longitud.

Por tanto existen biyecciones $\alpha_i : M(\tau_i) \to M(\tau_i')$ que conservan la estructura de los ciclos; es decir, que si $\tau_i = (j_1 ... j_s)$ y $\tau_i' = (j_1' ... j_s')$, entonces $\alpha_i(j_t) = j_t',\ \forall t$.

Además, como $|M(\sigma)| = |M(\sigma')|$, existe una biyección $\beta : \mathbb{N}_n \setminus M(\sigma) \to \mathbb{N}_n \setminus M(\sigma')$.

Sea ahora $\alpha \in S_n$ la biyección que se obtiene pegando las α_i y β. Es decir

$$\alpha(x) = \begin{cases} \alpha_i(x) & si\ x \in M(\tau_i) \\ \beta(x) & si\ x \notin M(\sigma) \end{cases}$$

Entonces, si $x \in M(\tau_i')$, esto quiere decir que $x = j_l'$ y $\alpha^{-1}(x) = j_l$

$$\alpha\tau_i\alpha^{-1}(x) = \alpha\tau_i\alpha_i^{-1}(x) = \alpha\tau_i(j_l) = \alpha\left(j_{\lfloor l+1 \rfloor_s}\right) = j'_{\lfloor l+1 \rfloor_s} = \tau_i'(j_l) = \tau_i'(x)$$

Y si $x \notin M(\tau_i')$, entonces $\alpha^{-1}(x) \notin M(\tau_i)$, y entonces

$$\alpha\tau_i\alpha^{-1}(x) = \alpha\alpha^{-1}(x) = x = \tau_i'(x)$$

Y se tiene que $\tau_i' = \alpha\tau_i\alpha^{-1}$. Esto ocurre para todo i, por lo que $\sigma' = \alpha\sigma\alpha^{-1}$ y tenemos el resultado.

Generadores de los Grupos Simétricos y Alternados

Esta proposición no sale en la lista, pero no tiene mucho sentido. La pongo.

Proposición 6.12

Para $n \geq 2$, los siguientes son conjuntos generadores de S_n:

1. El conjunto de todos los ciclos
2. El conjunto de todas las trasposiciones
3. El conjunto de $n-1$ transposiciones: $\{(1\ 2), (1\ 3), (1\ 4), ..., (1\ n-1), (1\ n)\}$
4. El conjunto de $n-1$ transposiciones: $\{(1\ 2), (2\ 3), (3\ 4), ..., (n-1\ n)\}$
5. El conjunto de una transposición y un $n-$ciclo: $\{(1\ 2), (1\ 2\ 3...n-1\ n)\}$

Demostración

1. Esto es cierto ya que toda permutación puede ponerse como producto de ciclos disjuntos (teorema 6.5).

   Para demostrar el resto de apartados basta comprobar que los elementos del conjunto dado en cada apartado se expresan como productos de los elementos del conjunto del apartado siguiente

2. Cada ciclo $\sigma = (i_1...i_s)$ puede escribirse como producto de trasposiciones no disjuntas:

$$\sigma = (i_1\ i_s)(i_1\ i_{s-1})...(i_1\ i_3)(i_1\ i_2)$$

3. Dado $\sigma = (i\ j)$, entonces

$$(1\ i)(1\ j)(1\ i) = (1\ j\ i)(1\ i) = (i\ j)$$

4. Dado $j \geq 2$, sea $\alpha = (2\ 3)(3\ 4)...(j-1\ j)$. Entonces

$$(1\ 2)^\alpha = \alpha^{-1}(1\ 2)\alpha = (2\ 3...j)^{-1}(1\ 2)(2\ 3...j) = (j\ j-1)...(4\ 3)(3\ 2)(1\ 2\ 3...j) = (j\ j-1)...(4\ 3)(1\ 3...j$$

$$= (j\ j-1)...(5\ 4)(1\ 4...j) = ... = (j\ j-1)(1\ j-1\ j) = (1\ j)$$

5. Sean $\tau = (1\ 2)$ y $\sigma = (1\ 2...n-1\ n)$.
   Como $\sigma^{j-1}(1) = j$ y $\sigma^{j-1}(2) = j+1$, entonces

$$\sigma^{j-1}\tau\sigma^{1-j} = \sigma^{j-1}(1\ 2)\sigma^{1-j} = (1\ j+1)\sigma^{1-j} = (j\ j+1)$$

Corolario 6.13

Sean p un número primo y H un subgrupo de S_p. Si H contiene una transposición y un $p-$ciclo, entonces $H = S_p$.

