

Álgebra II

Rodrigo Raya Castellano
Universidad de Granada
rjraya@correo.ugr.es

Índice

1. Prólogo	3
2. Tema 1: preliminares	4
2.1. El anillo de enteros módulo n	4
2.2. Función ϕ de Euler	5
3. Tema 2: grupos. Definiciones y ejemplos. Homomorfismos de grupos.	6
3.1. Definición de grupo y primeras propiedades	6
3.2. Ejemplos de grupos	7
3.2.1. Anillos y unidades de un anillo.	7
3.2.2. Grupo de las raíces n -ésimas de la unidad.	7
3.2.3. Grupo lineal general de orden n .	7
3.2.4. Grupos simétricos	8
3.2.5. Grupos diédricos.	10
3.2.6. Grupo de los cuaternios.	11
3.2.7. Grupo de Klein.	11
3.2.8. Grupo alternado.	11
3.3. Homomorfismos.	11
4. Tema 3: subgrupos. Órdenes e índices.	13
4.1. Definición de subgrupo. Ejemplos y primeros resultados.	13
4.2. Retículo de subgrupos de un grupo.	14
4.3. Producto de subgrupos.	15
4.4. Subgrupo generado por un conjunto.	15
4.5. Teorema de Lagrange.	16
4.6. Orden de un elemento.	17
4.7. Clasificación de los grupos cíclicos y descripción del retículo de subgrupos.	18
5. Tema 4: grupos cociente, teoremas de isomorfía y producto directo de grupos	19
5.1. Subgrupos normales	19
5.2. Grupo cociente	20
5.3. Teoremas de isomorfismo	21
5.4. Producto directo	23
5.4.1. Producto directo de grupos	23
5.4.2. Producto directo de homomorfismos	24
5.4.3. Producto directo interno	25
6. Grupos solubles	26
6.1. Grupos simples y series normales	26
6.2. Grupos solubles	30
7. Tema 6: G-conjuntos y p-grupos	34
7.1. G-conjuntos	34

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.



1. Prólogo

Las presentes notas fueron confeccionadas por mí durante el verano de 2016. Están basadas en los apuntes de la profesora María del Pilar Carrasco Carrasco del curso 2016-2017. Estas notas tienen lagunas en su redacción aunque los resultados más importantes del curso aparecen razonados. Si alguna persona quisiera completar el trabajo aquí realizado, sólo tiene que ponerse en contacto conmigo ya que será difícil que vuelva sobre ellas para completarlas. Así mismo existe una colección de ejercicios todavía más pequeña que estas notas y que podría ser también completada.

Quería por último agradecer a Andrés Herrera la elaboración de la plantilla de latex con la que he trabajado y a los compañeros del Doble Grado en Ingeniería Informática y Matemáticas de la Universidad de Granada que me han inspirado para realizar este tipo de aportaciones. Espero que estas notas te sirvan de ayuda querido lector para superar con mayor facilidades el curso de Álgebra II y quien sabe si profundizar más en aspectos que nosotros no pudimos. También quería recordarte que ni Pilar Carrasco ni yo hemos inventado la rueda (bueno quizá ella sí) y que encontrarás el contenido de estas notas parcialmente en muchos libros y en internet en particular en el sitio de preguntas y respuestas `math.stackexchange.com`. Una lista de libros más o menos completa y más o menos útil es la siguiente:

Basic Algebra I, N. Jacobson. W. H. Freeman and Company, 1985.
 A Book of Abstract Algebra, C. Pinter. McGraw-hill, 1982.
 Algebra, M. Artin. Prentice-Hall, 1991.
 Introduction to Group Theory, W. Ledermann. Logman Group, 1973.
 Topics in Geometric Group Theory, P. de la Harpe. The University of Chicago Press, 2000.
 Visual Group Theory, N. Carter. Mathematical Association of America, 2009.
 Algebra, L. Grove. Academic Press, 1983.
 History of Algebraic Geometry, J. Dieudonné. Wadsworth, In., 1985.
 Topics in Algebra, I. Herstein. Gin and Company, 1964.
 The theory of groups, H. Zassenhaus. Chelsea Publishing Company, 1949.
 Advanced Modern Algebra, J. Rotman. American Mathematical Society, 2010.
 Fraileigh (como se llame, el clásico).
 Abstract algebra, Dummit y Foote. John Wiley and Sons, 2004.
 Problems in Group Theory, J. Dixon. Blaisdell Publishing Company, 1967.
 Finite Group Theory, M. Aschbacher. Cambridge University Press, 2000.

Cabe destacar aunque no se siga el mismo orden en la Universidad de Granada:

Números, grupos y anillos. J. Dorronsoro y E. Hernández. Addison-Wesley, 1996.

2. Tema 1: preliminares

2.1. El anillo de enteros módulo n

Para cada $n \geq 1$ consideramos \mathbb{Z}_n que es el conjunto obtenido como cociente $\mathbb{Z}/n\mathbb{Z}$. Esto es, mediante la relación de equivalencia:

$$x \sim y \iff x, y \in \mathbb{Z}_n \iff x - y \in n\mathbb{Z} \iff n|(x - y)$$

Considerando en \mathbb{Z}_n la estructura de dominio euclídeo tenemos que por algoritmo de Euclides:

$$\forall a, b \in \mathbb{Z} \ b \neq 0 \ \exists! q, r \ a = bq + r \text{ con } 0 \leq r < |b|$$

y por tanto existen exactamente n clases de equivalencia en \mathbb{Z}_n y una colección de representantes es $\{0, 1, \dots, n-1\}$.

Denotaremos al resto r como $r = \text{res}(a, b)$ o $a \equiv r \pmod{b}$ y para poder operar con los representantes adecuados definiremos las operaciones:

$$i + j = \text{res}(i + j, n)$$

y

$$i \cdot j = \text{res}(i \cdot j, n)$$

.

Proposición 2.1.

\mathbb{Z}_n es un anillo conmutativo cuyo elemento neutro para la suma es la clase cuyo representante es el cero y cuyo elemento neutro para el producto es la clase cuyo representante es el uno. Además:

\mathbb{Z}_n es un cuerpo $\iff n$ es un número primo.

Demostración. Demostraremos sólo la última afirmación.

\Rightarrow Por reducción al absurdo, si \mathbb{Z}_n es un cuerpo y asumimos que n no es primo entonces n puede factorizarse como $n = r \cdot s$ donde $1 < r, s < n$. Luego en \mathbb{Z}_n se verifica que $0 = r \cdot s$ y por tanto a o b son divisores de cero. Esto es una contradicción ya que un cuerpo es siempre un dominio de integridad y en un dominio de integridad no hay divisores de cero distintos de cero.

\Leftarrow Por otro lado, si n es primo y tomamos $1 \leq r \leq n-1$ se verifica que $\text{mcd}(r, n) = 1$ y por el teorema de Bézout $\exists a, b \in \mathbb{Z}_n$ tales que $1 = ar + bn$ y tomando restos en \mathbb{Z}_n queda que $1 = br$ de donde b es el inverso de r .

□

Recordemos que las unidades de un anillo era el conjunto:

$$U(A) = \{a \in A : \exists a^{-1} \in A \text{ tal que } aa^{-1} = 1 = a^{-1}a\}$$

Las unidades de los anillos de enteros \mathbb{Z}_n son conocidas:

Proposición 2.2 (Unidades de los anillos de restos módulo n).

$$U(\mathbb{Z}_n) = \{r \in \mathbb{Z}_n : r \neq 0 \text{ y } \text{mcd}(r, n) = 1\}$$

Demostración. Llamemos $A = \{r \in \mathbb{Z}_n : r \neq 0 \text{ y } \text{mcd}(r, n) = 1\}$ y probemos la igualdad con $U(\mathbb{Z}_n)$ por doble inclusión.

Veamos que $A \subseteq U(\mathbb{Z}_n)$. Si $a \in A$ por el teorema de Bézout $\exists r, s \in U(\mathbb{Z}_n)$ tales que $1 = nr + as$ y tomando restos módulo n se verificará que $1 = as$. Luego $a \in U(\mathbb{Z}_n)$.

Veamos que $U(\mathbb{Z}_n) \subseteq A$. Si $u \in U(\mathbb{Z}_n)$ tenemos que en \mathbb{Z}_n , $\exists u^{-1}$ tal que $uu^{-1} = 1$ y por tanto, en \mathbb{Z} tendremos que $uu^{-1} = 1 + ny$. Sea $d = \text{mcd}(u, n)$ entonces d divide a u y divide a n por lo que debe dividir a 1, y por tanto, debe ser 1.

□

2.2. Función phi de Euler

Definición 2.1 (Función phi de Euler).

La función phi de Euler está dada por:

$$\phi(n) := |U(\mathbb{Z}_n)|$$

Proposición 2.3 (Propiedades de la función phi de Euler).

1. Si $\text{mcd}(m, n) = 1$ entonces $\phi(mn) = \phi(m)\phi(n)$.
2. Si $p \geq 1$ es un número primo entonces $\phi(p^e) = p^{e-1}(p-1)$.

Demostración. Veamos 1. Usamos la propiedad de las unidades del anillo producto que dice que

$$U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$$

y el teorema chino de los restos que dice que

$$\text{mcd}(m, n) = 1 \iff \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

De este modo, aplicando la primera propiedad se obtiene que

$$|U(\mathbb{Z}_m \times \mathbb{Z}_n)| = |U(\mathbb{Z}_m)| \times |U(\mathbb{Z}_n)| = \phi(m)\phi(n)$$

y aplicando la segunda y el hecho de que los isomorfismos mantienen el número de unidades del anillo tendremos que

$$\phi(mn) = |U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_m \times \mathbb{Z}_n)|$$

Veamos 2. Sea $p \geq 1$ un número primo.

$$\phi(p^e) = |U(\mathbb{Z}_{p^e})| = |\{r \in U(\mathbb{Z}_{p^e}) : r \neq 0, \text{mcd}(r, p^e) = 1\}| = |\mathbb{Z}_{p^e}| - |\{0, p, 2p, \dots, (p-1)p^{e-1}\}| = p^e - p^{e-1} = p^{e-1}(p-1)$$

□

3. Tema 2: grupos. Definiciones y ejemplos. Homomorfismos de grupos.

3.1. Definición de grupo y primeras propiedades

Definición 3.1.

Un grupo consiste de un conjunto G no vacío junto con una operación interna $G \times G \rightarrow G$ que llamaremos producto y tal que a cada pareja (x, y) le asigna el elemento xy y que verifica las siguientes propiedades:

1. Asociativa: $\forall x, y, z \in G (xy)z = x(yz)$
2. Existencia de elemento neutro: $\exists 1 \in G : 1x = x = x1 \forall x \in G$
3. Existencia de elemento simétrico: $\forall x \in G \exists x^{-1} \in G$ tal que $x^{-1}x = 1 = xx^{-1}$

Además se dice que G es un grupo conmutativo o abeliano si verifica:

4. $\forall x, y \in G \quad xy = yx$

Proposición 3.1.

Sea G un grupo:

1. El elemento neutro es único.
2. Para cada $x \in G$ el inverso es único.
3. Para cada $x \in G (x^{-1})^{-1} = x$. (Propiedad involutiva)
4. Para cualesquiera $a, b \in G$, las ecuaciones $aX = b$ y $Y a = b$ tienen solución única.
5. Si $xx = x$ entonces $x = 1$.
6. Para cada $(x_1, x_2, \dots, x_n) \in G^n$ definimos $\prod_{i=1}^n a_i = a_1 \dots a_n$ inductivamente como $\prod_{i=1}^1 a_i = a_1$ y para $n \geq 1$ $\prod_{i=1}^n a_i = (\prod_{i=1}^{n-1} a_i) a_n$.

Para cada $1 \leq m < n$ se verifica $\prod_{i=1}^n a_i = (\prod_{i=1}^m a_i)(\prod_{i=m+1}^n a_i)$. (Propiedad asociativa generalizada)

7. $(\prod_{i=1}^n a_i)^{-1} = \prod_{i=1}^n a_i^{-1} = a_n^{-1} \dots a_1^{-1}$.
8. Si para $a_1 = a_2 = \dots = a_n$ definimos $a^n := \prod_{i=1}^n a_i$. Se verifica que $\forall r, s \geq 1$ se tiene $a^r a^s = a^{r+s}$
9. $\forall n \geq 1$ se verifica $(a^n)^{-1} = (a^{-1})^n$ y podemos definir $a^{-n} := (a^n)^{-1} = (a^{-1})^n$ y $a^0 := 1$.
10. $\forall r, s \in \mathbb{Z}$ se verifica $a^r a^s = a^{r+s}$ y $a^{rs} = (a^r)^s$ (Producto de potencias de la misma base y potencia de una potencia)

Proposición 3.2 (Definición sin conmutación).

Sea G un conjunto no vacío con una operación interna $G \times G \rightarrow G$ verificando:

1. $\forall x, y, z \in G$ se verifica $(xy)z = x(yz)$.
2. $\exists 1 \in G$ tal que $x1 = x \forall x \in G$.
3. $\forall x \in G \exists x^{-1}$ tal que $xx^{-1} = 1$.

entonces se verifica que para todo $x \in G$:

1. $x1 = x = 1x$
2. $x^{-1}x = 1 = xx^{-1}$

de modo que las condiciones anteriores son necesarias y suficientes para que G sea un grupo.

Definición 3.2 (Orden de un grupo. Tabla de Cayley.).

Si G es un grupo finito, el número de elementos de G lo llamaremos orden de G y lo denotaremos por

Tabla 1: Tabla de Cayley genérica

	x_1	\dots	x_n
x_1	x_1x_1	\dots	x_1x_n
\dots	\dots	\dots	\dots
x_n	x_nx_1	\dots	x_nx_n

$|G|$. Además si $G = \{x_1, x_2, \dots, x_n\}$ podemos representarlo por su tabla de Cayley que aparece en la Tabla 1.

Algunas propiedades interesantes de esta tabla es que nos dice si el grupo es abeliano si y sólo si la tabla es simétrica y que en cada fila o columna aparece una y solo una vez cada elemento del grupo.

3.2. Ejemplos de grupos

3.2.1. Anillos y unidades de un anillo.

Si A es un anillo entonces $(A, +)$ es un grupo abeliano. Por otro lado, $(U(A), \cdot)$ es un grupo que será abeliano si A es un anillo conmutativo (esto es, si la operación producto es conmutativa). Esto nos da ya numerosos ejemplos:

$$\mathbb{Z} - U(\mathbb{Z}) = \{-1, 1\}$$

$$\mathbb{Q} - \mathbb{Q}^*$$

$$\mathbb{R} - \mathbb{R}^*$$

$$\mathbb{C} - \mathbb{C}^*$$

$$\mathbb{Z}_n - U(\mathbb{Z}_n) \text{ nótese } |\mathbb{Z}_n| = n, |U(\mathbb{Z}_n)| = \phi(n)$$

3.2.2. Grupo de las raíces n-ésimas de la unidad.

Consideramos para $n \geq 2$ el conjunto $\mu_n = \{z \in \mathbb{C}^* : z^n = 1\}$ con la operación producto de números complejos.

Otra forma de representar este grupo y la operación correspondiente de forma explícita es la siguiente:

$$\mu_n = \{\xi_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right) : 0 \leq k < n-1\}$$

$$\xi_k \cdot \xi_r = \xi_{res(k+r,n)} \quad 0 \leq k, r < n$$

de modo que esta es la versión multiplicativa de $(\mathbb{Z}_n, +)$, esto es, son isomorfos.

3.2.3. Grupo lineal general de orden n.

Consideramos para $n \geq 2$ el conjunto de las matrices de orden n con coeficientes sobre un cuerpo K , $M_n(K)$. construido sobre él se tiene el grupo lineal general de orden n definido como $Gl_n(K) := U(M_n(K))$. Claramente $Gl_n(K) = \{A \in M_n(K) : |A| \neq 0\}$ y será un grupo con el producto de matrices que en general no es abeliano.

