Notas de álgebra abstracta

Octavio Alberto Agustín Aquino

20 de diciembre de 2005

Índice

1. Grupos **1**
1.1. Ejemplos . . . 2
1.2. Propiedades elementales de los grupos . . . 2
1.3. Subgrupos . . . 3
1.4. Grupos cíclicos . . . 4
1.5. Clases laterales y el teorema de Lagrange . . . 5
1.6. Grupos normales y grupos cociente . . . 7
1.7. Homomorfismos . . . 9
1.8. Los teoremas de isomorfismo . . . 11
1.9. Producto directo de grupos . . . 12
1.10. El teorema de Cayley . . . 13
1.11. Acciones de grupo, órbitas y estabilizadores . . . 13
1.12. Conjugación . . . 14
1.13. Permutaciones y los grupos simétricos . . . 15
1.14. Ecuación de clases de un grupo finito . . . 18
1.15. Teorema de Cauchy . . . 19
1.16. La estructura de los p-grupos . . . 20
1.17. Los teoremas de Sylow . . . 20

1. Grupos

Un semigrupo es una pareja $(G, \cdot)$ donde G es un conjunto y $\cdot : G \times G \to G$ es una operación asociativa. En lo sucesivo la operación actuando sobre dos elementos de una estructura algebraica se expresará por simple yuxtaposición a menos que se indique lo contrario.

Un monoide es un semigrupo $(G, \cdot)$ con identidad, esto es, existe $e \in G$ tal que $ex = xe = x$ para todo $x \in G$.

Un elemento $u \in G$ en un monoide $(G, \cdot)$ es una unidad si existe u' tal que $u'u = uu' = e$, donde e es la identidad de G.

Si cada elemento de un monoide $(G, \cdot)$ es una unidad entonces a dicho monoide se le denomina grupo. Si, además, la operación del grupo es conmutativa, dicho grupo se dice abeliano.

Si el conjunto G de la estructura algebraica es finito, se dice que la estructura algebraica es finita, y la cardinalidad del conjunto se representa con $|G|$ y se denomina orden de la estructura algebraica. Si $(G, \cdot)$ es un grupo finito, entonces $|G|$ es el orden del grupo. En lo futuro sólo se escribirá el conjunto que sirve de base a la estructura algebraica, esto es, el grupo $(G, \cdot)$ se escribirá simplemente como G.

1.1. Ejemplos

Denotemos por E^n el espacio euclídeo n-dimensional. Una figura geométrica S puede verse como un subconjunto de E^n. Una simetría de S es una transformación $T : E^n \to E^n$ con la propiedad de que $T(S) = S$. El conjunto de todas las simetrías de S es un grupo, el llamado grupo simétrico de S, bajo la composición de funciones.

Para todo natural $n > 2$, el grupo diedral D_{2n} de orden $2n$ es el grupo de simetría de un polígono regular de n lados. Consiste en todas las rotaciones con ángulos $\frac{2\pi j}{n}$ con $j = 0, 1, 2, \ldots, n-1$ junto con las reflexiones respecto a los n ejes de simetría del polígono.

Las simetrías de un rectángulo que no sea un cuadrado constituyen un grupo de orden 4. Las simetrías son las siguientes: la identidad, la reflexión con respecto a los ejes vertical y horizontal, y rotación por π radianes. Si I denota la identidad, A y B las rotaciones con respecto a los ejes de simetría y C la rotación, tenemos que $A^2 = B^2 = C^2 = I$, $AB = BA = C$, $AC = CA = B$ y $BC = CB = A$. Este grupo es abeliano, y generalmente se le refiere como el grupo de Klein (en alemán, Kleinsche Viergruppe).

Las simetrías de un tetraedro regular tridimensional son un grupo. Cualquier permutación de los vértices del tetraedro puede ser efectuada por una simetría apropiada. Más aún, cada simetría está unívocamente determinada por la permutación de vértices que induce. Por lo tanto, el orden de este grupo es 24, puesto que hay 24 permutaciones en un conjunto con cuatro elementos. Sin embargo, este grupo no es abeliano.

1.2. Propiedades elementales de los grupos

Lema 1. *Hay exactamente un elemento identidad en un grupo.*

Demostración. Sean f, e dos elementos identidades en el grupo. Entonces $fe = ef = e = f$, y el resultado se sigue. □

Lema 2. *Un elemento* x *de un grupo* G *tiene exactamente un inverso.*

Demostración. Existe al menos un x' tal que $xx' = x'x = e$. Si z es otro elemento tal que $xz = e$ entonces $z = ez = (x'x)z = x'(xz) = x'e = x'$, y análogamente si $zx = e$. Luego el inverso está unívocamente determinado. □

El lema anterior permite escribir el inverso de x como x^{-1}.

Lema 3. *Sean* x *e* y *elementos de un grupo* G. *Entonces* $(xy)^{-1} = y^{-1}x^{-1}$.

Demostración. Según las propiedades de un grupo tenemos que

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) \\ &= x(ex^{-1}) = (xe)x^{-1} = xx^{-1} = e.\end{aligned}$$

Similarmente, $(y^{-1}x^{-1})(xy) = e$, y por lo tanto $(xy)^{-1} = y^{-1}x^{-1}$, según el lema anterior. □

Nótese que en particular $(x^{-1})^{-1} = x$, por la simetría de los requerimientos del inverso.

Definimos recursivamente x^n para cada entero no negativo n a través de $x^0 = e$ y $x^n = x^{n-1}x$, y como $x^{-n} = (x^n)^{-1}$ para los enteros negativos.

Teorema 1. *Sea* x *un elemento de un grupo* G. *Entonces* $x^{m+n} = x^m x^n$ *y* $x^{mn} = (x^m)^n$ *para cualesquiera enteros* m *y* n.

Demostración. Las identidades son obvias en el caso en que tanto m como n son nulos. Si ambos son positivos, acudimos a una doble inducción. Si ambos son negativos basta tomar el inverso de las identidades, y si difieren en signo se deducen fácilmente de los dos casos anteriores. □

Nótese también que en los grupos las expresiones $(xyz)w = x(yzw) = (xy)(zw)$, etcétera, son todas equivalentes, y por lo tanto el producto $xyzw$ o de cualquier número finito de términos está unívocamente determinado.

1.3. Subgrupos

Definición 1. Sea G un grupo. Un subconjunto H de G es un subgrupo de G si

1. La identidad de G está en H.
2. HH $\subseteq$ H, donde HH representa a todos los posibles productos de elementos de H.
3. $H^{-1} \subseteq H$, donde H^{-1} representa el conjunto de los inversos de todos los elementos de H.

Si H es un subgrupo de G se escribe $H \leq G$.

Según la definición $G \leq G$. Si $H \leq G$ y $H \neq G$, entonces escribimos $H < G$.

Lema 4. *Para que un subconjunto* H *no vacío de un grupo* G *sea un subgrupo sólo basta que se cumplan los puntos 2 y 3 de la definición.*

Demostración. En efecto, asumamos 2 y 3 y demostremos que se cumple 1. Sea $g \in G$. Por el inciso 3 tenemos que $g^{-1} \in G$, y por 2 se sigue que $gg^{-1} = e \in G$, y el lema queda demostrado. □

Lema 5. *Sea* x *un elemento de un grupo* G *y definamos el conjunto* $\langle x \rangle := \{x^i : i \in \mathbb{Z}\}$. *Entonces* $\langle x \rangle \leq G$.

Demostración. Puesto que $e = x^0$, según la definición, se satisface la primera propiedad de subgrupo. Por el teorema anterior, $x^m x^n = x^{m+n}$, para cualesquiera m y n enteros, y ya que $m + n$ también es un entero, se cumple la segunda propiedad de subgrupo. Por defínción, $(x^m)^{-1} = x^{-m}$, y claramente $-m$ también es un entero. Luego $\langle x \rangle^{-1} \subseteq \langle x \rangle$, y se satisface la tercera propiedad de subgrupo, y la prueba concluye. □

El subgrupo $\langle x \rangle$ se conoce como el subgrupo generado por x. El orden de x es el mínimo entero n positivo tal que $x^n = e$.

Lema 6. *Sea* G *un grupo y* $H, K \leq G$. *Entonces* $H \cap K \leq G$.

