UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA

DEPARTAMENTO DE MATEMATICA

"EXTENSION DE LOS TEOREMAS DE SYLOW"

TRABAJO PRESENTADO POR:

JOSE ROBERTO VEGA CEA

PARA OPTAR AL GRADO DE:

LICENCIADO EN MATEMATICA

Enero de 1978

San Salvador, El Salvador, Centro América

UNIVERSIDAD DE EL SALVADOR

RECTOR: HONORABLE CONSEJO DE ADMINISTRACION PROVISIONAL DE LA UNIVERSIDAD DE EL SALVADOR

SECRETARIO GENERAL: DR. RAFAEL ANTONIO OVIDIO VILLATORO

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO: ARQ. MANUEL ENRIQUE ALFARO

SECRETARIO: ING. LUIS A. CARBAJAL VALDEZ

DEPARTAMENTO DE MATEMATICA

JEFE DEL DEPARTAMENTO: ING. GABRIEL MELENDEZ MAYORGA

ASESOR: LIC. JOSE JAVIER RIVERA LAZO

INDICE

CAPITULO I

DEFINICIONES, CONCEPTOS Y PROPOSICIONES FUNDAMENTALES

CAPITULO II

TEOREMAS DE SYLOW

CAPITULO III

EXTENSION DE LOS TEOREMAS DE SYLOW

INTRODUCCION

El objetivo principal de este trabajo es presentar una generalización de los Teoremas de Sylow en los grupos solubles, pero, como es natural, para mostrar esta generalización, es necesario dar a conocer primero en que consisten tales teoremas y además estudiar algunas de sus aplicaciones más elementales en teoría de grupos.

Por lo anteriormente expuesto, es que nos hemos ocupado en el primer capítulo, en sentar las bases e introducir los conceptos fundamentales que nos servirán para desarrollar el segundo y parte del tercero.

En el último capítulo, se dan a conocer primero los conceptos de redes, series subinvariantes y principales, para luego, definir la estructura de grupo soluble y poder por último, abordar el tema principal -- que es la "Extensión de los Teoremas de Sylow".

CAPITULO I

DEFINICIONES, CONCEPTOS Y PROPOSICIONES FUNDAMENTALES

Un conjunto y una o más operaciones definidas en él, o que lo vinculan con otro conjunto, pueden constituir según las propiedades que cumpla o cumplan esa o esas operaciones, una estructura algebraica determinada.

Estudiadas las propiedades de una estructura, ellas son aplicables a todos los conjuntos que junto con las operaciones definidas en ellos o que los relacionan con otro conjunto, tengan esa misma estructura, lo cual facilita y simplifica notablemente su estudio.

Algunas de las estructuras algebraicas más conocidas son: Monoide, Semigrupo, Grupo, Anillo, Cuerpo y Espacio Vectorial.

En nuestro trabajo trataremos casi exclusivamente con grupos.

DEFINICION 1.1

Un conjunto G no vacío se dice que forma un grupo si en él está definida una operación binaria $*$, generalmente llamada producto tal que:

i) $a, b \in G$ implica que $a*b = c$; $c \in G$ (Ley de Cierre).

ii) $a, b, c \in G$ implica que $a*(b*c) = (a*b)*c$ (Ley Asociativa).

iii) Existe un elemento $e \in G$ tal que $a*e = e*a = a$ para todo $a \in G$. (Existencia del elemento identidad).

iv) Para todo $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a*a^{-1} = a^{-1}*a = e$. (Existencia de elemento inverso en G).

Algunos ejemplos de grupos son los siguientes

1º. Supongamos que G está constituído por el conjunto de los números enteros, Z con a*b, para a, b ∈ G, definida como la suma usual entre números enteros.

2º. Tomemos a G como el conjunto de los números racionales menos el cero, Q - {0} con a*b, para a, b ∈ G definida como el producto usual entre números racionales.

3º. Consideremos a G constituído por los números reales menos el menos uno, ℝ - {-1} con a*b, para a, b ∈ G, definida así: a*b = a + b + ab.

4º. Sea G el conjunto de los números racionales menos el cero, Q - {0} - con a*b, para a, b ∈ G, definida así: $a*b = \frac{ab}{2}$.

DEFINICION 1.2

Un grupo G se dice que es abeliano o conmutativo si para cualesquiera a, b ∈ G se tiene: a*b = b*a.

Un grupo que no es abeliano se llama no abeliano.

Como ejemplos de grupos abelianos podemos citar:

1º. El conjunto {0, 1, 2, 3} y la suma modular, módulo cuatro.

2º. El grupo formado por el conjunto {1, -1} y la multiplicación entre números reales.

3º. Sea $A \neq \phi$ y $P(A) = \{x/\ x \subset A\}$ y * una operación binaria definida en P(A) así: $X*Y = (X \cup Y) - (X \cap Y)$

Un subconjunto de los elementos de un grupo G, puede él mismo formar un grupo con respecto al producto definido en G. Este subconjunto

de elementos H se llama un subgrupo de G.

En cualquier grupo G la identidad e satisface $e^2 = e$. Además, si x es un elemento de G tal que $x^2 = x$, entonces $x = x^{-1} * (x^2) = x^{-1} * x = e$. Entonces la identidad de un subgrupo H, como ha de satisfacer $x^2 = x$, debe ser la misma que la identidad del grupo G.

En lo sucesivo por comodidad escribiremos la identidad e = 1 y $x*y = xy$.

TEOREMA 1.1

Un subconjunto no vacío H de un grupo G es un subgrupo si satisface las condiciones siguientes:

i) Si $a \in H$, $b \in H$, entonces $ab \in H$.

ii) Si $a \in H$, entonces $a^{-1} \in H$.

RPUEBA:

La condición uno garantiza la condición de cierre en H. La condición dos y la uno garantizan que la identidad está en H y además la condición dos afirma la existancia de inversos en H. Como los elementos en H están en G, entonces satisfacen la ley asociativa.

Un grupo G es llamado finito si está constituído por un número finito de elementos, de lo contrario es llamado infinito.

Como en algunos casos los hechos son totalmente diferentes para grupos finitos que para grupos infinitos, entonces aclaramos que en adelante trataremos con grupos finitos mientras no se diga lo contrario.

Para un subgrupo H de un grupo G defínese como clase lateral izquierda de H en G, al conjunto de elementos de la forma ha, h $\in$ H, a $\in$ G, a fijo. Para designar este conjunto escribimos Ha. En la misma forma, al conjunto de todos los elementos ah, con todos los h $\in$ H, a $\in$ G, a fijo, se llama clase lateral derecha de H en G y se nota aH.

TEOREMA 1.2

Dos clases laterales izquierdas de H en G son disjuntas o son idénticas.

PRUEBA

Sean las clases laterales Ha y Hb. Si Ha $\cap$ Hb = ϕ, no hay nada que probar. Supongamos entonces que Ha $\cap$ Hb $\neq$ ϕ, esto implica que existe c $\in$ Ha y c $\in$ Hb. Entonces $c = h_1 a$ y $c = h_2 b$ por lo que $h_1 a = h_2 b$ y $a = h_1^{-1} h_2 b$, $ha = h\, h_1^{-1} h_2 b$, $ha = h'b$ lo que implica que Ha c Hb. En la misma forma $b = h_2^{-1} h_1 a$ y $hb = h_2^{-1} h_1 a = h'a$, por lo que Hb c Ha. Luego Ha = Hb.

TEOREMA 1.3

Una claee lateral izquierda de H en G, tiene el mismo número de elementos que H.

PRUEBA

Sea Ha una clase lateral izquierda de H en G. Definamos la función ψ tal que ψ: H $\to$ Ha: h $\rightsquigarrow$ ha. Supongamos que para h_1, h_2 $\in$ H $\psi(h_1) = \psi(h_2)$, por lo que $h_1 a = h_2 a$ y $h_1 = h_2$ y ψ es inyectiva.

Ahora supongamos que tenemos b $\in$ Ha, luego b será de la forma $b = h_1 a = \psi(h_1)$ y ψ es sobreyectiva. Luego ψ es una biyección y por lo - tanto H y Ha tienen el mismo número de elementos.

Para las clases laterales derechas las pruebas son análogas.

El elemento $x = x1 = 1x$ pertenece a las clases laterales xH y Hx y se llama el representante de la clase lateral. Cualquier elemento $u \in Hx$ puede tomarse como representante puesto que por el Teorema 1.2 $Hu = Hx$.

Dado un grupo G y dos subgrupos H y K, no necesariamente distintos, al conjunto de elementos HaK, donde a es algún elemento fijo de G, se le llama clase lateral doble.

TEOREMA 1.4

Dos clases laterales dobles HaK y HbK son disjuntas o idénticas.

PRUEBA

Sea c $\in$ HaK y c $\in$ HbK, entonces $c = h_1 a k_1 = h_2 a k_2$, $a = h_1^{-1} h_2 b k_2 k_1^{-1}$, $hak = h h_1^{-1} h_2 b k_1 k_1^{-1} k$, luego Hak c Hbk. Por análogo razonamiento Hbk c Hak. Por lo que Hak = Hbk.

Una clase lateral doble H x K contiene todas las clases laterales izquierdas de H de la forma H x k y todas las clases laterales derechas de K de la forma h x K. Además H x K está constituído por la unión de todas - las clases laterales H x k y todas las clases laterales h x K.

TEOREMA 1.5

Sea G un grupo, H un subgrupo de G, y x, y $\in$ G. Entonces Hx = Hy si y solamente si $xy^{-1} \in H$.

PRUEBA

Asumamos que Hx = Hy. Entonces $x = 1x \in Hx = Hy$, luego x = hy para algún h $\in$ H. De donde $xy^{-1} = h \in H$. Ahora asumamos que $xy^{-1} \in H$. Entonces existe h $\in$ H tal que $xy^{-1} = h$ y x = hy. Tomemos $h_1 \in H$, entonces $h_1x = h_1hy$, por lo que Hx c Hy. Ahora veamos que si $xy^{-1} \in H$, también $(xy^{-1})^{-1} = y\,x^{-1} \in H$ y por igual razonamiento Hy c Hx. Luego Hx = Hy.

TEOREMA 1.6

Sea H un subgrupo de un grupo G. Entonces existe una biyección entre las clases laterales derechas de H en G y las clases laterales izquierdas de H en G.

PRUEBA

Definamos la función

$$\psi: \{Hx/\ x \in G\} \longrightarrow \{xH/\ x \in G\}$$

$$Hx \rightsquigarrow x^{-1}H$$

Veamos primero que la función ψ está bien definida. Si Hx = Hy, entonces por el Teorema 1.5, $x\,y^{-1} \in H$, lo que implica que $y\,x^{-1} \in H$ y por el mismo Teorema 1.5 $x^{-1}H = y^{-1}H$. Luego la función está bien definida. Si x, y $\in$ G con $\psi(Hx) = \psi(Hy)$, entonces $x^{-1}H = y^{-1}H$ y nuevamente por el teorema 1.5 $(x^{-1})^{-1}y^{-1} = x\,y^{-1} \in H$ de lo que se sigue por el mismo Teorema que Hx = Hy y la función es inyectiva.

Ahora tomemos x H $\in$ {xH/ x $\in$ G}, entonces xH = $(x^{-1})^{-1}H = \psi(Hx^{-1})$. Luego ψ es sobreyectiva y por lo tanto biyectiva.

Por lo visto en el Teorema anterior podemos afirmar que el número de clases laterales derechas de un subgrupo H en un grupo G es igual al número de clases laterales izquierdas de H en G.

Llámase índice de H en G al número cardinal r de clases laterales izquierdas o derechas de un subgrupo H en un grupo G y se nota [G: H].

Llámase orden de un grupo G al número cardinal n de elementos de G.

TEOREMA 1.7 (Teorema de Lagrange)

El orden de un grupo G es el producto del orden de un subgrupo H de G y el índice de H en G.

PRUEBA

El índice, r = [G: H], de H en G es el número de clases laterales izquierdas o derechas de H en G y por Teorema 1.3 una clase lateral de H en G, tiene el mismo número de elementos que H, que es el orden de H. Luego el orden de G es igual al producto de [G: H] por el orden de H.

TEOREMA 1.8

Sea G un grupo y H y K dos subgrupos de G tales que K c H c G, entonces [G: K] = [G: H][H: K].

PRUEBA

Como H es subgrupo de G y K es subgrupo de H entonces

$$G = H \cup Hx_2 \cup Hx_3 \cup \ldots\ldots \cup Hx_s \qquad y$$

$$H = K \cup Ky_2 \cup Ky_3 \cup \ldots\ldots \cup Ky_r$$

y

$$Hx_i \cap Hx_j = \phi, \quad i \neq j$$

$$Ky_i \cap Ky_j = \phi, \quad i \neq j$$

Luego, para $g \in G$, $g = hx_j$, $h \in H$, de forma única, y $h = Ky_i$, $k \in K$, también en forma única. Entonces las clases laterales de K en G serán Ky_ix_j, $i = 1, 2, \ldots, r$, $j = 1, 2, \ldots, s$. Para que dos de estas clases laterales sean iguales, tendrán que pertenecer a la misma clase lateral de H, luego tener el mismo x_j. Si multiplicamos Ky_ix_j por x_j^{-1} a la derecha, se ve que estas también habrían de tener la misma y_i. Entonces las clases laterales de K en G están dadas por Ky_ix_j, y estas son diferentes, por lo que $[G: K] = [G: H][H: K]$.

DEFINICION 1.3

Un grupo G es llamado cíclico si existe un elemento $a \in G$, a fijo, tal que todo elemento $x \in G$, es igual a una potencia a^i.

Si se da el caso en que todas las potencias de un elemento de $a \in G$ son distintas, entonces el número de elementos de G es indefinido y se dice que G es de orden infinito. Si es el caso de que no todas las potencias de a son distintas entonces se tendrá el caso $a^m = a^t$ con $m > t$ y m y t enteros, por lo que $a^{m-t} = 1$ con m-t positivo.

Si llamamos m al menor de los enteros positivos tal que $a^n = 1$, entonces se ve que los elementos del grupo son 1, a, a^2, ..., a^{n-1} y que su número es finito, por lo que se dice que el grupo G es de orden finito.

DEFINICION 1.4

Llamamos orden de un elemento $a \in G$ al orden del grupo cíclico $\langle a \rangle$ generado por el elemento.

TEOREMA 1.9

Sea G un grupo tal que $G \neq \{1\}$. Entonces G es un grupo cíclico de orden primo sí y sólo si G no tiene ningún subgrupo excepto él mismo y la identidad.

PRUEBA

Si G es un grupo cíclico de orden primo p, entonces por el teorema de Lagrange, G no puede tener subgrupos cuyo orden no sea p ó 1, y estos solo pueden ser el mismo G y {1}. Ahora si $G \neq \{1\}$ y además sus únicos subgrupos son él mismo y {1}, entonces existe $a \neq 1$, $a \in G$ tal que el grupo cíclico generado por a, $\langle a \rangle \neq \{1\}$ y por lo tanto $\langle a \rangle = G$. Además si a es de orden infinito, entonces a^2 genera un subgrupo propio, que es el que sus elementos son de la forma a^{2i}. Luego a es por fuerza de orden finito, n, y $a^n = 1$. Si n es primo la prueba está concluída, pero si no lo es, entonces $n = uv$, $u > 1$, $v > 1$ y entonces las potencias de a^u generan un subgrupo propio de orden v, por lo que n tiene que ser por fuerza primo y G un grupo cíclico finito de orden primo.

TEOREMA 1.10

Si A y B son subgrupos de un grupo G entonces $A \cap B$ es subgrupo de G.

PRUEBA

Sean $a, b \in A \cap B$, entonces $a, b \in A$ y $a, b \in B$, luego $ab \in A$ y $ab \in B$, lo que implica que $ab \in A \cap B$. Además si $a \in A \cap B$, entonces $a \in A$ y $a \in B$, luego $a^{-1} \in A$ y $a^{-1} \in B$, por lo que $a^{-1} \in A \cap B$, y por Teorema 1.1 afirmamos que $A \cap B$ es subgrupo de G.

DEFINICION 1.5

Si A y B son subgrupos de un grupo G, llamamos juntura de A y B al conjunto de todos los productos finitos $g_1 . g_2 . \ldots . g_s$, donde cada g_i pertenece a A ó B. Este conjunto lo representamos escribiendo $A||B$.

TEOREMA 1.11

Si A y B son subgrupos de un grupo G. Entonces $A||B$ es subgrupo de G.

PRUEBA

Sea $a_1 . \ldots . a_s \in A||B$ y $b_1 . b_2 . \ldots . b_r \in A||B$, entonces $a_1 . a_2 . \ldots . a_s . b_1 . b_2 , \ldots . b_r$ es el producto finito de s+r elementos de G en donde cada uno de ellos pertenece a A ó B, por lo que $a_1 . a_2 . \ldots . a_s . b_1 . b_2 . \ldots . b_r \in A||B$. Además si $g_1 . g_2 . \ldots . g_s \in A||B$ entonces $g_s^{-1} \ldots g_2^{-1} . g_1^{-1} \in A||B$, ya que cada g_i^{-1} pertenece a A ó B según

que g_i pertenezca a A ó B, y $g^{-1} \cdot \ldots \cdot g_2^{-1} g_1^{-1}$ es el inverso de $g_1 g_2 \cdots g_s$, puesto que

$g_1 g_2 \cdots g_s g_s^{-1} \cdots g_2^{-1} g_1^{-1} = g_s^{-1} \cdots g_2^{-1} g_1^{-1} g_1 g_2 \cdots g_s^{-1} = 1$. Luego por teorema 1.1 $A||B$ es subgrupo de G.

TEOREMA 1.12

Si A y B son subgrupos de un grupo G. Entonces

$[A||B: B] \geq [A: A \cap B]$.