3.2.4. Grupos simétricos

Sea X un conjunto no vacío. El grupo de permutaciones de X , denotado $S(X)$, es el conjunto de todas las aplicaciones biyectivas de X en X esto es $S(X) = \{f : X \rightarrow X : f \text{ es biyectiva}\}$ donde la operación considerada es la composición de funciones.

Para $n \geq 2$ definiremos el n -ésimo grupo simétrico o grupo de permutaciones de n elementos como $S_n = S(\{1, \dots, n\})$. Claramente, $|S_n| = n!$.

Representaremos un elemento $\alpha \in S_n$ como $\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$ y dadas dos permutaciones $\alpha, \beta \in S_n$ su producto es $\alpha\beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(\beta(1)) & \alpha(\beta(2)) & \dots & \alpha(\beta(n)) \end{pmatrix}$.

Se verifica que S_n es conmutativo si y sólo si $n = 2$.

Definición 3.3 (Permutaciones disjuntas).

Se dice que dos permutaciones $\alpha, \beta \in S_n$ son disjuntas si lo que mueve una lo deja fija la otra, esto es, $\alpha(x) \neq x \Rightarrow \beta(x) = x$.

Proposición 3.3.

Las permutaciones disjuntas conmutan.

Demostración. Supongamos que $\alpha(x) \neq x$, de modo que $\beta(x) = x$. Por tanto, $\alpha(\beta(x)) = \alpha(x)$ y, por otro lado, $\beta(\alpha(x)) = \alpha(x)$ ya que como α tiene que ser inyectiva y $\alpha(x) \neq x$, tiene que ser $\alpha(\alpha(x)) \neq x$ luego β fija a $\alpha(x)$ y se tiene la igualdad.

En otro caso, podríamos tener que $\beta(x) \neq x$ en cuyo caso se aplica un razonamiento análogo al anterior. Finalmente, si $\alpha(x) = x = \beta(x)$ entonces claramente $\alpha(\beta(x)) = x = \beta(\alpha(x))$. \square

Definición 3.4 (Ciclo).

Una permutación es un ciclo si existen x_1, \dots, x_r tales que $\alpha(x_1) = x_2, \dots, \alpha(x_r) = x_1$ y $\alpha(x) = x \forall x \notin \{x_1, \dots, x_r\}$. Lo denotaremos $\alpha = (x_1 x_2 \dots x_r)$ y diremos que tiene longitud r .

Observemos que esta notación no es unívoca y que un ciclo de longitud r tiene r notaciones diferentes. Observemos también que dos ciclos $\alpha = (x_1 x_2 \dots x_r)$ y $\beta = (y_1 x_2 \dots y_s)$ son disjuntos $\iff \{x_1 x_2 \dots x_r\} \cap \{y_1 x_2 \dots y_s\} = \emptyset$ lo que motiva el nombre utilizado.

Teorema 3.4 (Descomposición de una permutación en producto de ciclos disjuntos).

Sea $n \geq 2$. Toda permutación distinta de la identidad en S_n se expresa como producto de ciclos disjuntos de manera única salvo el orden de los ciclos y su primer elemento.

Demostración. La idea para demostrar la existencia de la descomposición parte de considerar permutaciones por ejemplo de tres elementos donde sólo se mueven dos. Entonces nos damos cuenta que por la inyectividad deben ser ciclos. Entonces se realiza una inducción sobre el número de elementos que mueve la permutación. Se construye un primer ciclo y se aplica la hipótesis de inducción.

Tomemos una permutación $\alpha \neq 1$ y sea s el número de elementos que mueve α . Si $s = 2$ necesariamente debe ser un ciclo de longitud dos. Ya que si x, y son los elementos que mueve α debe ser $\alpha(x) = y$ ya que si tuviéramos $\alpha(x) = z$ con $z \neq x, y$ entonces como $\alpha(z) = z$ se violaría la inyectividad de α . Por motivos análogos debe ser $\alpha(y) = x$.

Consideremos que $s > 2$ y tomemos x un elemento que es movido por α . Consideremos la lista $\{x, \alpha(x), \dots, \alpha^n(x)\}$ en esta lista debe haber repeticiones puesto que I_n tiene n elementos y la lista tiene

$n + 1$ elementos. Por tanto existirán $k, k' \in \mathbb{N}, k > k'$ tales que $\alpha^k(x) = \alpha^{k'}(x)$ luego $\alpha^{k-k'}(x) = x$. Consideremos el menor valor r tal que $\alpha^r(x) = x$ y formemos el ciclo $\alpha_1 = (x \alpha(x) \dots \alpha^{r-1}(x))$.

Consideremos la permutación α' que deja fijos los elementos que mueve α_1 y aplica α a los elementos que no mueve α_1 . Claramente ambas permutaciones son disjuntas. Pero hay que comprobar que $\alpha = \alpha_1 \alpha'$.

Tomemos un elemento y que sea movido por α_1 entonces $\alpha(y) = \alpha_1(\alpha'(y)) = \alpha_1(y) = \alpha(y)$. Tomemos un elemento que no es movido por α_1 , entonces $\alpha(y) = \alpha_1(\alpha'(y)) = \alpha_1(\alpha(y))$ y acabaríamos si demostramos que $\alpha(y)$ no es movido por α_1 . Pero esto es claro ya que podríamos aplicar el razonamiento anterior demostrando que existe un valor k tal que $\alpha^k(y) = y$ y por tanto y estaría en el ciclo, lo cual es una contradicción.

Ahora bien α' mueve $s - r < s$ elementos y por hipótesis de inducción existen $\alpha_2, \dots, \alpha_m$ ciclos disjuntos tales que $\alpha' = \alpha_2 \dots \alpha_m$ finalmente $\alpha = \alpha_1 \alpha_2 \dots \alpha_m$ y los ciclos son disjuntos.

Veamos ahora la unicidad de la descomposición. Tomemos dos descomposiciones distintas $\alpha = \alpha_1 \alpha_2 \dots \alpha_m$ y $\beta = \beta_1 \beta_2 \dots \beta_{m'}$ donde $m \leq m'$. Queremos demostrar que todos los ciclos salvo el orden y el primer elemento son iguales. Lo hacemos por inducción sobre m pero primeramente demostramos que el primer ciclo es igual en ambas descomposiciones.

En efecto, sea x un elemento tal que $\alpha_1(x) \neq x$. Entonces se puede escribir α_1 como $\alpha_1 = (x \alpha_1(x) \dots) = (x \alpha(x), \dots)$. Como las permutaciones β_i son disjuntas, se verifica que $\beta_i(x) \neq x$ para una sola de ellas y podemos suponer que $i = 1$ ya que permutaciones disjuntas conmutan. Tendremos $\beta_1 = (x \beta_1(x) \dots) = (x \alpha(x), \dots)$. En definitiva, $\alpha = \alpha_1 \alpha_2 \dots \alpha_m = \alpha_1 \beta_2 \dots \beta_{m'}$

Ahora, para $m = 1$ necesariamente se tendrá $m' = 1$ ya que en caso contrario tendríamos $1 = \beta_2 \dots \beta_{m'}$ lo que es una contradicción ya que son ciclos disjuntos. Por tanto se tendría la igualdad.

Aplicando la hipótesis de inducción fuerte, si $m > 1$ del hecho de que $\alpha = \alpha_1 \alpha_2 \dots \alpha_m = \alpha_1 \beta_2 \dots \beta_{m'}$ se deduce $\alpha_2 \dots \alpha_m = \beta_2 \dots \beta_{m'}$. De donde se tendrá que $m = m'$ y $\alpha_i = \beta_i$ con $i = 2, \dots, m$. \square

Proposición 3.5 (Propiedades de los ciclos).

Sea $n \geq 2$ y consideremos el grupo S_n :

1. $(x_1 x_2 \dots x_r)^{-1} = (x_r x_{r-1} \dots x_1)$ (inverso de un ciclo)
2. $(x_1 x_2 \dots x_r) = (x_1 x_2)(x_2 x_3) \dots (x_{r-1} x_r)$ (descomposición en transposiciones)
3. $\forall \alpha \in S_n \alpha(x_1 x_2 \dots x_r) \alpha^{-1} = (\alpha(x_1) \alpha(x_2) \dots \alpha(x_r))$. (conjugado)
4. $(x_1 x_2 \dots x_r)^k \neq 1$ si $1 \leq k < r$ y $(x_1 x_2 \dots x_r)^r = 1$. (el orden de un ciclo coincide con su longitud).

Demostración. \square

Definición 3.5 (Transposición).

Una transposición es un ciclo de longitud dos.

Teorema 3.6 (Teorema sobre la paridad de una permutación).

Dada una permutación $\alpha \in S_n$ y dos expresiones de α como producto de transposiciones $\alpha = \tau_1 \dots \tau_r$ y $\alpha' = \tau'_1 \dots \tau'_s$. Entonces $r \equiv s \pmod{2}$.

Demostración. La idea para demostrar este teorema es empezar con el caso de la identidad y demostrar que si mediante una transposición intercambio dos elementos, luego los tengo que volver a intercambiar. Luego, para cualquier permutación α se aplicará que $1 = \alpha \alpha^{-1}$. Veámoslo.

Supongamos que $1 = \tau_1 \dots \tau_r$ y demostremos que r no puede ser impar. Lo hacemos por el método del descenso infinito. Claramente, si $r = 1$ no es posible descomponer la identidad en una sola transposición.

Supongamos que r es un número impar mayor que uno y elijamos un elemento m que aparezca por primera vez en cierta transposición τ_j . Entonces $j < r$ porque si no m se movería y no volvería a su lugar. Veamos los posibles casos que se nos pueden presentar para el producto de las transposiciones τ_j y τ_{j+1} .

$$\tau_j \tau_{j+1} = \begin{cases} (mx)(mx) = 1 \\ (mx)(my) = (xy)(mx) \\ (mx)(yz) = (yz)(mx) \\ (mx)(xy) = (xy)(my) \end{cases}$$

En el primer caso hemos reducido el número de transposiciones a $r - 2$ y en el resto de los casos trasladamos m una transposición hacia delante. Como no puede ocurrir que $j = r$ necesariamente al repetir el proceso se llega al primer caso. Se obtiene así una sucesión descendente de números impares y por tanto si existiera la descomposición para r también existiría para 1. Como esto no es posible, se deduce que necesariamente $r \equiv 0 \pmod{2}$.

Para α arbitrario tenemos que si $\alpha = \tau_1 \dots \tau_r = \tau'_1 \dots \tau'_s$ entonces $1 = \alpha \alpha^{-1} = \tau_1 \dots \tau_r (\tau'_1 \dots \tau'_s)^{-1} = \tau_1 \dots \tau_r \tau'^{-1}_{s-1} \dots \tau'^{-1}_1 = \tau_1 \dots \tau_r \tau'_s \dots \tau'_1$ luego por el caso anterior $r + s \equiv 0 \pmod{2}$, esto es, $r \equiv s \pmod{2}$. \square

Definición 3.6 (Signatura de una permutación).

Diremos que una permutación α es par si se expresa como producto de un número par de transposiciones y diremos que es impar si se expresa como producto de un número impar de transposiciones. La signatura de una permutación será el número $s(\alpha)$ definido como $s(\alpha) = 1$ si α es una permutación par y $s(\alpha) = -1$ si $s(\alpha)$ es una permutación impar.

3.2.5. Grupos diédricos.

Para $n \geq 3$ definimos el n -ésimo grupo diédrico como el grupo de movimientos del plano real \mathbb{R}^2 que dejan fijo el polígono regular de n lados, esto es, $D_n = \{T : \mathbb{R}^2 \rightarrow \mathbb{R}^2 : T \text{ es isometría y } T(P_n) = P_n\}$ donde la operación es la composición de aplicaciones. Se verifica que $|D_n| = 2n$ donde conocemos explícitamente los elementos del grupo:

R_k es el giro centrado en el origen y ángulo $\frac{2k\pi}{n}$ con $0 \leq k < n$. S_1, \dots, S_n son las simetrías respecto de los n ejes de simetría de P_n , esto es:

- Si n es impar son las rectas que unen cada vértice con el origen.
- Si n es par son las rectas que unen vértices opuestos o los puntos medios de lados opuestos.

Este grupo se puede manejar de forma abstracta con las siguientes identidades fundamentales:

$$\begin{aligned} r^n &= 1 = s^2 \\ sr &= r^{-1}s \end{aligned}$$

de modo que se suele presentar el grupo D_n en la forma:

$$D_n = \langle r, s : r^n = 1 = s^2, sr = r^{-1}s \rangle$$

este tipo de notación indica a la izquierda los elementos que generan el grupo (en un sentido que precisaremos más tarde) y a la derecha las reglas de operación en el mismo. Notemos que estos grupos no son conmutativos.

3.2.6. Grupo de los cuaternios.

Consideremos el conjunto $Q_2 = \{1 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i := \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, j := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, -i := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, j := \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, -j := \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, k := \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, -k := \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}\}$ de matrices invertibles de orden dos y con coeficientes complejos y consideremos la operación dada por el producto usual de matrices. Dibujando la tabla de Cayley podemos ver que de hecho no es un grupo abeliano.

De nuevo, se puede dar una representación abstracta de este grupo mediante las relaciones:

$$(-1)^2 = 1$$

$$i^2 = j^2 = k^2 = -1$$

$$ij = k$$

$$(-1)x = x(-1) = -x \text{ con } x = i, j, k$$

el resto de relaciones se deduce a partir de estas. Se puede aplicar la regla del tornillo considerando el eje x como la unidad i (eje que sale hacia nosotros), el eje y como la unidad j (eje horizontal) y el eje z como la unidad k (eje vertical).

3.2.7. Grupo de Klein.

Definición 3.7 (Producto directo de grupos).

Dados dos grupos G_1 y G_2 definimos su producto directo como el grupo

$$G_1 \times G_2 = \{(x_1, x_2) : x_1 \in G_1, x_2 \in G_2\}$$

con la operación

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$$

El grupo de Klein es $\mu_2 \times \mu_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$ junto con la operación del producto de grupos.

Otra forma de presentar el grupo de klein es $K = \langle x, y : x^2 = y^2 = 1, xy = yx \rangle$.

3.2.8. Grupo alternado.

Para $n \geq 2$ definimos el n-ésimo grupo alternado A_n como el conjunto de las permutaciones pares de S_n . Esto es:

$$A_n = \text{Ker}(s) = \{\alpha \in S_n : \alpha \text{ es par}\} \leq S_n$$

Donde s es la aplicación signatura y Ker es el núcleo de dicha aplicación, conceptos que explicaremos pero que demuestran automáticamente que A_n es un grupo. Además, se puede demostrar que el orden de A_n es $\frac{n!}{2}$.

3.3. Homomorfismos.

Definición 3.8 (Homomorfismos de grupos).

Sean H y G dos grupos. Definimos un homomorfismo de grupos de G en H como una aplicación

$f : G \rightarrow H$ tal que

$$f(xy) = f(x)f(y) \quad \forall x, y \in G$$

Diremos que f es monomorfismo si es inyectiva, que f es epimorfismo si es sobreyectiva y que es isomorfismo si es biyectiva. Esto último lo denotaremos por \cong .

EJEMPLO 3.1: La aplicación signatura $s : S_n \rightarrow \mu_2$ es un homomorfismo de grupos.

En efecto, sean $\alpha, \beta \in S_n$ entonces por el teorema 3.6 podemos escribir $\alpha = \tau_1 \dots \tau_r$ y $\beta = \tau'_1 \dots \tau'_s$ de donde $s(\alpha) = (-1)^r$ y $s(\beta) = (-1)^s$. Pero entonces $\alpha\beta = \tau_1 \dots \tau_r \tau'_1 \dots \tau'_s$ luego $s(\alpha\beta) = (-1)^{r+s}$ de modo que $s(\alpha\beta) = s(\alpha)s(\beta)$.

Proposición 3.7.

