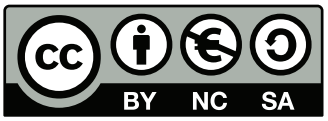
Álgebra II

LibreIM

Doble Grado de Informática y Matemáticas

Universidad de Granada

libreim.github.io/apuntesDGIIM



Álgebra II

LibreIM

Doble Grado de Informática y Matemáticas
Universidad de Granada

libreim.github.io/apuntesDGIIM

Índice

Parte I.
Teoría

1. Preliminares

1.1. El anillo de enteros módulo n

Para cada $n \geq 1$ consideramos el conjunto $\mathbb{Z}_n$, obtenido mediante el cociente $\mathbb{Z}/n\mathbb{Z}$. O lo que es lo mismo, 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:

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

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

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

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

y

$$ij = \text{res}(ij, n)$$

Proposición 1.1. $\mathbb{Z}_n$ 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 $1 = an + br$ 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:

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

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

Proposición 1.2 (Unidades de los anillos de restos módulo n). $\mathcal{U}(\mathbb{Z}_n) = \{r \in \mathbb{Z}_n : r \neq 0 \; y \; \text{mcd}(r,n) = 1\}$

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

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

Veamos que $\mathcal{U}(\mathbb{Z}_n) \subseteq A$. Si $u \in \mathcal{U}(\mathbb{Z}_n)$ 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.

□

1.2. Función phi de Euler

Definición 1.1 (Función phi de Euler). La función phi de Euler está dada por:

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

Proposición 1.3 (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

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

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

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

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

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

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

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

□

2. Grupos. Definiciones y ejemplos. Homomorfismos de grupos.

2.1. Definición de grupo y primeras propiedades

Definición 2.1 (Grupo). Un grupo es una estructura algebraica formada por un conjunto G y una operación interna $G \times G \to G$ a la que llamaremos *producto*. Esta operación asigna a cada pareja (x, y) el elemento xy y verifica las siguientes propiedades:

1. Asociativa: para todo $x, y, z \in G$, $(xy)z = x(yz)$.
2. Existencia de elemento neutro: existe en G un elemento, que notamos como 1, de tal forma que $1x = x = x1$ para todo $x \in G$.
3. Existencia de elemento simétrico: para todo $x \in G$ existe un elemento, que notamos como x^{-1}, tal que $x^{-1}x = 1 = xx^{-1}$.

Se dice que G es un grupo *conmutativo* o *abeliano* si verifica una cuarta propiedad:

4. Para todo $x, y \in G$, $xy = yx$.

Nota (Notación). Para cada $(x_1, x_2, ..., x_n) \in G^n$ definimos $\prod_{i=1}^{n} a_i = a_1 \dots a_n$ inductivamente como

$$\prod_{i=1}^{1} a_i = a_1 \quad \text{y para } n \geq 1, \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i \right) a_n .$$

Nota (Notación). Para $a_1 = a_2 = \ldots = a_n$ definimos

$$a^n = \prod_{1}^{n} a_i$$

Proposición 2.1. Un grupo G verifica las siguientes propiedades:

1. El elemento neutro es único.
2. Para cada $x \in G$ el inverso es único.
3. (Propiedad involutiva). Para cada $x \in G$, $(x^{-1})^{-1} = x$.
4. Para cualesquiera $a, b \in G$, las ecuaciones $aX = b$ y $Ya = b$ tienen solución única.
5. Si $xx = x$ entonces $x = 1$.

6. (Propiedad asociativa generalizada). Para cada $1 \leq m < n$ se verifica
$$\prod_1^n a_i = \left(\prod_1^m a_i\right)\left(\prod_{m+1}^n a_i\right).$$
7. Se cumple la siguiente igualdad
$$\left(\prod_1^n a_i\right)^{-1} = \prod_n^1 a_i^{-1} = a_n^{-1} \dots a_1^{-1}.$$
8. Se verifica que para cualesquiera $r, s \geq 1$ se tiene $a^r a^s = a^{r+s}$.
9. Para todo $n \geq 1$ se verifica que $(a^n)^{-1} = \left(a^{-1}\right)^n$ y podemos definir $a^{-n} = (a^n)^{-1} = \left(a^{-1}\right)^n$ y $a^0 = 1$.
10. (Producto de potencias de la misma base y potencia de una potencia). Para cualesquiera $r, s \in \mathbb{Z}$ se verifica $a^r a^s = a^{r+s}$ y $a^{rs} = (a^r)^s$.