PRUEBA

Sea $A \cap B = D$, entonces $D \subset A$ y por Teorema 1.10, D es subgrupo de G.

Sea $A = D \cup Dx_2 \cup Dx_3 \cup \ldots \cup Dx_r$ con $Dx_i \cap Dx_j = \phi$ para $i \neq j$, y $x_i \in A$. Podemos afirmar entonces que las clases laterales $B, Bx_2, \ldots, Bx_r$ son todas distintas en $A||B$. En efecto si $Bx_i = Bx_j$, $i \neq j$, entonces $x_i = b x_j$ con $b \in B$. Pero x_i y x_j pertenecen ambos a A, luego por ello también $b \in A$, de donde $b \in A \cap B = D$; luego las clases laterales Dx_i y Dx_j tienen en común el elemento $x_i = b x_j$, lo cual es contrario a lo supuesto.

TEOREMA 1.13

Si A y B son subgrupos de un grupo G, y si $[A||B: B]$ y $[A||B: A]$ son finitos y primos relativos, entonces $[A||B: B] = [A: A \cap B]$ y $[A||B: A] = [B: A \cap B]$.

PRUEBA

Por Teorema 1.8 afirmamos que

$$[A||B: A\cap B] = [A||B: B][B: A\cap B] = [A||B: A][A: A\cap B],$$

y por Teorema 1.12 afirmamos que $[A||B: B] \geq [A: A\cap B]$. Por hipótesis sabemos que $[A||B: B]$ y $[A||B: A]$ son primos relativos, entonces en la relación $[A||B: B][B: A\cap B] = [A||B: A][A: A\cap B]$, resulta que $[A||B: B]$ divide a $[A: A\cap B]$, lo que implica que $[A||B: B] \leq [A: A\cap B]$, luego concluimos que $[A||B: B] = [A: A\cap B]$ y por análogo razonamiento $[A||B: A] = [B: A\cap B]$.

DEFINICION 1.6

Si S es un conjunto cualquiera de elementos de un grupo G, y $x \in G$, entonces llamamos transformado de S por x al conjunto S^x cuyos elementos son de la forma $x^{-1} s x$, donde $s \in S$.

TEOREMA 1.14

Si S es subconjunto de un grupo G, $S \neq \phi$. Entonces S y S^x contienen el mismo número de elementos.

PRUEBA

Definamos la función $\psi: S \to S^x$: $s \rightsquigarrow x^{-1} s x$, Tomemos $\psi(s_1) = \psi(s_2)$, entonces $x^{-1}s_1x = x^{-1}s_2x$, $xx^{-1}s_1xx^{-1} = xx^{-1}s_2xx^{-1}$, $s_1 = s_2$, luego ψ es inyectiva. Tomemos $y \in S^x$, entonces por definición de S^x, y es de la forma $y = x^{-1} s x$, $s \in S$, luego $y = \psi(s)$, luego ψ es sobreyectiva y por lo tanto es una bi

yección entre S y S^x, de modo que S y S^x deben tener el mismo número de elementos.

DEFINICION 1.7

Si S y S' son dos conjuntos en G, H es un subgrupo de G, y existe algún $x \in H$ tal que $S' = S^x$, entonces decimos que S y S' son conjugados respecto a H.

Puede probarse que la relación de conjugación respecto a H es de equivalencia.

TEOREMA 1.15

Todo conjunto conjugado de un subgrupo de un grupo G es también un subgrupo de G.

PRUEBA

Sean H y K subgrupos de un grupo G y S un conjunto de elementos de G, tal que $S = K^x$, $x \in H$. Tomemos s_1 y s_2 que pertenecen a S, entonces $s_1 = x^{-1}k_1x$ y $s_2 = x^{-1}k_2x$ con k_1 y k_2 en K.

$s_1s_2 = x^{-1}k_1x\, x^{-1}k_2x = x^{-1}k_1k_2x$ y $k_1k_2 \in K$ por ser K subgrupo de G. Entonces $s_1s_2 \in S$. Además si $s \in S$ y $s = x^{-1}kx$, entonces existe $k^{-1} \in K$ y $s^{-1} = x^{-1}k^{-1}x$, $ss^{-1} = x^{-1}kx\, x^{-1}k^{-1}x = 1$. Luego por Teorema 1.1, S es subgrupo de G.

Si $x^{-1}Sx = S$, entonces $S = xSx^{-1}$. Si también $y^{-1}Sy = S$, entonces $S = (xy)^{-1}S(xy)$. Luego el conjunto de todos los $x \in H$ tales que

$S^x = S$ es un subgrupo de H al que llamaremos el normalizador de S en H y lo representaremos por $N_H(S)$.

También el conjunto de todos los $x \in H$ tales que $x^{-1}sx = s$ - para todo $s \in S$, puede mostrarse de modo análogo que es un subgrupo de H al que llamaremos el centralizador de S en H y lo representaremos por $C_H(S)$. Observamos que si S consta de un solo elemento, entonces el normalizador y el centralizador son idénticos. Cuando $H = G$ es habitual hablar simplemente del normalizador y del centralizador de S. Al centralizador de G en G se le llama el centro de G. Si $x \in C_H(S)$, entonces $x^{-1}sx = s$, para todo $s \in S$, lo que implica que $x^{-1}Sx = S$ y $x \in N_H(S)$, por lo que $C_H(S) \subset N_H(S)$.

TEOREMA 1.16

El número de conjugados de S respecto a H es el índice en H del normalizador de S en H.

PRUEBA

Escribamos $N_H(S) = D$ y supongamos que $H = D \cup Dx_2 \cup \ldots \cup Dx_r$, $r = [H: N_H(S)]$.

Entonces $x^{-1}Sx = y^{-1}Sy$, $x, y \in H$ si y sólo si, $S = (yx^{-1})^{-1} S(yx^{-1})$; es decir, $yx^{-1} \in D$ o $y \in D_x$.

Por lo que dos conjugados de S respecto a H son iguales si y sólo si los elementos transformantes pertenecen a la misma clase lateral izquierda de D. De donde deducimos que el número de conjudados distintos es el índice de D en H.

DEFINICION 1.8

Un subgrupo H de un grupo G es llamado subgrupo normal de G si $N_G(H) = G$, o sea que $x^{-1}Hx = H$ para todo $x \in G$.

TOEREMA 1.17

Si T es subgrupo normal de un grupo G, entonces el conjunto H cuyos elementos son las clases laterales izquierdas de T en G, y el producto de clases laterales izquierdas definido por $(Tx_i)(Tx_j) = Tx_k$, si $x_ix_j \in Tx_k$, tiene estructura de grupo.

PRUEBA

Probaremos que el producto está bien definido. Tomemos t_1x_i y t_2x_j, elementos arbitrarios de Tx_i y Tx_j respectivamente. Por ser T subgrupo normal: $t_1x_it_2x_j = t_1x_it_2x_i^{-1}x_ix_j = t_1x_ix_i^{-1}t_4x_ix_j =$

$t_1t_4x_ix_j = t_3x_ix_j$.

Pero si $x_ix_j \in Tx_k$, también $t_3x_ix_j \in Tx_k$.

Luego todos los productos de un elementos de Tx_i y un elemento de Tx_j -- son elementos de una misma clase lateral Tx_k. Entonces el producto depende solamente de las clases laterales y no de la elección de representantes; por lo que el producto en H está bien definido.

Como el producto está bien devinido, entonces $(T)(Tx_i) = Tx_i$ y $(Tx_i)(T) = (T)(Tx_i) = Tx_i$. Luego en H la identidad es T. El producto es asociativo, ya que $(Tx_i\ Tx_j)Tx_k = Tx_ix_j\ Tx_k = Tx_ix_jx_k = Tx_i\ Tx_jx_k =$

$Tx_i(Tx_j\ Tx_k)$.

Además, si $x_i^{-1} \in Tx_j$, entonces $Tx_i\ Tx_j$ contiene a $x_i x_i^{-1} = 1$ y $Tx_i\ Tx_j = T$. Luego en H, Tx_j es el inverso de Tx_i ya que también $Tx_j\ Tx_i$ contienen a $x_i^{-1} x_i = 1$ y $Tx_j\ Tx_i = T$. Ahora podemos afirmar que H es un grupo.

Al grupo H cuyos elementos son todos las clases laterales de un subgrupo normal T, de un grupo G, en G, le llamaremos grupo factor de G con respecto a T y lo representaremos $H = \frac{G}{T}$.

TEOREMA 1.18

Sea T un subgrupo normal de un grupo G. Hay entonces una correspondencia biunívoca entre los subgrupos K^* de $H = \frac{G}{T}$ y los subgrupos K de G tales que $G \supseteq K \supseteq T$, donde K consiste en todos los elementos de G mapeados sobre elementos de K^*. Si K^* es normal en H, entonces K es normal en G y recíprocamente. Además $[G: K] = [H: K^*]$.

PRUEBA

Sea la función

$$\psi: \{K/\ K \text{ es subgrupo de } G,\ K \supseteq T\} \to \{K^*/\ K^* \text{ es subgrupo de } H\}$$

$$K \rightsquigarrow K^* = \psi(K) = \{k\ T/\ k \in K\}$$

En esta función, la imagen de K, K subgrupo de G es, trivialmente, un subgrupo de H. Ahora, si K^* es un subgrupo de H, la imagen inversa K de K^*, contendrá a T, que es la imagen inversa de 1.

También la imagen inversa satisface trivialmente los requerimientos para ser subgrupo de G.

De aquí se deduce que la imagen inversa de un subgrupo K^* de H es un subgrupo único K tal que $G \supseteq K \supseteq T$, y la misma K^* es la imagen única

de K en la aplicación ψ. De aquí que $K \rightleftarrows K^*$ es una coreespondencia biunivoca entre $\{K/\ G \supseteq K \supseteq T\}$ y $\{K^*/\ H \supseteq K^* \supseteq 1\}$.

Si K^* es normal en H, entonces, puesto que $x^{-1}Tx = T \subseteq x^{-1}Kx$, se le puede aplicar la función a $x^{-1}Kx$ y $x^{-1}Kx \to x^{-1}K^*x^* = K^*$, de donde $x^{-1}Kx \subseteq K$ para caalquier x. Luego K es normal en G. De nuevo si K es normal en G, la normalidad de su imagen K^* en H es trivial. Finalmente -- probaremos que existe una biyección entre las clases laterales de un sub - grupo K en G y las clases laterales de su imagen K^* en H. En efecto, consideremos la función:

$$\psi: \{gK/\ g \in G\} \longrightarrow \{g^*K^*/\ g^* \in H\}$$

$$gK \rightsquigarrow g^*K^* = \{gT\ kT/\ k \in K\}$$

$$= \{gkT/\ k \in K\}$$

Tomemos $g_1^*K^* = g_2^*K^*$, entonces $\{g_1kT/\ k \in K\} = \{g_2kT/\ k \in K\}$.

Sea $g_1k_1 \in g_1K$, esto implica que $g_1k_1T \in \{g_1kT/\ k \in K\}$, por lo que $g_1k_1T \in \{g_2kT/\ k \in K\}$. Luego existe un $k_2 \in K$ y $t \in T$ tales que $g_1k_1 = g_2k_2t$, $k_2t \in K$. De donde $g_1k_1 \in g_2K$ y por lo tanto $g_1K \subseteq g_2K$. Por idéntico razonamiento $g_2K \subseteq g_1K$, por lo que $g_1K = g_2K$ y ψ es inyectiva. Ahora tomemos un $A \in \{g^*K^*/\ g^* \in H\}$, entonces A es de - la forma $A = \{g\,kT/\ k \in K,\ g \in G,\ g$ fijo$\}$ y $A = \psi(gK)$, por lo que ψ es sobreyectiva. Luego ψ es una iiyección. De donde $[G: K] = [H: K^*]$.

DEFINICION 1.9

Una aplicación ψ de un grupo G en un grupo H se dice que es un homomorfismo si para a, b $\in$ G cualesquiera siempre se tiene que $\psi(ab) = \psi(a)\,\psi(b)$.

EJEMPLO

$\psi: G \to G: \; x \rightsquigarrow x$ para todo $x \in G$ es un homomorfismo de G en G puesto que si x, y $\in$ G, $\psi(xy) = xy = \psi(x)\,\psi(y)$.

DEFINCION 1.10

Si ψ es un homomorfismo de un grupo G en un grupo H, entonces se llama núcleo de ψ, K_ψ, al conjunto $K_\psi = \{x \in G / \psi(x) = 1, \; 1 \in H\}$.

Si un homomorfismo cumple ser una inyeccción y sobreyección, entonces se le llama isomorfismo.

Un homomorfismo de un grupo G en si mismo se llama un endomorfismo de G u operador sobre G.

En un grupo G, si un endomorfismo cumple a la vez ser isomorfismo, entonces es llamado automorfismo.

Un automorfismo α_a de la forma $\alpha_a: x \to a^{-1}xa$ para todo $x \in G$ se denomina automorfismo interior.

Dos grupos G y H, entre los cuales se puede establecer un isomorfismo son llamados isomorfos.

DEFINICION 1.11

Un subgrupo H de un grupo G se dice que es admisible con respecto a una familia de endomorfismos Ω si para todo endomorfismo $\alpha \in \Omega$, $\alpha(H) \subseteq H$.

Si A y B son dos subgrupos admisibles con respecto a una fami - lia de endomorfismos Ω entonces para $\alpha \in \Omega$ y $x \in A||B$ se tiene que $\alpha(x) = \alpha(g_1 g_2 \ldots g_s)$ con $g_i \in A$ ó $g_i \in B$, $\alpha(x) = \alpha(g_1)\alpha(g_2)\ldots\alpha(g_s)$ - con $\alpha(g_i) \in A$ ó $\alpha(g_i) \in B$. Luego $\alpha(x) \in A||B$ y $\alpha(A||B) \subseteq A||B$, por lo que las junturas de grupos admisibles son subgrupos admisibles. Además si $\alpha \in \Omega$ y $x \in A \cap B$, entonces como $x \in A$ y $x \in B$, $\alpha(x) \in A$ y $\alpha(x) \in B$. Luego $\alpha(x) \in A \cap B$ y $\alpha(A \cap B) \subseteq A \cap B$ y las intersecciones de subgrupos admisibles son también subgrupos admisibles.

DEFINICION 1.12

Dos grupos A y B son llamados operadores isomorfos si hay una co rrespondencia $A \rightleftarrows B$ y también $\alpha_i \rightleftarrows \beta_i$ entre los grupos y los peeradores sobre ellos tal que $a \rightleftarrows b$ es un isomorfismo y $\alpha_i(a) \rightleftarrows \beta_i(b)$ en este isomorfismo.

TEOREMA 1.19

Dado un grupo G y un conjunto Ω de operadores sobre G, suponga - mos que A es un subgrupo admisible de G y T un subgrupo adminisle normal. Entonces $A \cap T$ es un subgrupo admisible normal de A y los grupos factores $\frac{A||T}{T}$ y $\frac{A}{A \cap T}$ son operadores isomorfos.

PRUEBA

Como A y T son admisibles respecto a Ω, entonces $A \cap T$ es admisi ble respecto a Ω. Si $u \in A \cap T$, $a \in A$, entonces $a^{-1} u a \in A$. Además co-

mo T es normal en G y $u \in T$, entonces $a^{-1} u a \in T$ y $a^{-1} u a \in A \cap T$, luego $A \cap T$ es normal en A.

Hagamos $A \cap T = D$ y

$$A = D \cup Da_2 \cup \dots \cup Da_r, \qquad Da_i \cap Da_j = \phi, \quad i \neq j$$

Afirmamos entonces que

$$A \,||\, T = T \cup Ta_2 \cup \dots \cup Ta_r,$$

usando los mismos representantes de las clases laterales de D en A. Tenemos en efecto que si $Ta_i = Ta_j$, entonces $a_i a_j^{-1} \in T$; pero $a_i a_j^{-1} \in A$, de donde $a_i a_j^{-1} \in A \cap T = D$, contrario a lo supuesto. Las clases laterales Ta_i son por lo tanto todas distintas. Por otra parte como T es un subgrupo normal, entonces $A \,||\, T = TA$, y por tanto cualquier clase lateral de T en $A \,||\, T$ es de la forma $Ta = Tda_i$, con $a = da_i$. Pero como $d \in T$, $Tda_i = Ta_i$, y por tanto las clases laterales Ta_i en $A \,||\, T$ cubren totalmente a $A \,||\, T$. Además la correspondencia $Da_i \overset{\rightarrow}{\leftarrow} Ta_i$ es una biyección entre las clases laterales de D en A y las de T en $A \,||\, T$, y por tanto una biyección entre los elementos de $\frac{A}{A \cap T}$ y los de $\frac{A \,||\, T}{T}$. Además, si $a_i a_j = d\, a_k$ con $d \in D$, como $D \subset T$, tendremos simultáneamente $Da_i\, Da_j = Da_i a_j = Dda_k = Da_k$ y $Ta_i Ta_j = Ta_i a_j = Tda_k = Ta_k$. Luego la correspondencia $Da_i \overset{\rightarrow}{\leftarrow} Ta_i$ es un un isomorfismo entre los grupos factores $\frac{A}{D}$ y $\frac{A \,||\, T}{T}$. Un operador $\alpha \in \Omega$ determina un operador en $\frac{A}{D}$ y también uno en $\frac{A \,||\, T}{T}$ por las reglas $\alpha(Da_i) = D\alpha(a_i)$

y $\alpha(Ta_i) = T\alpha(a_i)$. Para los operadores dados en esta forma, es inmediato que la correspondencia $Da_i \rightleftarrows Ta_i$ determina un isomorfismo de operadores. Lo que completa la prueba.