Demostración. Como $H, K \leq G$, la identidad e pertenece a ambos, y de ahí que a su intersección. Como ambos son subgrupos, si $x, y \in H \cap K$ entonces $xy \in H$, y $xy \in K$, luego $xy \in H \cap K$. Por la misma razón $x^{-1} \subset H \cap K$, y la prueba termina. □

El lema anterior se puede generalizar para cualquier colección de subgrupos de un grupo dado.

1.4. Grupos cíclicos

Definición 2. Un grupo G es cíclico si existe $x \in G$ tal que $\langle x \rangle = G$. A tal elemento se le denomina generador.

El grupo aditivo de los enteros es cíclico con el 1 como generador.

El grupo aditivo $\mathbb{Z}_n$ de las clases de equivalencia módulo n es cíclico.

Lema 7. *Sea* G *un grupo cíclico finito con generador* x*, y sea* j *y* k *enteros. Entonces* $x^j = x^k$ *si y sólo si* $j \equiv k (\mathrm{mod} |G|)$.

Demostración. Probaremos primero que $x^m = e$ para algún entero positivo m. Debe ser que $x^j = x^k$ para algunos enteros j y k con $j < k$, puesto que el grupo es finito. Sea $m = k - j > 0$; entonces $x^m = x^{k-j} = x^k x^{-j} = e$. Sea n el menor entero positivo tal que $x^n = e$. Según el algoritmo de la división, para cualquier entero i existen q y r tales que $i = qn + r$ con $0 \leq r < n$ (así q es el menor enter tal que $qn \leq i$). Por lo tanto, $x^i = (x^n)^q x^r = ex^r = x^r$. La elección de r garantiza que $x^r \neq e$ si $0 < r < n$. Se sigue que el entero i satisface $x^i = e$ si y sólo si n divide a i. Sean j y k enteros. Ahora $x^j = x^k$ si y sólo si $x^{j-k} = e$, y se sigue que esto es posible si y sólo si $j - k$ es divisible entre n. Dicho de otro modo, $j \equiv k(\mathrm{mod}|G|)$. Además, n es el orden del grupo pues cada x^i con $0 \leq i < n$ son distintos. □

Ahora clasificaremos todos los subgrupos de un grupo cíclico G. Sea x el generador de G. Dado un subgrupo H de G con más de un elemento, sea m el menor entero positivo tal que $x^m \in H$. Supongamos que $x^i \in H$ para algún entero i. Ahora i puede expresarse como $i = qm + r$, donde q y r son enteros y $0 \leq r < m$. Ahora $x^r = x^{i-qm} = x^i(x^m)^{-q}$, con $x^i, x^m \in H$, y por lo tanto $x^r \in H$. La elección de m asegura que $r = 0$, y de aquí que $i = qm$. Así que $x^i \in H$ si y sólo si i es algún múltiplo entero de m. Eso muestra que H es el grupo cíclico con x^m como generador, donde m es el mínimo entero positivo tal que $x^m \in H$.

Supongamos que el grupo G es finito. Sea s el orden de G. Entonces $x^s = e$, y de aquí que $x^s \in H$. Se sigue que s es un múltiplo entero de m, donde m es el mínimo entero tal que $x^m \in H$. Por lo tanto todos los subgrupos de un grupo finito G son el subgrupo trivial $\{e\}$ y los generados por x^m donde m es un divisor de s.

Consideremos el caso en el que G es infinito. Para cada entero m el elemento x^m genera un subgrupo de G y de hecho m es el mínimo entero tal que x^m pertenece al subgrupo. Por lo tanto G es un grupo cíclico infinito con generador x y cuyos subgrupos cíclicos son generados por x^m donde m es un entero no negativo.

1.5. Clases laterales y el teorema de Lagrange

Definición 3. Sea H un subgrupo de G. Una clase lateral izquierda de H en G es un subconjunto de G de la forma xH, donde $x \in G$ y

$$xH = \{y \in G : y = xh \text{ para algún } h \in H\}.$$

Similarmente, una clase lateral derecha de H en G es un subconjunto de G que es de la forma Hx donde $x \in G$ y

$$Hx = \{y \in G : y = hx \text{ para algún } h \in H\}.$$

Nótese que un subgrupo H de G es en sí mismo una clase lateral de H en G.

Lema 8. *Sea* H *un subgrupo de* G. *Entonces las clases laterales izquierdas de* H *en* G *tienen las siguientes propiedades:*

1. *Tenemos que* $x \in xH$ *para todo* $x \in G$.
2. *Si* x *e* y *son elementos de* G *y si* $y = xa$ *para algún* $a \in H$, *entonces* $xH = yH$.
3. *Si* x *e* y *son elementos de* G *y si* $xH \cap yH$ *es no vacío entonces* $xH = yH$.

Demostración. Sea $x \in G$. Entonces $x = xe$, donde e es la identidad de G. Pero $e \in H$, pues H es subgrupo de G. Se sigue que $x \in xH$. Esto prueba 1.

Sean x e y elementos de G, donde $y = xa$ para algún $a \in H$. Entonces $xh = y(a^{-1}h)$ para todo $h \in H$. Más aún $ah \in H$ y $a^{-1}h \in H$ para todo $h \in H$, pues $H \leq G$. Se sigue que $yH \subset xH$ y $xH \subset yH$ y por lo tanto $xH = yH$. Esto prueba 2.

Finalmente, supongamos que $x, y \in G$ y $xH \cap yH \neq \emptyset$. Sea $u \in xH \cap yH$, y así $u = xh_1 = yh_2$. Entonces $x = yh_2h_1^{-1}$, como $h_2h_1^{-1} \in H$, según el inciso 2 se sigue que $xH = yH$. □

De este lema se deduce que las clases laterales izquierdas constituyen una partición de G.

Lema 9. *Sea* H *un subgrupo finito de* G. *Entonces cada clase lateral izquierda de* H *en* G *tiene el mismo número de elementos que* H.

Demostración. Sea $H = \{h_1, h_2, \ldots, h_m\}$, donde $h_1, h_2, \ldots, h_m$ son distintos y sea x un elemento de G. Entonces la clase lateral derecha xH consiste en los elementos xh_j para $j = 1, \ldots, m$. Supongamos que j y k son enteros entre 1 y m para los cuales $xh_j = xh_k$. Entonces $h_j = x^{-1}(xh_j) = x^{-1}(xh_k) = h_k$, lo que contradice que los elementos son distintos. Se sigue que cada xh_j con $j = 1, \ldots, m$ son distintos, y que la clase lateral derecha xH tiene el mismo número de elementos que el subgrupo H, como se pedía. □

Teorema 2 (Lagrange). *Sea* G *un grupo finito, y sea* H *un subgrupo de* G. *Entonces el orden de* H *divide al orden de* G.

Demostración. Cada elemento de G pertenece a al menos una clase lateral izquierda de H en G, y como las clases forman una partición de G, se sigue que cada elemento de G pertenece exactamente a una clase lateral izquierda. Más aún, cada clase lateral izquierda de H contiene $|H|$ elementos. Por lo tanto $|G| = n|H|$ donde n es el número de elementos de H, y el resultado se sigue. □

Definición 4. Sea H un subgrupo de G. Si el número de clases laterales izquierdas de H en G es finito, tal número se denomina índice de H en G, y se denota por $[G : H]$.

Corolario 1. *Sea* x *un elemento de* G. *Entonces el orden de* x *divide al orden de* G.

Corolario 2. *Cualquier grupo finito de orden primo es cíclico.*

Demostración. Sea G el grupo finito de orden primo y x alguno de sus elementos distinto de la unidad. Entonces el orden de x es mayor que uno y divide al orden de G. Pero el orden de x debe dividir al de G, pero como $|G|$ es primo, debe ser que el orden de x es igual al de G. Luego G es un grupo cíclico generado por x. □

1.6. Grupos normales y grupos cociente

Sean A y B subconjuntos de G. El producto AB de los conjuntos A y B se define como $AB = \{xy : x \in A, x \in B\}$. Denotamos a $\{x\}A$ y $A\{x\}$ por xA y Ax, para todos los elementos x de G y subconjuntos A de G. La asociatividad del grupo G asegura que $(AB)C = A(BC)$ para cualesquiera subconjuntos A, B, C de G, luego el producto ABC está unívocamente determinado. El producto de un número finito de subconjuntos se extiende de manera obvia.