1. Para todo grupo G , la aplicación identidad $1 : G \rightarrow G$ es un homomorfismo de grupos.
2. Si G, H y L son grupos y $f : G \rightarrow H$, $g : H \rightarrow L$ son dos homomorfismos (respectivamente monomorfismos, epimorfismos o isomorfismos) entonces $g \circ f : G \rightarrow L$ es un homomorfismo (respectivamente monomorfismo, epimorfismo o isomorfismo).
3. Si $f : G \rightarrow H$ es un isomorfismo entonces $f^{-1} : H \rightarrow G$ es también un isomorfismo, $f \circ f^{-1} = 1_H$ y $f^{-1} \circ f = 1_G$.

Uno de los problemas que trataremos es la clasificación de grupos finitos. La clasificación de grupos abelianos finitos es materia del Álgebra I y se clasificarán los grupos abelianos no finitos hasta el orden quince. El objetivo es dado un tamaño del grupo saber cuántos grupos no isomorfos hay.

4. Tema 3: subgrupos. Órdenes e índices.

4.1. Definición de subgrupo. Ejemplos y primeros resultados.

Definición 4.1 (Subgrupos de un grupo).

Sea G un grupo. Un subgrupo H de G es un subconjunto no vacío de G que es cerrado bajo productos e inversos. Lo denotaremos como $H \leq G$.

Claramente, un subgrupo H de un grupo G es en sí mismo un grupo con la operación producto de G restringida a los elementos de H ya que la operación producto de G es interna en H y la operación inversión también. Además el elemento neutro también debe ser el mismo sin más que operar en $x1 = 1$.

EJEMPLO 4.1: 1. Subgrupos impropios de un grupo: todo grupo G admite dos subgrupos llamados impropios. El subgrupo trivial $1 = 1$ y el total G . Al resto de subgrupos se le llama subgrupos propios.

$$2. \mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$$

$$\mu_n \leq \mathbb{C}^*$$

$$m|n \Rightarrow \mu_m \leq \mu_n$$

3. En D_n tenemos el subgrupo de las rotaciones $H = \{1, r, r^2, \dots, r^{n-1}\}$ y subgrupos cíclicos de orden 2 $K = \{1, s\}$ y $L = \{1, r^i s\}$. Sin embargo, el conjunto de las simetrías $\{1, s, rs, r^2 s, \dots, r^{n-1} s\}$ no es un subgrupo de D_n .

4. En S_4 podemos considerar un subgrupo tipo Klein $K = \{1, \alpha_1 = (12)(34), \alpha_2 = (13)(24), \alpha_3 = (14)(23)\}$.

Proposición 4.1 (Criterio de subgrupo).

Un subconjunto H no vacío de un grupo G es un subgrupo si y sólo si se verifica que $\forall x, y \in G$ se tiene $xy^{-1} \in H$.

Demostración. \Rightarrow Si asumimos que H es un subgrupo de G como es cerrado para inversos e $y \in H$ entonces $y^{-1} \in H$ y como H es cerrado para productos y $x \in H$ se tiene que $xy^{-1} \in H$.

\Leftarrow Supongamos que $\forall x, y \in G$ se tiene $xy^{-1} \in H$. Sea $u, v \in H$ y veamos que $uv \in H$ tomemos $x = u, y = v^{-1}$ entonces por hipótesis $xy^{-1} = u(v^{-1})^{-1} = uv \in H$. Veamos también que H es cerrado para inversos. Sea $y \in H$ como la unidad también está en H , tomando $x = 1$ el producto $xy^{-1} = 1y^{-1} = y^{-1} \in H$ de donde H es cerrado para inversos. \square

Proposición 4.2 (Criterio de subgrupo para subconjuntos finitos).

Sea G un grupo y H un subconjunto finito no vacío de G .

H es un subgrupo de $G \iff$ el producto es interno en H .

Demostración. \Rightarrow Es parte de la definición de subgrupo.

\Leftarrow Falta demostrar que H es cerrado para inversos. Como H es finito necesariamente existen $k, r \in \mathbb{N}, k > r$ tales que $x^k = x^r$ luego $x^{k-r} = 1$ de donde $x^{k-r-1} = x^{-1}$. \square

Proposición 4.3 (Teorema de correspondencia entre homomorfismos y subgrupos).

1. Los homomorfismos preservan los subgrupos. Si $f : G \rightarrow G'$ es un homomorfismo de grupos, $H \leq G$ y $H' \leq G'$ entonces $f(H) \leq G'$ y $f^{-1}(H') \leq G$.

2. Definimos el núcleo de un homomorfismo f como $\text{Ker}(f) = f^{-1}(\{1\})$ y la imagen del homomorfismo f como $\text{Im}(f) = f(G)$. Claramente, el núcleo y la imagen son subgrupos de G y G' respectivamente. Además, f es monomorfismo $\iff \text{Ker}(f) = \{1\}$ y f es epimorfismo $\iff \text{Im}(f) = G'$.

Demostración. 1. En efecto, por ser $H \leq G$ se verifica que $\forall x, y \in H \ xy^{-1} \in H$ y por ser f homomorfismo, dados $f(x), f(y) \in f(H)$, $f(x)f(y)^{-1} = f(xy^{-1}) \in f(H)$.

De forma análoga, por ser $H' \leq G'$ se verifica que $\forall x, y \in H', xy^{-1} \in H'$ y por ser f homomorfismo, si $x_1 = f^{-1}(x)$ y $x_2 = f^{-1}(y)$ entonces $f(x_1x_2^{-1}) = f(x_1)f(x_2)^{-1} = xy^{-1}$ y eso nos dice que $x_1x_2^{-1} \in f^{-1}(H')$.

2. Si f es monomorfismo y tomo $x \in \text{Ker}(f)$ entonces $f(x) = 1$ pero siempre $f(1) = f(1 \cdot 1) = f(1)f(1)$ de donde $f(1) = 1$ pero entonces $x = 1$, con lo que $\text{Ker}(f) = \{1\}$.

Si $\text{Ker}(f) = \{1\}$ entonces f es inyectiva ya que si $f(x) = f(y)$ entonces $f(x)f(y)^{-1} = f(xy^{-1}) = 1$ de donde $xy^{-1} \in \text{Ker}(f)$ y por tanto $xy^{-1} = 1$ de donde $x = y$.

Por otro lado la equivalencia para el epimorfismo es la propia definición de sobreyectividad. \square

4.2. Retículo de subgrupos de un grupo.

Definición 4.2 (Retículo de subgrupos).

Recordemos que un retículo es un conjunto ordenado en el que cualquier par de elementos tiene supremo e ínfimo.

Si G es un grupo, denotaremos por $\text{Sub}(G) = \{H : H \text{ es un subgrupo de } G\}$. Se verifica que $\text{Sub}(G)$ tiene estructura de retículo y está ordenado por la relación de inclusión.

Proposición 4.4 (Ínfimo y supremo en el retículo de subgrupos).

1. Si $\{H_i\}_{i \in I}$ es una familia de subgrupos de un grupo G entonces $\bigcap_{i \in I} H_i$ es un subgrupo de G .

2. Si $H_1, H_2 \in \text{Sub}(G)$ entonces $\inf\{H_1, H_2\} = H_1 \cap H_2$ y $\sup\{H_1, H_2\} = \bigcap_{K \in \text{Sub}(G), H_i \leq K \ i=1,2} K$, esto es, el ínfimo es el heredado de la relación de orden de las partes de un conjunto y el supremo es la intersección de los subgrupos de G que contienen a H_1 y a H_2 .

Demostración. Utilizamos el criterio de subgrupo teniendo en cuenta que como $1 \in \bigcap_{i \in I} H_i$ entonces $\bigcap_{i \in I} H_i$ es no vacía.

Si $H_1, H_2 \in \text{Sub}(G)$, claramente, al ser $H_1 \cap H_2$ un subgrupo debe ser el ínfimo pues es heredado de la relación de orden de las partes de un conjunto. Por otro lado, la intersección dada por $\bigcap_{K \in \text{Sub}(G), H_i \leq K \ i=1,2} K$ es no vacía ya que $H_1 \leq G$ y $H_2 \leq G$. Veamos que en efecto es el supremo.

Claramente, $H_1 \leq \bigcap K$ y $H_2 \leq \bigcap K$. Por otro lado, si $L \in \text{Sub}(G)$ tal que $H_1 \leq L$ y $H_2 \leq L$ entonces L está en la lista de subgrupos intersecados y por tanto $\bigcap K \leq L$. \square

EJEMPLO 4.2 (La unión de subgrupos no tiene por qué ser un subgrupo): En D_4 consideramos $H_1 = \{1, s\} \leq D_4$ y $H_2 = \{1, rs\} \leq D_4$ pero $H_1 \cup H_2 = \{1, s, rs\} \not\leq D_4$

De hecho, si tengo dos subgrupos $H, K \leq G$ entonces $H \cup K \leq G \iff H \subseteq G \text{ o } K \subseteq G$.

La fórmula que me hemos dado para el supremo de subgrupos es muy poco práctica. Esto motiva las siguientes definiciones.

4.3. Producto de subgrupos.

Definición 4.3 (Producto de subgrupos).

Sea G un grupo, X e Y subconjuntos no vacíos de G . Entonces el producto de X e Y es

$$XY = \{xy : x \in X, y \in Y\}$$

Proposición 4.5 (Teorema del producto (Ledermann)).

Sean H, K subgrupos de un grupo G . Entonces:

HK es un subgrupo de $G \iff HK = KH$ en cuyo caso $H \vee K = HK$

Demostración.

□

Una forma de generalizar el teorema del producto es hacer infinitos productos con lo que se elimina la hipótesis de conmutación.

Proposición 4.6.

Sean H, K subgrupos de un grupo G . Entonces $H \vee K = \{h_1 k_1 \dots h_r k_r : h_i \in H, k_i \in K, r \geq 1\}$

Demostración.

□

4.4. Subgrupo generado por un conjunto.

Definición 4.4 (Subgrupo generado por un conjunto).

Sea G un grupo y X un subconjunto no vacío de G . Definimos el subgrupo de G generado por X y denotado por $\langle X \rangle$ como el menor subgrupo de G que contiene a X , esto es, $\langle X \rangle = \bigcap_{K \in \text{Sub}(G), X \subseteq K} K$.

Definición 4.5 (Conjunto generador de un grupo).

Sea G un grupo y X un subconjunto no vacío de G . Si $G = \langle X \rangle$ diremos que X es un conjunto de generadores de G .

Esta definición permite entender mejor la noción de supremo, en efecto, si H, K son subgrupos de G entonces $H \vee K = \bigcap_{T \leq G, H, K \leq T} T = \bigcap_{T \leq G, H \cup K \subseteq T} T = \langle H \cup K \rangle$, o sea, que el supremo de dos subgrupos es el subgrupo generado por su unión.

Proposición 4.7 (Expresión del subgrupo generado como palabras).

Sea X un subconjunto no vacío de un grupo G . Entonces $\langle X \rangle = \{x_1^{n_1} \dots x_r^{n_r} : x_i \in X, n_i \in \mathbb{Z}, r \geq 1\}$

Demostración.

□

Proposición 4.8.

Sea X un subconjunto no vacío de un grupo finito G . $\langle X \rangle = \{x_1^{n_1} \dots x_r^{n_r} : x_i \in X, n_i \geq 0, r \geq 1\}$

Demostración.

□

Definición 4.6 (Subgrupo cíclico generado por un elemento).

Sea G un grupo. Si $X = \{a\}$ entonces $\langle X \rangle = \langle a \rangle$ y lo llamaremos el subgrupo cíclico generado por a . Claramente $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ y en el caso en que G sea finito $\langle a \rangle = \{a^n : n \geq 0\}$

Definición 4.7 (Grupo cíclico).

Sea G un grupo. Si $X = \{a\}$ es un conjunto de generadores de G entonces $G = \langle a \rangle$ y diremos que G es un grupo cíclico.

EJEMPLO 4.3: 1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ teniendo en cuenta que la operación es la suma. De hecho veremos más adelante que todo grupo cíclico infinito es isomorfo a \mathbb{Z} .

2. $D_n = \langle r, s \rangle$.

3. $S_n = \langle X \rangle$ donde $X = \{(ij) : 1 \leq i, j \leq n\}$

4.5. Teorema de Lagrange.

Definición 4.8.

Si G es un grupo, H es un subgrupo de G y $x \in G$ definimos $xH = \{xh : h \in H\}$ y $Hx = \{hx : h \in H\}$.

Diremos que dos elementos $x, y \in G$ están relacionados por la izquierda si $y \in xH$ o equivalentemente $x \in yH$, dicho de otro modo, $xy^{-1} \in H$ o bien $y^{-1}x \in H$. Lo denotaremos por $x \sim_I y$.

Diremos que dos elementos $x, y \in G$ están relacionados por la derecha si $y \in Hx$ o equivalentemente $x \in Hy$, dicho de otro modo, $xy^{-1} \in H$ o bien $yx^{-1} \in H$. Lo denotaremos por $x \sim_D y$.

Se comprueba fácilmente que estas relaciones son de equivalencia y que la clase de equivalencia de un elemento x por la izquierda es xH y por la derecha es Hx .

Al conjunto de las clases de equivalencia por la izquierda lo denotaremos por $G/H := \{xH : x \in G\}$ y al conjunto de las clases de equivalencia por la derecha lo denotaremos por $H/G := \{Hx : x \in G\}$.

Proposición 4.9.

1. Las clases de equivalencia forman una partición de G . Además, se tiene que $xH = yH \iff x \sim_I y$ y $Hx = Hy \iff x \sim_D y$.

2. Existen biyecciones $f : H \rightarrow xH$ y $g : H \rightarrow Hx$ para cualquier $x \in G$. Existe una biyección $\lambda : G/H \rightarrow H/G$. En particular, el dominio y el codominio de estas biyecciones tienen el mismo número de elementos.

Demostración.

□

Definición 4.9 (Índice de un subgrupo de un grupo).

Sea G un grupo finito y H un subgrupo de G . Definimos el índice de H en G como el número de clases laterales a izquierda o derecha por la relación equivalencia anterior. Esto es, $[G : H] = |G/H| = |H/G|$. En otras palabras el índice es el número de partes de la partición inducida por H .

Teorema 4.10 (Teorema de Lagrange).

Sea G un grupo finito y $H \leq G$ entonces $|G| = [G : H]|H|$

Demostración. Pongamos $G = \sum_{i=1}^{[G:H]} x_i H$ donde entendemos el símbolo \sum como suma disjunta y x_i son representantes de las clases de equivalencia por la izquierda. Entonces tomando órdenes $|G| = \sum_{i=1}^{[G:H]} |x_i H| = \sum_{i=1}^{[G:H]} |H| = [G : H]|H|$. □

Corolario 4.11.

Si G es un grupo finito y $H \leq G$ entonces el orden de H divide al orden de G .

4.6. Orden de un elemento.

Definición 4.10 (Orden de un elemento).

Sea G un grupo y $a \in G$. Definimos el orden de a como $ord(a) = \begin{cases} \min\{r \geq 1 : a^r = 1\} & \text{si } \exists r \geq 1 : a^r = 1 \\ \infty & \text{en otro caso} \end{cases}$

Claramente, si G es finito el orden de sus elementos es finito.

Proposición 4.12 (Otra definición del orden de un elemento).

El orden de un elemento es igual al orden del subgrupo que genera si es finito y es infinito si el subgrupo generado es infinito.

Demostración. Veamos en primer lugar que si $ord(a) = n$ entonces $\langle a \rangle = \{1, a, \dots, a^{n-1}\}$.

Por definición $\langle a \rangle = \{a^r : r \in \mathbb{Z}\}$ y dividiendo r entre n tendremos $r = nq + s$ donde $0 \leq s < n$. Resulta que $a^r = a^s \in \{1, a, \dots, a^{n-1}\}$. Luego hemos demostrado que $\{a^r : r \in \mathbb{Z}\} \subseteq \{1, a, \dots, a^{n-1}\}$. Y como la otra inclusión es evidente hemos demostrado la igualdad. Y más adelante veremos que dos grupos cíclicos del mismo orden son isomorfos.