Verificaremos que un subgrupo K de un grupo G es un subgrupo normal si y sôlo si es admisible respecto a la familia de automorfismos interiores de G. En efecto, si K es normal en G y α_a pertenece a la familia de automorfismos interiores de G, entonces se tiene para $\alpha_a(k) \in \alpha_a(K)$, $\alpha_a(k) = a^{-1}ka \in a^{-1}Ka = K$, y $\alpha_a(K) \subseteq K$. Luego K es admisible. Tomemos ahora a K como subgrupo admisible respecto a los automorfismos interiores de G, entonces $\alpha_a(K) \subseteq K$ para todo a, $a \in G$, y $\alpha_a(k) = a^{-1}ka \in K$. Por lo que K es normal en G.

DEFINICION 1.13

Si H es un subgrupo de un grupo G y H es admisible respecto a todos los automorfismos de G entonces H es llamado un subgrupo característico. Si H es admisible respecto a todos los endomorfismos, entonces H es llamado un subgrupo totalmente invariante.

Como ejemplo de un subgrupo característico tenemos el centro Z de un grupo G, ya que $zg = gz$ para todo $g \in G$, implica que para un automorfismo α tenemos $\alpha(z)\alpha(g) = \alpha(g)\alpha(z)$, y como al recorrer g todos los elementos de G, $\alpha(g)$ recorrerá todos los elementos de G, concluimos que $\alpha(z) \in Z$.

Hay que hacer notar que el centro de un grupo no es necesariamen

te un subgrupo totalmente invariante. Como ejemplo consideremos el grupo G de orden 16 definido por las relaciones $a^4 = 1$, $b^2 = c^2 = 1$, $ba = a^{-1}b$, $ca = ac$, $cb = bc$ y cuyos elementos constituyen el conjunto $\{1, a, a^2, a^3, b, c, ab, ac, ba, bc, a^2b, a^2c, a^3c, abc, bac, a^2bc\}$. Aquí el centro Z es de orden 4 y está formado por el conjunto $\{1, a^2, c, a^2c\}$ el cual es generado por a^2 y c. Pero la aplicación $a \to b$, $b \to b$, $c \to b$ define un endomorfismo de G que nos lleva del elemento del centro c al -- elemento b que no es del centro.

Trataremos ahora de definir el producto directo de dos grupos. Sean A y B dos grupos, podemos formar, partiendo de ellos, el conjunto de todos los pares ordenados (a, b), $a \in A$, $b \in B$. Estos pares ordenados serán los elementos de un nuevo grupo, que llamaremos el producto directo $A \times B$, en donde definiremos el producto por la regla $(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2)$. Se ve con claridad que si se toma (1, 1) como elemento identidad, entonces el conjunto $A \times B$ y el producto definido en él satisface los axiomas de grupo, puesto que la validez de estos axiomas solo depende de la validez de los mismos para A y B.

Por otra parte puede establecerse un isomorfismo entre $A \times B$ y $B \times A$, que es la correspondencia $(a, b) \rightleftarrows (b, a)$, de modo que podemos hablar del producto directo de dos grupos sin especificar el orden. Además puede establecerse el isomorfismo $a \rightleftarrows (a, 1)$, entre A y el conjunto de elementos de $A \times B$ con la identidad como segundo elemento.

En forma análoga $b \rightleftarrows (1, b)$ es un isomorfismo entre B y el sub -

grupo de elementos (1, b). Por lo anterior es que algunas veces identificamos a A y B con estos subgrupos y de acuerdo con ella decimos que $G = A \times B$ es el producto directo de sus subgrupos A y B.

Como $(a, 1)(1, b) = (a, b) = (1, b)(a, 1)$, se sigue que en $A \times B$ todo elemento de A conmuta o permuta con todo elemento de B; es decir $ab = ba$ para $a \in A$ y $b \in B$.

En el producto directo $(a,b)^{-1} = (a^{-1}, b^{-1})$. De aquí que $(a_1, b_1)^{-1}(a_2, 1)(a_1, b_1) = (a^{-1}a_2a_1, 1)$, luego A es un subgrupo normal De $A \times B$. Por idéntica razón B es un subgrupo normal de $A \times B$. El único elemento que es simultâneamente de la forma (a, 1) y de la forma (1, b) es (1, 1), por lo que $A \cap B = 1$. Por otra parte $A \| B$ incluye todos los productos de la forma $(a, 1)(1, b) = (a, b)$, de donde $A \| B = A \times B$.

TEOREMA 1.20

Un grupo G es isomorfo al producto directo de dos subgrupos A y B si A y B son subgrupos normales tales que $A \cap B = 1$ y $A \| B = G$.

PRUEBA

Supongamos que A y B son subgrupos normales de G, con $A \cap B = 1$, $A \| B = G$. Consideremos un elemento $a^{-1}b^{-1}ab$ con $a \in A$ y $b \in B$, entonces $a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in A$ y además $a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)b \in B$ por ser A y B normales. Luego $a^{-1}b^{-1}ab \in A \cap B = 1$, por lo que $a^{-1}b^{-1}ab = 1$ y $ab = ba$. Ahora tomemos $g \in G$, g es tal que $g = x_1 x_2 \dots x_s$, con $x_i \in A$ ó $x_i \in B$, probaremos primero que este g puede expresarse en la forma ab, $a \in A$, $b \in B$. Por ser B normal un producto $ba = aa^{-1}ba = ab'$

y por ser A normal, $ba = bab^{-1}b = a'b$ de modo que podemos escribir el -- producto de forma que ningún $b \in B$ preceda a un $a \in A$, por lo que el pr_ ducto ab toma la forma $ab = a_1 \cdot a_2 \cdot \ldots \cdot a_j \cdot b_{j+1} \cdot b_{j+2} \cdot \ldots \cdot b_s$ donde $a_i \in A$ y $b_i \in B$. Luego $G = A \amalg B = AB$, de donde g puede ponerse en la forma $g = ab$, $a \in A$, $b \in B$. Por otra parte, esta forma es única, ya que si $a_1b_1 = a_2b_2$, entonces $a_2^{-1}a_1 = b_2b_1^{-1} \in A \cap B = 1$, de donde $a_1 = a_2$ y $b_1 = b_2$. Si $g \in G$, $g = ab$, establezcamos la función $\psi: G \longrightarrow A \times B$.

$$g=ab \rightsquigarrow (a,b)$$

Si $\psi(g_1) = \psi(g_2)$, $g_1 = a_1b_1$, $g_2 = a_2b_2$, entonces $(a_1,b_1) = (a_2,b_2)$ lo que implica que $a_1 = a_2$ y $b_1 = b_2$, por lo que $g_1 = g_2$ y es in - yección.

Si $(a, b) \in A \times B$, entonces existe $g = ab \in AB = G$, de modo que $\psi(g) = (a,b)$ por lo que ψ es sobreyección. Además si $g_1, g_2 \in G$, $g_1 = a_1b_1$, $g_2 = a_2b_2$, entonces $g_1g_2 = a_1b_1a_2b_2 = (a_1a_2)(b_1b_2)$ y $\psi(g_1g_2) = (a_1a_2, b_1b_2) = (a_1, b_1)(a_2, b_2) = \psi(g_1)\psi(g_2)$, y ψ preser- va los productos y es un isomorfismo entre G y $A \times B$.

Podemos definir el producto directo de cualquier número de gru - pos, finito o infinito. Supongamos que nos es dado un sistema de grupos A_i donde i toma los valores de un sistema de índices I. Construimos pro- ductos formales $\prod_{i \in I} a_i$. Un producto formal es simplemente una elección - de un elemento a_i de cada uno de los grupos A_i. Todos los productos forma_

les forman un grupo que es el producto cartesiano de los A_i, donde la regla del producto es:

$$\prod_{i\in I} a_i \cdot \prod_{i\in I} b_i = \prod_{i\in I} c_i, \qquad c_i = a_i b_i, \quad \text{para todo } i \in I.$$

El subgrupo del producto cartesiano en que $a_i = 1$ para todos, salvo un número finito de índices, se llama el producto directo de los A_i. Claramente, producto directo y producto cartesiano coinciden cuando el número de factores es finito. En ambos casos, los elementos $\prod_{i\in I} a_i$, en donde $a_i = 1$ para $i \neq j$, forman un subtrupo normal isomorfo a A_j, e identificando A_j con este subgrupo en cada caso, observamos que

$A_j \cap (\coprod_{i\neq j} A_i) = 1$. Aquí $\coprod_{i\in I} A_i$ es la juntura.

TEOREMA 1.21

Un grupo G es isomorfo al producto directo de subgrupos A_i, $i \in I$, si:

1) Todo A_i es un sugrupo normal

2) $A_j \cap (\coprod_{i\neq j} A_i) = 1$ para todo $j \in I$

3) $G = \coprod_{i\in I} A_i$

PRUEBA

Por 1) y 2) cada a_j permuta con todo producto finito de a_i-es con $i \neq j$. Además por 1), 2) y 3) cada $g \in G$ se puede expresar como un producto finito de elmennros de los A_i, y, aparte del orden, tiene una forma única como producto en que aparezca, cuando más, un factor de cada A_i.

Esto nos da un isomorfismo entre G y el producto directo de los A_i. Un elemento de G puede ponerse en la forma $g = 1$ ó $g = b_1 b_2 \ldots b_m$, $b_k \neq 1$, $k = 1, 2, \ldots, m$ donde las b son de diferente A_i. Aquí g se corresponde con el elemento $\prod_{i \in I} a_i$, donde $a_i = b_k$ si hay un $b_k \in A_i$ en el producto para g y $a_i = 1$ en otro caso. Esta correspondencia nos da el isomorfismo entre G y el producto directo de los A_i.

Trataremos ahora un poco los grupos abelianos. Consideremos el grupo multiplicativo de todos los números complejos excepto el cero. Este grupo es de orden infinito y es abeliano, además contiene elementos de orden infinito y también de todos los órdenes finitos. Como puede observarse, su estructura nos parece más o menos complicada, sin embargo resulta ser más o menos sencilla si la comparamos con la de algunos grupos abelianos de orden infinito.

Si en un grupo abeliano A encontramos elementos a y b tales que $a^n = 1$, $b^m = 1$, entonces $(a^{-1})^n = 1$ y $(ab)^{mn} = 1$, luego el conjunto de los elementos de orden finito en cualquier grupo abeliano A forman un subgrupo F. Todo endomorfismo α de A mapea un elemento de orden finito en un elemento de orden finito. Por tanto F es un subgrupo totalmente invariante de A. Además si llamamos grupo periódico a todo grupo en el que todos sus elementos son de orden finito, entonces F es también un grupo periódico.

Un grupo en el que ningún elemento excepto la identidad es de orden finito es llamado grupo aperiódico o sin torsión.

.22

Sea F el subgrupo formado por todos los elementos de orden finito de un grupo abeliano A. Entonces $\frac{A}{F}$ es aperiódico.

PRUEBA

Supongamos que $x \in \frac{A}{F}$, $x \neq 1$ es de orden finito m. Entonces en el homomorfismo $\psi: A \to \frac{A}{F}$: $u \rightsquigarrow x$ tenemos que $u^m \rightsquigarrow x^m = 1$, de donde $u^m \in F$ y u^m es de orden finito, digamos n. Luego $(u^m)^n = 1$, $u^{mn} = 1$ y u es de orden finito, por lo que $u \in F$ y $\psi(u) \rightsquigarrow 1 = x$, lo que es contrario al supuesto.

Diremos que un conjunto de elementos $(a_i)_{i \in J}$ de un grupo abeliano A es independiente si un producto finito $\prod_i a_i^{e_i} = 1$ solamente cuando $a_i^{e_i} = 1$ para todo i. Si los a_i son independientes y además generan A, decimos que los a_i forman una base de A. Tenemos por tanto que los elementos a_i forman una base de A si y sólo si A es el producto directo de los grupos cíclicos generados por los a_i.

Si un grupo abeliano A está generado por los elementos $a_1, a_2, \ldots, a_r$, entonces, toto elemento de A es de la forma $a_1^{u_1}, a_2^{u_2}, \ldots, a_r^{u_r}$, donde los u_i son enteros. Además si $a_1^{x_1} \ldots a^{x_r} = 1$ es una relación de estos generadores, decimos que $a_1^{-x_1}, \ldots, a_r^{-x_r} = 1$ es su relación inversa.

De un conjunto S de relaciones que se verifican en A podemos derivar otras tomando el producto de relaciones de S e inversas de relacio-

nes de S. Dos conjuntos de relaciones S_1 y S_2 son llamados equivalentes si las relaciones de cada conjunto pueden derivarse de esta forma de las del otro. Decimos que un conjunto S es un conjunto de relaciones definitorias para A si toda relación que se verifica en A puede derivarse de las de S. Puede probarse que un conjunto arbitrario de relaciones S sobre generadores $a_1, a_2, \ldots, a_r$ es un conjunto de relaciones definitorias para aquel grupo abeliano A generado por $a_1, a_2, \ldots, a_r$ en que las relaciones derivadas de S se verifican, pero ninguna otra se verifica.

TEOREMA 1.23

Un grupo abeliano generado por un número finito de elementos, r, tiene una base de cuando más r elementos.

PRUEBA

El teorema es cierto para $r = 1$, pues entonces el grupo es cíclico. Supongamos que A está generado por $a_1, a_2, \ldots, a_r$. Entonces la prueba se basará en la inducción sobre r, y para un r fijo sobre el mínimo entero positivo m tal que $x_i = m$ en una relación

$$a_1^{x_1} \; a_2^{x_2} \; \ldots \; a_r^{x_r} = 1$$

Si la única relación existente es aquella en que todos los $x_i = 0$, entonces A es el producto directo de los grupos cíclicos infinitos $\langle a_i \rangle$ y el teorema es cierto. De otro modo, alguna relación o su inversa contendrán algunos exponentes positivos. Runumeremos los a_i de modo que el mínimo exponente positivo en una relación es $x_1 = m$. Si $m = 1$

$$a_1 = a_1^{-x_1} \; a_2^{-x_2} \; \ldots \; a_r^{-x_r}$$

y A está generado por los r-1 elementos $a_2, a_3, \ldots, a_r$, y por inducción el teorema es cierto. Supongamos ahora que $x_1 = m > 1$ en la relación

$$(1) \qquad a_1^m \cdot a_2^{x_1} \cdot \ldots \cdot a_r^{x_r} = 1.$$

Sean $y_1, y_2, \ldots, y_r$ los exponentes en otra relación. Entonces, para -- cualquier entero K, de tal relación y la (1) podemos derivar una relación con exponentes $y_1 - km$, $y_2 - kx_2, \ldots, y_r - kx_r$, Podemos escoger k de modo que $0 \leq y_1 - km < m$. Pero como m era el exponente mínimo en cual -- quier relación, debemos tener $y_1 - km = 0$, de donde la relación con exponentes $y_1, y_2, \ldots, y_r$ puede derivarse de la relación (1) y la rela -- ción con exponentes $0, y_2 - kx_2, \ldots, y_r - kx_r$. Luego el conjunto de todas las relaciones para A es equivalente al conjunto S consistente en la rela ción (1) y las relaciones en las que tan solo aparecen $a_2, a_3, \ldots, a_r$.

En la relación (1) sea $x_2 = k_2 m + s_2, \ldots, k_r m + s_r$, donde he - mos escogido k_i, $i = 2, 3, \ldots, r$ tales que $0 \leq s_i < m$. Si tomamos un nuevo elemento

$$a_1^* = a_1 a_2^{k_2} \cdot \ldots \cdot a_r^{k_r},$$

entonces $a_1^*, a_2, a_3, \ldots, a_r$ generan también a A, y en términos de estos generadores, la relación (1) toma la forma

$$(2) \qquad a_1^{*m} \cdot a_3^{s_2} \cdot \ldots \cdot a_r^{s_r} = 1.$$

Si aquí algún s_i es diferente de cero, ha de ser un número positivo menor que m y podemos aplicar nuestra hipótesis de inducción. Pero si

$s_2 = \ldots = s_r = 0$, entonces (2) se hacer

$$(3) \qquad a_1^{*m} = 1$$

y como la relación (1) y las relaciones en las que solo aparecen $a_2, a_3, \ldots, a_r$ constituyen un conjunto definitorio de relaciones para A en términos de los generadores $a_1, a_2, \ldots, a_r$, se sigue que la relación (3) y las relaciones en que tan solo aparecen $a_2, a_3, \ldots, a_r$ forman un conjunto definitorio de relaciones en términos de los generadores $a_1^*, a_2, \ldots, a_r$. Luego A es el producto directo del grupo cíclico de orden m generado por a_1^* y el grupo generado por los r-1 elementos $a_2, a_3, \ldots, a_r$ que por nuestra hipótesis de inducción es el producto directo de, cuando más, r-1 grupos cíclicos. Quedando así el teorema probado en todos los casos.

TEOREMA 1.24

Si x es un elemento de orden mn en un grupo G, com m y n enteros y primos relativos. Entonces x tiene una representación única $x = yz = zy$, donde y es de orden m y z de orden n. Tanto y como z son potencias de x.

PRUEBA

Decir que m y n son primos relativos es afirmar que el máximo común divisor de m y n $(m, n) = 1$. Entonces por el Algoritmo de Euclides, existen enteros u y v tales que $um + vn = 1$, y de aquí inferimos que $x = x^{(um + vn)} = x^{um}\, x^{vn} = x^{vn}\, x^{um}$. Sean $y = x^{vn}$, $z = x^{um}$. Entonces

$x = yz = zy$ y $y^m = x^{vnm} = 1$, y $z^n = x^{umn} = 1$. Luego el orden de y es algún divisor m_1 de m, y el de z algún divisor n_1 de n. Pero de $x = yz = zy$ se sigue que el orden de x es un divisor $m_1 n_1$ de mn. Pero el orden de x es mn, luego $m_1 = m$ y $n_1 = n$, por lo que el orden de y es m y el de z es n. Si x tuviera una segunda representación $x = y_1 z_1 = z_1 y_1$ con y_1 de orden m y z de orden n, entonces y_1 y z_1 permutarían con x, -- puesto que $xy_1 = y_1 z_1 y_1 = y_1 x$ y $xz_1 = z_1 y_1 z_1 = z_1 x$. Pero entonces y_1 y z_1 permutarían con y y z, que son potencias de x. Ahora bien, $yz = x = y_1 z_1$ nos lleva a $w = y_1^{-1} y = z_1 z^{-1}$. Pero y y y_1 son elementos que permutan de orden m, y z y z_1 son elementos que permutan de orden n. Luego el elemento w satisface $w^m = 1$ y también $w^n = 1$, y como $(m, n) = 1$, esto implica $w = 1$; de modo que $y_1 = y$ y $z_1 = z$. Esto rrueba la unicidad de la representación.