Si $A, B, C \subset G$ y $A \subset B$, entonces claramente $AC \subset BC$ y $CA \subset CB$.

Nótese que si H es un subgrupo de un grupo G y x es un elemento de G entonces xH es la clase lateral izquierda de H en G que contiene a x. Similarmente, Hx es la clase lateral derecha de H en G que contiene a x.

Si H es un subgrupo de G entonces $HH = H$. De hecho $HH \subset H$, puesto que el producto de dos elementos de un subgrupo es en sí un elemento de H. También $H \subset HH$ puesto que $h = eh$ para cualquier elemento $h \in H$, donde e es la identidad de G y que pertenece a H.

Definición 5. Un subgrupo N de un grupo G se dice normal en G si $xnx^{-1} \in N$ para cada $n \in N$ y $x \in G$, y lo denotamos por $N \lhd G$.

Definición 6. Un grupo no trivial G se denomina simple si sus únicos subgrupos normales son el grupo total y el subgrupo trivial $\{e\}$.

Lema 10. *Cada subgrupo de un grupo abeliano es normal.*

Demostración. Sea N un subgrupo de un grupo abeliano G. Entonces

$$xnx^{-1} = (xn)x^{-1} = (nx)x^{-1} = n(xx^{-1}) = ne = n$$

para todo $n \in N$ y $x \in G$, y el resultado se sigue. □

Proposición 1. *Un subgrupo* N *de un grupo* G *es un grupo normal de* G *si y sólo si* $xNx^{-1} = N$ *para todos los elementos de* x *de* G.

Demostración. Supóngase que N es normal en G. Sea x un elemento de G. Entonces $xNx^{-1} \subset N$, según la definición. Reemplazando x por x^{-1} vemos también que $x^{-1}Nx \subset N$, y así $N = x(x^{-1}Nx)x^{-1} \subset xNx^{-1}$, y de aquí se concluye que $xNx^{-1} = N$.

Recíprocamente, si N es un subgrupo de G que cumple con $xNx^{-1} = N$, por definición se satisface que N es normal. □

Corolario 3. *Un subgrupo* N *de un grupo* G *es normal si y sólo si* $xN = Nx$ *para todo* $x \in G$.

Demostración. Sea N un subgrupo de G, y sea x un elemento de G. Si $xNx^{-1} = N$, entonces $Nx = (xNx^{-1})x = xN$. Recíprocamente, si $xN = Nx$, entonces $xNx^{-1} = Nxx^{-1} = Ne = N$, y según teorema esto implica que $N \lhd G$. □

Sea N un subgrupo normal de G. Por el corolario anterior podemos eliminar la distinción entre clases laterales izquierdas y derechas de N y decir simplemente clases laterales de un subgrupo normal.

Lema 11. *Si* N *es un subgrupo normal de un grupo* G *y sean* x *e* y *elementos de* G. *Entonces* $(xN)(yN) = (xy)N$.

Demostración. Si N es un subgrupo normal de G, entonces $yN = Ny$, y por lo tanto $(xN)(yN) = x(Ny)N = x(yN)N = xy(NN)$. Pero $NN = N$, puesto que N es un subgrupo de G. Por lo tanto $(xN)(yN) = (xy)N$, como se pedía. □

Proposición 2. *Sea* G *un grupo, y sea* N *un subgrupo normal de* G. *Entonces el conjunto de todas las clases de* N *en* G *es un grupo bajo la multiplicación de clases. El elemento identidad es* N *mismo, y el inverso de la clase* xN *es* $x^{-1}N$ *para todo* x *en* G.

Demostración. Según el lema anterior la operación está bien definida, y el resto de la proposición es claro. □

Definición 7. Sea N un subgrupo normal de un grupo G. El grupo cociente G/N se define como el grupo de las clases laterales de N en G con el producto de clases.

Ejemplo 1. Consideremos el grupo diedral D_8, que representa el grupo de simetrías de un cuadrado plano. Entonces

$$D_8 = \{I, R, R^2, R^3, T_1, T_2, T_3, T_4\},$$

donde I es la transformación identidad, R un rotación en sentido antihorario entorno al centro del cuadrado en un ángulo $\pi/2$, y T_1, T_2, T_3 y T_4 son las reflexiones con respecto a las bisectrices del cuadrado: la horizontal, una diagonal, la vertical y la otra diagonal respectivamente. Sea $N = \{I, R^2\}$. Entonces N es

un subgrupo de D_8. Las clases laterales izquierdas de N en D_8 son N, A, B y C, donde

$$A = \{R, R^3\},\ B = \{T_1, T_3\},\ C = \{T_2, T_4\}.$$

pues $R = RI$, $R^3 = RR^2$ (la clase lateral izquierda de R); $T_1 = T_1 I$, $T_3 = T_1 R^2$ (la clase lateral izquierda de T_1); y $T_2 = T_2 I$, $T_4 = T_2 R^2$.

Más aún N, A, B y C son también clases laterales derechas de N en D_8, y por lo tanto N es normal en D_8. Al multiplicar las clases entre sí tenemos que $AB = BA = C$, $AC = CA = B$ y $BC = CB = A$.

1.7. Homomorfismos

Definición 8. Un homomorfismo $\theta : G \to K$ de un grupo en otro es una función con la propiedad $\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$ para cada $g_1, g_2 \in G$.

Ejemplo 2. Sea q un entero. La función que va del grupo $\mathbb{Z}$ de enteros a sí mismo definida por $\theta(n) = qn$ es un homomorfismo.

Ejemplo 3. Sea x un elmento de un grupo G. La función $\theta(n) = x^n$ es un homorfismo que va de $\mathbb{Z}$ a G pues $x^{m+n} = x^m x^n$.

Lema 12. *Sea* $\theta : G \to K$ *un homomorfismo. Entonces* $\theta(e_G) = e_K$*, donde* e_G *y* e_K *son los elementos identidad de* G *y* K *respectivamente. También* $\theta(x^{-1}) = (\theta(x))^{-1}$ *para todo* x *en* G.

Demostración. Sea $z = \theta(e_G)$. Entonces $z^2 = \theta(e_G)\theta(e_G) = \theta(e_G e_G) = \theta(e_G) = z$. Pero eso implica que $z = e_K$.

Sea x un elemento de G. El elemento $\theta(x^{-1})$ satisface $\theta(x)\theta(x^{-1}) = \theta(xx^{-1}) = \theta(e_G) = e_K$, y similarmente $\theta(x^{-1})\theta(x) = e_K$. La unicidad del inverso asegura que $\theta(x^{-1}) = (\theta(x))^{-1}$. □

Definición 9. Un isomorfismo $\theta : G \to K$ entre grupos G y K es un homomorfismo biyectivo. Dos grupos son isomorfos si existe un isomorfismo entre ello.

Ejemplo 4. Sea D_6 el grupo de simetrías de un triángulo equilatero en el plano con vértices A, B y C, y sea S_3 el grupo de permutaciones del conjunto $\{A, B, C\}$. La función una simetría del triángulo a su correspondiente permutación de sus vértices es un isomorfismo entre el grupo diedral D_6 y el grupo simétrico S_3.

Ejemplo 5. Sea $\mathbb{R}$ el grupo aditivo de los números reales, y sea $\mathbb{R}^+$ el grupo multiplicativo de los reales estrictamente positivos. La función $\theta : \mathbb{R} \to \mathbb{R}^+$ definida por $\theta(x) = e^x$ es un isomorfismo entre ambos grupos, pues preserva las operaciones y es biyectiva. El inverso del isomorfismo es la función $\theta^{-1}(x) = \ln x$.

He aquí alguna terminología adicional en lo concerniente a los homomorfismos.

- Un monomorfismo es un homomorfismo inyectivo.
- Un epimorfismo es un homomorfismo sobreyectivo.
- Un endomorfismo es un homorfismo que mapea a un grupo en sí mismo.
- Un automorfismo es un isomorfismo que mapea a un grupo en sí mismo.

Definición 10. El núcleo $\mathrm{nuc}\theta$ de un homomorfismo $\theta : G \to K$ es el conjunto de todos los elementos de G que son mapeados por θ al elemento identidad de K.