Demostración

Podemos suponer que H contiene a $(1\ 2)$ y un p-ciclo $\sigma = (a_1\ a_2 ... a_p)$. Podemos suponer que $a_1 = 1$ porque es un ciclo. Entonces, si $a_i = 2$, se tiene que $\sigma^{i-1}(1) = 2$, y se tiene que $\sigma^{i-1} = (1\ 2\ b_3 ... b_p)$. Como p es primo, entonces $i-1, p$ son coprimos, y su mcm es $(i-1)\,p$, pues en caso contrario σ^{i-1} sería la identidad. Si renombramos los $b_i = i$, entonces tenemos que $\sigma^{i-1} = (1\ 2\ 3 ... p)$, y llega hasta el p por lo mencionado anteriormente, σ^{i-1} lo podemos aplicar p veces hasta que nos dé la identidad, por tanto ha de tener p elementos.

Entonces $(1\ 2), (1\ 2 ... p) \in H$, por la proposición anterior, estas dos permutaciones son generadores de S_p, luego $H = S_p$.

Proposición 6.20

Los siguientes son sistemas de generadores de A_n:

1. El conjunto de todos los productos de dos transposiciones, disjuntas o no
2. El conjunto de todos los 3−ciclos.

Demostración

1. Sea $\sigma \in A_n$, entonces, como las trasposiciones son generadores de S_n, podemos escribir σ como producto de trasposiciones. Además, $Sg(\sigma) = 1$, porque está en A_n, y las trasposiciones tienen signo -1. Como $Sg(ab) = Sg(a)\,Sg(b)$, entonces σ debe ser producto de una cantidad par de trasposiciones, como queríamos ver.
2. Todos los 3-ciclos están en A_n porque son permutaciones pares. Entonces, usando 1. para demostrar 2., solo hay que probar que cada producto de dos trasposiciones distintas se puede escribir como producto de 3-ciclos, pero esto es cierto porque

$$(i\ j)(i\ k) = (i\ k\ j)$$

$$(i\ j)(k\ l) = (j\ l\ k)(i\ k\ j)$$

con i, j, k, l son distintos dos a dos.

Teorema de Abel

Lema 6.23

Si un subgrupo normal H de A_n, con $n \geq 5$, contiene un 3-ciclo, entonces $H = A_n$.

Demostración

Sea σ un 3−ciclo en H. Por la proposición 6.20 (la anterior), basta ver que cualquier otro 3−ciclo σ' está en H. Sabemos por el teorema 6.9 que existe $\alpha \in S_n$ tal que $\sigma' = \sigma^\alpha$, de modo que si $\alpha \in A_n$, entonces $\sigma' \in H$, por la normalidad de H en A_n. Por tanto, podemos suponer que α es una permutación impar. Como σ cambia solo 3 elementos y $n \geq 5$, existe una trasposición β disjunta de σ, por lo que $\sigma^\beta = \sigma$. Por tanto

$$\sigma^{\beta\alpha} = \left(\sigma^\beta\right)^\alpha = \sigma^\alpha = \sigma'$$

y como $\beta\alpha$ está en A_n por ser el producto de dos permutaciones impares, la normalidad de H en A_n implica que $\sigma' \in H$, como queríamos ver.

Teorema de Abel (6.24)

Si $n \geq 5$, entonces A_n es un grupo simple.

Demostración

Supongamos que $H \neq \{1\}$ es un subgrupo normal de A_n y veamos que $H = A_n$. Por el lema anterior, basta ver que H contiene un 3-ciclo.

Sea $1 \neq \sigma \in H$ tal que $r = |M(\sigma)|$ sea mínimo, es decir, $|M(\alpha)| \leq r,\ \forall 1 \neq \alpha \in H$.