COROLARIO 1.1

Si x es un elemento de orden $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r$ donde $(n_i, n_j) = 1$ para $i \neq j$. Entonces x tiene una representación única $x = x_1 \cdot x_2 \cdot \ldots \cdot x_r$ donde $x_j x_i = x_i x_j$ y x_i es de orden n_i y cada x_i es una potencia de x.

PRUEBA

Aplicando repetidamente el Teorema 1.24 queda probado este corolario.

Particularmente si consideramos a n como $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$,

donde P_1 , P_2 , ..., P_r son primos distintos, se puede aplicar el corolario anterior haciendo $n_i = p_i^{e_i}$.

Tomemos ahora un grupo abeliano A con la condición de que A sea periódico. Tomemos el conjunto P formado por los elementos de A cuyos órdenes son potencias de un primo fijo p, en donde se incluye la identidad - como potencia de orden $p^0 = 1$, si $x^{p^a} = 1$, y $y^{p^b} = 1$, entonces si $c = \text{máx}(a,b)$ tendremos que $(xy)^{p^c} = 1$ y $(x^{-1})^{p^c} = 1$. Luego P es subgrupo de A. Al subgrupo P le llamamos el p-subgrupo de Sylow, S(p). A P le llamamos también un p-grupo abeliano.

TEOREMA 1.25

Si A es un grupo abeliano periódico, entonces A es el producto de sus subgrupos de Sylow.

PRUEBA

Tomemos la juntura de los subgrupos de Sylow de A, $\coprod_p S(p)$. Esta juntura es subgrupo de A. Pero, para $x \in A$, podemos afirmar que x es de - orden $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ y $x = x_1 \cdot x_2 \cdot \ldots \cdot x_r$ con $x_i \in S(p_i)$, esto - por el corolario 1.1; luego todo elemento x de A pertenece también a la juntura $\coprod_p S(p)$, por lo que $A = \coprod_p S(p)$.

Como la juntura es isomorfo con el producto directo, entonces la prueba está completa.

TEOREMA 1.26

Un grupo abeliano finito de orden $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ es el producto directo de los subgrupos de Sylow $S(p_1)$, $S(p_2)$, ..., $S(P_r)$. En esta

expresión $S(p_i)$ ez de orden $p_i^{e_i}$ y es el producto directo de grupos cícli-
cos de órdenes $p_i^{e_{i1}}, \ldots, p_i^{e_{is}}$, donde $e_{i1} + \ldots + e_{is} = e_i$.

PRUEBA

Si tomamos un grupo abeliano A, de orden n, entonces el orden de cualquiera de sus elementos será un divisor de n, luego un p-subgrupo de Sylow, tal que p es un primo que no divida a n tiene que consistir so-lamente en la identidad, y por lo tanto, si $p_1, p_2, \ldots, p_r$ son los distintos primos que dividen a n, entonces el grupo A, es el producto directo $S(p_1).\ S(p_2).\ \ldots\ .S(p_r)$. Ahora trataremos los órdenes de los $S(p_i)$. Cada $S(p_i)$ puede ser la identidad o el producto directo de grupos cíclicos de órdenes $p_i^{e_{i1}}, p_i^{e_{i2}}, \ldots, p_i^{e_{is}}$, entonces el orden de $S(p_i)$ será el producto de estos órdenes. Supongamos que el orden de $S(p_i)$ es $p_i^{t_i}$, con $t_i = e_{i1} + e_{i2} + \ldots + e_{is}$ y como el orden n de A es el producto de los órdenes de los $S(p_i)$, entonces por factorización única del entero n, tendrá que ser $p_i^{t_i} = p_i^{e_i}$ en cada caso, y el teorema queda así demostrado.

TEOREMA 1.27

Todo subgrupo de un grupo cíclico infinito diferente de la identidad es un grupo cíclico infinito de índice finito, y hay un subgrupo -- único para cada índice finito. Todo subgrupo de un grupo cíclico finito de orden n es un grupo cíclico de orden que divide a n, y hay un subgrupo único para cada divisor de n de orden igual a ese divisor.

PRUEBA

Sea G un grupo cíclico generado por un elemento b y H un subgrupo de G y $H \neq \langle 1 \rangle$. Si $b^i \in H$, entonces $b^{-i} \in H$ y uno u otro de estos exponentes es positivo. Supongamos que m es el exponente positivo mínimo de cualquier elemento que pertenezca a H, y sea b^t un elemento cualquiera de H. Entonces escogiendo r adecuadamente tenemos $t = mr + s$ con $0 \leq s < m$. Luego $b^t = (b^m)^r b^s$. Como tanto b^t como b^m pertenecen a H, se sigue que b^s pertenece también a H. Pero si s es un entero distinto de cero y $0 \leq s < m$, esto estaría en conflicto con la definición de m como el mínimo exponente positivo de b que aparece en un elemento de H. Luego $s = 0$, y $b^t = (b^m)^r$, y todos los elementos de H resultan ser potencias de b^m de donde H es cíclico. Como para cualquier u que sea entero tenemos $u = km + i$, donde $i = 0, 1, \ldots, (m-1)$ verificamos facilmente que

$$G = H \cup Hb \cup \ldots \cup Hb^{m-1}.$$

Esta ecuación contiene todas las posibles clases laterales de H y estas son diferentes, ya que $b^i = hb^j$ con $i \neq j$ en el rango de 0 a m-1 nos daría una potencia positiva de b más pequeña que m en H, que sería b^{i-j} o $b^{j=i}$. Luego $[G: H] = m$, de donde afirmamos que m es la menor potencia positiva de b que pertenece a H y también es el índice de H en G. Así -- pues si G es infinito, como para todo m positivo los elementos de la forma $(b^m)^r$, $r \in Z$, forman un subgrupo de G, entonces hay un subgrupo único $\langle b^m \rangle$ de índice m de G.

Si G es finito de orden n, entonces $b^n = 1$, luego $n = mr$, y m es un divisor de n.

Entonces para cualquier m que divida a n, si n = mr, tenemos los elemen - tos 1, b^m, b^{2m}, ..., $b^{(r-1)m}$ que forman un subgrupo de orden r e índice m. Como n = mr puede ser cualquier factorización de n en dos factores, vemos que hay un y solamente un subgrupo de G de orden r para cada r divisor de n.

Como una consecuencia del Teorema 1.26 y del Teorema 1.27 pode - mos afirmar el enunciado siguiente

COROLARIO 1.2

Si G es un grupo abeliano de orden n y p es un primo que divide a n, entonces existe b ∈ G tal que b es de orden p.

Si A(p) es un p-grupo abeliano finito, entonces A(p) puede escribirse como producto directo de grupos cíclicos en varias formas. Así, si suponemos que $a^8 = 1$ y $b^4 = 1$, entonces A(2) = <a> x <b> es de orden 32. En la misma forma si ponemos que c = ab y $d = a^4b$, entonces $c^8 = a^8b^8 = a^8(b^4)^2 = 1$ y $d^4 = a^{16}b^4 = (a^8)^2b^4 = 1$; quedando $a = c^5d^{-1}$ y $b = c^4d$ Ahora A(2) = <c> x <d>. Observamos que A(2) es el producto - directo de grupos cíclicos en dos formas diferentes, pero el número de factores y sus órdenes son los mismos. En general este resultado es cierto para p-grupos abelianos finitos, pero no es cierto para grupos abelianos - finitos que no sean p-grupos abelianos. Así por ejemplo el grupo cíclico de orden 6 es el producto de grupos cíclicos de orden 2 y 3.

Si A(p) es un p-grupo abeliano que es el producto directo de grupos cíclicos de órdenes p^{e_1}, p^{e_2}, ..., p^{e_r}, entonces estos números son lla

mados los invariantes del grupo. En el caso en que todos los invariantes son $p, p, \ldots p$, decimos que A(p) es un grupo abeliano elemental. Puede verse fácilmente que los invariantes de un p-grupo abeliano A(p), determinan a A(p) salvo isomorfismo. La importancia de estos invariantes se destaca en el teorema siguiente:

TEOREMA 1.28

Si un p-grupo obeliano finito A es el producto directo de grupos cíclicos en dos formas, $A = A_1 \times A_2 \times \ldots \times A_r = B_1 \times B_2 \times \ldots \times B_s$, entonces el número de cactores es el mismo en ambos casos, $r = s$, y los órdenes de $A_1, A_2, \ldots, A_r$ son los mismos, después de cierta reordenación, que los de los $B_1, B_2, \ldots, B_s$.

PRUEBA

La prueba la haremos aplicando inducción sobre el orden de A, tomando en cuenta que cuando el orden de A es p el teorema resulta trivial.

Supongamos que A es un p-grupo abeliano cualquiera y denotemos por A_p al subgrupo cuyos elementos x satisfacen $x^p = 1$ y por A^p al subgrupo cuyos elementos son de la forma y^p con $y \in A$. Supongamos que A tiene una base $a_1, a_2, \ldots, a_r$ donde a_i es de orden p^{e_i}, $i = 1, 2, \ldots, r$ y numeremos las a-es de forma que $e_1 \geq e_2 \geq \ldots \geq e_r$. Verificamos entonces que Ap tiene una vase $a_1^{p^{e_1-1}}, \ldots, a_r^{p^{e_r-1}}$ y es de orden p^r. Si A es un abeliano elemental, entonces $A^p = 1$. En caso de no ser A abeliano elemental, sea e_m el último exponente mayor que 1, es decir,

$e_1 \geq \ldots \geq e_m \geq e_{m+1} = \ldots = e_r = 1$. Entonces A^p tiene una base $a_1^p, a_2^p, \ldots, a_m^p$.

Sea $b_1, b_2, \ldots, b_s$ una segunda base de A, donde b_i es de orden p^{f_i}, $i = 1, 2, \ldots, s$ y $f_1 \geq f_2 \geq \ldots \geq f_s$. Entonces A_p es de orden p^r por ser $a_1, a_2, \ldots, a_r$ una base de A, y de orden p^s por ser también $b_1, b_2, \ldots, b_s$ base de A. Luego $r = s$. Si A es abeliano elemental, la prueba está completa, pero si no lo es, sea $f_1 \geq f_2 \geq \ldots \geq f_n > f_{n+1} = \ldots = f_s = 1$. Entonces A^p tiene invariantes $p^{e_1-1}, p^{e_2-1}, \ldots, p^{e_m-1}$ y también invariantes $p^{f_1-1}, p^{f_2-1}, \ldots, p^{f_n-1}$. Por inducción $m = n$ y $e_1-1 = f_1-1, \ldots, e_m-1 = f_m-1$. De esto y del hecho de ser $s = r$, se sigue que $e_1 = f_1, \ldots, e_r = f_r$.

Como consecuencia de lo anterior podemos enunciar el siguiente:

COROLARIO 1.3

Si dos p-grupos abelianos finitos no tienen los mismos invariantes, no son isomorfos.

CAPITULO II

TEOREMAS DE SYLOW

En este capítulo destacaremos la importancia de tres teoremas - conocidos como los tres teoremas de Sylow. El primero de estos teoremas garantiza la existencia de subgrupos cuyos órdenes son una potencia de un número primo, el segundo nos asegura que en todo grupo finito G, los p-subgrupos de Sylow son conjugados y el tercero que nos sirve para calcular el número de p-subgrupos de Sylow que hay en un grupo finito G. Además el -- concepto de producto directo junto con los teoremas de Sylow, nos permiten clasificar los grupos finitos, de los cuales estudiaremos los de pequeño orden, orden menor o igual a 11.

El Teorema de Lagrange asegura que el orden de un subgrupo H de un grupo G, divide al orden de G. Pero en general no es cierto que si un número m divide al orden de un grupo G, entonces existe un subgurpo H de G cuyo orden es m. Sin embargo, si m es primo entonces con seguridad existe H subgrupo de G tal que H es de orden m. Este y otros resultados constituyen los teoremas de Sylow.

DEFINICION 2.1

Llámase una clase de elementos conjugados de x en un grupo G al conjunto $\overline{x} = \{y^{-1} xy / \ y \in G\}$.

En el Teorema 1.16 si S consta de un solo elemento s, los conjugados respecto a G forman una clase. Por tanto las clases de elementos -- conjugados en G son una partición de los elementos de G, y puede escribirse

$$G = C_1 \cup C_2 \cup \ldots \cup C_s$$

en donde los C_i son clases distintas y cada elemento de G se encuentra - exactamente en una sola clase. La identidad 1 es siempre una clase. Por el teorema 1.16 el número de elementos en una clase C_i es el índice de un subgrupo y por tanto un divisor del orden del grupo.

TEOREMA 2.1

Si G es un grupo finito y p es un primo que divide al orden de G, entonces G contiene un elemento de orden p.

PRUEBA

Sea G un grupo de orden $n = mp$. Si $m = 1$, entonces orden de G - igual p y G es el grupo cíclico de orden p y el teorema es cierto. Procedamos por inducción sobre m. Si G contiene un subgrupo propio H cuyo índice [G: H] no es divisible por p, entonces p divide al orden de H, luego por inducción H contiene un elemento de orden p. Supongamos ahora que todo subgrupo propio de G tiene un índice divisible por p, entonces $n = n_1 + n_2 + \ldots + n_s$, donde cada n_i es el número de conjugados en - una clase de elementos de G. Cada $n_i \neq 1$ es el índice de un subgrupo -- propio de G, luego por hipótesis, divisible por p. Pero $n_1 = 1$ por ser la identidad una clase. Luego el número de n_i - s tales que $n_i = 1$ habría de ser un múltiplo de p. Un elemento a_i es una clase en G si y sólo si pertenece al centro Z de G. Luego el centro Z sería de orden divisible por p. Pero para $z \in Z$ y cualquier $g \in G$ tenemos que $zg = gz$, de donde, forzosamente todos los elementos de Z permutan entre si y Z es un grupo abeliano. Pero por el corolario 1.2, Z contiene un elemento de orden P.

TEOREMA 2.2 (Primer Teorema de Sylow)

Si $n = p^m s$ es el orden de un grupo G donde p es primo y p no divide a s, entonces existen subgrupos de G de órdenes p^i, $i = 1,2,\ldots,m$, y cada subgrupo de orden p^i, $i = 1,2,\ldots,m-1$, es un subgrupo normal de al menos un subgrupo de orden p^{i+1}.

PRUEBA

Efectuaremos esta prueba por inducción sobre i. Por el teorema 2.1 afirmamos que G contiene un subgrupo de orden p. Sea P un subgrupo de orden p^i, $i \geq 1$. Escribamos G en términos de clases laterales dobles de P,

$$G = P \cup Px_2P \cup \ldots \cup Px_rP,$$

y sea a_j el número de clases laterales derechas de P incluidas en Px_jP. Entonces $[G: P] = a_1 + a_2 + \ldots + a_r$, donde $a_j = [x_j^{-1}Px_j : x^{-1}Px_j \cap P]$, y $a_1 = 1$ para la clase lateral doble $P1P = P$. Ahora bien, $a_j = 1$ o una potencia de p. Como p divide a $[G: P]$, entonces el número de las a_j iguales a 1 debe ser un múltiplo de p. Si $a_j = 1$ entonces $x^{-1}Px_j = P$ y x_j debe pertenecer al normalizador K de P, y $Px_j = x_jP$ está incluido en K. Reciprocamente, si $x_j \in K$, entonces $x_j^{-1}Px_j = P$ y $a_j = 1$. Luego $[K: P]$ es el número de las $a_j = 1$ y por tanto p divide a $[K: P]$. Luego el grupo factor $\frac{K}{P}$ tiene orden igual al $[K: P]$ y es divisible por p. Luego $\frac{K}{P}$ contiene un subgrupo J^* de orden p. Ahora por el teorema 1.17

$J^* = \frac{J}{P}$, donde $J \subset K$ y $[J: P] = [J^*: 1] = p$; luego J es un subgrupo de orden p^{i+1} que contiene a P como un subgrupo normal.

DEFINICION 2.2

Un grupo P es un p-grupo si todo elemento de P excepto de identidad tiene como orden una potencia de un primo p.

DEFINCION 2.3

Un subgrupo S de un grupo G es un subgrupo de Sylow de G si y solo si es un p-grupo y no está contenido propiamente en ingún p-grupo que sea un subgrupo de G.

De acuerdo a estas definiciones podemos expresar dos consecuencias del primer Teorema de Sylow.

COROLARIO 2.1

Todo grupo finito G de orden $n = p^m s$ con p que no divide a s, p primo, contiene un subgrupo de Sylow de orden p^m, y todo p-grupo que es un subgrupo de G está contenido en un subgrupo de Sylow de G.

Cada grupo de orden p^m es un p-grupo. Por Teorema 2.1 si el orden de un grupo es divisible por dos primos diferentes, no puede ser un p-grupo. Luego todo p-grupo finito es de orden igual a una potencia de p, digamos p^m.

COROLARIO 2.2

Todo subgrupo de un p-grupo P de orden p^m está contenido en un subgrupo maximal de orden p^{m-1}, y todos los subgrupos maximales son subgrupos normales.