Si $ord(a) = \infty$ entonces el grupo cíclico generado por a es isomorfo al grupo de los números enteros con la suma $\langle a \rangle = \{a^r : r \in \mathbb{Z}\} \cong \mathbb{Z}$ mediante el isomorfismo $f : \mathbb{Z} \rightarrow \langle a \rangle$ tal que $f(n) = a^n$. \square

Corolario 4.13.

Si G es un grupo finito entonces para cualquier $a \in G$ se verifica que $ord(a) \mid |G|$.

Proposición 4.14 (Propiedades del orden de un elemento).

Suponiendo que el orden de a es finito:

1. $a^m = 1$ con $m \geq 1 \iff ord(a) \mid m$
2. $ord(a^r) = \frac{ord(a)}{mcd(ord(a), r)}$
3. $\langle a \rangle$ tiene $\phi(ord(a))$ generadores distintos.

En cualquier caso:

4. *El orden es un invariante por isomorfismo. Esto es, si $f : G \rightarrow G'$ es un isomorfismo entonces $ord(a) = ord(f(a))$ para cualquier a .*

Demostración. Sea $n = ord(a)$,

(1) \Rightarrow Supongamos que $a^m = 1$ y si escribimos $m = nq + r$ con $0 \leq r < n$ entonces $1 = a^m = a^{nq}a^r = a^r$ y necesariamente debe ser $r = 0$ ya que si no tendríamos un entero menor que n que como potencia de a da uno en contradicción con la definición de orden de un elemento. Luego $m = nq$ y por tanto $n \mid m$

\Leftarrow Si $n \mid m$ entonces $m = nq$ y entonces $a^m = a^{nq} = (a^n)^q = 1$.

(2) Gracias a (1) como $(a^r)^{\frac{n}{mcd(n,r)}} = (a^n)^{\frac{r}{mcd(n,r)}} = 1$ entonces $ord(a^r) \mid \frac{n}{mcd(n,r)}$.

Por otro lado, supongamos que $(a^r)^m = 1$ y veamos que entonces $\frac{n}{mcd(n,r)} \mid m$. Claramente $n \mid rm$ luego $rs = nt$ para cierto t y entonces $\frac{r}{mcd(n,r)}m = \frac{n}{mcd(n,r)}t$ luego $\frac{n}{mcd(n,r)} \mid \frac{r}{mcd(n,r)}m$ y como $mcd\left(\frac{r}{mcd(n,r)}, \frac{n}{mcd(n,r)}\right) = 1$ por el lema de Euclides necesariamente $\frac{n}{mcd(n,r)} \mid m$. Y concluimos que $\frac{n}{mcd(n,r)} \mid ord(a^r)$.

(3) Utilizando (2) $ord(a^r) = \frac{n}{mcd(n,r)}$ y por tanto si $mcd(n, r) = 1$ se verificará que $\langle a \rangle = \langle a^r \rangle$ ya que ambos conjuntos tienen el mismo número de elementos distintos y están escogidos de la misma familia. Por tanto se trata de determinar cuantos valores r verifican que $mcd(n, r) = 1$, esto es precisamente $\phi(n)$.

(4) Supongamos para empezar que n es finito. $f(a)^n = f(a^n) = f(1) = 1$ luego $n | \text{ord}(f(a))$ y sea ahora cualquier m tal que $f(a)^m = 1$ entonces $1 = f(a)^m = f(a^m)$ y como f es inyectiva necesariamente $a^m = 1$ por (1) debe ser $n | m$ luego $\text{ord}(f(a)) | n$ y por tanto $n = \text{ord}(f(a))$.

Supongamos ahora que n es infinito y supongamos por reducción al absurdo que existe una potencia m tal que $f(a)^m = 1$ entonces $f(a^m) = 1$ y por la inyectividad $a^m = 1$ en contradicción con el hecho de que el orden de a es infinito. \square

Proposición 4.15 (Cálculo del orden de permutación).

1. Sean $\alpha, \beta \in S_n$ dos permutaciones disjuntas entonces $\text{ord}(\alpha\beta) = \text{mcm}(\text{ord}(\alpha), \text{ord}(\beta))$.
2. Dado $\alpha \in S_n$ con $\alpha \neq 1$ entonces $\text{ord}(\alpha) = \text{mcm}(\text{longitudes de los ciclos disjuntos en que descompone } \alpha)$.

Demostración. \square

4.7. Clasificación de los grupos cíclicos y descripción del retículo de subgrupos.

Teorema 4.16 (Teorema de clasificación).

1. Si H y H' son dos grupos cíclicos del mismo orden entonces son isomorfos.
2. Si G es un grupo cíclico generado por a entonces si $\text{ord}(a) = n$ entonces $G \cong (\mathbb{Z}_n, +)$ y si $\text{ord}(a) = \infty$ entonces $G \cong (\mathbb{Z}, +)$. Al grupo cíclico de orden n lo denotaremos $C_n = \langle x : x^n = 1 \rangle$.
3. Si G es un grupo de orden $|G| = p$ con p un número primo entonces $G \cong C_p$.

Demostración. \square

Obsérvese también en este momento que los grupos cíclicos son abelianos.

Teorema 4.17 (Descripción del retículo de subgrupos de un grupo cíclico).

1. Si G es grupo cíclico infinito entonces $G \cong \mathbb{Z}$ y $\text{Sub}(\mathbb{Z}) = \{n\mathbb{Z} : n \geq 0\}$ y la relación de inclusión viene dada por $m\mathbb{Z} \subseteq n\mathbb{Z} \iff n | m$.
- Supongamos que G es un grupo cíclico finito es decir es de la forma $C_n = \langle x : x^n = 1 \rangle$.
2. Si d es divisor de n entonces $\langle x^{n/d} \rangle$ es un subgrupo de C_n cíclico de orden d .
3. Si H es un subgrupo de C_n no trivial y $s = \min\{r \geq 1 : x^r \in H\}$ entonces $s | n$ y $H = \langle x^s \rangle$.
4. (Identificación de subgrupos) Denotemos por $\text{Div}(n)$ a los divisores de n . La aplicación

$$f : \text{Div}(n) \rightarrow \text{Sub}(C_n)$$

tal que

$$d \mapsto \langle x^{n/d} \rangle$$

es una biyección.

5. (Relación de inclusión) Sean $d_1, d_2 \in \text{Div}(n)$.

$$\langle x^{n/d_1} \rangle \leq \langle x^{n/d_2} \rangle \iff d_1 | d_2$$

Demostración. \square

5. Tema 4: grupos cociente, teoremas de isomorfía y producto directo de grupos

5.1. Subgrupos normales

Definición 5.1 (Subgrupo normal).

Sea H un subgrupo de un grupo G . H es normal en G si $aH = Ha \forall a \in G$ en cuyo caso escribiremos $H \trianglelefteq G$.

EJEMPLO 5.1: 1. Todos los subgrupos de un grupo abeliano son normales.

2. Los subgrupos impropios de un grupo son normales.

3. $A_3 \trianglelefteq S_3$ pero $\langle (12) \rangle \not\trianglelefteq S_3$.

4. El subgrupo de las rotaciones de D_3 es normal en D_3 .

Lema 5.1 (Conjugado de un subgrupo por un elemento).

Sea H un subgrupo de un grupo G . Para cada $a \in G$ el conjunto $aHa^{-1} = \{axa^{-1} : x \in H\}$ es un subgrupo de G que llamaremos el conjugado de H por el elemento a .

Demostración. Utilizaremos el criterio 4.1. En efecto, dados dos elementos de aHa^{-1} sean ah_1a^{-1} , ah_2a^{-1} entonces $(ah_1a^{-1})(ah_2a^{-1})^{-1} = ah_1a^{-1}ah_2^{-1}a^{-1} = ah_1h_2^{-1}a^{-1}$ y como H es un subgrupo, se verifica que $h_1h_2^{-1} \in H$ de donde $ah_1h_2^{-1}a^{-1} \in aHa^{-1}$. \square

Teorema 5.2 (Condición de normalidad).

Sea N un subgrupo de un grupo G . $N \trianglelefteq G \iff aNa^{-1} = N \forall a \in G \iff aNa^{-1} \leq N \forall a \in G$ esto es, un subgrupo es normal si contiene a todos sus conjugados.

Demostración. La clave de esta demostración es darse cuenta que la operación "multiplicar por un elemento de un grupo" mantiene cardinalidades ya que la aplicación $f : N \rightarrow aN$ tal que $f(n) = an$ es biyectiva.

\Rightarrow Si $N \trianglelefteq G$ entonces por definición $aN = Na \forall a \in G$. Por tanto, $aNa^{-1} = Naa^{-1} = N$. Esto implica que $aNa^{-1} \leq N \forall a \in G$.

\Leftarrow Supongamos que $aNa^{-1} \leq N \forall a \in G$. Como aNa^{-1} tiene el mismo cardinal que N y $aNa^{-1} \leq N$, se tiene la igualdad es decir que $aNa^{-1} = N \forall a \in G$. Asumiendo la igualdad, entonces $aN = aa^{-1}Na = Na$ de donde se deduce la normalidad. \square

EJEMPLO 5.2: 1. Si $f : G \rightarrow G'$ es un homomorfismo entonces $\text{Ker}(f) \trianglelefteq G$.

En efecto, sea $a \in G$ y $n \in \text{Ker}(f)$ entonces $ana^{-1} \in \text{Ker}(f)$ ya que $f(ana^{-1}) = f(a)f(n)f(a^{-1}) = f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1$.

2. $K = \{1, (12)(34), (13)(24), (14)(23)\} \trianglelefteq S_4$.

Si $\alpha \in S_4$ y $\beta \in K$ entonces por la proposición 3.5 $\alpha\beta\alpha^{-1} = \alpha(ij)(kl)\alpha^{-1} = \alpha(ij)\alpha^{-1}\alpha(kl)\alpha^{-1} = (\alpha(i)\alpha(j))(\alpha(k)\alpha(l)) \in K$ ya que se tiene en cuenta que como $i \neq j \neq k \neq l$ entonces las imágenes también son distintas y que los ciclos disjuntos conmutan.

Proposición 5.3 (Condición de normalidad para subgrupos finitamente generados).

Si $N = \langle x_1, \dots, x_r \rangle \leq G$ entonces $N \trianglelefteq G \iff ax_ia^{-1} \in N \forall a \in G$ con $i = 1, \dots, r$.

Demostración. $\langle X \rangle = \{x_1^{n_1} \dots x_r^{n_r} : x_i \in X, n_i \in \mathbb{Z}, r \geq 1\}$

\Rightarrow Por el criterio 5.2 $aNa^{-1} \leq N \forall a \in G$ de donde claramente $ax_i a^{-1} \in N \forall a \in G$.

\Leftarrow Supongamos que $ax_i a^{-1} \in N \forall a \in G$ y veamos que $aNa^{-1} \leq N \forall a \in G$. Como $N = \langle x_1, \dots, x_r \rangle$ podemos tomar un elemento genérico de N sea $x_1^{n_1} \dots x_r^{n_r}$ y demostrar que el producto $ax_1^{n_1} \dots x_r^{n_r} a^{-1} \in N$.

Para empezar, si $x_i \in \{x_1, \dots, x_r\}$ y $n \in \mathbb{Z}$ entonces $ax_i^n a^{-1} \in N$ ya que si n es positivo se trata de una simple inducción en n y si n es negativo entonces considero que $ax_i^n a^{-1} = a(x_i^{-n})^{-1} a^{-1} = (ax_i^{-n} a^{-1})^{-1}$ y como $ax_i^{-n} a^{-1} \in N$ entonces $(ax_i^{-n} a^{-1})^{-1} \in N$.

Ahora, como $r \geq 1$ podemos aplicar inducción para probar que $ax_1^{n_1} \dots x_r^{n_r} a^{-1} \in N$ para lo que basta introducir a y a^{-1} entre cada potencia x_i . \square

EJEMPLO 5.3: $A_n \trianglelefteq S_n \forall n \geq 2$.

Basta utilizar el hecho de que A_n está generado por los ciclos de longitud tres y que $\alpha(ijk)\alpha^{-1} = (\alpha(i)\alpha(j)\alpha(k))$.

Teorema 5.4 (Extensión del teorema de correspondencia entre subgrupos y homomorfismos).

Sea $f : G_1 \rightarrow G_2$ un homomorfismo.

1. Si $H_2 \trianglelefteq G_2$ entonces $f^{-1}(H_2) \trianglelefteq G_1$.
2. Si $H_1 \trianglelefteq G_1$ y f es epimorfismo entonces $f(H_1) \trianglelefteq G_2$.

Como consecuencia la normalidad de un subgrupo es invariante por epimorfismo.

Demostración. Usemos el criterio 5.2.

1. Sea $g \in G_1$ y $h \in f^{-1}(H_2)$. Veamos que $ghg^{-1} \in f^{-1}(H_2)$. En efecto, como $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H_2$ ya que por hipótesis $f(h) \in H_2$ y $f(g) \in G_2$ y $H_2 \trianglelefteq G_2$.
2. Sea $h = f(h_1) \in f(H_1)$ y $g \in G_2$. Como f es epimorfismo entonces existe $g_1 \in G_1$ tal que $g = f(g_1)$ entonces $ghg^{-1} = f(g_1)f(h_1)f(g_1)^{-1} = f(g_1 h_1 g_1^{-1}) \in f(H_1)$ ya que $H_1 \trianglelefteq G_1$.

Claramente si f es epimorfismo f preserva hacia adelante y hacia detrás los subgrupos normales. \square

5.2. Grupo cociente

Definición 5.2 (Grupo cociente).

Sea G un grupo y $N \trianglelefteq G$ y consideremos el conjunto de las clases laterales a izquierda G/N . Definimos el producto en dicho conjunto como $(aN)(bN) = (ab)N$. Es fácil comprobar que con esta definición G/N tiene estructura de grupo y lo llamaremos grupo cociente de G por N .

EJEMPLO 5.4: 1. Si G es abeliano entonces G/N es abeliano para cualquier subgrupo N de G .

Definición 5.3 (Proyección canónica).

La aplicación $p : G \rightarrow G/N$ tal que $p(a) = aN$ es un epimorfismo llamado proyección canónica.

Proposición 5.5 (Retículo de subgrupos del grupo cociente).

Sea G un grupo y $N \trianglelefteq G$ entonces se verifica:

1. Si $H \leq G$ y $N \leq H$ entonces $N \trianglelefteq H$ y podemos definir el grupo cociente H/N que será un subgrupo de G/N .
2. Si H_1, H_2 son subgrupos tales que N es normal en H_1 y en H_2 entonces $\frac{H_1}{N} = \frac{H_2}{N} \iff H_1 = H_2$.

3. Si L es un subgrupo del cociente entonces existe un único H subgrupo de G tal que N es subgrupo de H y $L = H/N$.

En consecuencia $Sub(G/N) = \{\frac{H}{N} : H \in Sub(G) \text{ y } N \leq H\}$

Demostración. 1. Se aplica la condición de normalidad y se ve claramente que si $N \trianglelefteq G$ entonces necesariamente es normal en todo subgrupo contenido en G . Obsérvese que esto no quiere decir que la normalidad sea transitiva es decir que $H_1 \trianglelefteq H_2 \trianglelefteq H_3$ no quiere decir que $H_1 \trianglelefteq H_3$. Un buen ejemplo de esto se tiene en D_4 con $\{1, s\} \trianglelefteq \{1, s, r^2, r^2s\} \trianglelefteq D_4$ pero $\{1, s\} \not\trianglelefteq D_4$.

Veamos ahora que $H/N \leq G/N$ usando el criterio de subgrupo. Sean $xN, yN \in H/N$ entonces $(xN)(yN)^{-1} = (xy^{-1})N$ y ya que H es un subgrupo se verifica que $(xy^{-1})N \in H/N$.