Demostración.

1. Asúmase que z_1, z_2 son elementos neutros. Entonces dado un $e \in G$, $z_1 e = e = z_2 e$. De modo que $z_1 = z_2$.
2. Asúmase que i_1, i_2 son dos elementos inversos de un x. Entonces dado un $e \in G$,
$$i_1 = i_1 1 = i_1 x i_2 = 1 i_2 = i_2$$
.
3. Se tiene que $(x^{-1})^{-1}$ es el inverso de x^{-1}. También x es inverso de x^{-1}. Como el inverso es único se tiene que $(x^{-1})^{-1} = x$.

□

Proposición 2.2 (Definición sin conmutación). Sea G un conjunto no vacío con una operación interna $G \times G \to G$ que verifica:

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

Con estas condiciones 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 2.2 (Orden de un grupo). Llamamos *orden* al número de elementos de un grupo finito G y lo notamos como $|G|$.

La *tabla de Cayley* de un grupo describe cómo es su operación. Para un grupo cualquiera $G = \{x_1, x_2, \ldots, x_n\}$, es de la forma:

	x_1	$\ldots$	x_n
x_1	x_1x_1	$\ldots$	x_1x_n
$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_n	x_nx_1	$\ldots$	x_nx_n

Figura 1: Tabla de Cayley para un grupo G.

Corolario 2.1. Un grupo es abeliano si y solo si su tabla de Cayley es simétrica.

Corolario 2.2. En cada fila o columna de una tabla de Cayley aparece una única vez cada elemento del grupo.

Demostración. Basta observar que si $a \in G$, $x \mapsto ax$ es una aplicación biyectiva en G. □

2.2. Ejemplos de grupos

2.2.1. 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 dicha operación producto es conmutativa. Esto nos da ya numerosos ejemplos:

$\mathbb{Z} - \mathscr{U}(\mathbb{Z}) = \{-1, 1\}$, $\quad \mathbb{Q} - \mathbb{Q}^*$, $\quad \mathbb{R} - \mathbb{R}^*$, $\quad \mathbb{C} - \mathbb{C}^*$, $\quad \mathbb{Z}_n - \mathscr{U}(\mathbb{Z}_n)$.

Nótese que $|\mathbb{Z}_n| = n, |\mathscr{U}(\mathbb{Z}_n)| = \phi(n)$.

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

El conjunto $\mu_n = \{z \in \mathbb{C}^* : z^n = 1,\ n \geq 2\}$, llamado conjunto de las *raíces n-ésimas de la unidad*, unido con la operación producto de los números complejos, forman el grupo de nombre análogo.

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

$$\mu_n = \left\{ \xi_k = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right), \quad k = 0, 1, \ldots, n-1 \right\},$$

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

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

2.2.3. Grupo lineal general de orden n.

A partir del conjunto de las matrices orden $n \geq 2$ con coeficientes sobre un cuerpo K, $\mathscr{M}_n(K)$, y el producto usual de matrices, podemos obtener el *grupo*

lineal general de orden n, definido como

$$\mathrm{GL}_n(K) := \mathscr{U}(\mathscr{M}_n(K)) = \{A \in \mathscr{M}_n(K) : |A| \neq 0\}\,.$$

2.2.4. Grupos simétricos

Dado un conjunto no vacío X, definimos el *grupo de sus permutaciones* o *grupo simétrico*, $\mathscr{S}(X)$, como el grupo formado por el conjunto de todas las aplicaciones biyectivas de X en X y la operación de composición de funciones.