Supognamos que el orden de P es $p^m = p^m.1$, entonces por el Primer Teorema de Sylow P contiene subgrupos de órdenes p^i, $i = 1,2,\ldots, m$, de modo que $P_1 \subset P_2 \subset \ldots \subset P_m$ y de órdenes $p, p^2, p^3, \ldots, p^m$ respectivamente y existirá un subgrupo de orden p^{m-1} que será un subgrupo normal de al menos un subgrupo de orden p^m que no puede ser otro más que P.

TEOREMA 2.3 (Segundo Teorema de Sylow)

En un grupo finito G los p-subgrupos de Sylow son conjugados.

PRUEBA

Sean P_1 y P_2 dos p-subgrupos de Sylow. Entonces $G = P_1P_2 \cup P_1x_2P_2 \cup \ldots \cup P_1x_sP_2$. Sea b_i el número de clases laterales derechas de P_2 incluidas en $P_1x_iP_2$. Entonces $b_i = [x_i^{-1}P_1x_i : x_i^{-1}P_1x_i \cap P_2]$ y es 1 óuna potencia de p. Pero $b_1 + b_2 + \ldots + b_s = [G: P_2]$ no es un múltiplo de p. Luego para algún i, $b_i = 1$ y $x_i^{-1}P_1x_i = P_2$.

TEOREMA 2.4 (Tercer Teorema de Sylow)

El número de p-subgrupos de Sylow de un grupo finito G es de la forma $1 + kp$, y es un divisor del orden de G.

PRUEBA

Si existe solamente un p-subgrupo de Sylow, entonces el teorema es trivial. Sea S_0 un p-subgrupo de Sylow y $S_1, S_2, \ldots, S_r$ los restantes. Se pueden agrupar estos en conjuntos disjuntos de conjugados entre

si con respecto a la transformación por elementos de S_0. Por el Segundo - Teorema de Sylow, S_i es el único p-subgrupo de Sylow en su normalizador K_i. Luego el normalizador de S_i, con $i \neq 0$, es un subgrupo propio de S_0, y por tanto, el número de conjugados de S_i bajo S_0 es una potencia de p, p^e, $e \geq 1$. De aquí que $r = p^{e_1} + \ldots + p^{e_s} = kp$, y hay $1+r = 1+kp$ p-subgrupos de Sylow de G. El número de p-subgrupos de Sylow es, por el Segundo Teorema - de Sylow, el índice del normalizador de S_0, luego un divisor del orden de G.

TEOREMA 2.5

Sea G un grupo finito, P un p-subgrupo de Sylow de G y K el normalizador de P en G. Si se tiene un subgrupo H, de G tal que $G \supseteq H \supseteq K \supseteq P$, entonces H es su propio normalizador en G.

PRUEBA

Supongamos $x^{-1}Hx = H$. Entonces $H \supseteq x^{-1}Px = P'$, que debe ser un - p-subgrupo de Sylow de H. Luego para algún $u \in H$, $u^{-1}P'u = P$, de donde $u^{-1}x^{-1}Pxu = P$ y $xu \in K$. Luego $x \in H$, y H es su propio normalizador.

Gracias a los Teoremas de Sylow podemos tratar el problema de la construcción de grupos finitos, ya que ellos nos afirman que si el orden de un grupo G es $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, entonces para cada i hay un subgrupo de orden $p_i^{e_i}$, y además que todos los subgrupos de este orden son isomorfos, puesto que son conjugados.

La construcción de grupos finitos puede considerarse en dos partes: 1a. la construcción de grupos cuyo orden es igual a una potencia de un primo y 2a. la combinación de grupos cuyos órdenes son iguales a potencias --

de primos que dividen a un número n, con el objeto de formar un grupo de orden n.

Nos ocuparemos en esta oportunidad de resolver la primera parte, ya que haciéndolo así tendremos construidos los subgrupos que utilizaremos en la solución de la segunda, la cual se dejará para el próximo capítulo.

Un hecho de mucha importancia sobre los p-grupos lo constituye - el teorema que enunciamos a continuación.

TEOREMA 2.6

El centro de un p-grupo finito es siempre mayor que la identi - dad.

PRUEBA

Si P es un p-grupo finito, entonces escribamos P en la forma; $P = C_1 \cup C_2 \cup \ldots \cup C_r$ donde C_1 consta solo de la identidad y todas las C_i son clases. Sea h_i el número de elementos en C_i, entonces por el teorema 1.11 es el índice de un subgrupo de P, por lo que h_i es 1 para un elemento del centro o una potencia de p en otro caso. Pero si P es de orden p^m debemos tener $p^m = h_1 + h_2 + \ldots + h_r$ en donde $h_1 = 1$, luego los restantes $h_2, h_3, \ldots, h_r$, no pueden ser todos potencias de p, por lo que debe haber alguna de las h-es posteriores a h_1 igual a 1. Esto implica que el centro de P es mayor que la identidad.

Del Primer Teorema de Sylow también se desprende que en un p-grupo, ningun subgrupo propio es su propio normalizador. También el recípro

co de esta consecuencia es verdadera y lo probaremos en el teorema siguiente:

TEOREMA 2.7

En un grupo finito G ningún subgrupo propio es su propio normalizador si y solamente si G es el producto directo de sus subgrupos de Sylow.

PRUEBA

Supongamos que ningún subgrupo propio de G es su propio normalizador. Supongamos que K es el normalizador de un subgrupo de Sylow P. Entonces $G \supseteq K \supseteq K \supseteq P$ y por teorema 2.5 K es su propio normalizador; pero como G no tiene ningún subgrupo propio que sea su propio normalizador, entonces debe ser K = G. Luego P es un subgrupo normal de G. De esto y el teorema 1.21 se sigue que $G = \coprod_{i \in I} P_i$. Luego G es el producto directo de sus subgrupos de Sylow. Ahora supongamos que $G = P_1 \times P_2 \times \ldots \times P_r$ donde P_i es un grupo de orden $P_i^{e_i}$ y $P_j \neq P_i$ si $i \neq j$. Si $g = g_1 g_2 \ldots g_r$ con $g_i \in P_i$, las condiciones del corolario 1.1 se verifican y cada g_i es una potencia de g. Luego cuando un elemento g pertenece a un subgrupo H de G, cada uno de sus componentes g_i es también un elemento de H. Luego H mismo debe ser un producto directo $H = H_1 \times H_2 \times \ldots \times H_r$, donde $H_i = H \cap P_i$ es un subgrupo de P_i. Si H es un subgrupo propio de G, entonces algún H_j es un subgrupo propio de P_j, y reemplazando este H_j por un subgrupo mayor de P_j en el que H_j sea normal, obtenemos un subgrupo mayor que el H en el que H es normal.

Intentaremos ahora un somero estudio de grupos cuyo orden sea menor o igual que once.

Supongamos un grupo G de orden primo p, $p \leq 11$. G no puede tener ningún subgrupo propio y por lo tanto debe ser un grupo cíclico, generado por cualquier elemento diferente de la identidad, puesto que por el teorema 1.9 sabemos que un grupo G no constituído tan solo por la identidad no tiene ningún subgrupo propio si y solo si G es un grupo cíclico de orden primo. Por lo anterior podemos afirmar que salvo isomorfismo no existe más que un sólo grupo de orden 1, 2, 3, 5, 7, 11.

Supongamos un grupo G de orden p^2, p = 2, 3. Este grupo G, si no es cíclico, contendrá dos subgrupos distintos de orden p, digamos el grupo generado por a, $\langle a \rangle$ y el grupo generado por b, $\langle b \rangle$, donde $a^p = 1$, $b^p = 1$ y $\langle a \rangle \cap \langle b \rangle = 1$. Además, por el corolario 2.2 ambos subgrupos serán normales, de donde por el teorema 1.22 afirmamos que $G = \langle a \rangle \times \langle b \rangle$; por lo que G es un grupo abeliano con a, b como base. De modo que existen, salvo isomorfismo, dos grupos de orden p^2, el cíclico, cuya relación definitoria es $a^{p_2} = 1$ y el abeliano elemental, con relaciones definitorias $a^p = 2$, $b^p = 1$, $ab = ba$. Como hemos dicho que p = 2,3, podemos afirmar que existen, salbo isomorfismos, dos grupos distintos de orden 4 y 9. En efecto podemos considerar los grupos llamados Z_4 y grupo de Klein que son de orden cuatro y de definen de acuerdo a las tablas siguientes:

Z_4

·	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Grupo de Klein

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Supongamos que G es de orden pq, donde $p < q$, p y g son primos. Por el Tercer Teorema de Sylow 2.4, el número de subgrupos de orden q es de la forma $1 + kp$ y divide a p, luego debe ser 1, y el único subgrupo de orden q será normal, digamos $\langle b \rangle$, con $b^q = 1$. El número de subgrupos de orden p es de la forma $1 + kp$ y divide a q, por lo que es 1 ó q. Si es 1 tenemos para algún a un subgrupo normal $\langle a \rangle$ con $a^p = 1$, y G es el producto directo de $\langle a \rangle$ y $\langle b \rangle$. Pero aquí $c = ab$ es de orden pq y G es cíclico. Falta solamente el caso en que $1 + kp = q$ subgrupos de orden p, donde un subgrupo $\langle a \rangle$ de orden p no es normal. Entonces tenemos $a^p = 1$, $b^p = 1$, y como $\langle b \rangle$ es normal, $a^{-1}ba = b^r$ paaa algún r. Si $r = 1$, entonces G es abeliano y es el grupo cíclico mencionado anteriormente. Luego $r \neq 1$. Entonces $a^{-1}b^ia = b^{ir}$ para todo i, y en particular $a^{-1}b^ra = b^{r^2}$, de donde $a^{-2}ba^2 = a^{-1}b^ra = b^{r^2}$. Más generalmente encontramos que $a^{-j}ba^j = b^{r^j}$. Luego para $j = p$ tenemos $b = a^{-p}ba^p = b^{r^p}$, de donde r^p es congruente con 1 módulo q. Por lo expuesto concluimos que existen, salvo isomorfismo, so

lamente dos grupos de orden pq, con $p < q$, p y q primos y $q = 1 + kp$. Si $q \neq 1 + kp$, entonces solamente existe uno. Luego existe, salvo isomorfismo, solamente dos grupos distintos de orden 6 y de orden 10.

Para grupos de orden p^3, con p primo hay tres tipos distintos de grupos abelianos, con invariantes respectivos (p^3), (p^2, p) y (p, p, p) cuyas relaciones definitorias son:

1a. $a^{p^3} = 1$

2o. $a^{p^2} = 1, \quad b^p = 1, \quad ba = ab$

3o. $a^p = 1, \quad b^p = 1, \quad c^p = 1, \quad ba = ab, \quad ca = ac,$
$cb = bc.$

Supongamos que $p = 2$, y consideremos los grupos no abelianos de orden 8. No puede haber ningún elemento de orden 8, pues en tal caso el grupo sería cíclico. Si todos los elementos son de orden 2, entonces $(ab)^2 = 1$, o sea $abab = 1$, $ba = a^2bab^2 = ab$, y el grupo es abeliano. Debe por lo tanto haber un elemento de orden 4, digamos $a^2 = 1$. Si $b \notin \langle a \rangle = A$, entonces $G = A \cup Ab$ y $b^2 \in A$. Si $b^2 = a$ ó $b^2 = a^3$, entonces b es de orden 8 y el grupo G es cíclico. Luego $b^2 = 1$ ó $b^2 = a^2$. También $b^{-1}ab \in A$, pues A es normal, y $b^{-1}ab = a$ ó $b^{-1}ab = a^3$, puesto que es un elemento de orden 4. Pero si $b^{-1}ab = a$, entonces G será abeliano. Luego $b^{-1}ab = a^3$. Hemos encontrado entonces dos grupos no abelianos, de orden 8, distintos cuyas relaciones definitorias son:

$$1o.\quad a^4 = 1, \qquad b^2 = 1, \qquad b^{-1}ab = a^3$$

$$2o.\quad a^4 = 1, \qquad b^2 = a^2, \qquad b^{-1}ab = a^3$$

Al primero se le conoce con el nombre de grupo diedro y al segundo con el de grupo cuaternio.

De lo anterior se desprende que existen solamente, salbo isomorfismo, cinco grupos disnintos de orden 8, de los cuales tres son abelianos y dos son no abelianos.

La tabla siguiente nos resume el número de grupos distintos que existen para cada orden, siendo el orden menor o igual que once.

Orden del Grupo	1	2	3	4	5	6	7	8	9	10	11
Nº de Grupos Distintos	1	1	1	2	1	2	1	5	2	2	1

CAPITULO III

EXTENSION DE LOS TEOREMAS DE SYLOW

La extensión de los Teoremas de Sylow consiste en una generalización de dichos teoremas para grupos solubles en términos de subgrupos cuyo orden m es primo relativo con su índice n sin el requerimiento de que m -- sea la potencia de un primo.

Para tratar este tema es necesario, como es natural, dar algunos conceptos y definiciones que nos permiten llegar a definir y conocer algunas propiedades de los grupos solubles, ya que ellos constituyen el objeto principal de estudio en este capítulo.

DEFINICION 3.1

Un conjunto parcialmente ordenado es un sistema S de elementos en el que está definida una relación $a \supseteq b$ para algunos pares de elementos de S tales que

i) $a \supseteq a$

ii) Si $a \supseteq b$ y $b \supseteq c$, entonces $a \supseteq c$

iii) Si $a \supseteq b$ y $b \supseteq a$, entonces $a = b$

Si además el conjunto S satisface que

iv) Para cualquier a, b ó $a \supseteq b$ ó $b \supseteq a$, entonces decimos que S es un conjunto simplemente ordenado o una cadena.

En algunas ocasiones escribiremos $b \subseteq a$ como equivalente a $a \supseteq b$. También escribiremos $a \supset b$ si $a \supseteq b$ y $a \neq b$. Otra notación que usaremos es $a > b$, que leeremos "a cubre a b" y que significa, $a \supset b$ y $a \supseteq x \supseteq b$ implica $x = a$ ó $x = b$.

DEFINICION 3.2

Una cota superior de un subconjunto T de un conjunto S parcialmente ordenado es un elemento x de S tal que $x \supseteq t$ para todo t de T. En la misma forma, cuna cota inferior de T es un y tal que $t \supseteq y$ para todo t de T.

DEFINICION 3.3

Un supremo (Sup) de un subconjunto T de un conjunto S parcialmente ordenado, es un elemento x tal que:

i) x es cota superior de T.

ii) Si z es una cota superior de T entonces $z \supseteq x$.

En la misma forma un ínfimo (Inf) de T, es un y tal que:

i) y es una cota inferior de T.

ii) Si z es una cota inferior de T, entonces $y \supseteq z$.

En general un subconjunto T no necesariamente tiene que poseer un supremo o un infimo, pero si lo tiene entonces, ya sea supremo o ínfimo, es único, ya que de no serlo, se contendrían cada uno al otro, lo que por ser S un conjunto parcialmente ordenado implicaría que son iguales.

DEIFNICION 3.4

Una red es un conjunto parcialmente ordenado tal que cualesquiera dos de sus elementos a, b tienen un supremo $a \sqcup b$ y un infimo o intersección $a \cap b$.

Como tanto $a \sqcup b$ como $a \cap b$ son únicos, entonces $\sqcup$ y la intersección son operaciones binarias bien definidas en una red.

TEOREMA 3.1

En una red se verifican las siguientes leyes:

1º. Leyes de Idempotencia $x \cap x = x$ y $x \sqcup x = x$

2º. Leyes Conmutativas $x \cap y = y \cap x$ y $x \sqcup y = y \sqcup x$

3º. Leyes Asociativas $x \cap (y \cap z) = (x \cap y) \cap z$ y $z \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$

4º. Leyes de Absorción $x \cap (x \sqcup y) = x$ y $x \sqcup (x \cap y) = x$.

PRUEBA

Para las leyes de 1, 2 y 4 se ve claramente que son consecuencia inmediata de las definiciones de supremo e ínfimo. Para 3 sean $y \cap z = u$ y $x \cap u = w$. Aquí w es una cota inferior de x y u, y por tanto lo es de x, y y z. Pero cualquier cota inferior de x, y y z está contenida en u, luego en $x \cap u = w$. Luego w es el ínfimo de x, y y z. Pero análogamente $(x \cap y) \cap z$ es el ínfimo de x, y y z, de donde $x \cap (y \cap z) = (x \cap y) \cap z$. Por igual razonamiento, tanto $x \sqcup (y \sqcup z)$ como $(x \sqcup y) \sqcup z$ son ambos el supremo de x, y y z, por lo que $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$.

DEFINCIIN 3.5

Una red L_1 se dice que es isomorfa a una red L_2 si hay una fun -- ción biyectiva $x_i \overset{\rightarrow}{\leftarrow} y_i$ entre los elementos x_i de L_1 y y_i de L_2 tal que $x_i \cap x_j \overset{\rightarrow}{\leftarrow} y_i \cap y_j$ y $x_i \sqcup x_j \overset{\rightarrow}{\leftarrow} y_i \sqcup y_j$.

DEFINICION 3.6

Una red L es llamada modular si satisface que si $a \supseteq b$, entonces $a \sqcup (b \cup c) = b \sqcup (a \cap c)$.

Una red se dice que satisface la condición minimal si cualquier cadena $a_1 \supset a_2 \supset a_3 \supset \ldots$ es necesariamente finita, y que satisface la condición maximal si cualquier cadena $a_1 \subset a_2 \subset a_3 \subset \ldots$ es necesariamente finita.

DEFINICION 3.7

En una red L, una cadena finita $x = x_0 \supseteq x_1 \supseteq \ldots \supseteq x_d = y$ se dice que es maximal si x_i cubre a x_{i+1} para $i = 0, 1, \ldots, d-1$ es decir, si $x = x_0 > x_1 > \ldots > x_d = y$. De tal cadena se dice que tiene lognitud d.