2. \Rightarrow Lo hacemos por doble inclusión. En efecto, sea $x \in H_1$ entonces $xN \in H_1/N = H_2/N$ por tanto existe $y \in H_2$ tal que $xN = yN$ luego $xy^{-1} \in N \leq H_2$ luego $x \in H_2$. Análogamente se procede para la otra inclusión.

\Leftarrow Es evidente.

3. ¿Quién puede ser el subgrupo que estamos buscando? Si entendemos el paso al cociente como 'pegar' elementos en uno solo el subgrupo que buscamos es precisamente el que al pegarse da L . La función de pegado es la famosa proyección canónica esto es:

$$H := p^{-1}(L) = \{x \in G : p(x) \in L\} = \{x \in G : xN \in L\}$$

Claramente, $N \leq H$ ya que N es el elemento neutro del cociente y la igualdad se deduce por doble inclusión. La unicidad es consecuencia de 2.

Por 3, $Sub(G/N) \subseteq \{\frac{H}{N} : H \in Sub(G) \text{ y } N \leq H\}$ y por 1, se tiene la otra inclusión. \square

5.3. Teoremas de isomorfismo

Proposición 5.6 (Teorema de factorización de un homomorfismo mediante la proyección canónica). Sea $f : G \rightarrow G'$ un homomorfismo de grupos y sea $N \trianglelefteq G$ con $N \leq Ker(f)$ entonces existe un único homomorfismo $\bar{f} : G/N \rightarrow G'$ tal que $\bar{f} \circ p = f$. Además:

- (1) \bar{f} es epimorfismo $\iff f$ es epimorfismo
- (2) \bar{f} es monomorfismo $\iff N = Ker(f)$

Demostración. Veamos que \bar{f} está bien definido. Si $aN = a'N \iff a'^{-1}a \in N \Rightarrow_{N \leq Ker(f)} f(a'^{-1}a) = f(a'^{-1})f(a) = f(a')^{-1}f(a) = 1 \Rightarrow f(a) = f(a')$. Además claramente f es un homomorfismo de grupos y $\bar{f} \circ p = f$.

Veamos ahora la unicidad. Sea g otro homomorfismo $g : G/N \rightarrow G'$ tal que $g \circ p = f$ entonces $(g \circ p)(a) = g(aN) = f(a)$ y por tanto $g = \bar{f}$.

Veamos (1). $Im(\bar{f}) = \{\bar{f}(aN) : aN \in G/N\} = \{f(a) : a \in G\} = Im(f)$.

Veamos (2). $Ker(\bar{f}) = \{aN \in G/N : \bar{f}(aN) = f(a) = 1\} = Ker(f)/N$ y la doble implicación se sigue del hecho de que si \bar{f} es inyectiva entonces $Ker(\bar{f}) = \{1\}$ y por tanto $Ker(f) = N$ y si $Ker(f) = N$ entonces $Ker(\bar{f}) = \{1\}$ de donde \bar{f} es inyectiva. \square

El siguiente teorema nos dice que la única manera de definir un homomorfismo es llevar las clases módulo el núcleo cada una a un cierto valor distinto.

También se puede entender el teorema como que todo homomorfismo se puede imitar mediante un paso al cociente seguido de un isomorfismo.

Teorema 5.7 (Primer teorema de isomorfismo).

Sea $f : G \rightarrow G'$ un homomorfismo de grupos entonces $G/\text{Ker}(f) \cong \text{Img}(f)$ mediante el isomorfismo $a\text{Ker}(f) \mapsto f(a)$.

Demostración. Apliquemos el teorema de factorización al epimorfismo $f : G \rightarrow \text{Img}(f)$ teniendo en cuenta que $N = \text{Ker}(f) \trianglelefteq G$ y se obtiene que la aplicación $\bar{f} : G/\text{Ker}(f) \rightarrow \text{Img}(f)$ tal que $\bar{f}(a\text{Ker}(f)) = f(a)$ es el único isomorfismo. \square

Corolario 5.8 (Fórmula de las dimensiones).

Sea $f : G \rightarrow G'$ un homomorfismo con G un grupo finito entonces $|G| = |\text{Ker}(f)| |\text{Im}(f)|$.

Demostración. Como $G/\text{Ker}(f) \cong \text{Img}(f)$ entonces $|G/\text{Ker}(f)| = \frac{|G|}{|\text{Ker}(f)|} = |\text{Img}(f)|$. \square

La lectura adecuada del siguiente teorema indica como única condición previa para que se dé el isomorfismo la normalidad del subgrupo que es despedido por el isomorfismo.

Teorema 5.9 (Segundo teorema de isomorfismo o del doble cociente).

Sea G un grupo y $N \trianglelefteq G$.

Sea $H \in \text{Sub}(G)$ tal que $N \leq H$. Entonces:

$H/N \trianglelefteq G/N \iff H \trianglelefteq G$ y en tal caso $G/H \cong \frac{G/N}{H/N}$ mediante el isomorfismo $aH \mapsto (aN)H/N$.

Demostración. \Rightarrow Supongamos que $H/N \trianglelefteq G/N$. Para ver que $H \trianglelefteq G$ vamos a ver que es el núcleo de cierto homomorfismo.

Consideremos las proyecciones canónicas p, q de G en G/N y de G/N en $(G/N)/(H/N)$ respectivamente de modo que la composición es $f = q \circ p : x \mapsto (xN)H/N$ y calculemos el núcleo.

$$\text{Ker}(f) = \{x \in G : f(x) = H/N\} = \{x \in G : xN \in H/N\}$$

y comprobamos que este último conjunto es igual a H por doble inclusión.

Claramente $H \subseteq \text{Ker}(f)$. Veamos la otra inclusión. Si $x \in \text{Ker}(f) \Rightarrow xN \in H/N$ es decir, que existe $h \in H$ tal que $xN = hN \Rightarrow h^{-1}x \in N \leq H$ luego existe $h' \in H$ tal que $h^{-1}x = h' \Rightarrow x \in H$.

\Leftarrow Supongamos que $H \trianglelefteq G$ y usemos el criterio de normalidad (claramente $H/N \leq G/N$). Dado $xN \in G/N$ consideramos $(xN)(hN)(x^{-1}N) = (xhx^{-1})N$ y por la normalidad de H en G se tiene la implicación.

Finalmente, aplicando el primer teorema de isomorfismo se tiene que $G/H = G/\text{Ker}(f) \cong \text{Img}(f) = (G/N)/(H/N)$. \square

La lectura adecuada del siguiente teorema indica como única condición previa para que se dé el isomorfismo la normalidad del subgrupo que divide en solitario en el grupo total.

Teorema 5.10 (Tercer teorema de isomorfismo).

Sea G un grupo y $H, K \leq \text{Sub}(G)$ siendo $K \trianglelefteq G$. Entonces:

1. $HK = KH$ y por tanto $HK \in \text{Sub}(G)$ y $K \trianglelefteq HK$.

2. $H \cap K \trianglelefteq H$.
3. $H/H \cap K \cong HK/K$.

Demostración. 1. Sea $x \in HK$ entonces $x = hk$ con $h \in H, k \in K$ y al ser $K \trianglelefteq G$ se tiene la igualdad $hK = Kh$. Por tanto, existirá un $k' \in K$ tal que $x = k'h$ de donde $x \in KH$. La otra inclusión es análoga y se tiene la igualdad $HK = KH$.

Por el teorema 4.5, se tiene que $HK \in \text{Sub}(G)$ y claramente $K \trianglelefteq HK$.

2. Demostraremos este apartado mediante el uso de la aplicación $g = p \circ i : H \rightarrow G/K$ tal que $g(x) = xK$. Por tanto,

$$\text{Ker}(g) = \{h \in H : hK = K\} = \{h \in H : h \in K\} = H \cap K$$

Además,

$$\text{Img}(g) = \{g(h) : h \in H\} = \{hK : h \in H\} = HK/K$$

Obsérvese que como K no está incluído en H no se tiene H/K sino HK/K . Esto es así porque HK es el supremo de H y K y por tanto los contiene a ambos. Dado un h puedo arrancar un k de la K .

3. Es consecuencia del primer teorema de isomorfismo. □

5.4. Producto directo

5.4.1. Producto directo de grupos

Definición 5.4 (Producto directo de grupos).

Dados G_1, \dots, G_n grupos su producto directo es el grupo $G_1 \times \dots \times G_n = \{(x_1, \dots, x_n) : x_i \in G_i, 1 \leq i \leq n\}$ con la operación producto componente a componente. Lo denotaremos por $\prod_{k=1}^n G_k$.

Definición 5.5 (Proyecciones e inyecciones canónicas).

La proyección canónica sobre la i -ésima componente es la aplicación $p_i : \prod_{k=1}^n G_k \rightarrow G_i$ tal que $p_i((x_1, \dots, x_n)) = x_i$. Claramente, las proyecciones canónicas son epimorfismos.

La inyección canónica desde la j -ésima componente es la aplicación $u_j : G_j \rightarrow \prod_{k=1}^n G_k$ tal que $u_j(x) = (1, \dots, x, \dots, 1)$ donde la x está situada en el j -ésimo lugar. Claramente, las inyecciones canónicas son monomorfismos.

Obsérvese que si $K_i \leq G_i$ entonces $\prod_{i=1}^n K_i \leq \prod_{i=1}^n G_i$.

EJEMPLO 5.5 (Un subgrupo del producto que no es producto de subgrupos): En $\mathbb{Z} \times \mathbb{Z}$, la diagonal $\{(x, x) : x \in \mathbb{Z}\}$ es un subgrupo del producto que no es producto de subgrupos.

Proposición 5.11 (Factores del producto).

Sean G_1, \dots, G_n grupos y $G = \prod_{k=1}^n G_k$.

1. $G_j \cong \text{Img}(u_j)$ e identificando G_j con dicha imagen $G_j \trianglelefteq G$ y $G/G_j \cong \prod_{k=1, k \neq j}^n G_k$.
2. $\prod_{k=1, k \neq j}^n G_k \cong \text{Ker}(p_j)$ e identificando $\prod_{k=1, k \neq j}^n G_k$ con $\text{Ker}(p_j)$ tendríamos $\prod_{k=1, k \neq j}^n G_k \trianglelefteq G$.
3. Con las identificaciones dadas en 1., si $x \in G_i$ e $y \in G_j$ con $i \neq j$ entonces $xy = yx$.

Demostración. 1. Como u_j es un monomorfismo es claro que $\text{Img}(u_j) \cong G_j$. Considerando el homomorfismo $\phi : G \rightarrow G_1 \times \dots \times G_{j-1} \times G_{j+1} \times \dots \times G_n$ tal que $\phi((g_1, \dots, g_n)) = (g_1, \dots, g_{j-1}, g_{j+1}, \dots, g_n)$ se tendrá que $\text{Ker}(\phi) = G_j$ luego G_j es normal en G . Por el primer teorema de isomorfismo $G/G_j = \prod_{k=1, k \neq j}^n G_k$.

2. Obsérvese que $Ker(p_j) = \{(g_1, \dots, g_{j-1}, 1, g_{j+1}, \dots, g_n) : g_j \in G_j \forall j \neq i\}$ y la aplicación $\phi : Ker(p_j) \rightarrow \prod_{k=1, k \neq j}^n G_k$ tal que $\phi((g_1, \dots, 1, \dots, g_n)) = (g_1, \dots, g_n)$.

3. $xy = (1, \dots, 1, g_i, 1, \dots, g_j, \dots, 1) = yx$. □

En resumen, tenemos que formalmente se identificará

$$G_j = \{(1, \dots, g, \dots, 1) : g \in G_i\}$$

y

$$\prod_{k=1, k \neq j}^n G_k = \{(g_1, \dots, 1, \dots, g_n) : g_i \in G_i\}$$

5.4.2. Producto directo de homomorfismos

Definición 5.6.

Sean $f_i : G_i \rightarrow H_i$ homomorfismos de grupos con $i = 1, \dots, n$. El homomorfismo producto es

$$\prod f_i : \prod_{i=1}^n G_i \rightarrow \prod_{i=1}^n H_i$$

tal que $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$.

Sean p_i, q_i las proyecciones desde los productos $\prod_{i=1}^n G_i$ y $\prod_{i=1}^n H_i$ y consideremos el siguiente diagrama:

$$\begin{array}{ccc} \prod_{i=1}^n G_i & \xrightarrow{\prod f_i} & \prod_{i=1}^n H_i \\ \downarrow p_i & & \downarrow q_i \\ G_i & \xrightarrow{f_i} & H_i \end{array}$$

Proposición 5.12 (Propiedad universal del homomorfismo producto).

1. $\prod f_i$ es el único homomorfismo que hace conmutativo al diagrama anterior es decir que se da $q_i(\prod f_i) = f_i p_i$ con $i = 1, \dots, n$.
2. $\prod f_i$ es monomorfismo (respectivamente epimorfismo, isomorfismo) $\iff f_i$ es monomorfismo (respectivamente epimorfismo, isomorfismo) $\forall i = 1, \dots, n$.

Consideremos ahora el monomorfismo

$$\phi : Aut(G_1) \times \dots \times Aut(G_n) \rightarrow Aut(G_1 \times \dots \times G_n)$$

tal que

$$(f_1, \dots, f_n) \mapsto \prod_{i=1}^n f_i$$

.

Teorema 5.13 (Caracterización del producto directo).

Sean G_1, \dots, G_n grupo finitos.

1. $|\prod_{i=1}^n G_i| = \prod_{i=1}^n |G_i|$.
 2. $ord((x_1, \dots, x_n)) = mcm(ord(x_1), \dots, ord(x_n))$.
- Supongamos ahora que $mcd(|G_i|, |G_j|) = 1 \forall i \neq j$ entonces:

3. Si G_i es un grupo cíclico $\implies \prod_{i=1}^n G_i$ es cíclico.
4. Si $L \leq \prod_{i=1}^n G_i$ entonces existen $K_i \leq G_i$ tal que $L = \prod_{i=1}^n K_i$.
5. $\prod_{i=1}^n \text{Aut}(G_i) \cong \text{Aut}(\prod_{i=1}^n G_i)$ y el isomorfismo es ϕ .

5.4.3. Producto directo interno

Sea G un grupo, $H, K \leq G$ y $\lambda : H \times K \rightarrow G$ tal que $\lambda((h, k)) = hk$.

En cualquiera de las situaciones del siguiente teorema diremos que G es producto directo interno de H y K .

Teorema 5.14 (Condiciones de producto directo interno).

Son equivalentes:

1. λ es un isomorfismo.
2. $H, K \trianglelefteq G$, $HK = G$ y $H \cap K = \{1\}$.
3. $hk = kh \forall k \in K$ y $h \in H$, $G = H \vee K$ y $H \cap K = \{1\}$.
4. $hk = kh \forall k \in K$ y $h \in H$ y además para cada $g \in G \exists! h \in H, k \in K$ tales que $g = hk$

Demostración.

□

Generalizamos para n subgrupos.

Tomados $H_1, \dots, H_n \leq G$ consideramos el homomorfismo $\phi : \prod H_i \rightarrow G$ tal que $(h_1, \dots, h_n) \mapsto h_1 \dots h_n$.

En cualquiera de las situaciones del siguiente teorema diremos que G es producto directo interno de $H_1 \dots H_n$.

Teorema 5.15 (Condiciones de producto directo interno).

Son equivalentes:

1. ϕ es un isomorfismo.
2. $H_i \trianglelefteq G \forall i = 1, \dots, n$, $\prod_{i=1}^n H_i = G$ y $(H_1 \dots H_{i-1}) \cap H_i = \{1\} \forall i = 2, \dots, n$.
3. $h_i h_j = h_j h_i \forall h_i \in H_i \forall h_j \in H_j \forall i \neq j$, $G = H_1 \vee \dots \vee H_n, (H_1 \dots H_{i-1}) \cap H_i \forall i = 2, \dots, n$.
4. $h_i h_j = h_j h_i \forall h_i \in H_i \forall h_j \in H_j \forall i \neq j$, tal que para cada $g \in G \exists! h_1 \in H_1, \dots, h_n \in H_n$ tal que $g = h_1 \dots h_n$.