En particular, el *enésimo* grupo simétrico o grupo de permutaciones de n elementos se define como $\mathscr{S}_n = \mathscr{S}(\{1,\dots,n\})$. Es trivial comprobar que $|\mathscr{S}_n| = n!$.

Para representar un elemento $\alpha \in \mathscr{S}_n$, al que llamaremos *permutación*, utilizaremos la notación

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}.$$

El producto de dos permutaciones viene dado por su composición:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(\beta(1)) & \alpha(\beta(2)) & \dots & \alpha(\beta(n)) \end{pmatrix}.$$

Se verifica que $\mathscr{S}_n$ es conmutativo si y sólo si $n = 2$.

Definición 2.3 (Permutaciones disjuntas). Se dice que dos permutaciones $\alpha, \beta \in \mathscr{S}_n$ son *disjuntas* si *lo que mueve una lo deja fijo la otra*, esto es,

$$\alpha(x) \neq x \Rightarrow \beta(x) = x\,.$$

Proposición 2.3. 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 $\alpha(\beta(x)) = x = \beta(\alpha(x))$. □

Definición 2.4 (Ciclo). Una permutación α es un *ciclo* si:

1. Existen $x_1,\dots,x_r$ tales que $\alpha(x_1) = x_2,\dots,\alpha(x_r) = x_1$.
2. $\alpha(x) = x$ para todo $x \notin \{x_1,\dots,x_r\}$.

Denotaremos un ciclo como $\alpha = (x_1\, x_2\, \dots\, x_r)$ 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

$$\alpha = (x_1\, x_2 \dots x_r) \text{ y } \beta = (y_1\, y_2 \dots y_s)$$

son disjuntos si y solo si $\{x_1, x_2, ..., x_r\} \cap \{y_1, y_2, ..., y_s\} = \emptyset$, lo que motiva el nombre utilizado.

Teorema 2.1 (Descomposición de una permutación en producto de ciclos disjuntos). Toda permutación distinta de la identidad en $\mathcal{S}_n$ (con $n \geq 2$) puede expresarse 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 $\{x, \alpha(x), ...\alpha^n(x)\}$ 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 $\alpha_1 = (x\, \alpha(x) ... \alpha^{r-1}(x))$.

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 $\alpha_2, ..., \alpha_m$ ciclos disjuntos tales que $\alpha' = \alpha_2 ... \alpha_m$ finalmente $\alpha = \alpha_1\alpha_2 ... \alpha_m$ y los ciclos son disjuntos.

Veamos ahora la unicidad de la descomposición. Tomemos dos descomposiciones distintas $\alpha = \alpha_1\alpha_2 ... \alpha_m$ y $\beta = \beta_1\beta_2 ... \beta_{m'}$ 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 $\alpha_1 = (x\, \alpha_1(x) ...) = (x\, \alpha(x), ...)$. 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 $\beta_1 = (x\, \beta_1(x) ...) =$

$(x\ \alpha(x), ...)$. En definitiva, $\alpha = \alpha_1\alpha_2...\alpha_m = \alpha_1\beta_2...\beta_{m'}$

Ahora, para $m = 1$ necesariamente se tendrá $m' = 1$ ya que en caso contrario tendríamos $1 = \beta_2...\beta_{m'}$ 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 $\alpha = \alpha_1\alpha_2...\alpha_m = \alpha_1\beta_2...\beta_{m'}$ se deduce $\alpha_2...\alpha_m = \beta_2...\beta_{m'}$. De donde se tendrá que $m = m'$ y $\alpha_i = \beta_i$ con $i = 2, ..., m$. □

Definición 2.5 (Transposición). Una *transposición* es un ciclo de longitud dos.