Ejemplo 6. Sea el conjunto $\{1, -1\}$ dotado con la multiplicación de enteros y sea $\theta : \mathbb{Z} \to \{1, -1\}$ el homomorfismo definido por $\theta(n) = (-1)^n$. El núcleo del homomorfismo es el subgrupo de $\mathbb{Z}$ consistente en todos los enteros pares.

Proposición 3. *Sean* G *y* K *grupos y* $\theta : G \to K$ *un homomorfismo entre ellos. Entonces el núcleo del homorfismo es* $\{e\}$ *si y sólo si el homomorfismo es inyectivo, donde* e *es el elemento identidad de* G.

Demostración. Supongamos que $\mathrm{nuc}\theta = \{e\}$. Si $\theta(x) = \theta(y)$ entonces $\theta(x)\theta(y)^{-1} = e'$; $\theta(xy^{-1}) = e'$, donde e' es el elemento identidad de K. Por lo tanto $xy^{-1} \in \mathrm{nuc}\theta$, lo cual implica que $xy^{-1} = e$, y así $x = y$, de donde se deduce que el homomorfismo es inyectivo.

Ahora propongamos que θ es un homomorfismo inyectivo. Sean x e y elementos del núcleo de θ. Entonces $\theta(x) = \theta(y) = e'$, y dada la inyectividad del homomorfismo, se concluye $x = y$. Pero el núcleo de θ es un subgrupo de G, lo que implica que es el subgrupo trivial $\{e\}$. □

Lema 13. *Sean* G *y* K *grupos y* $\theta : G \to K$ *un homomorfismo entre ellos. Entonces* $\mathrm{nuc}\theta \lhd G$.

Demostración. Sean x e y elementos de $\mathrm{nuc}\theta$. Entonces $\theta(x) = e'$ e $\theta(y) = e'$, siendo e' el elemento identidad en K. Pero entonces $\theta(xy) = \theta(x)\theta(y) = e'e' = e'$, de donde $xy \in \mathrm{nuc}\theta$. También $\theta(x^{-1}) = (\theta(x))^{-1} = e'^{-1} = e'$, y por lo tanto $x^{-1} \in \mathrm{nuc}\theta$, y de aquí que $\mathrm{nuc}\theta \leq G$. Además

$$\theta(gxg^{-1}) = \theta(g)\theta(x)\theta(g)^{-1} = \theta(g)\theta(g)^{-1} = e',$$

por lo que $\mathrm{nuc}\theta \lhd G$. □

Si N es un subgrupo normal de un grupo G entonces N es núcleo del homomorfismo cociente $\theta : G \to G/N$ definido por $\theta(g) = gN$. Se sigue que un subgrupo N de G es normal si y sólo si es núcleo de algún homomorfismo.

Proposición 4. *Sean* G *y* K *grupos,* θ *un isomorfismo entre ellos y* N *un subgrupo normal de* G. *Supóngase que* $N \subset \mathrm{nuc}\theta$. *Entonces el isomorfismo* $\theta : G \to K$ *induce un homomorfismo* $\widehat{\theta} : G/N \to K$ *que envía a* $gN \in G/N$ *a* $\theta(g)$. *Más aún,* $\widehat{\theta}$ *es inyectiva si y sólo si* $N = \mathrm{nuc}\theta$.

Demostración. Sean x e y elementos de G. Tenemos que $xN = yN$ si y sólo si $x^{-1}y \in N$. También $\theta(x) = \theta(y)$ si y sólo si $x^{-1}y \in \text{nuc}\theta$, pues $\theta(xy^{-1}) = e$. Por lo tanto si $N \subset \text{nuc}\theta$ entonces $\theta(x) = \theta(y)$ siempre que $xN = yN$, y por lo tanto $\theta : G \to K$ induce una función bien definida $\widehat{\theta} : G/N \to K$ que envía a $gN \in G/N$ a $\theta(g)$. Esta función es un homomorfismo puesto que $\widehat{\theta}((xN)(yN)) = \widehat{\theta}(xyN) = \theta(xy) = \theta(x)\theta(y) = \widehat{\theta}(xN)\widehat{\theta}(yN)$.

Supóngase ahora que $N = \text{nuc}\theta$. Entonces $\theta(x) = \theta(y)$ si y sólo si $xN = yN$. Por lo tanto el homomorfismo $\widehat{\theta} : G/N \to K$ es inyectivo. Recíprocamente, si $\widehat{\theta} : G/N \to K$ es inyectiva entonces el núcleo de $\widehat{\theta}$ consiste únicamente en la identidad de G/N, que es precisamente N. □

Corolario 4. *Sean* G *y* K *grupos, y* $\theta : G \to K$ *un homomorfismo entre ellos. Entonces* $\theta(G) \cong G/\text{nuc}\theta$.

Demostración. Hay que demostrar que $\theta(G) \leq K$. Sean $x, y \in \theta(G)$. Tenemos que $x = \theta(x')$ e $y = \theta(y')$ donde $x', y' \in G$, y así $xy = \theta(x')\theta(y') = \theta(x'y')$, pero también $x'y' \in G$, luego $xy \in \theta(G)$, y por un lema anterior $x^{-1} \in \theta(G)$. Entonces $\theta(G) \leq K$, y según la proposición anterior, la función $\widehat{\theta} : G/N \to \theta(G)$ es biyectiva, y el corolario se sigue. □

1.8. Los teoremas de isomorfismo

Lema 14. *Sean* H *y* K *subgrupos de un grupo* G. *Entonces* HK *es un subgrupo de* G *si y sólo si* $HK = KH$.

Demostración. Supongamos que $HK \leq G$. Sea $u \in HK$. Entonces $u = hk$ para $h \in H$ y $k \in K$ y $u^{-1} = k^{-1}h^{-1} \in HK$, pues HK es un grupo. Pero también $k^{-1}h^{-1} \in KH$, luego $HK \subset KH$, y de forma totalmente análoga $KH \subset HK$, lo que permite concluir que $KH = HK$.

Ahora supongamos que $KH = HK$, y sean $x, y \in KH$. Entonces $x = k_1h_1$ y $y = k_2h_2$, donde $k_1, k_2 \in K$ y $h_1, h_2 \in H$. Pero también $h_1k_2 = k_2'h_1'$, pues $HK = KH$, luego $xy = k_1h_1k_2h_2 = k_1k_2'h_1'h_2 \in KH$. También $x^{-1} = h_1^{-1}k_1^{-1}$, luego $x^{-1} \in HK = KH$. Esto nos permite concluir que $KH \leq G$. □

Corolario 5. *Sea* G *un grupo,* H *un subgrupo de* G *y* N *un subgrupo normal de* G. *Entonces* HN *es un subgrupo de* G. *Además,* N *es normal en* HN.

Demostración. Un grupo normal conmuta con cualquier subconjunto de G, en particular con cualquier subgrupo de G. □

Teorema 3 (Primer Teorema de Isomorfismo). *Sea* G *un grupo,* H *un subgrupo de* G *y* N *un subgrupo normal de* G. *Entonces*

$$\frac{HN}{N} \cong \frac{H}{N \cap H}.$$

Demostración. Cada elemento de HN/N es una clase lateral de N que es de la forma hN para algún $h \in H$. Por lo tanto haciendo $\varphi(h) = hN$ para todo $h \in H$ tenemos que $\varphi : H \to HN/N$ es un homomorfismo suprayectivo. Sea $x \in \text{nuc}\varphi$ y así $\varphi(x) = e'$. Pero $e' = N$, y éso sólo ocurre si $x \in N$, y como $x \in H$, se sigue que $x \in H \cap N$. Si $x \in H \cap N$, es claro que $x \in \text{nuc}\varphi$. Luego $\text{nuc}\varphi = H \cap N$. Ahora $\varphi(H) \cong H/\text{nuc}\varphi$, según el corolario de la sección anterior, y dada la sobreyectividad de φ, el teorema se sigue. □

Teorema 4 (Segundo Teorema de Isomorfismo). *Sean M y N subgrupos normales de un grupo G, con $M \subset N$. Entonces*

$$\frac{G}{N} \cong \frac{G/M}{N/M}.$$

Demostración. Hay un homomorfismo bien definido $\theta : G/M \to G/N$ que envía gM a gN para todo $g \in G$. Más aún, el homomorfismo es sobreyectivo y $\text{nuc}\theta = N/M$, pues naturalmente si $g \in N$, $\theta(gM) = gN = N$, que es la identidad de G/N, y si $\theta(gM) = gN = N$, eso implica que $g \in N$, luego $gM \in N/M$. Nuevamente, por el corolario de la sección anterior, $\theta(G) \cong G/\text{nuc}\theta$, esto es $\theta\left(\frac{G}{M}\right) = \frac{G}{N} \cong \frac{G/M}{N/M}$, como se requería. □