DEFINCION 3.8

Un elemento x de una red L tiene dimensión finita d, escrita d(x) si L tiene un elemento cero 0, siempre que toda cadena desde x a 0 sea finita y que d sea la longitud de la cadena maximal de mayor longitud desde x a 0.

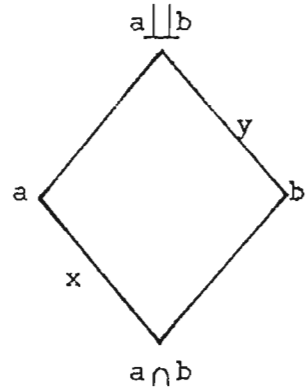
En cualquier red, el conjunto de las x tales que $a \supseteq x \supseteq b$ forman una subred a la que llamaremos el cociente $\frac{a}{b}$. Dos cocientes que pueden ser puesto en las formas $\frac{a \| b}{b}$ y $\frac{a}{a \cap b}$ se dice que son perspectivos uno con respecto al otro, y si $\frac{a_i}{b_i}$ es perspectivo con $\frac{a_{i+1}}{b_{i+1}}$. Para $i = 1,2, \ldots, n-1$, decimos que $\frac{a_i}{b_i}$ es proyectivo con $\frac{a_n}{b_n}$.

TEOREMA 3.2

En una red modular, los cocientes perspectivos son isomorfos.

PRUEBA

Sean los cocientes $\frac{a||b}{b}$ y $\frac{a}{a\cap b}$, en una red modular. Definamos para cualquier x en $\frac{a}{a\cap b}$ $y(x) = x||b$. Para cualquier y en $\frac{a||b}{b}$, definamos a su vez $x(y) = y\cap a$.



La primera aplicación lleva elementos de $\frac{a}{a\cap b}$ a elementos de $\frac{a||b}{b}$ y la segunda lleva elementos de $\frac{a||b}{b}$ a elementos de $\frac{a}{a\cap b}$. Para un x en $\frac{a}{a\cap b}$, se tiene, $x[y(x)] = (x||b)\cap a$. Como $a \supseteq x$, podemos aplicar la ley modular y $a\cap(x||b) = x||(a\cap b) = x$, ya que $x \supseteq a\cap b$. Tenemos pues que $x[y(x)] = x$. Analogamente, para y en $\frac{a||b}{a}$, por aplicación de la ley modular $y[x(y)] = y$. Luego $x \to y(x)$ y $y \to x(y)$ nos proporciona una función biyectiva entre los dos cocientes. Además esta función preserva las operaciones de la red. En efecto, para x_1, x_2 en $\frac{a}{a\cap b}$, tenemos:

$y(x_1||x_2) = (x_1||x_2)||b = (x_1||b)||(x_2||b) = y(x_1)||y(x_2)$. Además, si $x_1 = x(y_1)$ y $x_2 = x(y_2)$, se tiene:

$x_1\cap x_2 = x(y_1)\cap x(y_2) = (y_1\cap a)\cap(y_2\cap a) = (y_1\cap y_2)\cap a = x(y_1\cap y_2)$.

De donde $y(x_1\cap x_2) = y[x(y_1\cap y_2)] = y_1\cap y_2 = y(x_1)\cap y(x_2)$. Luego am-

bas operaciones se preservan en la función $x \to y(x)$. En análoga forma pue de demostrarse que también la función $y \to x(y)$ preserva las operaciones de la red.

TEOREMA 3.3

En una red cuyos elementos son de dimensión finita, la ley

$$d(x) + d(y) = d(x||y) + d(x \cap y)$$

se verifica si y sólo si la red es modular.

PRUEBA

Por el teorema 3.2 en una red modular los cocientes $\frac{x||y}{x}$ y $\frac{y}{x \cap y}$ son isomorfos. La longitud de una cadena maximal finita en cada uno de estos es respectivamente $d(x||y) - d(x)$ y $d(y) - d(x \cap y)$. Por isomo fismo estas dos longitudes son iguales, o sea que

$$d(y) - d(x \cap y) = d(x||y) - d(x)$$

por lo que $d(x) + d(y) = d(x||y) + d(x \cap y)$.

Reciprocamente, supongamos que $d(x) + d(y) = d(x||y) + d(x \cap y)$ se verifica en una red. Supongamos $A \supset B$; consideremos las expresiones $A \cap (B||C)$ y $B||(A \cap C)$.

Tenemos aqui:

$$B \subset A$$

$$B \subset B||C$$

$$B \subset A \cap (B||C)$$

$$A \cap C \subset A$$

$$A \cap C \subset C \subset B||C$$

$$A \cap C \subset A \cap (B||C)$$

$$B||(A\cap C) \subseteq A\cap(B||C)$$

De donde estas dos últimas expresiones serân iguales si sus dimensiones -- son iguales. Pero usando

$$d(x) + d(y) = d(x||y) + d(x\cap y)$$

se tiene:

$$d(A\cap C) + d(B) = d[B||(A\cap C)] + d[B\cap(A\cap C)]$$

de donde:

$$d(B) + d(A\cap C) = d[B\cap(A\cap C)] = d[B||(A\cap C)]$$

$$d(B) + d(A\cap C) - d(B\cap C) = d[B||(A\cap C)]$$

$$d(B||C) - d(C) + d(A\cap C) = d[B||(A\cap C)]$$

$$d(B||C) + d(A) - d(A||C) = d[B||(A\cap C)]$$

$$d(A) + d(B||C) - d(A||(B||C) = d[B||(A\cap C)]$$

$$d[A\cap(B||C)] = d[B||(A\cap C)]$$

Por lo que $A\cap(B||C) = B||(A\cap C)$ y la ley modular se verifica.

En têmrinos de la relaciôn de cubrimiento $A > B$, definimos dos propiedades de semimodularidad que pueden verificarse en una red.

DEFINICION 3.9

Semimodularidad inferior: Una red es inferiormente semimodular si siempre que $A > B$ y $A > C$, $B \neq C$, entonces $B > B\cap C$ y $C > B\cap C$.

Semimodularidad superior: Una red es superiormente semidomular si siempre que $A < B$ y $A < C$, $B \neq C$, entonces $B < B||C$ y $C < B||C$.

Se ve con claridad que las dos clases de semimodularidad son dua-

les, y por lo visto en el teorema 3.2 las dos son concecuencia de la modu laridad.

Estudiaremos ahora una cadena de subgrupos de un grupo G, en don de cada uno de ellos es subgrupo normal del que le precede. Así:

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n$$

en donde cada A_i es un subgrupo normal de A_{i-1}, es una cadena en la cual a los grupos A_i se le da el nombre de grupos subinvarientes de G y a la cadena se le llama serie subinvariante. Si además cada A_i es subgrupo nor - mal de G, entonces llamaremos a la cadena $G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n$, se rie normal o serie invariante. Una serie normal en la que cada A_i es un subgrupo maximal normal contenido en A_{i-1} se llamará una serie principal. - Una serie subinvariante en la que cada A_i es un subgrupo maximal normal de A_{i-1} se llamará una serie de composición. En la terminología de redes, si las inclusiones en $G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n$ son cubrimientos, una se - rie normal se llama una serie principal, y una serie subinvariante se llama una serie de composición. Podemos además exigir que los grupos A_i sean -- subgrupos admisibles con respecto al conjunto de operadores Ω.

Supongamos que $G = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_n = H$ es una serie de composición de un grupo G a un grupo H. Entonces por definición A_{i+1} es un -- subgrupo normal maximal de A_i. Por lo que $\frac{A_i}{A_{i+1}}$ es un grupo simple (Un grupo G es llamado simple cuando no contiene ningún subgrupo normal propio),

ya que un subgrupo normal de $\frac{A_i}{A_{i+1}}$ se correspondería con un subgrupo normal de A_i que contuviera a A_{i+1}; esto según el teorema 1.18. De aquí que si $\frac{A_i}{A_{i+1}}$ es abeliano, entonces no puede contener nigún subgrupo propio y además debe ser finito de orden primo.

Cuando se tienen dos series subinvariantes de subgrupos admisibles desde un grupo G a un grupo H, entonces es posible refinar ambas series por la inserción de grupos subinvariantes admisibles adicionales. Con objeto de probar este hecho importante demostraremos dos lemas, pero antes definiremos cuando es que dos subgrupos son permutables.

Diremos que los subgrupos A y B de un grupo G son permutables si los subconjuntos de G, AB y BA son iguales. Cuando esto sucede se verifica con facilidad que $A||B = AB = BA$, y $AB = BA$ es un subgrupo.

LEMA 3.1

Sean A, B, C subgrupos de un grupo G tales que $A \supseteq B$. Entonces una condición suficiente para que

$$A \cap (B||C) = B||(A \cap C)$$

se verifique, es que B y C sean permutables.

PRUEBA

Por teorema 3.3 sabemos que si $A \supseteq B$, entonces

$$B||(A \cap C) = A \cap (B||C)$$

Falta, entonces probar la inclusión opuesta. Un elemento $a \in A \cap (B||C)$ es de la forma $a = bc$, con $a \in A$, $b \in B$, $c \in C$ pues a

simultáneamente ha de ser un elemento de A y también de $B\|C$, y como B y C permutan, los elementos de $B\|C$ son de la forma bc. Aquí $c = b^{-1}a \in A$ ya que $B \subseteq A$. De donde este $c \in A \cap C$, y por tanto $bc \in B\|(A \cap C)$. Luego $A \cap (B\|C) \subseteq B\|(A \cap C)$, y el lema está probado.

LEMA 3.2

Sean $U = A_0 \supseteq A_1 \supseteq \ldots \supseteq A_n = V$ y $U = B_0 \supseteq B_1 \supseteq \ldots \supseteq B_m = V$ dos cadenas de U a V en una red modular. Entonces es posible refinar ambas cadenas finitas por inserción de elementos adicionales $A_{i-1} = A_{i,0} \supseteq A_{i,1} \supseteq \ldots \supseteq A_{i,m} = A_i$, $i = 1,2, \ldots, n$ y $B_{j-1} = B_{j,0} \supseteq B_{j,1} \supseteq \ldots \supseteq B_{j,m} = B_j$, $j = 1,2, \ldots, m$, de tal forma que los cocientes $\frac{A_{i,\,j-1}}{A_{i,j}}$ y $\frac{B_{j,\,i-1}}{B_{j,i}}$ sean proyectivos.

PRUEBA

Pongamos $A_{i,j} = A_i\|(A_{i-1} \cap B_j)$, $B_{j,i} = B_j\|(B_{j-1} \cap A_i)$, $i = 1,2, \ldots, n$ y $j = 1,2, \ldots, m$.

Aquí $\frac{A_{i,j-1}}{A_{i,j}}$ es perspectivo con $\frac{A_{i-1} \cap B_{j-1}}{(A_{i-1} \cap B_j)\|(A_i \cap B_{j-1})}$, ya que por ser $B_j \subseteq B_{j-1}$ tenemos:

$$(A_{i-1} \cap B_{j-1})\|A_i\|(A_{i-1} \cap B_j) = A_i\|(A_{i-1} \cap B_{j-1}).$$

Además $(A_{i-1} \cap B_{j-1}) \cap [A_i \amalg (A_{i-1} \cap B_j)]$

$= (A_{i-1} \cap B_j) \amalg (A_{i-1} \cap B_{j-1} \cap A_i)$

$= (A_{i-1} \cap B_j) \amalg (A_i \cap B_{j-1})$,

usando la modularidad en las expresiones anteriores. Análogamente $\frac{B_{j,\,i-1}}{B_{j,i}}$ es perspectivo al cociente

$$\frac{A_{i-1} \cap B_{j-1}}{(A_{i-1} \cap B_j) \amalg (A_i \cap B_{j-1})}$$

y con esto el teorema está probado.

TEOREMA 3.4 (Teorema de Refinamiento)

Sea G un grupo con operadores Ω, y sean $G = A_0 \supseteq A_1 \supseteq \ldots \supseteq A_n = H$ y $G = B_0 \supseteq B_1 \supseteq \ldots \supseteq B_m = H$ dos series subinvariantes de subgrupos admisibles desde G a H. Entonces es posible refinar ambas series por la inserción de grupos subinvariantes admisibles adicionales

$$A_{i-1} = A_{i,0} \supseteq A_{i,1} \supseteq \ldots \supseteq A_{i,m} = A_i, \qquad i = 1, \ldots, n$$

y

$$B_{j-1} = B_{j,0} \supseteq B_{j,1} \supseteq \ldots \supseteq B_{j,n} = B_j, \qquad j = 1, \ldots, m$$

de tal forma que los grupos cocientes

$$\frac{A_{i,\,j-1}}{A_{i,j}} \quad \text{y} \quad \frac{B_{j,\,i-1}}{B_{j,i}}$$

sean operadores isomorfos.

PRUEBA

Por el teorema 1.19 los grupos cocientes perspectivos de subgrupos admisibles son operadores isomorfos. Por tanto, para demostrar este teorema por la prueba del lema 3.2 debemos mostrar que en los cocientes $\frac{X}{Y}$ que en ella aparecen Y es normal en X y que el uso de la ley modular es -- válido. Como la juntura e intersección de subgrupos admisibles es también admisible, todos los subgrupos usados en la prueba son admisibles. Ahora $A_{i,j} = A_i \amalg (A_{i-1} \cap B_j)$ es un subgrupo normal de $A_{i,\,j-1} = A_i \amalg (A_{i-1} \cap B_{j-1})$ ya que tanto A_i como $A_{i-1} \cap B_j$ son transformados en si mismos por $A_{i-1} \cap B_{j-1}$. Analogamente, $B_{j,i}$ es normal en $B_{j,\,i-1}$. Tanto $A_{i-1} \cap B_j$ como $A_i \cap B_{j-1}$, y por tanto también su juntura, son subgrupos normales de $A_{i-1} \cap B_{j-1}$, de donde $\dfrac{A_{i-1} \cap B_{j-1}}{(a_{i-1} \cap B_j) \amalg (a_i \cap B_{j-1})}$ es un grupo cociente. En $(A_{i-1} \cap B_{j-1}) \cap [A_i \amalg (A_{i-1} \cap B_j)]$, como A_i es normal en A_{i-1}, A_i permuta con cualquier subgrupo de A_{i-1} y en particular con $A_{i-1} \cap B_j$. Luego por el lema 3.1 la ley modular puede aplicarse, quedando, con esto, probado el teorema.

TEOREMA 3.5

Sea H un subgrupo normal de un grupo G tal que hay una serie de composición de G a H. Entonces hay una serie principal de G a H

$$G = B_0 \supseteq B_1 \supseteq \cdots \supseteq B_m = H$$

y cada grupo factor $\frac{B_i}{B_{i+1}}$ es el producto directo de un número finito de -- grupos simples isomorfos. Recíprocamente, si tal serie existe con $\frac{B_i}{B_{i+1}}$ - como un producto directo de un número finito de grupos simples isomorfos, entonces hay una serie de composición de G a H.

PRUEBA

Toda serie normal de G a H puede refinarse a una serie de composición por la inserción de nuevos términos. De donde cualquier serie normal de G a H es necesariamente más corta que una serie de composición y por tanto de longitud finita. De donde debe haber una serie principal de G a H

$$G = B_0 \supseteq B_1 \supseteq \dots \supseteq B_m = H.$$

Si $m = 1$, $\frac{G}{H}$ es un grupo simple y el teorema es cierto. Usemos inducción sobre m, de donde cada uno de los $\frac{B_0}{B_1}, \dots, \frac{B_{m-2}}{B_{m-1}}$ es el producto directo de un número finito de grupos simples isomorfos. Queda probar que $\frac{B_{m-1}}{B_m}$ es el producto directo de un número finito de grupos simples isomorfos.

Cualquier subgrupo normal de $\frac{B_{m-1}}{B_m}$ corresponde a un grupo normal en B_{m-1} que contiene a B_m. Por tanto existe un subgrupo minimal normal $\frac{K}{B_m}$ donde $K \supseteq B_m$ y K es normal en B_{m-1}. Si $K = B_{m-1}$, entonces $\frac{B_{m-1}}{B_m}$ es simple y no queda nada por probar. Consideremos ahora los conjugados K_j de K respecto a $G.K_j \subseteq B_{m-1}$, ya que B_{m-1} es normal en G. Por otra parte,

como las transformaciones por un elemento de G' inducen un automorfismo en B_{m-1} cada K_j es un subgrupo normal de B_{m-1}. Además $\coprod_j K_j$ es un subgrupo normal de G ya que la transformación por un elemento de G lo único que hace es permutar los K_j entre ellos. De aquí que $\coprod_j K_j = B_{m-1}$ ya que no hay ningún subgrupo normal de G entre B_{m-1} y B_m. Tenemos $K = K_1$, $K_2 \not\subset K_1$, $K_3 \not\subset K_1 \coprod K_2$, y $K_j \not\subset K_1 \coprod \ldots \coprod K_{j-1}$. Cada uno de los $U_j = K_1 \coprod \ldots \coprod K_j$ es un subgrupo normal de B_{m-1} y contiene al U_{j-1} precedente. Como hay una serie de composición de G a B_m que incluye a B_{m-1}, sólo puede haber un número finito de U_{j-es} de donde para algún j finito, $B_{m-1} = K_1 \coprod \ldots \coprod K_j$. Ahora bien, un K_i no contenido en la juntura de los restantes K debe intersectar la juntura de los restantes en B_m, ya que cada K es un subgrupo minimal normal de B_{m-1} que contiene a B_m. De donde, prescindiendo de los K contenidos en la juntura del resto,

$\frac{B_{m-1}}{B_m} = \frac{K_1}{B_m} \coprod \ldots \coprod \frac{K_s}{B_m}$, donde cada $\frac{K_i}{B_m}$ es un subgrupo normal de $\frac{B_{m-1}}{B_m}$ intersector de la juntura de los restantes en la identidad. Pero por el teorema 1.23, $\frac{B_{m-1}}{B_m}$ es el producto directo de $\frac{K_1}{B_m}, \ldots, \frac{K_s}{B_m}$. Ahora bien, si $\frac{K_1}{B_m}$ tuviera un subgrupo normal propio, éste sería un subgrupo normal de $\frac{B_{m-1}}{B_m}$, ya que sería normal en $\frac{K_1}{B_m}$ y seguramente normalizado por los restan

tes factores directos. Pero se había supuesto que $\frac{K_1}{B_m}$ era un subgrupo minimal normal; por tanto $\frac{K_1}{B_m}$ es un grupo simple y $\frac{B_{m-1}}{B_m}$ es el producto directo de los s grupos simples isomorfos.