Proposición 2.4 (Propiedades de los ciclos). Consideremos el grupo $\mathcal{S}_n$, con $n \geq 2$. Los ciclos sumplen las siguientes propiedades:

1. (Inverso de un ciclo). $(x_1\, x_2\, \dots\, x_r)^{-1} = (x_r\, x_{r-1}\, \dots\, x_1)$.
2. (Descomposición en transposiciones)

$$(x_1\, x_2\, \dots\, x_r) = (x_1\, x_2)(x_2\, x_3)\dots(x_{r-1}\, x_r)\,.$$

3. (Conjugado). Para todo $\alpha \in \mathcal{S}_n$,

$$\alpha(x_1\, x_2 \dots x_r)\alpha^{-1} = (\alpha(x_1)\, \alpha(x_2) \dots \alpha(x_r))\ .$$

4. El orden de un ciclo coincide con su longitud:

$$(x_1\, x_2 \dots x_r)^k \neq 1 \quad \text{si} \quad 1 \leq k < r \quad \text{y} \quad (x_1\, x_2 \dots x_r)^r = 1\,.$$

Demostración. □

Teorema 2.2 (Paridad de una permutación). Dada una permutación $\alpha \in \mathcal{S}_n$ y dos expresiones de α como producto de transposiciones, $\alpha = \tau_1 \dots \tau_r$ y $\alpha = \tau'_1 \dots \tau'_s$. Entonces $r \equiv s \mod 2$.

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 $1 = \tau_1...\tau_r$ 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 transladamos 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 $r \equiv 0(mod 2)$.

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

Definición 2.6 (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.

2.2.5. Grupos diédricos.

Para $n \geq 3$ definimos el n-ésimo *grupo diédrico* (D_n) como el grupo de movimientos del plano real $\mathbb{R}^2$ que dejan fijo el polígono regular de n lados, P_n. Formalmente,

$$D_n = \{T : \mathbb{R}^2 \to \mathbb{R}^2 : T \text{ es isometría y } T(P_n) = P_n\}.$$

La operación de este grupo 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 $0 \leq k < n$.
- $S_1, ..., S_n$ 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:

$r^n = 1 = s^2$, $\quad sr = r^{-1}s$,

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.

2.2.6. Grupo de los cuaternios.

Consideremos el conjunto de matrices invertibles de orden dos y con coeficientes complejos $Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$, donde

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{-1} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \text{i} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \text{-i} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$\text{j} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad \text{-j} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \quad \text{k} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \text{-k} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}.$$

Este conjunto, unido a la operación dada por el producto usual de matrices forman el *grupo de los cuaternios*. 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:

$$(-1)^2 = 1\,, \quad i^2 = j^2 = k^2 = -1\,, \quad ij = k\,,$$
$$(-1)\,x = x\,(-1) = -x, \quad \text{con } x = i, j, k$$

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).

2.2.7. Grupo de Klein.

Definición 2.7 (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

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

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

$$K = \langle x, y \ : x^2 = y^2 = 1, \ \ xy = yx \rangle\,.$$

2.2.8. 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:

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

Donde σ 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 $\frac{n!}{2}$.

2.3. Morfismos

Definición 2.8 (Morfismo de grupos). Sean H y G dos grupos. Definimos un *morfismo* (u *homomorfismo*) de grupos de G en H como una aplicación

$$f : G \to H$$

que verifica:

1. $f(xy) = f(x)f(y)$ para cualesquiera $x, y \in G$.
2. $f(1) = 1$.

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

Ejemplo 2.1. La aplicación signatura $s : S_n \to \mu_2$ es un morfismo de grupos.

En efecto, sean $\alpha, \beta \in S_n$ entonces por el teorema 2.2 podemos escribir $\alpha = \tau_1 ... \tau_r$ y $\beta = \tau'_1 ... \tau'_s$ de donde $s(\alpha) = (-1)^r$ y $s(\beta) = (-1)^s$. Pero entonces $\alpha\beta = \tau_1 ... \tau_r \tau'_1 ... \tau'_s$ luego $s(\alpha\beta) = (-1)^{r+s}$ de modo que $s(\alpha\beta) = s(\alpha)s(\beta)$.

Proposición 2.5. Un morfismo es isomorfismo si y solo si es biyectivo.