1.9. Producto directo de grupos

Sean $G_1, \ldots, G_n$ grupos y sea G el producto cartesiano $G_1 \times \cdots \times G_n$ considerando a $G_1, \ldots, G_n$ como conjuntos. Los elementos de G son n-adas $(x_1, \ldots, x_n)$ donde $x_i \in G_i$ para $i = 1, \ldots, n$. Definamos una operación binaria en G de la siguiente manera:

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

Claramente la operación hereda su asociatividad de las operaciones definidas en $G_1, \ldots, G_n$. El elemento identidad es, evidentemente, $(e_1, \ldots, e_n)$, donde $e_i \in G_i$ para $i = 1, \ldots, n$ es la identidad de G_i. También es trivial comprobar que el inverso de $(x_1, \ldots, x_n)$ es precisamente $(x_1^{-1}, \ldots, x_n^{-1})$. Ahora G, junto con la operación antes descrita, es un grupo llamado producto directo de $G_1, \ldots, G_n$ y se denota por $G_1 \times \cdots \times G_n$.

Ejemplo 7. Sean C_2 y C_3 grupos cíclicos de orden 2 y 3, respectivamente. Entonces $C_2 \times C_3$ es un grupo cíclico de orden 6, y $C_2 \times C_2$ es isomorfo al grupo de Klein.

Consideremos primeramente a $C_2 \times C_3$. Sean x e y los generadores de C_2 y C_3 respectivamente, y sean e y e' los elementos identidad de C_2 y C_3. Entonces $C_2 = \{e, x\}$ y $C_3 = \{e', y, y^2\}$. Los elementos de $C_2 \times C_3$ son (e, e'), (e, y), (e, y^2), (x, e'), (x, y), (x, y^2). Sea $z = (x, y)$; vemos que $z^2 = (e, y^2)$, $z^3 = (x, e')$, $z^4 = (e, y)$, $z^5 = (x, y^2)$ y (e, e'). Vemos que $n = 6$ es el mínimo entero para el

cual $z^n = e$. Como el número de elementos de $C_2 \times C_3$ es también 6, se deduce que $C_2 \times C_3$ es un grupo cíclico de orden 6, cuyo generador es $z = (x, y)$.

Ahora examinemos a $C_2 \times C_2$, cuyos elementos son $I = (e, e)$, $A = (e, x)$, $B = (x, e)$ y $C = (x, x)$. Entonces $AB = (x, x) = BA = C$, $AC = (x, e) = CA = B$ y $BC = (e, x) = CB = A$, lo que lo hace isomorfo al grupo de Klein, como se afirmaba.

1.10. El teorema de Cayley

Teorema 5 (Cayley). *Sea* G *un grupo de orden* n. *Entonces* G *es isomorfo al grupo isomorfo a algún subgrupo de* S_n, *el grupo de las permutaciones de un conjunto de* n *elementos.*

Demostración. Para cada elemento x de G, sea $\sigma_x : G \to G$ definida por $\sigma_x(g) = xg$ para todo $g \in G$. Entonces

$$\sigma_{x^{-1}}(\sigma_x(g)) = x^{-1}(xg) = (x^{-1}x)g = g$$

y

$$\sigma_x(\sigma_{x^{-1}}(g)) = x(x^{-1}g) = (xx^{-1})g = g,$$

para todo $g \in G$. Al tener σ_x una inversa $\sigma_{x^{-1}}$, se sigue que es una biyección. Por lo tanto es una permutación de los elementos de G, por lo que podemos definir la función $\theta : G \to S_n$ a través de $\theta(x) = \sigma_x$, con $x \in G$. Tal función es un homorfismo, pues $\sigma_{xy}(g) = (xy)g = x(yg) = x\sigma_y(g) = \sigma_x(\sigma_y(g)) = \sigma_x \circ \sigma_y(g)$, lo que indica que $\theta(xy) = \sigma_{xy} = \sigma_x\sigma_y = \theta(x)\theta(y)$. El homomorfismo es inyectivo, pues si $\sigma_x = \sigma_y$ entonces $xg = yg$ para todo $g \in G$, lo que implica que $x = y$, según la cancelación en grupos, lo que indica que el homomorfismo es inyectivo. Además $\theta(G) \leq S_n$, luego G es isomorfo a algún subgrupo de S_n. □

1.11. Acciones de grupo, órbitas y estabilizadores

Definición. Una acción izquierda de un grupo G en un conjunto X asocia a cada $g \in G$ y $x \in X$ un elemento $g(x) \in X$ de tal modo que $g(h(x)) = (gh)(x)$ y $e(x) = x$ para $g, h, e \in G$ donde e denota la identidad en G.

Dada acción izquierda de un grupo G en un conjunto X, la órbita de $x \in X$ es el subconjunto $\{g(x) : g \in G\}$ de X, esto es, el conjunto de todas las actuaciones de G sobre x, y el estabilizador de x es el subgrupo $\{g : g(x) = x\}$ de G, esto es, el subgrupo de los elementos de G que dejan invariante a x. En efecto, si $h, g \in H$ donde H es el estabilizador de x en G, tenemos que $(hg)(x) = h(g(x)) = h(x) = x$, y también $e(x) = h^{-1}h(x) = h^{-1}(x) = x$, y tenemos que $H \leq G$.

Lema 15. *Sea* G *un grupo finito que actúa en un conjunto* X *por la izquierda. Entonces la órbita de* $x \in X$ *contiene* $[G : H]$ *elementos, donde* $[G : H]$ *es el índice del estabilizador* H *de* x *en* G.

Demostración. Probaremos que la función $\theta : G/H \to X$ definida por $\theta(gH) = g(x)$ está bien definida. Supongamos que $gH = g'H$. Entonces $g = g'u$, donde $u \in H$. Entonces $g(x) = (g'u)(x) = g'(u(x)) = g'(x)$, puesto que u pertenece al estabilizador de x en G. Luego $g = g'$, y esto prueba que θ es una función.

A continuación demostramos que es inyectiva. Supongamos que $g(x) = f(x)$, con $g, f \in G$. Entonces $f^{-1}g(x) = e(x) = x$, y de aquí que $f^{-1}g \in H$, lo que equivale a que $fH = gH$, y de aquí que la función θ sea inyectiva. Además, su imagen es la órbita de x al barrer θ a todo G, y el teorema queda demostrado. □

1.12. Conjugación

Definición. Dos elementos h y k de un grupo G se dicen conjugados si $k = ghg^{-1}$ para algún $g \in G$.

La relación R definida por hRk si y sólo si h y k son conjugados es de equivalencia. En efecto, como $h = ehe^{-1}$ se tiene que es reflexiva; ya que $k = ghg^{-1}$ para algún $g \in G$ tenemos que $g^{-1}kg = h$, luego kRh implica hRk; finalmente si hRk y kRl entonces $k = ghg^{-1}$ y $l = g'kg'^{-1}$ para $g, g' \in G$, y así $l = gg'hg'^{-1}g^{-1} = gg'h(gg')^{-1}$, y como $gg' \in G$, se tiene que hRl.

Los elementos de la partición de G que induce R se denominan clases de conjugación de G. El grupo G es la unión disjunta de tales clases. Más aún, la clase de conjugación del elemento identidad no contiene otro elemento de G.

Supongamos que el grupo G es abeliano. Sea $h \in G$ arbitrario y sea $[h]$ su clase de conjugación. Tomemos $k \in [h]$. Entonces $k = ghg^{-1}$ para algún $g \in G$. Como G es abeliano, $k = gg^{-1}h = eh = h$. Luego $[h] = \{h\}$. Recíprocamente, supongamos que para todo $h \in G$ se cumple que $[h] = \{h\}$. Sean $h \in G$ cualquier. Entonces para todo $g \in G$, $h = ghg^{-1}$, lo que implica que $hg = gh$, y como h y g fueron arbitrarios, se sigue que G es abeliano. Podemos concluir entonces que G es abeliano si y sólo si sus clases de conjugación consisten en un solo elemento cada una.