Para la parte recíproca del teorema obsérvese que $B_m \subset K \subset U_2 \subset U_3 \subset \ldots \subset B_{m-1}$ es parte de una serie de composición, ya que cada grupo factor es simple.

En un grupo G al elemento $x^{-1}y^{-1}xy$ se le llama el conmutador de x y y, y escribimos $x^{-1}y^{-1}xy = (x, y)$. Definimos también conmutadores de orden más alto por la regla recursiva $(x_1,\ldots,x_{n-1},x_n) = ((x_1,\ldots,x_{n-1}),x_n)$. Estos son los conmutadores simples. Más generalmente, el conjunto de todos los elementos que pueden obtenerse por conmutaciones sucesivas se llama el complejo de conmutadores: por ejemplo, ((a,b), (c,d,e)). Definimos el peso w de un conmutador en forma recursiva diciendo que los elementos g de G son de peso uno, $w(g) = 1$, y estableciendo $w(x,y) = w(x) + w(y)$. Así el peso de un elemento que es un conmutador depende de la forma del conmutador por el cual se expresa y no del elemento en si mismo.

Por la definición $(x,y) = 1$ si y sólo si $yx = xy$. Luego todos los conmutadores en G son 1 si y sólo si G es abeliano, y los conmutadores pueden considerarse como midiendo la extensión a que un grupo se aleja de ser abeliano. El subgrupo G' de G generado por todos los conmutadores $x^{-1}y^{-1}xy$ es llamado el subgrupo conmutador o grupo derivado. Claramente G' es un subgrupo totalmente invariante de G.

TEOREMA 3.6

El grupo factor $\frac{G}{G'}$ es abeliano. Si K es un subgrupo normal de G tal que $\frac{G}{K}$ es abeliano, entocces $K \supseteq G'$.

PRUEBA

En la aplicación $G \to \frac{G}{G'} = H$, sean u, v elementos arbitrarios de H, y supongamos $x \to u$, $y \to v$. Entonces $x^{-1}y^{-1}xy \to u^{-1}v^{-1}uv$. Pero $x^{-1}y^{-1}xy \in G'$, de donde $x^{-1}y^{-1}xy \to 1 = u^{-1}v^{-1}uv$, por lo que $vu = uv$ y $\frac{G}{G'}$ es abeliano. Supongamos ahora que $\frac{G}{K}$ es abeliano. Para $x, y \in G$ y $x \to u$, $y \to v$ en $G \to \frac{G}{K}$, tenemos $x^{-1}y^{-1}xy \to u^{-1}v^{-1}uv = 1$. Luego todo conmutador $x^{-1}y^{-1}xy$ pertenece a K, y por tanto $K \supseteq G'$.

DEFINICION 3.10

Un grupo G se dice que es soluble si la sucesión $G \supseteq G' \supseteq G'' \supseteq \dots \supseteq G^{(i)} \supseteq \dots$, donde cada grupo $G^{(i)}$ es el grupo derivado del precedente, termina en la identidad en un número finito de pasos, digamos $G^{(e)} = 1$.

Si observamos la sucesión $G \supseteq G' \supseteq G'' \supseteq \dots \supseteq \dots \supseteq G^{(i)}$, claramente vemos que por aplicación directa del teorema 3.6 los grupos $\frac{G^{(i)}}{G^{(i+1)}}$ son abelianos y además si $G^{(i)} = G^{(i+1)}$, entonces $G^{(i)} = G^{(j)}$ para todo $j \geq i$. De donde las inclusiones en la definición de grupo soluble son todas propias hasta que $G^{(i)} = 1$.

TEOREMA 3.7

Todos los subgrupos y grupos factores de un grupo soluble, son solubles.

PRUEBA

Sea G un grupo soluble y H un subgrupo de G. Entonces, por definición $H' \subseteq H'$, ya que H' está generado por todos los conmutadores de elementos en H y G' por todos los conmutadores en G. Luego $H'' \subseteq G''$, etc., y por tanto si $G^{(e)} = 1$, también $H^{(e)} = 1$ y H es soluble.

Claro que $H^{(i)}$ puede ser la identidad para lagún $i < e$. Si $Q = \frac{G}{K}$ es un grupo factor de G, consideremos el homomorfismo $G \to Q$. Todo conmutador en Q es la imagen de un conmutador en G, luego $G' \to Q'$. Continuando así, $G^{(e)} \to Q^{(e)}$ de donde $Q^{(e)} = 1$ si $G^{(e)} = 1$ y de nuevo $Q^{(i)}$ puede ser la identida para algún $i < e$.

TEOREMA 3.8 (Teorema de Jordan-Holder)

Si $G = A_0 \supset A_1 \supset \dots \supset A_n = H$ y

$G = B_0 \supset B_1 \supset \dots \supset B_m = H$ son dos series principales (o dos series de composición) con operadores Ω, entonces $m = n$ y los grupos factores $\frac{A_{i-1}}{A_i}$ son operadores isomorfos a los grupos factores $\frac{B_{j-1}}{B_j}$ en algún orden.

PRUEBA

Este teorema es una consecuencia directa de la biyección que existe entre los grupos factores que aparecen en el teorema 3.4 (Teoreaa de Refinamiento) de modo que se cumple que $m = n$.

En el caso de series normales, todos los subgrupos, por ser subgrupos normales, son admisibles respecto a todos los automorfismos interiores $x \to a^{-1}xa$, y podemos incluir todos los automorfismos interiores en el conjunto de operadores Ω.

TEOREMA 3.9

Un grupo de orden finito es soluble si y sólo si los grupos factores en una serie de composición de G a 1 son cíclicos de orden primo.

PRUEBA

Supognamos $G = A_0 \supset A_1 \supset \ldots \supset A_r = 1$, donde cada $\frac{A_{i-1}}{A_i}$, $i = 1, 2, \ldots, r$ es cíclico de algún orden primo. Por el teorema 3.6, como $\frac{G}{A_1}$ es abeliano, $A_1 \supseteq G'$. Análogamente, $A_2 \supseteq A_1' \supseteq G''$, y finalmente $A_r \supseteq G^{(r)}$ luego $G^{(r)} = 1$ y G es soluble. Reciprocamente, supongamos que G es soluble y finito. Como $\frac{G}{G'}$ es abeliano, en

$$G \supset G' \supset G'' \supset \ldots \supset G^{(e)} = 1,$$

existirá un subgrupo maximal normal $A_1 \supseteq G'$. Como $\frac{G}{A_1}$ es simple y abeliano, entonces es cíclico de orden primo. Análogamente, como A_1 es soluble, A_1 contiene un subgrupo maximal normal A_2 tal que $\frac{A_1}{A_2}$ es cíclico de orden primo. Continuando tenemos $G = A_0 \supset A_1 \supset \ldots \supset A_r = 1$ con cada $\frac{A_{i-1}}{A_i}$ cíclico de orden primo. Por el teorema 3.8 (Teorema de Jordan-Holder) podemos afirmar que lo mismo es cierto para todas las series de composición.

TEOREMA 3.10

Si G es un grupo soluble finito y $G = C_0 \supset C_1 \supset \ldots \supset C_s = 1$ es una serie principal, entonces los grupos factores

$\frac{C_{i-1}}{C_i}$, $i = 1, 2, \ldots, s$ son grupos abelianos.

PRUEBA

Atendiendo al teorema 3.5 afirmamos que $\frac{C_{i-1}}{C_i}$ es el producto directo de grupos simples isomorfos y por el teorema 3.7 afirmamos que estos grupos simples son solubles y por tanto cíclicos de orden primo. Luego $\frac{C_{i-1}}{C_i}$ es el producto directo de grupos cíclicos del mismo orden primo p y un grupo abeliano elemental.

TEOREMA 3.11

Si G es un grupo, las tres propiedades siguientes son equivalentes.

1) G es soluble.

2) G tiene una serie normal finita $G = A_0 \trianglerighteq A_1 \trianglerighteq A_2 \trianglerighteq \ldots \trianglerighteq A_s = 1$ en la que cada $\frac{A_{i-1}}{A_i}$, $i = 1, \ldots, s$ es abeliano.

3) G tiene una serie subinvariante finita

$$G = B_0 \trianglerighteq B_1 \trianglerighteq \ldots \trianglerighteq B_t = 1$$

en la que cada $\frac{B_{i-1}}{B_i}$, $i = 1, \ldots, t$, es abeliano.

PRUEBA

Si G es soluble, entonces su serie derivada $G \supset G' \supset G'' \supset \ldots \supset G^{(r)} = 1$ es una serie normal finita en la que $\frac{G^{(i-1)}}{G^{(i)}}$ es abeliano para $i = 1, 2, \ldots, r$, de donde la propiedad 2 se cumple y se verifica también la 3. Ahora supongamos que se cumple la propiedad 3, entonces $G = B_0 \supseteq B_1 \supseteq \ldots \supseteq B_t = 1$ es una serie subinvariante con $\frac{B_{i-1}}{B_i}$ abeliano para $i = 1, 2, \ldots, t$, luego como $\frac{G}{B_1} = \frac{B_0}{B_1}$ es abeliano se tiene que $B_1 \supseteq G'$. Análogamente, si $B_{i-1} \supseteq G^{(i-1)}$, entonces $B_i \supseteq B'_{i-1} \supseteq G^{(i)}$. Por lo tanto, finalmente, $1 = B_t \supseteq G^{(t)}$, y $G^{(t)} = 1$, de donde G es soluble.

COROLARIO 3.1

Un grupo G es soluble si tiene un subgrupo normal H tal que tanto H como $\frac{G}{H}$ sean solubles.

PRUEBA

Si $\frac{G}{H} \supseteq \frac{A_1}{H} \supseteq \ldots \supseteq \frac{A_{r-1}}{H} \supseteq \frac{H}{H}$, y $H \supseteq B_1 \supseteq \ldots \supseteq B_{s-1} \supseteq 1$ son series que satisfacen la tercera propiedad del teorema 3.11 para $\frac{G}{H}$ y H, respectivamente, entonces $G \supseteq A_1 \supseteq \ldots \supseteq A_{r-1} \supseteq H \supseteq B_1 \supseteq \ldots \supseteq B_{s-1} \supseteq 1$ es una serie que satisface la segunda propiedad del teorema 3.11 y por lo tanto G es soluble.

Abordaremos ahora la propia extensiôn de los Teoremas de Sylow,

explicando primero en que consiste tal extensión.

Sabemos ya que todo subgrupo de Sylow de un grupo finito goza de la propiedad de que su orden $m = p^a$, p primo, es primo con relación a su índice n, o sea que el máximo común divisor de m y n es igual a 1. Pues - bien, el Sr. Philip Hall en su trabajo titulado "A note on soluble group", publicado en J. London Math. Soc. 3(1928), 98-105, ha mostrado que los teo remas de Sylow se gereralizan para grupos solubles en términos de subgrupos cuyo orden m es primo con relación al índice n pero sin el requerimiento de que m sea la potencia de un primo. Esta generalización es lo que constituye la extensión de los teoremas de Sylow y es lo que mostraremos en lo que sigue.

TEOREMA 3.12

Sea G un grupo soluble de orden mn donde m y n son primos relativos, (m,n) = 1. Entonces:

1) G posee al menos un subgrupo de orden m.
2) Dos subgrupos cualesquiera de orden m son conjugados.
3) Cualquier subgrupo cuyo orden m' divide a m está contenido en un subgrupo de ordem m.
4) El número h_m de subgrupos de orden m puede ser expresado como un pro - ducto de factores, cada uno de los cuales (a) es congruente con 1 módulo algún factor primo de m, y (b) es una potencia de un primo y divide a uno de los factores principales de G.

PRUEBA

La prueba será por inducción sobre el orden de G, observando que es tirvialmente cierta cuando el orden de G es una potencia de un primo, puesto que de ser así, las propiedades (1) y (3) se dan en el primer teorema de Sylow y la propiedad (2) es el resultado del segundo teorema de -- Sylow, quedando la propiedad (4) como un resultado más fuerte que el tercer teorema de Sylow. Además la prueba se apoyará en la estructura de una serie principal de G como se vió en el teorema 3.3 y en la estructura de los grupos factores, según teorema 1.18.

CASO 1.

G tiene un subgrupo normal propio H de orden $m_1 n_1$ e índice $m_2 n_2$ donde $m = m_1 m_2$, $n = n_1 n_2$ y $n_1 < n$.

Para la propiedad (1) $\frac{G}{H}$ por inducción contiene un subgrupo de orden m_2 que corresponde a un subgrupo D de G de orden mn_1. D por inducción contiene un subgrupo de orden m.

Para la propiedad (2), si M y M' son dos subgrupos de orden m, $M\amalg H = MH$ y $M'\amalg H = M'H$ son subgrupos cuyos ordenes dividen $m_1 m_2 m_1 n_1$ ya que según teorema 1.19 $\frac{M\amalg H}{H}$ y $\frac{M}{M\cap H}$ son operadores isomorfos, $\frac{M\amalg H}{H} \cong \frac{M}{M\cap H}$. Como el orden también divide a mn, debe dividir a mn_1. Pero es también un múltiplo de m y un múltiplo de n_1. De donde tanto $M\amalg H$ como $M'\amalg H$ son de orden $mn_1 = m_1 n_1 m_2$, y por tanto $\frac{M\amalg H}{H}$ y $\frac{M'\amalg N}{H}$ son subgru-

pos de $\frac{G}{H}$ de orden m_2 y son por inducción conjugados.

Si a^* en $\frac{G}{H}$ transforma $\frac{M'\|H}{H}$ en $\frac{M\|H}{H}$, y a en G nos lleva a a^* por el homomorfismo $G \to \frac{G}{H}$, entonces $a^{-1}(M'\|H)$ a nos lleva a una imagen en $\frac{M\|H}{H}$; en otras palabras $a^{-1}(M'\|H)a = M\|H$. Aquí $a^{-1}M'a$ y M son de orden m - en M H y son por inducción conjugados. De donde M y M' son conjugados - de G.

Para la propiedad (3), si M_1 es un subgrupo de orden m', un divisor de m, entonces el orden $\frac{M_1\|H}{H}$ es un divisor de m_2 y por tanto pertenece a un subgrupo de $\frac{G}{H}$ de orden m_2. Luego M_1 pertenece al correspondiente subgrupo de G de orden mn_1 y por inducción sobre este grupo M_1 pertenece a un subgrupo de orden m.

Para la propiedad (4), siguiendo a la prueba de (2), el número h_m de conjugados de M de orden m es el producto de h_{m_2}, el número de subgrupos de orden m_2 en $\frac{G}{H}$ y el número de conjugados de M en $M\|H = D$. Aquí los -- factores principales de D dividen a los de G y los factores principales de $\frac{G}{H}$ son un subconjunto de los de G. Luego por inducción h_m es el producto de dos factores, los cuales satisfacen la propiedad (4) por lo que la pro - piedad se prueba.

Fijémonos ahora en que el subgrupo normal mínimo K en una serie - principal es de orden p^a con p un primo. K satisfará los requerimientos para el H del caso 1 a menos que $n = p^a$. Luego podemos suponer que todo sub-

grupo minimal normal es de orden p^a. Pero como subgrupos de Sylow de -- orden p^a solo puede haber uno.

CASO 2.

G contiene un subgrupo minimal normal único K de orden $n = p^a$.

Para la propiedad (1) sea L un subgrupo normal minimal que contiene propiamente a K. Entonces $\frac{L}{K}$ es de orden q^b con $q \neq p$. Sea Q un subgrupo de Sylow de L de orden q^b y sea M el normalizador de Q en G. -- Consideremos $M \cap K = T$. T es un subgrupo normal de M y, como un subgrupo de K, es abeliano elemental. Todo elemento de T permuta con todo elemento de Q, ya que un conmutador de un elemento en Q y un elemento en T pertenece a $T \cap Q = 1$. Luego T pertenece al centro C de L, que, como un subgrupo característico de L, es un subgrupo normal de G. Como K es minimal y único, $C = K$ ó $C = 1$. Si $C = K$, entonces $L = K \times Q$, y Q es un subgrupo normal de G en contra de la unicidad de K. Luego $T = C = 1$. Luego Q es su propio normalizador en L y tiene tantos conjugados en L como su índice en L; es decir, Q tiene $n = p^a$ conjugados en L. Cualquier conjugado de Q en G está en L, ya que L es normal. De donde Q tiene $n = p^a$ conjugados en G, de donde M es de índice $n = p^a$ en G y por tanto de orden m.

Para la propiedad (2) y (4), los normalizadores de los p^a conjugados de Q son conjugados y distintos. Luego tenemos p^a subgrupos conjugados de orden m. Además $p^a \equiv 1 \pmod{q}$ como el número de subgrupos de Sylow de orden q^b en L. Ahora bien, si M' es un subgrupo cualquiera de orden m, el orden de $M' \amalg L$ es divisible por ambos m y n, de donde $M' \amalg L = G$. Como $\frac{G}{L} = \frac{M'}{M' \cap L}$, vemos que $M' \cap L$ es de orden q^b y por lo tanto un conju

gado de Q. Además, $M' \cap L$ es normal en M', de donde M' es el normalizador de un conjugado de Q. Luego los p^a subgrupos conjugados de orden m ya encontrados constituyen todos los subgrupos de orden m. Lo que prueba tanto (2) como (4).