Proposición 2.6.

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

El principal problema a tratar en esta asignatura es la clasificación de grupos finitos. La clasificación de grupos abelianos finitos es materia del Álgebra I. Se

clasificarán los grupos abelianos no finitos hasta el orden quince. El objetivo es, dado el tamaño del grupo, saber cuántos grupos no isomorfos hay.

3. Subgrupos. Órdenes e índices.

3.1. Definición de subgrupo. Ejemplos y primeros resultados.

Definición 3.1 (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 3.1. 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 $H = \{1, r, r^2, ..., r^{n-1}\}$ y subgrupos cíclicos de orden 2: $K = \{1, s\}$ y $L = \{1, r^i s\}$. Sin embargo, el conjunto de las simetrías $\{1, s, rs, r^2 s, ..., r^{n-1}s\}$ 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 3.1 (Criterio de subgrupo). Un subconjunto H no vacío de un grupo G es un subgrupo si y sólo si se verifica que $\forall x, y \in H$ 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. □

Proposición 3.2 (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 $x^{k-r-1} = x^{-1}$. □

Proposición 3.3 (Teorema de correspondencia entre homomorfismos y subgrupos). 1.Los homomorfismos preservan los subgrupos. Si $f : G \to G'$ 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 $Ker(f) = f^{-1}(\{1\})$ y la imagen del homomorfismo f como $Im(f) = f(G)$. Claramente, el núcleo y la imagen son subgrupos de G y G' respectivamente. Además, f es monomorfismo $\iff Ker(f) = \{1\}$ y f es epimorfismo $\iff Im(f) = G'$.

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 $x \in Ker(f)$ 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 $Ker(f) = \{1\}$.

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

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

3.2. Retículo de subgrupos de un grupo.

Definición 3.2 (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 $Sub(G) = \{H : H$ es un subgrupo de G$\}$. Se verifica que $Sub(G)$ tiene estructura de retículo y está ordenado por la relación de inclusión.

Proposición 3.4 (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 $\cap_{i \in I} H_i$ es un subgrupo de G.

2. Si $H_1, H_2 \in Sub(G)$ entonces $inf\{H_1, H_2\} = H_1 \cap H_2$ y $sup\{H_1, H_2\} = \cap_{K \in Sub(G), H_i \leq K\ i=1,2} K$, 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 $1 \in \cap_{i\in I} H_i$ entonces $\cap_{i\in I} H_i$ es no vacía.

Si $H_1, H_2 \in Sub(G)$, 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 $\cap_{K\in Sub(G), H_i\leq K\, i=1,2} K$ es no vacía ya que $H_1 \leq G$ y $H_2 \leq G$. Veamos que en efecto es el supremo.

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

Ejemplo 3.2. 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 $H_1 \cup H_2 = \{1, s, rs\} \nleq D_4$

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

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

3.3. Producto de subgrupos.

Definición 3.3 (Producto de subgrupos). Sea G un grupo, X e Y subconjuntos no vacíos de G. Entonces el producto de X e Y es

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

El siguiente teorema del producto lo hemos encontrado atribuido a Ledermann:

Proposición 3.5 (Teorema del producto). 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. $\Rightarrow$ Si HK es un subgrupo de G. Entonces dados $h, k \in HK$ tendríamos que $HK \ni (h^{-1}k^{-1})^{-1} = kh$ y, por tanto, $KH \subseteq HK$. La otra inclusión se demuestra de manera análoga.
$\Leftarrow$ La unidad pertenece a HK. Dados $hk, h'k' \in HK$ el producto $hkh'k'$ podemos verlo como $h(kh')k'$ donde $kh' \in KH$, pero como $KH = HK$, existen $h'', k'' \in HK$ tales que $hkh'k' = hh''kk'' \in HK$. Para un elemento $hk \in HK$ su inverso $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Por tanto, HK es un subgrupo. □

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

Proposición 3.6. Sean H, K subgrupos de un grupo G. Entonces $H \vee K = \{h_1k_1...h_rk_r : h_i \in H, k_i \in K, r \geq 1\}$

Demostración. Llamemos productos infinitos al miembro de la derecha y denotémoslo por P.