Sea G un grupo, y para un elemento $h \in G$ consideremos el conjunto $C(h)$ definido por $C(h) = \{g \in G : gh = hg\}$. Sean $u, v \in C(h)$. Tenemos que $(uv)h = u(vh) = u(hv) = (uh)v = (hu)v = h(uv)$. Por lo tanto $uv \in C(h)$. También $h = he = h(uu^{-1}) = uh(u^{-1})$, por lo que $u^{-1}h = hu^{-1}$, lo que implica que $u^{-1} \in C(h)$. Entonces $C(h) \leq G$.

Definición. Sea G un grupo. El centralizador $C(h)$ de un elemento $h \in G$ es el subgrupo de G definido por $C(h) = \{g \in G : gh = hg\}$.

Lema 16. *Sea* G *un grupo finito, y sea* $h \in G$. *Entonces el número de elementos de la clase de conjugación de* H *es igual al índice* $[G : C(h)]$ *del centralizador* $C(h)$ *de* h *en* G.

Demostración. Probaremos que la función $\theta : G/C(h) \to G$ definida por $\theta(gC(h)) = ghg^{-1}$ está bien definida y es inyectiva. Sean $g_1C(h) = g_2C(h)$, con $g_1, g_2 \in G$. Entonces $g_1 = g_2u$, con $u \in C(h)$, lo que implica que $g_1hg_1^{-1} = g_2uhu^{-1}g_2^{-1} = g_2huu^{-1}g_2^{-1} = g_2hg_2^{-1}$, lo que comprueba que θ es una función legítima. Supongamos que $g_1hg_1^{-1} = g_2hg_2^{-1}$, esto implica que $g_2^{-1}g_1h = hg_2^{-1}g_1$, por lo cual $g_2^{-1}g_1 \in C(h)$, y a su vez que $g_1C(h) = g_2C(h)$, lo que indica que θ es inyectiva. Como la imagen de θ es la clase de conjugación de h, se tiene el resultado. □

Sea H sea un subgrupo de un grupo G. Tomemos $u, v \in gHg^{-1}$. Entonces $u = gh_1g^{-1}$ y $v = gh_2g^{-1}$, por lo tanto $uv = gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1}$, y como $h_1h_2 \in H$, se sigue que $uv \in gHg^{-1}$. También $u^{-1} = gh_1^{-1}g^{-1}$, y $h_1^{-1} \in H$, por lo que $u^{-1} \in gHg^{-1}$, lo que comprueba que $gHg^{-1} \leq G$.

Definición. Dos subgrupos H y K de un grupo G se dicen conjugados si $K = gHg^{-1}$ para algún $h \in G$.

La relación de conjugación de grupos también es una relación de equivalencia en el conjunto de todos los subgrupos de G.

1.13. Permutaciones y los grupos simétricos

Una permutación de un conjunto S es una función biyectiva $p : S \to S$ de S en sí mismo. La permutación identidad de un conjunto S es la permutación que fija a cada elemento de S.

Las permutaciones de un conjunto de un conjunto finito S se representa convenientemente en forma de dos filas

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ p(x_1) & p(x_2) & \cdots & p(x_n) \end{pmatrix},$$

donde $x_1, \ldots, x_2 \in S$. Así, por ejemplo,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

representa la permutación del conjunto $\{1, 2, 3\}$ que envía $1 \to 2$, $2 \to 3$ y $3 \to 1$.

Ejemplo 8. Hay dos permutaciones de un conjunto $\{a, b\}$ con dos elementos. Éstos son la permutación identidad $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ y la trasposición $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ que intercambia a y b.

Ejemplo 9. Hay seis permutaciones del conjunto $\{a, b, c\}$ de tres elementos. Éstas son

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix},$$
$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}.$$

Sea S un conjunto. Entonces la composición de dos permutaciones es una también una permutación (la composición de dos biyecciones es una biyección). También cualquier permutación p de S tiene una inversa p^{-1} que también es una permutación (pues la inversa de una biyección es una biyección). La composición de funciones, como es bien sabido, es asociativa. Por lo tanto el conjunto de todas las permutaciones de S es un grupo bajo la composición de funciones.

Definición. Para cada natural n el grupo simétrico Σ_n es el grupo de permutaciones del conjunto $\{1, \ldots, n\}$.

Sean $a_1, \ldots, a_n$ los distintos elementos de S. Denotamos por $(a_1 a_2 \cdots a_n)$ a la permutación de S que envía a_i a a_{i+1} para $i = 1, 2, \ldots, n-1$ y a_n a a_1, y deja a todos los demás elementos de S fijos. Tal permutación se denomina ciclo de orden n, o n-ciclo. Un 2-ciclo se llama también una transposición.

(Nótese que al evaluar la composición de ciclos, debe hacerse de derecha a izquierda, según la convención para evaluar la composición de funciones.)

Ejemplo 10. Hay 24 permutaciones del conjunto $\{a, b, c, d\}$. Son las siguientes: la identidad, las seis transposiciones $(ab), (ac), (ad), (bc), (bd)$ y (cd); los ocho 3-ciclos $(bcd), (bdc), (acd), (adc), (abd), (adb), (abc)$ y (acb); los seis 4-ciclos $(abcd), (abdc), (acbd), (acdb), (adbc)$ y $(adcb)$; y tres permutaciones más $(ab)(cd), (ac)(bd)$ y $(ad)(bc)$.

Dos ciclos $(a_1 a_2 \cdots a_m)$ y $(b_1 b_2 \cdots b_n)$ se dicen disjuntos si los conjuntos $\{a_1, a_2, \ldots, a_m\}$ y $\{b_1, b_2, \ldots, b_n\}$ son disjuntos. Es fácil ver que el producto de dos ciclos disjuntos conmuta.

Proposición 5. *Cualquier permutación de un conjunto finito S es la permutación identidad, un ciclo, o una composición de dos o más ciclos disjuntos.*

Demostración. Haremos la prueba por inducción sobre el número de elementos de S. El resultado es trivial si S tiene un solo elemento. Supongamos que la proposición es verdadera para todas las permutaciones de un conjunto con menos de k elementos. Demostraremos que también es válida para un conjunto con k elementos.

Sea S un conjunto con k elementos y p una permutación de S. Escojamos un elemento a_1 de S, y sean los elementos $a_2, a_3, a_4, \ldots$ de S definidos por $p(a_i) = a_{i+1}$ para todos los enteros positivos i. Sea n el entero positivo más grande para el cual los elementos $a_1, \ldots, a_n$ son distintos. Afirmamos que $p(a_n) = a_1$.

La elección de n garantiza que $a_1, \ldots, a_n, a_{n+1}$ no son distintos. Por lo tanto $a_{i+1} = a_j$ para algún entero positivo j entre 1 y n. Si $j > 1$ entonces tendríamos que $a_j = p(a_{j-1})$ y $a_j = p(a_n)$, lo que es imposible puesto que p es una función biyectiva. Por lo tanto $j = 1$, y así $p(a_n) = a_1$. Sea $\sigma_1 = (a_1 \cdots a_n)$.