Para la propiedad (3), sea M' un subgrupo de orden m' que divide a m. Entonces, si M es de orden m, $M \cap (M' \| K) = M^*$ es de orden m', y por la propiedad (2) para $M' \| K$, M^* es conjugado de M'. De donde M' está contenido en un conjugado de M, probando así a (3).

Puede probarse que la primera propiedad del teorema 3.12 caracteriza a los grupos solubles; pero para ello necesitamos de un teorema, llamado teorena de Burnside, el cual asegura que un grupo G de orden $p^a q^b$, - donde p y q son primos, es soluble. Pero para probar este teorema necesitamos apartarnos mucho del objeto que se persigue en este trabajo, por lo que lo aceptamos como cierto y dejamos para el lector acucioso, investigarlo en las obras siguientes:

1º. Group Theory, Rudolf Kochendoerffer,
McGraw-Hill. London, Capítulo 13, página 278.

2º. Teoría de los Grupos, Marshall Hall, Jr.,
Editorial F. Trillas, S.A. México, Capítulo 16,
Página 301.

En un grupo G de orden g, un p-complemento es un subgrupo S'_p cuyo índice p^e es la potencia máxima de p que divide a su orden g. Por tanto la primera propiedad del teorema 3.12 asegura la existencia de p-complementos en los grupos solubles.

Usando el resultado del teorema de Burnside probaremos el si -- guiente:

TEOREMA 3.13

Si un grupo G contiene un p-complemento para cada primo p que divida a su orden, entonces G es soluble.

PRUEBA

Sea g el orden de G y $g = p_1^{e_1} \dots p_r^{e_r}$, donde los p_i son primos. Si H_1 y H_2 son subgrupos de índices $p_i^{e_i}$ y $p_j^{e_j}$, respectivamente, entonces como los índices son primos relativos según teorema 1.13, $H_{12} = H_1 \cap H_2$ es de índice $p_i^{e_i}$ y $p_j^{e_j}$. La intersección de H_{12} con un p_k-complemento será de nuevo por el teorema 1.13 de índice $p_i^{e_i} p_j^{e_j} p_k^{e_k}$. Continuando de esta forma, si $g = nm$ con $(m,n) = 1$, podemos encontrar un subgrupo de orden m e índice n, que será la intersección de p-complementos para primos p que dividen a n. Luego la existencia de p-complementos es - suficiente para probar la existencia de un subgrupo de orden m primo a su índice n y por tanto para probar completamente la primera propiedad.

Supondremos que es cierto el teorema para grupos de orden menor que g y procederemos por inducción. En un grupo de orden p^a todo subgrupo maximal es de índice p y un subgrupo normal (según corolario 2.2), y por - tanto un grupo de orden p^a es soluble. Aceptamos el teorema de Burnside - de que un grupo de orden $p^a q^b$ es soluble, y de aquí que ahora solo podamos considerar casos en que el orden de G es divisible por al menos tres -

primos distintos. G contiene un subgrupo H de orden $p^a q^b = m$ primo con su índice n, $mn = g$, donde p y q son dos primos diferentes que dividen a g. Ahora bien , H, como grupo soluble, contiene un subgrupo normal mínimo K que, por el teorema 3.10, es abeliano elemental con la potencia de un primo como orden, digamos p^i. K estará contenido en un subgrupo de Sylow $P \subseteq H \subseteq G$ de orden p^a. Aquí un q-complemento L^* en G contendrá un subgrupo de Sylow P^* conjugado de P en G. De donde una transformación por algún elemento de G llevará L^* a un q-complemento L que contenga a P. -- Aquí $L \supseteq P$ y $H \supseteq P$, y por tanto, por sus órdenes, $L \cap H = P$, $L \| H = G$, y en realidad, $LH = G$, ya que LH contienen g elementos distintos. Así -- pues, toda clase lateral de L contiene un elemento de H, por tanto, todos los conjugados de L se obtienen por transformaciones por elementos $h \in H$. Pero $h^{-1}Lh \supseteq K$, ya que $h^{-1}Kh = K$, pues K es normal en H. Luego la intersección M de los conjugados de L es un subgrupo de G, ya que $K \subseteq M \subset L$, y siendo una intersección de un conjunto completo de conjugados es un subgrupo normal de G.

Por tanto G contiene un subgrupo normal propio M. Si S'_p es un p-complemento en G, entonces $S'_p \cap M$ es un p-complemento en M y $\frac{S'_p \| M}{M}$ es un p-complemento en $\frac{G}{M}$. Luego tanto M como $\frac{G}{M}$ poseen p-complementos y por inducción son solubles. Luego G es soluble.

En el capítulo anterior cuando tratamos el problema de la construcción de grupos finitos, dividimos el caso en dos partes, primero la cons --

trucción de grupos que tienen como orden la potencia de un primo, y segundo, la combinación de grupos de órdenes potencias de primos que dividen a un número n para formar un grupo de orden n. La primera parte ya fué -- tratada pero la segunda es de la que nos ocuparemos ahora.

El problema tiene solución cuando todos los subgrupos de Sylow con cíclicos, aunque para resolverlo necesitamos conocer algunos teoremas previos.

TEOREMA 3.14

Sea G un grupo de orden g y sea C una clase de h elementos conjugados. El número de soluciones de $x^n = c$, donde c recorre C es un múltiplo de (hn, g).

PRUEBA

Designemos por A(k, n) al conjunto de aquellos elementos de G cuya enésima potencia se encuentra en el subconjunto K de G, y sea a(k, n) el número de elementos en A(k, n). Para g = 1, (hn, g) = (hn, 1) = 1, y el resultado es trivial, mientras que para n = 1 el número de soluciones es h = (h,g). Usaremos inducción sobre g y n, suponiendo que el teorema - es cierto para cualquier $g' \leq g$ y $n' < n$.

Si $c' = u^{-1}cu$ y $x^n = c$, entonces $(u^{-1}xu)^n = c'$, dando una correspondencia uno a uno entre las soluciones para un elemento c y cualquiera de sus conjugados. Por tanto a(C, n) = h.a(c, n). Si $x^n = c$, entonces $x^{-1}cx = c^{-1}(x^n)x = x^n = c$, y las soluciones de $x^n = c$ se encuentran en el normalizador N_c de C, que por el teorema 1.14 es de orden $\frac{g}{h}$. De don

de si $h > 1$, siendo cierto el teorema para N_c, $a(c, n)$ es un múltiplo de $(n, \frac{g}{h})$, y por tanto, $a(C, n) = h.a(c, n)$ es un múltiplo de $h(n, \frac{g}{h}) = (hn, g)$, quedando probado el teorema.

Supongamos ahora $h = 1$. Si $n = n_1 n_2$, $(n_1, n_2) = 1$, $n_1 > 1$, $n_2 > 1$, y si $D = A(C, n_2)$, entonces $A(C, n) = A(D, n_1)$. D consta de clases completas. Por inducción (n_1, g) es un divisor de $a(C, n)$ y, análogamente, (n_2, g) es un divisor de $a(C, n)$. Pero entonces, como (n_1, g) y (n_2, g) son primos relativos, su producto $(n_1, g)(n_2, g) = (n_1 n_2, g) = (n, g)$ divide a $a(C, n)$, probándose así el teorema. Podemos ahora suponer que $n = p^e$, es la e-ésima potencia de un primo. Si p divide al orden u de C, entonces un elemento x en $A(c, n)$ tiene orden nu. Entonces exactamente n elementos en el subgtupo cíclico generado por x pertenecen a $A(c, n)$ y todos ellos generan el mismo subgrupo. De donde $A(c, n)$ es divisible por n.

Finalmente supongamos que $n = p^e$ es primo relativo al orden u de c. Como $h = 1$, c está en el centro de G. Los elementos en el centro de G cuyos órdenes no son admisibles por p forman un grupo abeliano B cuyo orden b no es divisible por p.

Sean ahora c_1 y c_2 dos elementos de B. Como p no divide a b, la ecuación $c_2 = c_1 y^n$ tiene una solución única y en B. Pero entonces si $x^n = c_1$, tenemos $(xy)^n = c_2$ y por tanto, $a(c, n)$ tiene el mismo valor para todo $c \in B$. Finaleente la ecuación

$$g = \sum_{c \notin B} a(C, n) + ba(c, n)$$

cuenta los g elementos de G de acuerdo a la clase en que se encuentran sus n-ésimas potencias, contando primero para aquellas clases que no están en B, y al final para B, b veces el número para una de ellas. Ahora bien, (n, g) divide cada término a(C, n) en la primera suma, puesto que cada -- término de ella se encuentra cubierto por la inducción o una parte previa de la prueba. Además como (n, g) divide a g y es primo con b, debe seguir se que (n, g) divide a a(c, n), completándose así la prueba del teorema en todos los casos.

Este teorema no es más que la generalización del teorema de Frobenius y hay que observar que si c es la identidad, entonces h = 1 y tenemos la forma original del teorema. Aquí $x^g = 1$ para todos los elementos, y por tanto, si (n, g) = m, de $x^n = 1$ se sigue $x^m = 1$.

TEOREMA 3.15

Si el orden de un grupo G es divisible por n, entonces el número de soluciones de $x^n = 1$ en G es un múltiplo de n.

Observemos que como la identidad satisface las ecuaciones, el número de soluciones no es cero y debe por tanto ser al menos n.

Es interesante hacer notar que con relación a este teorema hay una conjetura que dice: Si n divide al orden de G y hay exactamente n soluciones de $x^n = 1$ entonces las soluciones forman un subgrupo normal de G. Queda al lector investigar sobre esta conjetura.

TEOREMA 3.16

Si dos grupos factores consecutivos de grupos derivados

$G' \supset G'' \supset G''' \supset \ldots$ de un grupo G son cíclicos, entonces el último es la identidad.

PRUEBA

Podemos tomar $G''' = 1$, tomando $\frac{G'}{G''}$ y $\frac{G''}{G'''}$ como cíclicos, y debemos demostrar que $G'' = 1$. Sea b un generador de G''. Ahora G es el normalizador de G'', y si Z_b es el centralizador de G'', $\frac{G}{Z_b}$ es isomorfo a un grupo de automorfismos de un grupo cíclico, y, por tanto, abeliano. De donde $Z_b \supseteq G'$. Pero entonces G'' es el centro de G' y G' está dado por la adjunción de un solo elemento a G''. Pero entonces G' es abeliano, y por tanto $G'' = 1$, como queríamos demostrar.

DEFINICION 3.11

Un grupo G es metacíclico si $\frac{G}{G'}$ y G' son ambos cíclicos.

TEOREMA 3.17

Si los subgrupos de Sylow de un grupo finito G de orden g son todos cíclicos, entonces G es metacíclico y está generado por dos elementos a y b con las relaciones definitorias:

$$a^m = 1, \qquad b^n = 1, \qquad b^{-1}ab = a^r, \qquad mn = g,$$

$$[(r-1)n, m] = 1, \qquad r^n \equiv 1 \pmod{m}.$$

Recíprocamente, un grupo dado por tales relaciones definitorias tiene todos sus subgrupos de Sylow cíclicos.

PRUEBA

Tenemos que mostrar primero que G es soluble. Sea $g = p_1^{e_1} \ldots p_s^{e_s}$,

$p_1 < p_2 < \ldots < p_s$ la descomposición de g en sus factores primos. Mos - traremos que para $m = p_j^{f_j} p_{j+1}^{e_{j+1}} \ldots p_s^{e_s}$, $f_j \leq ej$, la ecuación $x^m = 1$ tiene exactamente m soluciones. Esto es seguramente cierto para $m = g$. - Luego es suficiente mostrar que si $x^{mp} = 1$ tiene exactamente mp solucio nes y p es el primo más pequeño que divide a mp, entonces $x^m = 1$ tiene - exactamente m soluciones. Como el subgrupo de Sylow que pertenece a p es cíclico, entonces si p^{f+1} es la mayor potencia de p que divide a pm, hay elementos de orden p^{f+1} en G; por tanto no todas las soluciones de $x^{mp} = 1$ son también soluciones de $x^m = 1$. De donde las km soluciones de $x^m = 1$, según teorema 3.15 son una parte propia de las soluciones de $x^{mp} = 1$, y por tanto $1 \leq k < p$. Un elemento que satisface $x^{mp} = 1$ pero no $x^m = 1$ - tiene un orden t exactamente divisible por p^{f+1}. Habra aquí $\phi(t)$ elemen - tos, todos generando el mismo grupo cíclico, todos los cuales tienen un orden exactamente divisible por p^{f+1}. Como p^{f+1} divide a t, $\phi(t)$ es divi- sible por p-1. De donde $pm - km = (p-k)m$, el número de elementos que sa tisfacen $x^{mp} = 1$ pero no $x^m = 1$, es divisible por p-1. Como p era el -- primo mínimo que dividía a m, p-1 no tiene ningún factor en común con m. Luego p-1 divide a p-k, y como $1 \leq k < p$, esto es posible solamente si k=1 es decir, si $x^m = 1$ tiene exactamente m soluciones. En particular para $m = p_s^{e_s}$, $x^m = 1$ tiene exactamente m soluciones.- Pero hay un subgrupo de Sylow de este orden que debe por tanto ser un subgrupo normal de G. Es te es cíclico y, por tanto, soluble.

Hemos mostrado que un grupo G con subgrupos cíclicos de Sylow debe tener un subgrupo normal H. Luego ambos H y $\frac{G}{H}$ también tienen subgrupos cíclicos de Sylow. Podemos suponer inductivamente que H y $\frac{G}{H}$ son solubles y por tanto G es tabbién soluble, ya que un grupo de orden primo es soluble.

Un grupo abeliano cuyos subgrupos de Sylow son cíclicos es él mismo cíclico. De donde en $G \supset G' \supset G'' \supset \ldots$ los grupos factores son cíclicos y por el teorema 3.16 $G'' = 1$. Si $G' = 1$, entonces G es cíclico y este caso está cubierto si tomamos $b = 1$, $r = 1$, $n = 1$, $m = g$. Supongamos pues $G' \neq 1$, y sea a un generador de G' con $a^m = 1$. Sea b un elemento de una clase lateral G'b que es un generador del grupo cíclico factor $\frac{G}{G'}$. Aquí a y b generan G, y $b^{-1}ab = a^r$ con $r \neq 1$, ya que G' es un subgrupo normal; si $r = 1$, G sería abeliano y por tanto cíclico, en contra de lo supuesto. Si $\frac{G}{G'}$ es de orden n, entonces $b^{-n} ab^n = a^{r^n} = a$ y $r^n \equiv 1 \pmod{m}$. Ahora bien, todo elemento de G es de la forma $b^j a^i$, de donde el commutador más general $(b^u a^v, b^j a^i)$ -- puede expresarse en términos de conmutadores de la forma (a^k, b^t); estos - en turno son potencias de $a^{-1}b^{-1}ab = a^{r-1}$. Luego a^{r-1} genera G' y por tanto $(r-1, m) = 1$. Ahora $b'' \in G'$ es una potencia a^j de a tal que permuta con b, de donde $a^{rj} = a^j$, pero como $(r-1, m) = 1$, $j=0$ y por tanto $b^n = 1$.

Si m y n tuvieran un factor primo p en común, $a^{m/p}$ y $b^{n/p}$ generarían un subgrupo no cíclico de orden p^2, en contrario al hecho de que los subgrupos de Sylow son cíclicos. De donde (m, n) = 1. Esto completa la parte directa de la prueba.

Reciprocamente, supóngamos que m, n, r y g satisfacen las relaciones definitorias. Entonces $a \to a^r$, como $r^n \equiv 1 (\text{mod } m)$, es un automorfismo del grupo cíclico generado por a, cuya n-ésima potencia (y posiblemente una potencia inferior) es la identidad. Así con mn elementos $b^j a^i$, j módulo n, i módulo m, y la ley de producto $b^j a^i . b^k a^t = b^{j+k} a^h$, $h = ir^k + t$, podemos verificar la ley asociativa y la existencia de inversos de donde tenemos un grupo de orden g = mn con relaciones $a^m = 1$, $b^n = 1$, $b^{-1}ab = a^r$ y podemos observar que la ley del producto es una consecuencia de estas relaciones definitorias. En este grupo cada conmutador es una potencia de $a^{-1}b^{-1}ab = a^{r-1}$, de donde como (r-1, m) = 1, G' está generado por a. Como (m, n) = 1, todo subgrupo de Sylow es un conjugado del subgrupo $\langle a \rangle$ o del subgrupo $\langle b \rangle$ y por tanto cíclico.

COROLARIO 3.1

Todo grupo G en cuyo orden no aparecen cuadrados es matecíclico del tipo descrito en el teorema 3.17.

Se sigue esto de que los subgrupos de Sylow son todos de orden primo y necesariamente cíclicos.

BIBLIOGRAFIA

1) Kochendorffer, R., GROUP THEORY, McGraw-Hill
London, 1970.

2) Mitchell A.R. - Mitchell R.W., AN INTRODUCTION TO ABSTRACT ALGEBRA,
Wadsworth Publishing Company, 1970.

3) Hall M., TEORIA DE LOS GRUPOS, Editorial F. Trillas, 1969.

4) Birkhoff-Mac Lane, ALGEBRA MODERNA, Editorial Vicens Vives, 1963.

5) Herstein I.N., ALGEBRA MODERNA, Editorial Trillas, 1973.

6) Paley H. - Weichsel P.M., A FIRST COURSE IN ABSTRACT ALGEBRA,
Holt Rinehart and Winston, 1966.

7) Baumslag B. - Chandler B., TEORIA DE GRUPOS,
Libros McGraw-Hill, 1972.