Demostración.

□

6. Grupos solubles

6.1. Grupos simples y series normales

Definición 6.1 (Serie normal y refinamiento).

Dado un grupo G , una serie normal de G es una sucesión finita de grupos de la forma

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_n = G \quad (1)$$

A los grupos H_i se les llama términos de la serie y a los cocientes H_i/H_{i-1} se les llama factores de G .

La serie se dice propia si las inclusiones son todas estrictas, esto es, si $H_i \subsetneq H_{i+1}$ $i = 0, 1, \dots, n-1$. En este caso diremos que la longitud de la serie es n (esto es, G no se cuenta).

Supongamos una serie normal

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_m = G \quad (2)$$

Diremos que la serie (1) es un refinamiento de la serie (2) si $m \leq n$ y además todos los grupos de (2) aparecen en (1) (esto es, si la serie (1) es más larga que la serie (2)). El refinamiento se dirá propio si $m < n$.

EJEMPLO 6.1: 1. $\{1\} \trianglelefteq A_4 \trianglelefteq S_4$

2. $\{1\} \trianglelefteq K \trianglelefteq S_4$

3. $\{1\} \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$ refina a las dos series anteriores.

4. $\{1\} \trianglelefteq C_2 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$ donde C_2 no es normal en A_4 ni en S_4 . De hecho, no hay más refinamientos de esta.

Definición 6.2 (Serie de composición).

Una serie de composición de un grupo G es una serie normal, propia y que no admite refinamientos propios. Los factores de una serie de composición se llaman factores de composición de G (ya que sólo dependen de G).

(Motivar la definición de grupo simple como en 168 del libro de la UNAM).

Definición 6.3 (Grupo simple).

Un grupo G es simple si $G \neq \{1\}$ y no tiene subgrupos normales propios.

Claramente, la noción de grupo simple se mantiene por isomorfismo.

EJEMPLO 6.2: 1. Si $|G| = p$ primo entonces G es simple ya que ni siquiera tiene subgrupos propios.

2. Si G es abeliano, G es simple $\iff G \cong C_p$ con p un número primo.

En efecto,

\Leftarrow Si $G \cong C_p$ con p primo los subgrupos de G son los improprios.

\Rightarrow Si G es abeliano y simple para empezar G no es trivial por definición y entonces podemos tomar $x \in G \setminus \{1\}$ y como G es abeliano el subgrupo $\langle x \rangle$ será normal en G . Como G es simple, necesariamente $G = \langle x \rangle$, luego G es cíclico.

Faltaría por ver que G es de orden finito. Para ello consideremos el orden de x . Si fuera infinito entonces $G \cong \mathbb{Z}$ pero \mathbb{Z} no es simple porque tiene infinitos subgrupos y la simplicidad es un invariante por isomorfismo.

Además necesariamente el orden del grupo debe ser primo. Pues si no fuera primo existirían subgrupo propios según el teorema que describe el retículo de subgrupos de un grupo cíclico y como el grupo es abeliano se tendría que serían normales.

El siguiente teorema caracteriza a los grupos simples como los ladrillos básicos de construcción de las series de composición al modo de los números primos en \mathbb{Z} .

Teorema 6.1 (Condición de factores simples).

Sea $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_n = G$ una serie normal.

La serie es de composición $\iff H_i/H_{i-1}$ son simples para todo $i = 1, \dots, n$.

Demostración. \Rightarrow Supóngase que la serie es de composición y supongamos por reducción al absurdo que existe un i tal que H_i/H_{i-1} no es simple. Por tanto existiría un subgrupo normal propio K/H_{i-1} que por el segundo teorema isomorfismo implicaría que $H_{i-1} \triangleleft K \triangleleft H_i$. Ahora bien, por ser una serie de composición no puede admitir refinamientos propios y llegamos a una contradicción.

\Leftarrow Para empezar el hecho de que los cocientes sean simples H_i/H_{i-1} me dice que la serie es propia ya que $H_i/H_{i-1} \neq \{1\} \implies H_{i-1} \triangleleft H_i$.

Supongamos ahora que $\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_m = G$ es un refinamiento propio de la serie (con lo que en particular $m > n$). Sea K_l el mayor de los que no aparecen en la serie original de modo que $l < m$ y además K_{l+1} aparece en la original. Sea $K_{l+1} = H_r$.

Se tiene que $H_{r-1} \triangleleft K_l \triangleleft K_{l+1} = H_r$ de donde $K_l/H_{r-1} \triangleleft H_r/H_{r-1}$ y K_l/H_{r-1} es no trivial. Como H_r/H_{r-1} es simple llegamos a una contradicción. \square

EJEMPLO 6.3: 1. Probemos que en efecto la serie $\{1\} \trianglelefteq C_2 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$ no admite refinamientos propios. Para ello calculamos los cocientes sucesivos.

$C_2/\{1\} \cong C_2$ que es simple puesto que es abeliano.

$K/C_2 \cong C_2$ ya que $|K/C_2| = 2$.

$A_4/K \cong C_3$ ya que $|A_4/K| = 3$.

$S_4/A_4 \cong C_2$ ya que $|S_4/A_4| = 2$.

$2\mathbb{Z}$ no tiene series de composición.

Si tuviera una serie de composición $\{0\} = t_1\mathbb{Z} \trianglelefteq \dots \trianglelefteq t_{n-1}\mathbb{Z} \trianglelefteq \mathbb{Z}$, en particular $(t_1\mathbb{Z})/\{0\} \cong t_1\mathbb{Z}$ debería ser simple, pero se trata de un grupo abeliano que tiene como subgrupos los múltiplos de t_1 y los subgrupos de un grupo abeliano son todos normales.

Teorema 6.2 (Existencia de una serie de composición para grupos finitos).

Si G es un grupo finito entonces tiene al menos una serie de composición.

Demostración. Procedamos por inducción fuerte sobre $|G|$.

Si $|G| = 2$ entonces la serie $\{1\} \trianglelefteq G$ es una serie de composición.

Si $|G| > 2$ entonces tomamos K el mayor subgrupo normal contenido propiamente en G . Obsérvese que al menos $\{1\}$ es normal en G y que existirá un mayor subgrupo normal ya que el retículo de subgrupos es finito.

Por hipótesis de inducción, dicho subgrupo K admite una serie de composición

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_r = K$$

de modo que la serie

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K \trianglelefteq G$$

es una serie de composición para G . \square

EJEMPLO 6.4: La serie de composición del grupo no tiene por qué ser única. Así $\{1\} \triangleleft \langle r^2 \rangle \triangleleft \langle r \rangle \triangleleft D_4$ y si $K = \langle r^2, s \rangle$ es uno de los subgrupos de Klein tenemos $\{1\} \triangleleft \langle s \rangle \triangleleft K \triangleleft D_4$. Y observamos que los factores en ambos casos son isomorfos a C_2 .

La pregunta es si dadas dos series de composición existirá alguna relación entre ellas.

Definición 6.4 (Series equivalentes).

Dadas dos series normales de G ,

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

y

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$$

Diremos que estas dos series son equivalentes o isomorfas si:

- 1) $m = n$
- 2) $\exists \sigma \in S_n$ tal que $G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i)-1}$ con $i = 1, \dots, n$.

Esto es, tienen la misma longitud y factores isomorfos salvo el orden en que ocurren.

Probamos a continuación el Cuarto teorema de isomorfía, que nos será útil para demostrar para demostrar el lema de Schreier para lo cual usaremos dos lemas previos.

Lema 6.3 (Ley Modular o Regla de Dedekind).

Sea G un grupo. $A, B, C \leq G$ con $A \leq C$. Entonces $A(B \cap C) = (AB) \cap C$

Demostración. Procedemos por doble inclusión

\subseteq Si tomo un elemento de $A(B \cap C)$ entonces es producto de un elemento $a \in A$ y de un elemento de $x \in B \cap C$. Como $x \in B$ se tiene que $ax \in AB$ y como $A \leq C$ se tiene que $ax \in C$ de donde $ax \in (AB) \cap C$.

\supseteq Recíprocamente si tomo un elemento de $(AB) \cap C$ entonces será de la forma $z = ab$ con $z \in C$ y $a \in A, b \in B$. Pero a también está en C y eso nos permite afirmar que $b = a^{-1}ab \in C$ de donde $z \in A(B \cap C)$. Como se quería. \square

Lema 6.4 (Consecuencia del tercer teorema de isomorfía).

Sea G un grupo. $A, B, C \leq G$ y $B \trianglelefteq A$. Entonces se verifica:

- i) $B \cap C \cong A \cap C$ y $\frac{A \cap C}{B \cap C} \cong \frac{B(A \cap C)}{B}$
- ii) Si además $C \trianglelefteq G$ entonces $BC \trianglelefteq AC$ y $\frac{AC}{BC} \cong \frac{A}{B(A \cap C)}$

Demostración. i) Basta aplicar el tercer teorema de isomorfismo con $H = A \cap C$ y $K = B$.

ii) Puesto que $C \trianglelefteq G$ por la proposición 4.5 se tendrá que $BC, AC \leq G$ y como $B \trianglelefteq A$ claramente $BC \leq AC$.

Veamos que $BC \trianglelefteq AC$. Sea $ac \in AC$ y $bc' \in BC$, entonces $(ac)(bc')(ac)^{-1} = (aca^{-1})(aba^{-1})(ac'c^{-1}a^{-1}) \in CBC = BCC = BC$ por ser $B \trianglelefteq A, C \trianglelefteq G$ y $BC = CB$.

El isomorfismo se deduce al aplicar el tercer teorema de isomorfismo para $H = A$ y $K = BC$ teniendo en cuenta que por la regla de Dedekind $(BC) \cap A \cong B(A \cap C)$ y que $HK = ABC = AC$ ya que $B \leq A$. \square

Lema 6.5 (Cuarto teorema de isomorfía).

Sea G un grupo y C_1, A_1, C_2, A_2 subgrupos de G tales que $C_1 \trianglelefteq A_1$ y $C_2 \trianglelefteq A_2$. Entonces:

1. $(A_1 \cap C_2)C_1 \trianglelefteq (A_1 \cap A_2)C_1$.
2. $(C_1 \cap A_2)C_2 \trianglelefteq (A_1 \cap A_2)C_2$.
3. $(A_1 \cap A_2)C_1 / (A_1 \cap C_2)C_1 \cong (A_1 \cap A_2)C_2 / (A_2 \cap C_1)C_2$.

Demostración. Considérese como espacio ambiente A_2 y apliquemos el tercer teorema de isomorfismo para $K = C_2$ y $H = A_1 \cap A_2$. Entonces $H \cap K = A_1 \cap A_2 \cap C_2 = A_1 \cap C_2 \trianglelefteq A_1 \cap A_2$ y análogamente $A_2 \cap C_1 \trianglelefteq A_1 \cap A_2$. Entonces es fácil razonar que su producto $B = (A_1 \cap C_2)(A_2 \cap C_1) \trianglelefteq A_1 \cap A_2$ (para ello utilícese la proposición 4.5 y el teorema 5.2).

Aplicamos el apartado ii) del lema 6.4 para el producto B , $A = A_1 \cap A_2$ y $C = C_1$ entonces

$$BC = BC_1 = (A_1 \cap C_2)(A_2 \cap C_1)C_1 = (A_1 \cap C_2)C_1 \trianglelefteq (A_1 \cap A_2)C_1$$

y

$$\frac{AC}{BC} \cong \frac{(A_1 \cap A_2)C_1}{(A_1 \cap C_2)C_1} \cong \frac{A}{B(A \cap C)} = \frac{A_1 \cap A_2}{B(A_1 \cap A_2 \cap C_1)} = \frac{A_1 \cap A_2}{(A_1 \cap C_2)(A_2 \cap C_1)}$$

. Por simetría se obtendría el punto 2 y el segundo isomorfismo. \square

Teorema 6.6 (Lema de refinamiento de Schreier (1928)).

Dos series de un grupo G admiten refinamientos equivalentes.

Demostración. Sean

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

y

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$$

dos series normales para el grupo G .

Para $i \in I_n$ y $j \in I_m$ notaremos $G_{ij} = (G_i \cap H_j)G_{i-1}$ ($i \neq 0$) y $H_{ij} = (H_j \cap G_i)H_{j-1}$ ($j \neq 0$). Se tiene que

$$G_{i-1} = G_{i0} \leq G_{i1} \leq \dots \leq G_{im} = G_i \quad (1)$$

y

$$H_{j-1} = H_{0j} \leq H_{1j} \leq \dots \leq H_{nj} = H_j \quad (2)$$

Usando el lema con $C_1 = G_{i-1} \trianglelefteq A_1 = G_i$ y $C_2 = H_{j-1} \trianglelefteq A_2 = H_j$ de aquí se obtiene que $G_{ij-1} \trianglelefteq G_{ij}$ y que $H_{i-1j} \trianglelefteq H_{ij}$ y se obtiene que en (1) y (2) las series son normales. Además, por el cuarto teorema de isomorfía $G_{ij}/G_{ij-1} \cong H_{ij}/H_{i-1j}$.

Para ver que las series obtenidas son equivalentes basta ver que tienen la misma longitud.

$$1 = G_0 \trianglelefteq G_{10} \trianglelefteq G_{11} \trianglelefteq \dots \trianglelefteq G_{1m} = G_1 = G_{20} \trianglelefteq G_{21} \trianglelefteq \dots \trianglelefteq G_{2m} = G_2 \trianglelefteq \dots \trianglelefteq G_{nm} = G_n = G$$

Cuya longitud es $n + (m-1)n = nm$.

$$1 = H_0 \trianglelefteq H_{01} \trianglelefteq H_{02} \trianglelefteq \dots \trianglelefteq H_{n1} = H_1 = H_{02} \trianglelefteq H_{12} \trianglelefteq \dots \trianglelefteq H_{n2} = H_2 \trianglelefteq \dots \trianglelefteq H_{nm} = H_m = G$$

Cuya longitud es nm . \square

Teorema 6.7 (Teorema de Jordan-Hölder).

Sea G un grupo finito, entonces:

- 1) Toda serie normal de G admite un refinamiento que es una serie de composición de G .
- 2) Cualesquiera dos series de composición de G son equivalentes.

Demostración. 1. Denotemos por S_1 a una serie normal de G y por S_2 a una serie de composición de G , que existe puesto que G es finito. Por el lema de refinamiento de Schreier ambas series admiten refinamientos equivalentes.

S_1 admite un refinamiento equivalente a un refinamiento de S_2 y como S_2 es de composición el refinamiento de S_1 es equivalente a la serie S_2 .

Pero una serie que sea equivalente a una serie de composición necesariamente ha de ser una serie de composición ya que los factores de ambas series salvo el orden son isomorfos y como los de la serie de composición son simples por la condición de factores simples se deduce que tenemos una serie de composición.

2. Por el lema de refinamiento de Schreier las series de composición S_1 y S_2 admiten refinamientos equivalentes. Pero como S_1 y S_2 son series de composición sus refinamientos coinciden con S_1 y S_2 luego son equivalentes. \square

Definición 6.5 (Longitud y factores de un grupo finito).

Sea G un grupo finito.

La longitud de G es la longitud de cualquier serie de composición de G . Lo denotaremos por $L(G)$.

Los factores de composición de G son los factores de cualquiera de sus series de composición. Al conjunto de los factores de composición lo denotaremos por $\text{Fact}(G)$.

6.2. Grupos solubles

Definición 6.6 (Grupo soluble).

Un grupo G es soluble si tiene una serie normal $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ cuyos factores G_i/G_{i-1} con $i = 1, \dots, n$ son abelianos.

Notemos que la solubilidad de un grupo es invariante por homomorfismo.