Sea T conjunto $S - \{a_1, a_2, \ldots, a_n\}$. Por lo tanto, si $x \in T$ se tiene que $p(x) \neq a_i$ con $a_i \in \{a_1, a_2, \ldots, a_n\}$, y de aquí que $p(x) \in T$. Podemos definir así la función $q : T \to T$ definida por $q(x) = p(x)$ para todo $x \in T$, y tiene una inversa bien definida por $q^{-1} : T \to T$ donde $q^{-1}(x) = p^{-1}(x)$. Se sigue que q es una permutación de T. La hipótesis de inducción garantiza que q o es la permutación identidad de T, o es un ciclo, o puede ser expresada como un producto dos o más ciclos disjuntos. Estos ciclos se extienden a permutaciones de S que fijan a los elementos $a_1, \ldots, a_n$ y estas permutaciones de S también son ciclos. Se sigue que o bien $p = \sigma_1$ (y q es la permutación identidad), o bien $p = \sigma_1 \cdots \sigma_m$, son ciclos disjuntos de S que fijan a $a_1, \ldots, a_n$ y que corresponden a ciclos de T. Luego el resultado sigue siendo válido para permutaciones de conjuntos con k elementos, y por el principio inductivo el teorema queda establecido. □

Lema 17. *Cada permutación de un conjunto finito con más de un elemento puede expresarse como una composición finita de transposiciones.*

Demostración. Cada ciclo puede ser expresado como una composición de transposiciones. De hecho, si $a_1, \ldots, a_n$ son los distintos elementos de un conjunto finito S entonces

$$(a_1 a_2 \cdots a_n) = (a_1 a_2)(a_2 a_3) \cdots (a_{n-1} a_n).$$

Se sigue de la anterior proposición que una permutación de S que no sea la permutación identidad puede ser expresada como una composición finita de transposiciones. Más aún la permutación identidad puede escribirse como la composición de cualquier transposición consigo misma, siempre que S tenga más de un elemento. El resultado queda probado. □

Teorema 6. *Una permutación de un conjunto finito no puede ser expresada simultáneamente como un producto de un número par de transposiciones y como un producto de un número impar de transposiciones.*

Demostración. Como el conjunto es finito podemos representarlo como el conjunto $\{1, \ldots, n\}$ donde n es el número de elementos del conjunto. Sea $F : \mathbb{Z}^n \to \mathbb{Z}$ la función que envía a cada n-ada $(m_1, \ldots, m_n)$ de enteros al producto $\prod_{i \leq j < k \leq n}(m_k - m_j)$ de las cantidades $m_k - m_j$ para todos los pares (j, k) de enteros que satisfacen $i \leq j < k \leq n$. Nótese que $F(m_1, \ldots, m_n)$ no se anula siempre que los enteros $m_1, \ldots, m_n$ sean distintos. Si se transponen dos elementos $m_1, \ldots, m_n$, el signo de F cambia, puesto que el número de factores del producto $\prod_{i \leq j < k \leq n}(m_k - m_j)$ que cambian su signo es impar. Por ejemplo,

si intercambiamos m_t y m_s con $1 \leq s < t < n$, entonces el factor $(m_t - m_s)$ cambia por $-(m_t - m_s)$, y los factores $m_t - m_i$ por $-(m_i - m_s)$, mientras que los factores $m_i - m_s$ cambian por $-(m_t - m_s)$. Así, todos los cambios de signo se cancelan excepto el de $-(m_t - m_s)$. Pero toda permutación σ del conjunto $\{1, 2, \ldots, n\}$ es un producto de transposiciones. Se sigue que a cada permutación σ le corresponde un número ε_σ tal que

$$F(m_{\sigma(1)}, \ldots, m_{\sigma(n)}) = \varepsilon_\sigma F(m_1, \ldots, m_n).$$

Por las propiedades del producto se sigue que $\varepsilon_{\sigma\tau} = \varepsilon_\sigma \varepsilon_\tau$ para cualesquiera permutaciones σ y τ. Por lo anteriormente discutido, si τ es una permutación, entonces $\varepsilon_\tau = -1$. Se sigue que si σ se expresa como una composición de r y s transposiciones, entonces $\varepsilon_\sigma = (-1)^r$ y $\varepsilon_\sigma = (-1)^s$, luego $(-1)^r = (-1)^s$, por lo que r y s deben diferir en un número par. Pero eso ocurre si, y sólo si, ambos son pares o impares, y el teorema queda demostrado. □

1.14. Ecuación de clases de un grupo finito

Definamos el conjunto

$$Z(G) = \{g \in G : gh = hg \text{ para todo } h \in G\}.$$

Es claro que los elementos de $Z(G)$ conmutan entre sí. Sea h un elemento arbitrario de G. Como e satisface que $eh = he = h$, tenemos que $Z(G)$ es no vacío. Sean g y f elementos de $Z(G)$. Entonces $(gf)h = g(fh) = g(hf) = (hf)g = h(fg) = h(gf)$, y también $(g^{-1}h)^{-1} = h^{-1}g = gh^{-1} = (hg^{-1})^{-1}$, luego $g^{-1}h = hg^{-1}$; de aquí que $Z(G)$ es un subgrupo de G, y además es abeliano.

Según la definición de $Z(G)$, $hgh^{-1} = hh^{-1}g = eg = g$, por lo que $hZ(G)h^{-1} = Z(G)$, esto es, $Z(G)$ es normal en G.

Definición. El conjunto $Z(G)$ se denomina centro de G.

Sea G un grupo finito. La relación de conjugación divide parte al conjunto G en clases de equivalencia disjuntas. Cada elemento de $Z(G)$ es una sola clase de equivalencia, y toda clase de equivalencia que consta de un solo elemento está en $Z(G)$, luego $Z(G)$ consiste en todos los elementos de G que son clases de equivalencia de un solo elemento, según lo visto en la sección de conjugación y por ser $Z(G)$ abeliano. Sean ahora r el número de clases de conjugación contenidas en $G - Z(G)$, y $n_1, \ldots, n_r$ el número de elementos de cada una. Como las clases de conjugación constituyen una partición, se tiene que $n_i > 1$ para $i = 1, \ldots, r$ y que

$$|G| = |Z(G)| + n_1 + \cdots + n_r.$$

A esta ecuación se le conoce como ecuación de clases del grupo G.

Proposición 6. *Sea G un grupo finito, y p un número primo. Supóngase que para algún k entero positivo p^k divide al orden de G. Entonces, o bien*

p^k *divide al orden de algún subgrupo propio de* G *o* p *divide al orden del centro de* G.

Demostración. Escojamos los elementos $g_1, \ldots, g_r$ de $G - Z(G)$, donde $Z(G)$ es el centro de G, tales que cada uno de ellos es un representante de cada una de las r clases de conjugación contenidas en $G - Z(G)$. Sea n_i el número de elementos de la clase de conjugación de g_i y sea $C(g_i)$ el centralizador de de g_i para $i = 1, \ldots, r$. Entonces $C(g_i) < G$, pues de otro modo $g_i \in Z(G)$, lo cual contradice su elección. Por lo tanto, $|G| = n_i \, |C(g_i)|$, pues por el teorema de Lagrange $|C(g_i)|$ divide a $|G|$, y además lo hace tantas veces como elementos tiene la clase de conjugación de g_i, esto es, n_i veces. Por lo tanto, si p^k divide al orden de G y no divide al orden de ningún subgrupo propio de G (en particular, $C(g_i)$), debe ser que divide a n_i, y así p divide a n_i, para cada $i = 1, \ldots, r$. Transpongamos la ecuación de clases

$$|G| - (n_1 + \cdots + n_r) = |Z(G)| \, .$$

se ve claramente que p divide a ambos términos del primer miembro de la ecuación anterior, luego p divide a $|Z(G)|$, como se quería demostrar. □

1.15. Teorema de Cauchy

Teorema 7 (Cauchy). *Si* G *un grupo finito y* p *un número primo que divide al orden de* G *entonces* G *contiene un elemento de orden* p.

Demostración. Para el grupo finito de orden 1 el aserto se cumple por vacuidad, pues no hay primo que divida al 1. Supongamos ahora que cada grupo finito cuyo orden es divisible por p y menor que $|G|$ contiene un elemento de orden p.

Si p divide al orden de algún subgrupo propio de G entonces ese subgrupo contiene al elemento requerido de orden p.

De no ser el caso y p no divide al orden de ningún subgrupo propio de G, por la proposición anterior se tiene que p divide al orden de $Z(G)$, luego $G = Z(G)$, por lo cual G es abeliano. Sea ahora un subgrupo H maximal de G. Si $|H|$ es divisible por p entonces la hipótesis de inducción asegura que H tiene un elemento de orden p. Supongamos entonces que $|H|$ no es divisible por p. Escojamos $g \in G - H$ y sea C el subgrupo cíclico de G generado por g. Como G es abeliano, $C \lhd G$, por lo que $HC \leq G$. Entonces $HC = G$, pues $HC \neq H$ al ser $H \subseteq HC$ y HC es un subgrupo de G. Por el primer teorema de isomorfismo

$$\frac{G}{H} \cong \frac{C}{H \cap C}.$$

Ahora p divide a $|G/H|$, pues $|G/H| = |G| \, / \, |H|$ y p divide a $|G|$, pero no a $|H|$. Por lo tanto p divide a $|C/H \cap C| = |C| \, / \, |H \cap C|$. Como $H \cap C \leq H$, entonces p no divide a $|H \cap C|$. Debe ser que p divide a C. Así si $m = |C| \, / p$, entonces g^m es el elemento requerido de orden p. El teorema de Cauchy queda probado. □

1.16. La estructura de los p-grupos

Definición. Sea p un número primo. Un p-grupo cuyo orden es alguna potencia p^k de p, donde k es un entero positivo.