Ahora veremos que debe ser $r = 3$, por lo que σ será un 3-ciclo en H y habremos terminado.

Sabemos que no puede ser $r = 1$, porque una permutación no puede cambiar un único elemento.

Tampoco puede ser $r = 2$ porque todas las permutaciones de H son pares ($H \subset A_n$).

Supongamos, buscando una contradicción, que $r > 3$. Se tienen dos posibilidades:

1. Que en la factorización de σ en ciclos disjuntos, aparezca alguno de longitud ≥ 3

   Entonces, σ debe cambiar al menor 5 elementos. Si solo cambiase 4, como en su factorización aparece un ciclo de longitud ≥ 3, entonces σ debe ser un 4-ciclo, y sería impar#. Podemos suponer, sin pérdida de generalidad (porque al fin y al cabo aquí los números solo son etiquetas), que $1, 2, 3, 4, 5 \in M(\sigma)$ y que alguno de los ciclos disjuntos que componen σ es de la forma (1 2 3...), con longitud al menos 3. Sea $\alpha = (3\ 4\ 5)$. Como $\alpha \in A_n$ y H es normal en A_n, entonces $\sigma^\alpha \in H$, y entonces $\beta = \sigma^{-1}\sigma^\alpha \in H$.

   Si $\sigma(i) = i$, entonces $i > 5$ y, por tanto, $\alpha(i) = i$, y esto implica que $\beta(i) = i$, por lo que $M(\beta) \subset M(\sigma)$, y la inclusión es estricta, porque $\sigma(1) = 2$, mientras que $\beta(1) = \sigma^{-1}\alpha^{-1}\sigma\alpha(1) = \sigma^{-1}\alpha^{-1}\sigma(1) = \sigma^{-1}\alpha^{-1}(2) = \sigma^{-1}(2) = 1$.

   Por tanto, $\beta \in H$ cambia menos de r elementos, por lo que debe ser $\beta = 1$, por la elección de r. Esto quiere decir que $\sigma^\alpha = \sigma \implies \sigma\alpha = \alpha\sigma$. Pero esto no es cierto, porque

   $$\sigma\alpha(2) = \sigma(2) = 3,\ \alpha\sigma(2) = \alpha(3) = 4\#$$

   Por tanto, esta primera posibilidad lleva a una contradicción.

2. Que σ sea producto de, al menos dos, trasposiciones disjuntas.

   En este caso, reordenando los elementos de $\mathbb{N}_n$ podemos asumir que $\sigma = (1\ 2)(3\ 4)...$ (puede haber más trasposiciones en el producto o no).

   Sea, de nuevo, $\alpha = (3\ 4\ 5)$. Como antes, tomamos $\beta = \sigma^{-1}\sigma^\alpha \in H$. Si $i \neq 5$ y $\sigma(i) = i$, entonces $i \neq 3, 4, 5$ y, por tanto, $\alpha(i) = i$, de donde se sigue que $\beta(i) = i$, por lo que $M(\beta) \subset M(\sigma) \cup \{5\}$.

   Pero $\beta(1) = \sigma^{-1}\alpha^{-1}\sigma\alpha(1) = \sigma^{-1}\alpha^{-1}\sigma(1) = \sigma^{-1}\alpha^{-1}(2) = \sigma^{-1}(2) = 1$ y $\beta(2) = \sigma^{-1}\alpha^{-1}\sigma\alpha(2) = \sigma^{-1}\alpha^{-1}\sigma(2) = \sigma^{-1}\alpha^{-1}(1) = \sigma^{-1}(1) = 2$, luego β fija 1 y 2. Sin embargo σ los mueve. Por tanto, β cambia menor de r elementos y debe ser $\beta = 1$, de nuevo se tiene que $\sigma\alpha = \alpha\sigma$. Pero

   $$\sigma\alpha(3) = \sigma(4) = 3\ \alpha\sigma(3) = \alpha(4) = 5\#$$

   Y, de nuevo, llegamos a una contradicción.

Por tanto, ha de ser $r = 3$, por lo que hay un 3-ciclo en H y el lema anterior nos da el resultado.