EJEMPLO 6.5: Todo grupo abeliano es soluble ya que $\{1\} \trianglelefteq G$ es una serie normal y además $G/\{1\} = G$ es abeliano.

Teorema 6.8 (Caracterización por factores de un grupo finito soluble).

Sea G un grupo finito. Entonces equivalen:

- 1) Los factores de composición de G son cíclicos de orden primo.
- 2) G tiene una serie normal con factores cíclicos.
- 3) G es soluble.

Demostración. Claramente $1) \implies 2) \implies 3)$.

Veamos que $3) \implies 1)$. En efecto, sea $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ una serie normal para G cuyos cocientes G_i/G_{i-1} son abelianos con $i = 1, \dots, n$.

Por el teorema de Jordan-Hölder dicha serie admite un refinamiento que es una serie de composición $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$. Si demostramos que los cocientes además de ser simples son abelianos habríamos terminado ya que un grupo abeliano y simple es cíclico de orden primo.

Consideremos $G_{j-1} \trianglelefteq H_{r-1} \trianglelefteq H_r \trianglelefteq G_j$ y por el segundo teorema de isomorfismo tenemos que $H_r/H_{r-1} \cong (H_r/G_{j-1})/(H_{r-1}/G_{j-1})$ y dado que $H_r/G_{j-1} \leq G_j/G_{j-1}$ que es abeliano, es también él mismo abeliano. En consecuencia el cociente es abeliano y por isomorfismo hemos acabado. \square

EJEMPLO 6.6: S_2 es un grupo abeliano y por tanto es soluble. Se verifica que $\text{Fact}(S_2) = \{C_2\}$.

En S_3 tenemos la serie de composición $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ de donde $\text{Fact}(S_3) = \{C_2, C_3\}$ y por tanto S_3 es un grupo soluble.

En S_4 consideramos la serie de composición $\{1\} \trianglelefteq C \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$ con factores $\text{Fact}(S_4) = \{C_2, C_3, C_2, C_2\}$ y por tanto S_4 es un grupo soluble.

Proposición 6.9 (Relación de la solubilidad con cocientes y subgrupos).

Sea G un grupo:

1. Si G es soluble y $H \leq G \implies H$ es soluble.
2. Si G es soluble y $N \trianglelefteq G \implies G/N$ es soluble.
3. Si $N \trianglelefteq G$ tal que N y G/N son solubles $\implies G$ es soluble.

Demostración. 1. Sea $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ con G_i/G_{i-1} abeliano. Vamos a ver que $\{1\} = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \dots \trianglelefteq G_n \cap H = G$ hace soluble a H .

Considerando como espacio ambiente H_i tenemos la normalidad de $G_{i-1} \trianglelefteq G_i$ y podemos aplicar el tercer teorema de isomorfía a $K = G_{i-1}$ y $H = H \cap H_i$ de modo que $\frac{H \cap G_i}{H \cap G_{i-1}} = \frac{H \cap G_i}{H \cap G_i \cap G_{i-1}} \cong \frac{(H \cap G_i)G_{i-1}}{G_{i-1}} \leq \frac{G_i}{G_{i-1}}$ que es un grupo abeliano. Se concluye ya que los subgrupos de grupos abelianos son abelianos.

2. Como en 1. sea $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ con G_i/G_{i-1} abeliano. Entonces claramente (revisar notas) $G_i N \trianglelefteq G_{i+1} N$ y la serie $\{1\} = G_0 N/N \trianglelefteq G_1 N/N \trianglelefteq \dots \trianglelefteq G_n N/N = G/N$ nos dirá que G/N es abeliano.

En efecto, $\frac{G_i N/N}{G_{i-1} N/N} \cong \frac{G_i N}{G_{i-1} N} \cong \frac{G_i}{G_i \cap G_{i-1} N} \cong \frac{G_i/G_{i-1}}{\frac{G_i \cap G_{i-1} N}{G_{i-1}}}$. Donde en la primera igualdad se utiliza el segundo teorema de isomorfismo gracias a la normalidad de N en G y en la segunda igualdad se utiliza el tercer teorema de isomorfismo con $H = G_i$ y $K = G_{i-1} N$ y en la última igualdad se vuelve a usar el segundo teorema de isomorfismo con la normalidad de G_{i-1} en G_i . Por ser el numerador abeliano se deduce que los cocientes de la nueva serie son abelianos y hemos acabado.

3. De la solubilidad de N deducimos que existe una serie $\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_r = N$ con N_i/N_{i-1} abeliano. Como G/N es soluble existe otra serie $\{1\} = G_0/N \trianglelefteq G_1/N \trianglelefteq \dots \trianglelefteq G_n/N = G/N$ con $(G_i/N)/(G_{i-1}/N) \cong G_i/G_{i-1}$ abeliano.

Por tanto la serie $\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_r = N = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ hace al grupo G soluble. \square

Corolario 6.10 (Solubilidad de los grupos diédricos).

D_n es un grupo soluble $\forall n \geq 3$.

Demostración. Consideremos $N = \langle r \rangle$. Como $[D_n : N] = 2$ sabemos que $N \trianglelefteq D_n$. Como N es abeliano, es soluble y como $|D_n/N| = 2$ entonces $D_n/N \cong C_2$ que es un grupo abeliano y por tanto es soluble. Finalmente, aplicando 3. se llega a que D_n es soluble. \square

Teorema 6.11 (Teorema de Abel).

A_n es un grupo simple $\forall n \geq 5$.

Corolario 6.12 (Solubilidad de los grupos de permutaciones).

S_n es soluble $\iff n \leq 4$.

Demostración. En efecto, si $n \leq 4$ por el ejemplo anterior anterior sabemos que S_n es soluble. Ahora, si $n > 4$ sabemos que A_n es simple por el teorema de Abel y por tanto la serie $\{1\} \trianglelefteq A_n \trianglelefteq S_n$ es una serie de composición ya que sus factores son $\{C_2, A_n\}$ que son simples y ya que A_n no es cíclico ni de orden primo por la caracterización por factores de un grupo finito soluble se tiene que S_n no es soluble. \square

Definición 6.7 (Subgrupo conmutador).

Dado un grupo G y $x, y \in G$, su conmutador es $[x, y] := xyx^{-1}y^{-1}$. Es claro que $xy = [x, y]yx$ y es por ello que se llama conmutador. El subgrupo conmutador o primer derivado de G es

$$[G : G] := \langle \{[x, y] : x, y \in G\} \rangle$$

Proposición 6.13 (Propiedades del subgrupo conmutador).

1. G es abeliano $\iff [G, G] = 1$.
2. $[G, G] \trianglelefteq G$.
3. $G/[G, G]$ es abeliano y se le llama el abelianizado del grupo G , G_{ab} .
4. Si $f : G \rightarrow A$ es un homomorfismo y A es abeliano entonces $[G, G] \leq \text{Ker}(f)$.
5. Si $N \trianglelefteq G$ entonces G/N es abeliano $\iff [G, G] \leq N$. En otras palabras, el conmutador es el subgrupo más pequeño que hace abeliano al cociente.

Demostración. 1. Es evidente.

2. Basta usar la condición de normalidad $a[x, y]a^{-1} = [axa^{-1}, aya^{-1}] \in [G : G]$.

3. $(x[G : G])(y[G : G]) = (xy)[G : G] = (yx[y^{-1}x^{-1}])[G : G] = yx[G : G] = (y[G : G])(x[G : G])$.

4. $f([x, y]) = f(x)f(y)f(x)^{-1}f(y)^{-1} = f(x)f(x)^{-1}f(y)f(y)^{-1} = 1$ de donde $[x, y] \in \text{Ker}(f)$.

5. \Leftarrow Si $[G : G] \trianglelefteq N$ entonces $(xN)(yN) = (xy)N = [x, y]yxN = yxN = (yN)(xN)$.

\Rightarrow Si G/N es abeliano entonces $[G : G] \leq \text{Ker}(p) = N$ donde p es la proyección canónica. \square

Definición 6.8 (Derivado y serie derivada de un grupo).

Dado un grupo G , el n -ésimo derivado de G es por recurrencia:

$$G^0 := G$$

$$G^1 := [G, G]$$

$$G^{n+1} := [G^n, G^n] \quad n \geq 1$$

En estas condiciones tenemos una serie normal, en general no finita de la forma

$$G^{n+1} \trianglelefteq G^n \trianglelefteq \dots \trianglelefteq G^1 \trianglelefteq G$$

llamada serie derivada del grupo G cuyos factores son abelianos.

Teorema 6.14 (Caracterización por derivados de un grupo soluble).

Sea G un grupo:

G es soluble $\iff \exists n$ tal que $G^n = \{1\}$.

En otras palabras, G es soluble si y sólo si la serie derivada es finita.

Demostración. \Rightarrow Si G es soluble y $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ es una serie tal que G_i/G_{i-1} es abeliano entonces vamos a probar que para todo k se verifica que $G^{(k)} \leq H_{n-k}$. De donde para $k = n$ se tendría que $G^{(n)} \leq H_{n-n} = H_0 = \{1\}$ de donde $G^{(n)} = \{1\}$.

Para $k = 1$ se verifica que como G/G_{n-1} es abeliano entonces $[G, G] \leq G_{n-1}$.

Para $k > 1$ tomemos como hipótesis de inducción que $G^{(k)} \leq G_{n-k}$. Por tanto como $G_{n-k}/G_{n-(k+1)}$ es abeliano entonces $G^{(k+1)} \leq [G_{n-k}, G_{n-k}] \leq G_{n-(k+1)}$. Y hemos acabado.

\Leftarrow En efecto, si $\exists n$ tal que $G^{(n)} = \{1\}$ entonces la serie derivada es finita y sus cocientes son abelianos por la propiedad del abelianizado. \square

7. Tema 6: G-conjuntos y p-grupos

7.1. G-conjuntos

Definición 7.1 (Acción por la izquierda).

Sea G un grupo y X un conjunto no vacío.

Una acción por la izquierda del grupo G sobre el conjunto X consiste en una aplicación $G \times X \rightarrow X$ tal que $(g, x) \mapsto g_x$ cumpliendo dos condiciones:

1. $1_x = x \quad \forall x \in X$.
2. $(g_1 g_2)_x = g_{1_{g_2 x}} \quad \forall g_1, g_2 \in G \text{ y } x \in X$.

A X se llamará G -conjunto y G se llamará dominio de operadores. Al valor g_x se le llama "g actuando sobre x".

Proposición 7.1.

Dar una acción de G sobre X equivale a dar un homomorfismo $G \rightarrow S(X)$.

Demostración. Para cada $g \in G$ definiríamos la aplicación $\phi(g) : X \rightarrow X$ tal que $x \mapsto g_x$. A esta aplicación se la conoce como representación asociada a la acción.

Recíprocamente, dado un homomorfismo de grupos $\phi : G \rightarrow S(X)$ la aplicación $G \times X \rightarrow X$ tal que $(g, x) \mapsto g_x := \phi(g)(x)$ es una acción por la izquierda. \square

Definición 7.2 (Núcleo de una acción, acción fiel).

Definimos el núcleo de una acción como el núcleo de su homomorfismo representante ϕ esto es $\text{Ker}(\phi) = \{g \in G : \phi(g) = \text{id}_X\} = \{g \in G : g_x = x \quad \forall x \in X\}$.

Diremos que una acción es fiel si $\text{Ker}(\phi) = \{1\}$.

EJEMPLO 7.1: 1. Dados G y X arbitrarios, la acción trivial es $G \times X \rightarrow X$ tal que $g_x = x \quad \forall g \in G$ y $\forall x \in X$. La representación asociada es el homomorfismo trivial de G a $S(X)$.

2. La restricción de una acción $\phi : G \times X \rightarrow X$ a un subgrupo $H \leq G$ es también una acción $\phi' : H \times X \rightarrow X$ dada por la composición de la inclusión i y la acción ϕ .

3. Sea $G = S_n$ y $X = I_n$ entonces $S(X) = S_n$ y la identidad en S_n define la acción $S_n \times X \rightarrow X$ dada por $(\sigma, i) \mapsto \sigma(i)$. Esta acción es fiel.

4. Sea $G = S_n$ y X cualquiera no vacío. Notamos por X^n al producto cartesiano de X n veces. Se tiene la siguiente acción $G \times X^n \rightarrow X^n$ tal que $(\sigma, (x_1, \dots, x_n)) \mapsto (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$. Esta acción es fiel.

5. Si G es un grupo cualquiera y tomamos $X = G$. Definimos la acción por traslación de G sobre sí mismo como $G \times G \rightarrow G$ tal que $(g, h) \mapsto g_h := gh$. Esta acción es fiel.

6. Sea G un grupo finito y tomamos $X = G$. La acción por conjugación de G sobre sí mismo es $G \times G \rightarrow G$ tal que $(g, h) \mapsto ghg^{-1}$ y además su representación asociada es la que a cada elemento le hace corresponder su automorfismo interior. Su núcleo coincide con el centro del grupo, $Z(G)$.

7. Sea G un grupo y $X = \text{Sub}(G)$. Consideremos la acción $G \times \text{Sub}(G) \rightarrow \text{Sub}(G)$ tal que $(g, H) \mapsto gHg^{-1}$. Claramente $\text{Ker}(\phi) = \{g \in G : gH = Hg \quad \forall \text{Sub}(G)\}$. Obsérvese que es una generalización de la acción por conjugación.

Teorema 7.2 (Teorema de Cayley).

Todo grupo finito es isomorfo a un subgrupo del grupo de permutaciones del mismo orden que el grupo.

Demostración. Sea $|G| = n$ entonces naturalmente $S(G) \cong S_n$.

Consideremos la acción por traslación sobre G , ϕ . Como ϕ es un monomorfismo, su dominio y su imagen son isomorfos, esto es, $\phi(G) \cong G$. Téngase en cuenta también que $\phi(G)$ es un subgrupo de $S(G)$. Por tanto, sabemos que G es isomorfo a un subgrupo de $S(G)$. El primer isomorfismo nos dice que es isomorfo a un subgrupo de S_n . \square

Definición 7.3 (Órbitas y acción transitiva).

Dados $x, y \in X$ diremos que $x \sim y \iff \exists g \in G$ tal que $y = g_x$. Se tiene una relación de equivalencia cuya clase de equivalencia es $O(x) = \{y \in G : y \sim x\} = \{g_x : x \in G\}$.

En otras palabras la órbita de un elemento es el resultado de aplicar todos los elementos de G a x .

La acción es transitiva si $O(x) = O(y) \forall x, y \in X$, esto es, si $\forall x, y \in X \exists g \in G$ tal que $y = g_x$.

Definición 7.4 (Estabilizador).

Para cada $x \in X$ el estabilizador de x en G es $Stab_G(x) = \{g \in G : g_x = x\}$. Se verifica que el estabilizador es un subgrupo de G .

Proposición 7.3 (Relación entre el estabilizador y las órbitas).

1. Sea G es un grupo finito actuando sobre un conjunto X . Entonces para cada $x \in X$, $O(x)$ es finito y además $|O(x)| = [G : Stab_G(x)]$. En particular, $|O(x)| \mid |G|$.
2. Si $O(x) = O(y)$ entonces los estabilizadores son subgrupos conjugados. Esto es, $\exists g \in G : gStab_G(x)g^{-1} = Stab_G(y)$.

Definición 7.5 (Elementos fijos por una acción).

$x \in X$ es fijo por la acción si $g_x = x \forall g \in G$. De forma equivalente se tiene que $O(x) = \{x\}$ o bien que $Stab_G(x) = G$. Al conjunto de elementos fijos por la acción lo denotaremos por $Fix_G(X)$.

EJEMPLO 7.2: 1. Consideramos la acción por traslación. Claramente la órbita de cualquier elemento h es

$$O(h) = G$$

En particular, es una acción transitiva.