Dados $x = \prod_{i=1}^{r} h_i k_i, y = \prod_{i=1}^{s} h_i' k_i'$ se tiene que $xy^{-1} = (\prod_{i=1}^{r} h_i k_i)(1k_s')(h_s'^{-1}k_{s-1}'^{-1})\cdots(k_2'^{-1}1) \in P$. Por tanto, P es un subgrupo de G.

Por otra parte, como $H, K \leq P$ sin más que considerar elementos de la forma $h = h\cdot 1, k = 1\cdot k$ y como si $H, K \leq L$ entonces $P \leq L$ al ser la operación producto interna, se tiene que P es ciertamente el supremo de H y K. □

3.4. Subgrupo generado por un conjunto.

Definición 3.4 (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 $< X >$ como el menor subgrupo de G que contiene a X, esto es, $< X >= \cap_{K \in Sub(G), X \subseteq K} K$.

Definición 3.5 (Conjunto generador de un grupo). Sea G un grupo y X un subconjunto no vacío de G. Si $G =< X >$ 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 $H \vee K = \cap_{T \leq G, H, K \leq T} T = \cap_{T \leq G, H \cup K \subseteq T} T =< H \cup K >$, o sea, que el supremo de dos subgrupos es el subgrupo generado por su unión.

Proposición 3.7 (Expresión del subgrupo generado como palabras). Sea X un subconjunto no vacío de un grupo G. Entonces $< X >= \{x_1^{n_1} ... x_r^{n_r} : x_i \in X, n_i \in \mathbb{Z}, r \geq 1\}$

Demostración. Para empezar demuestro que el miembro derecho es un subgrupo. Llamemos a este conjunto de la derecha el conjunto de las palabras en X y denotemoslo por T.

Si $a = x_1^{n_1} \cdots x_2^{n_r}, b = y_1^{m_1} \cdots y_s^{m_s}$ son palabras en X entonces $ab^{-1} = x_1^{n_1} \cdots x_2^{n_r} y_s^{-m_s} \cdots y_1^{-m_1}$ es una palabra en X.

Por tanto, el conjunto de las palabras en X es un subrupo de G para el producto.

Vamos a ver por doble inclusión que ambos subgrupos son iguales.

$\subseteq$) Como $X \subseteq T$, claramente, $< X > \subseteq T$ ya que $< X >$ es el más pequeño de los subgrupos que contienen a X.

$\supseteq$) Como $< X >$ es un subgrupo de G y $X \subseteq < X >$, necesariamente $T \subseteq < X >$. □

Proposición 3.8 (Subgrupo generado por un conjunto finito). Sea X un subconjunto no vacío de un grupo finito G. Entonces:

$$\langle X \rangle = \{x_1^{n_1} ... x_r^{n_r} : x_i \in X, n_i \geq 0, r \geq 1\}$$

Demostración. Llamemos palabras directas al miembro de la derecha de la igual-

dad anterior y denotémoslo por T.

Por lo anterior $T \subseteq < X >$. Ahora, como G es finito, en $\{x, x^2, \cdots\}$ existirán i, j tales que $x^i = x^j, i > j$ luego $x^{i-j} = 1$ y por tanto T contiene a los inversos de los elemntos de X. En consecuencia, se tiene la otra inclusión. □

Definición 3.6 (Subgrupo cíclico generado por un elemento). Sea G un grupo. Si $X = \{a\}$ entonces $< X >=< a >$ y lo llamaremos el subgrupo cíclico generado por a. Claramente $< a >= \{a^n : n \in \mathbb{Z}\}$ y en el caso en que G sea finito $< a >= \{a^n : n \geq 0\}$

Definición 3.7 (Grupo cíclico). Sea G un grupo. Si $X = \{a\}$ es un conjunto de generadores de G entonces $G =< a >$ y diremos que G es un grupo cíclico.