En lo sucesivo p es un número primo.

Lema 18. *Sea* G *un* p*-grupo. Entonces existe un subgrupo normal de* G *de orden* p *que está contenido en el centro de* G.

Demostración. Sea $|G| = p^k$. Entonces p^k divide al orden del grupo pero no divide al orden de ningún subgrupo propio de G. Se sigue por una proposición anterior que p divide al orden de $Z(G)$. Se sigue del teorema de Cauchy que el centro de G contiene algún elemento de orden p. Este elemento genera un subgrupo cíclico de orden p, y este subgrupo es normal pues sus elementos conmutan con cada elemento de G. □

Proposición 7. *Sea* G *un* p*-grupo, y* H *un subgrupo propio de* G. *Entonces existe un subgrupo* K *de* G *tal que* $H \lhd K$ *y* K/H *es un grupo cíclico de orden* p.

Demostración. Si G es de orden 1, la proposición se cumple por vacuidad. Supongamos entonces que el resultado es válido para todos los p-grupos de orden menor o igual a G. Sea Z el centro de G. Entonces ZH es un subgrupo de G, pues Z es normal en G. Supongamos que $ZH \neq H$. Entonces H es un subgrupo normal de ZH. El grupo cociente ZH/H es un p-grupo (pues todos los subgrupos de G son p-grupos) y contiene un subgrupo K_1 de orden p, según el lema anterior. Sea $K = \{g \in ZH : gH \in K_1\}$, es decir, el grupo homomorfo a K_1 contenido en ZH. Entonces $H \lhd K$ y $K/H \cong K_1$, y así K es el subgrupo de G que se buscaba.

Finalmente supóngase que $ZH = H$. Entonces $Z \subset H$. Sea $H_1 = \{hZ : h \in H\}$. Entonces H_1 es un subgrupo de G/Z. Pero G/Z es un p-grupo, y $|G/Z| < |G|$, puesto que $|Z| \geq p$, según el lema anterior. La hipótesis de inducción garantiza la existencia de un subgrupo K_1 de G/Z tal que $H_1 \lhd K_1$ y K_1/H_1 es cíclico de orden p. Sea $K = \{g \in G : gZ \in K_1\}$. Entonces $H \lhd K$ y $K/H \cong K_1/H_1$. Luego K es el grupo solicitado. □

Por inducción se obtiene el siguiente resultado.

Corolario 6. *Sea* G *un* p*-grupo. Entonces existen subgrupos* $G_0, G_1, \ldots, G_n$ *de* G*, donde* G_0 *es el subgrupo trivial, y* $G_n = G$ *tales que* $G_{i-1} \lhd G_i$ *y* G_i/G_{i-1} *es un grupo cíclico de orden* p *para* $i = 1, 2, \ldots, n$.

1.17. Los teoremas de Sylow

Definición. Sea G un grupo finito tal que $|G|$ es divisible por p. Un p-subgrupo de G es un subgrupo cuyo orden es una potencia de p. Un p-subgrupo

de Sylow de G es un subgrupo cuyo orden es p^k, con k el máximo entero positivo tal que p^k divide a $|G|$.

Teorema 8 (Primer Teorema de Sylow). *Sea* G *un grupo finito, y sea* p *un divisor del orden de* G. *Entonces* G *contiene un* p*-subgrupo de Sylow.*

Demostración. Para el grupo trivial el teorema es válido por vacuidad. Supongamos entonces que el teorema se cumple para todos los grupos de orden menor al de G cuyo orden es divisible por p tienen al subgrupo de Sylow deseado. Sea k el mayor entero positivo para el cual p^k divide a $|G|$. Si p^k divide al orden de algún subgrupo propio H de G, por la hipótesis de inducción H tiene el p-subgrupo de Sylow requerido. Si p^k no divide al orden de ningún subgrupo propio de G, entonces p divide al orden de $Z(G)$, por una proposición anterior. Por el teorema de Cauchy, $Z(G)$ tiene un elemento de orden p, y este elemento engendra un subgrupo normal N de G de orden p. La hipótesis de inducción asegura que G/N tiene un p-subgrupo de Sylow L de orden p^{k-1}, pues $|G/N| = |G|/p$. Sea $K = \{g \in G : gN \in L\}$. Entonces $|K| = p\,|L| = p^k$, y así K es el p-subgrupo de Sylow de G buscado. □

Teorema 9 (Segundo Teorema de Sylow). *Sea* G *un grupo finito, y sea* p *un divisor del orden de* G. *Se cumplen:*

1. *Todos los* p*-subgrupos de Sylow de* G *son conjugados.*
2. *Cualquier* p*-subgrupo de* G *está contenido en algún* p*-subgrupo de Sylow de* G.
3. *Si* r *el número de* p*-subgrupos de Sylow en* G, *entonces* r *divide al orden de* G *y* $r \equiv 1\,(\mathrm{mod} p)$.

Demostración. Sea K un p-subgrupo de Sylow de G, y sea X el conjunto de las clases izquierdas de K en G. Sea H un p-subgrupo de G. Entonces H actúa sobre X a la derecha, donde $h(gK) = (hg)K$ para todo $h \in H$ y $g \in G$. Más aún, $h(gK) = gK$ si y sólo si $g^{-1}hg \in K$. Así, un elemento gK de X es fijo bajo H si y sólo si $g^{-1}Hg \subset K$.

Sea $|G| = p^k m$, donde k y m son enteros positivos y m es coprimo con p. Sea $|K| = p^k$. El número de clases laterales izquierdas de K en G es $|G|/|K| = m$, luego el conjunto X tiene m elementos. Por lo tanto el número de elementos de cualquier órbita (para la acción de H sobre X) divide al orden de H, puesto que es el índice en H del estabilizador de algún elemento de esa órbita. Pero el número de elementos en cada órbita debe ser alguna potencia de p, pues H es un p-grupo. Por lo tanto, si un elemento de X no queda fijo bajo H entonces el número de elementos de su órbita es divisible por p. Pero X es la unión disjunta de órbitas bajo la acción de H. Por lo tanto, si m' denota al número de elementos de X que quedan invariantes por H, entonces $m - m'$ es divisible por p.

Sin embargo, m no es divisible por p. Se sigue m' no es nulo y que m' no es divisible por p. Luego existe al menos un elemento g de G tal que $g^{-1}Hg \subset K$. Pero entonces H está contenido en el p-subgrupo de Sylow gKg^{-1}. Por lo tanto cada p-subgrupo está contenido en un p-subgrupo de Sylow de G, y este p-subgrupo de Sylow es conjugado con el p-subgrupo de Sylow K dado. En particular, cualesquiera dos p-subgrupos de Sylow son conjugados.

Sólo resta probar que el número r de p-subgrupos de Sylow de G divide al orden de G y que $r \equiv 1 \,(\mathrm{mod} p)$. Al aplicar lo examinado anteriormente con $H = K$, vemos que $g^{-1}Kg = K$ para algún $g \in G$ si, y sólo si, gK es un punto fijo de la acción de K en X. Pero el número de elementos de G para los cuales gK es un punto fijo es $m'|K|$, donde m' es el número de puntos fijos en X. Se sigue que el número de elementos de G para los cuales $g^{-1}Kg = K$ es $p^k m'$. Pero cada p-subgrupo de Sylow es de la forma $g^{-1}Kg$ para algún $g \in G$. En consecuencia el número r de p-subgrupos de Sylow en G está dado por $r = |G|/p^k m' = m/m'$. En particular, r divide a $|G|$. Pero ya sabemos que $m - m'$ es divisible entre p, pues m' es coprimo con p, al serlo también m y p. También $m - m'$ es divisible entre m', pues $\frac{m-m'}{m'} = \frac{m}{m'} - 1 = r - 1$. Juntando todo, vemos que $m - m'$ es divisible por $m'p$, por lo cual p divide a $r - 1$, esto es, $r \equiv 1 \,(\mathrm{mod} p)$, y la demostración termina. $\square$