Además

$$Stab_G(h) = \{1\}$$

y por tanto

$$Fix(G) = \emptyset$$

2. Consideremos la acción por conjugación. Claramente la órbita de cualquier elemento h es

$$O(h) = \{ghg^{-1} : g \in G\}$$

a esto lo llamaremos clase de conjugación del elemento h y lo denotaremos por $Cl(h)$. El estabilizador será

$$Stab_G(h) = \{g \in G : ghg^{-1} = h\}$$

a esto se le llama centralizador y lo denotaremos por $C_G(h)$. El nombre de centralizador proviene de la siguiente igualdad:

$$Fix(G) = Z(G) = \cap_{h \in G} C_G(h)$$

Consideremos la acción por traslación sobre G , ϕ . Como ϕ es un monomorfismo, su dominio y su imagen son isomorfos, esto es, $\phi(G) \cong G$. Téngase en cuenta también que $\phi(G)$ es un subgrupo de $S(G)$. Por tanto, sabemos que G es isomorfo a un subgrupo de $S(G)$. El primer isomorfismo nos dice que es isomorfo a un subgrupo de S_n . \square

Definición 6.3 (Órbitas y acción transitiva).

Dados $x, y \in X$ diremos que $x \sim y \iff \exists g \in G$ tal que $y = g_x$. Se tiene una relación de equivalencia cuya clase de equivalencia es $O(x) = \{y \in G : y \sim x\} = \{g_x : x \in G\}$.

En otras palabras la órbita de un elemento es el resultado de aplicar todos los elementos de G a x .

La acción es transitiva si $O(x) = O(y) \forall x, y \in X$, esto es, si $\forall x, y \in X \exists g \in G$ tal que $y = g_x$.

Definición 6.4 (Estabilizador).

Para cada $x \in X$ el estabilizador de x en G es $Stab_G(x) = \{g \in G : g_x = x\}$. Se verifica que el estabilizador es un subgrupo de G .

Proposición 6.3 (Relación entre el estabilizador y las órbitas).

1. Sea G es un grupo finito actuando sobre un conjunto X . Entonces para cada $x \in X$, $O(x)$ es finito y además $|O(x)| = [G : Stab_G(x)]$. En particular, $|O(x)| \mid |G|$.
2. Si $O(x) = O(y)$ entonces los estabilizadores son subgrupos conjugados. Esto es, $\exists g \in G : gStab_G(x)g^{-1} = Stab_G(y)$.

Definición 6.5 (Elementos fijos por una acción).

$x \in X$ es fijo por la acción si $g_x = x \forall g \in G$. De forma equivalente se tiene que $O(x) = x$ o bien que $Stab_G(x) = G$. Al conjunto de elementos fijos por la acción lo denotaremos por $Fix_G(X)$.

EJEMPLO 6.2: 1. Consideramos la acción por traslación. Claramente la órbita de cualquier elemento h es $O(h) = G$. En particular, es una acción transitiva. Además $Stab_G(h) = \{1\}$ y por tanto $Fix(G) = \emptyset$.

2. Consideremos la acción por conjugación. Claramente la órbita de cualquier elemento h serán los elementos conjugados por elementos de g , a esto lo llamaremos clase de conjugación del elemento h y lo denotaremos por $Cl(h)$. El estabilizador estará formado por los elementos que conmutan con el h . A esto se le llama centralizador y lo denotaremos por $C_G(h)$. En consecuencia $Fix(G) = Z(G)$.

3. Consideremos la generalización para subgrupos de la acción por conjugación. Claramente $O(H) = \{gHg^{-1} : g \in G\}$ y $Stab_G(H) = \{g \in G : gHg^{-1} = H\}$. a este estabilizador se le conoce como el normalizador de H en G y se le denota por $N_G(H)$. Se caracteriza por ser el mayor subgrupo de G en el que H es normal. Por tanto, $Fix(Sub(G)) = \{H \in Sub(G) : H \trianglelefteq G\}$.

Si X es finito entonces $|X| = \sum_{i=1}^n |O(x_i)|$

Considerando que Δ es un conjunto de representantes de las órbitas entonces:

$$|X| = |Fix_G(X)| + \sum_{x_i \notin Fix_G(X), x_i \in \Delta} |O(x_i)| = |Fix_G(X)| + \sum_{x_i \notin Fix_G(X), x_i \in \Delta} [G : Stab_G(x_i)]$$

Con el ejemplo anterior podemos particularizar esta fórmula cuando se usa la acción por conjugación.

Proposición 6.4 (Fórmula de las clases).

Dado un grupo G finito y $\Delta = \{g_1, \dots, g_n\}$ un conjunto de representantes de las clases de conjugación:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G), x_i \in \Delta} |Cl(x_i)| = |Z(G)| + \sum_{x_i \notin Z(G), x_i \in \Delta} [G : C_G(x_i)]$$

6.2. p-grupos

Definición 6.6 (p-grupo y p-subgrupo).

Sea p un número primo. Un grupo G se dice un p-grupo si todos sus elementos tienen orden una potencia de p . Un subgrupo H de G que es un p-grupo se dirá p-subgrupo de G .

EJEMPLO 6.3: Si $|G| = p^n$ para algún n entonces G es un p-grupo pues si $g \in G$ entonces $\text{ord}(g) | p^n$ de donde $\text{ord}(g) = p^k$ con $0 \leq k \leq n$.

El siguiente teorema es parcialmente el recíproco del teorema de Lagrange.

Teorema 6.5 (Teorema de Cauchy).

Dado un grupo finito G y p un número primo que divida al orden de G entonces $\exists a \in G$ tal que $\text{ord}(a) = p$. En particular, G contiene p-subgrupos.

Corolario 6.6.

Sea G un grupo finito.

G es un p-grupo $\iff \exists n \geq 0$ tal que $|G| = p^n$.

Teorema 6.7 (Teorema de Burnside).

Todo p-grupo G , no trivial y finito verifica que $|Z(G)| \geq p$. En particular, $Z(G)$ es no trivial.

Demostración. La estrategia es usar la fórmula de las clases $|G| = |Z(G)| + \sum_{x_i \notin Z(G), x_i \in \Delta} [G : C_G(x_i)]$ y demostrar que p divide a los dos sumandos que no son $|Z(G)|$.

Por un lado p divide a $|G|$ ya que G es un p-grupo y por tanto tiene orden p^n donde $n \geq 1$ ya que por hipótesis G no es un grupo no trivial y es finito.

Como $[G : C_G(g_i)] \mid |G|$ deducimos que $[G : C_G(g_i)] = p^{t_i}$ con $0 \leq t_i \leq n$. Nuestro objetivo es demostrar que $t_i \geq 1$ cuando $g_i \notin Z(G)$.

En efecto, como $C_G(g_i) = \{h \in G : g_i h = h g_i\}$ y si $[G : C_G(g_i)] = 1$ entonces $C_G(g_i) = G$ de donde $g_i \in Z(G)$ y llegamos a una contradicción.

En conclusión $p \mid |Z(G)|$ y como $|Z(G)| \geq 1$ entonces $|Z(G)| \geq p$. □

Corolario 6.8.

Sea p un número primo. Si G es un grupo con $|G| = p^2$ entonces G es abeliano.

Corolario 6.9 (Corolario a los teoremas de Burnside y Cauchy).

Si G es un p-grupo finito entonces es un grupo soluble.

6.3. Teoremas de Sylow

Los teoremas de Sylow son especialmente útiles para determinar los subgrupos de cierto orden guiándonos y respondiendo algunas preguntas del tipo: ¿cómo de grandes son esos subgrupos?, ¿cómo se relacionan dichos subgrupos?, ¿cuántos subgrupos hay?, ¿son normales?.

En otro sentido proveen de recíprocos del teorema de Lagrange.

Teorema 6.10 (Primer teorema de Sylow).

Sea G un grupo finito y p un número primo divisor de $|G|$. Entonces para cada potencia $p^i \mid |G|$ existe un subgrupo H tal que $|H| = p^i$.

Demostración. Lo hacemos por inducción fuerte sobre i .

Para el caso base $i = 1$ utilizamos el teorema de Cauchy y se obtiene un $a \in G$ con $\text{ord}(a) = p$ y basta tomar $H = \langle a \rangle$.

Sea $i \geq 1$ y supongamos que el resultado es cierto para j con $j < i$. Por tanto supongamos que $p^i \mid |G|$ y hagamos una segunda inducción fuerte sobre $|G|$.

Para el caso base consideremos $|G| > p^i$ y que el resultado es cierto para todo grupo cuyo orden sea menor que el de G y sea divisible por p^i . Distinguimos dos casos:

1. Si $\exists K < G$ tal que $p \nmid [G : K]$.

En este caso necesariamente $p^i \mid |K|$ y como además $|K| < G$ podemos aplicar la hipótesis de inducción fuerte para afirmar que $\exists H \leq K$ tal que $|H| = p^i$.

2. Si resulta que $\forall K \leq G$ se verifica que $p \mid [G : K]$.

En este caso usamos la fórmula de las clases para deducir que $p \mid Z(G)$. Por el teorema de Cauchy $\exists T \leq Z(G)$ tal que $|T| = p$.

Utilizando que todo subgrupo del centro es siempre un subgrupo normal de G y la hipótesis de inducción sobre i , vamos a construir un subgrupo cuyo orden es precisamente p^i .

Consideremos G/T .

Como $p^i \mid |G|$ y $|T| = p$ entonces $p^{i-1} \mid |G/T|$.

Usando la hipótesis de inducción en i , $\exists L \leq G/T$ tal que $|L| = p^{i-1}$.

Por la descripción del retículo de subgrupos del grupo cociente, sabemos que $L = H/T$ con $T \leq H$.

Por tanto, $p^{i-1} = |L| = |H|/|T|$ de donde $|H| = p^{i-1}|T| = p^i$. □

Estos p -subgrupos se encuentran incluidos en p -subgrupos de orden mayor como precisará el segundo teorema de Sylow.

Definición 6.7 (p -subgrupo de Sylow).

Sea G un grupo finito y p un número primo divisor de $|G|$. Sea p^k la máxima potencia de p que divide a $|G|$ (es decir, $|G| = p^k m$ con $p \nmid m$). Los p -subgrupos de G de orden p^k se llaman p -subgrupos de Sylow de G .

Lema 6.11.

Bajo la hipótesis del teorema siguiente.

Sea P un p -subgrupo de Sylow de G y $H \leq G$ un p -subgrupo tal que $H \leq N_G(P)$. Entonces $H \leq P$.

Demostración. Consideramos como grupo ambiente $N_G(P)$ de modo que tenemos que $P \trianglelefteq N_G(P)$ y que $H \leq N_G(P)$ así que aplicando el tercer teorema de isomorfismo $H/(P \cap H) \cong HP/P$ y por tanto $r = [H : P \cap H] = [HP : P]$.

Como P y H son p -grupos, $|P| = p^k$ y $|H| = p^t$ con $t \leq k$.

Como $r \mid |H|$ necesariamente $r = p^s$. Por otra parte como $P \leq HP \leq G$ por el ejercicio 13 de la relación 2 se verifica que $m = [G : P] = [G : HP][HP : P]$ de donde $r \mid m$. Por lo tanto habrá de ser $r = 1$ luego $HP = P$ y por tanto $H \leq P$. □

Teorema 6.12 (Segundo teorema de Sylow).

Sea G un grupo finito y p un divisor de $|G|$. Supongamos que $|G| = p^k m$ con $p \nmid m$. Sea n_p el número de p -subgrupos de Sylow de G .

1. Si $H \leq G$ es un p -subgrupo entonces $\exists P \leq G$ p -subgrupo de Sylow tal que $H \leq P$.
2. Todos los p -subgrupos de Sylow de G son conjugados.
3. $n_p | m$ y $n_p \equiv 1 \pmod{p}$ (Tercer teorema de Sylow).

Demostración. Sobre el conjunto S de los p -subgrupos de Sylow consideramos la acción por conjugación de G sobre S dada por $\lambda : G \times S \rightarrow S$ tal que $(g, P) \mapsto gPg^{-1}$. Observemos que S es no vacío por el primer teorema de Sylow y que la acción está bien definida ya que el conjugado de un p -subgrupo es un p -subgrupo.

Dado $P_1 \in S$ y sea $T = O(P_1)$ su órbita bajo la acción. Sabemos que $|T| = [G : N_G(P_1)][G : P_1] = m$ ya que $[G : P_1] = [G : N_G(P_1)][N_G(P_1) : P_1]$ y porque $[G : P_1] = |G|/|P_1|$ y se aplica la definición de p -grupo de Sylow. Por tanto concluimos que $p \nmid |T|$.

1. Sea $H \leq G$ un p -subgrupo. Podemos restringir la acción por conjugación a H y a T como $\lambda' : H \times T \rightarrow T$ tal que $(h, P) \mapsto hPh^{-1}$.

Utilizando que las órbitas para esta acción $\{O(P'_1), \dots, O(P'_r)\}$ son una partición de T se tiene que

$$|T| = \sum_{i=1}^r |O(P'_i)| = \sum_{i=1}^r [H : \text{Stab}_H(P'_i)] = \sum_{i=1}^r [H : H \cap P'_i]$$

Asumiendo esta última igualdad que luego comprobaremos, como $p \nmid |T|$ y $[H : H \cap P'_i]$ es un divisor de $|H|$ que es una potencia de p , entonces existe un i tal que $[H : H \cap P'_i] = 1$ de donde $H = H \cap P'_i$ luego $H \leq P'_i$ de modo que H pertenece a un p -subgrupo de Sylow.

Concluimos con la afirmación que dejábamos pendiente. Dado $P \in T$, $\text{Stab}_H(P) = \{h \in H : hPh^{-1} = P\} = H \cap N_G(P)$ y bastaría ver la igualdad de este conjunto con $H \cap P$.

\supseteq Como $P \trianglelefteq N_G(P)$ entonces $H \cap P \leq H \cap N_G(P)$.

\subseteq Como $H \cap N_G(P) \leq N_G(P)$ y $H \cap N_G(P) \leq H$ de lo segundo deducimos que $H \cap N_G(P)$ es un p -subgrupo de G (aplíquese el teorema de Lagrange). Y combinando este hecho con el primero obtenemos por el lema que $H \cap N_G(P) \leq P$. Combinando las inclusiones se obtiene que $H \cap N_G(P) \leq H \cap P$.

2. Sean P_1 y P_2 dos p -subgrupos de Sylow. Aplicando el apartado 1. con $T = O(P_1)$ para P_2 existirá un P' tal que $P_2 \leq P'$ y como P' está en la órbita de P_1 se deduce que $P_2 \leq gP_1g^{-1}$ y como ambos tienen el mismo orden se verifica $P_2 = gP_1g^{-1}$.

3. Por el apartado 2. tenemos que $S = T$ de donde $n_p = |S| = |T|$ y por tanto $n_p | m$.

En la fórmula $|T| = \sum_{i=1}^r [H : H \cap P'_i]$ tomemos $H = P_1$ de modo que $n_p = \sum_{i=1}^r [P_1 : P_1 \cap P'_i]$. Como los índices dividen al orden del grupo P_1 que es una potencia de p y p no divide a n_p , necesariamente existe algún índice que vale uno.

$$[P_1 : P_1 \cap P'_i] = 1 \iff P_1 = P_1 \cap P'_i = P_1 \leq P'_i \iff P_1 = P'_i.$$

De donde sólo hay un índice que vale uno y por tanto $n_p = 1 + pl$ de donde $n_p \equiv 1 \pmod{p}$. □

Corolario 6.13 (Condición de normalidad para la unicidad del p -subgrupo).

Sea G un grupo finito y P un p -subgrupo de Sylow de G . Entonces equivalen:

$$n_p = 1 \iff P \trianglelefteq G.$$

Corolario 6.14.

Sea G un grupo finito con $|G| = p_1^{r_1} \dots p_k^{r_k}$ y supongamos que $n_{p_i} = 1 \ \forall i$. Sean P_i los únicos p -subgrupos asociados. Entonces G es el producto directo interno de los P_i y $\text{Aut}(G) \cong \text{Aut}(P_1) \times \dots \times \text{Aut}(P_k)$.