Ejemplo 3.3. 1. $\mathbb{Z} =< 1 >=< -1 >$ 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. $D_n =< r,s >$.
3. $S_n =< X >$ donde $X = \{(ij) : 1 \leq i, j \leq n\}$

3.5. Teorema de Lagrange.

Definición 3.8 (Clases laterales asociadas a un subgrupo). 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 3.9. 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 $f : H \to xH$ y $g : H \to Hx$ para cualquier $x \in G$. Existe una biyección $\lambda : G/H \to H/G$. En particular, el dominio y el codominio de estas biyecciones tienen el mismo número de elementos.

Demostración. □

Definición 3.9 (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 3.1 (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 3.1. Si G es un grupo finito y $H \leq G$ entonces el orden de H divide al orden de G.

3.6. Orden de un elemento.

Definición 3.10 (Orden de un elemento). Sea G un grupo y $a \in G$. Definimos el orden de a como $ord(a) = \begin{cases} min\{r \geq 1 : a^r = 1\} & si\ \exists r \geq 1 : a^r = 1 \\ \infty & en\ otro\ caso \end{cases}$

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

Proposición 3.10 (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 $< a >= \{1, a, ..., a^{n-1}\}$.

Por definición $< a >= \{a^r : r \in \mathbb{Z}\}$ y dividiendo r entre n tendremos $r = nq + s$ donde $0 \leq s < n$. Resulta que $a^r = a^s \in \{1, a, ..., a^{n-1}\}$. Luego hemos demostrado que $\{a^r : r \in \mathbb{Z}\} \subseteq \{1, a, ..., a^{n-1}\}$. 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 $< a >= \{a^r : r \in \mathbb{Z}\} \cong \mathbb{Z}$ mediante el isomorfismo $f : \mathbb{Z} \to < a >$ tal que $f(n) = a^n$. □

Corolario 3.2. Si G es un grupo finito entonces para cualquier $a \in G$ se verifica que $ord(a)||G|$.

Proposición 3.11 (Propiedades del orden de un elemento). Suponiendo que el orden de a es finito:
1. $a^m = 1$ con $m \geq 1 \iff ord(a)|m$

2. $ord(a^r) = \frac{ord(a)}{mcd(ord(a),r)}$
3. $< a >$ tiene $\phi(ord(a))$ generadores distintos.
En cualquier caso:
4. El orden es un invariante por isomorfismo. Esto es, si $f : G \to G'$ 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 $n|m$

$\Leftarrow$ Si $n|m$ 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 $ord(a^r)|\frac{n}{mcd(n,r)}$.

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

(3) Utilizando (2) $ord(a^r) = \frac{n}{mcd(n,r)}$ y por tanto si $mcd(n,r) = 1$ se verificará que $< a >=< a^r >$ 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 $n|ord(f(a))$ 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 $ord(f(a))|n$ y por tanto $n = ord(f(a))$.

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. □

Proposición 3.12 (Cálculo del orden de permutación). 1. Sean $\alpha, \beta \in S_n$ dos permutaciones disjuntas entonces $ord(\alpha\beta) = mcm(ord(\alpha), ord(\beta))$.
2. Dado $\alpha \in S_n$ con $\alpha \neq 1$ entonces $ord(\alpha) = mcm$(longitudes de los ciclos disjuntos en que descomponeα).

Demostración. □

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

Teorema 3.2 (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 $ord(a) = n$ entonces $G \cong (\mathbb{Z}_n, +)$ y si $ord(a) = \infty$ entonces $G \cong (\mathbb{Z}, +)$. Al grupo cíclico de orden n lo denotaremos $C_n =< x : x^n = 1 >$.
3. Si G es un grupo de orden $|G| = p$ con p un número primo entonces $G \cong C_p$.

Demostración. □

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

Teorema 3.3 (Descripción del retículo de subgrupos de un grupo cíclico). 1. Si G es grupo cíclico infinito entonces $G \cong \mathbb{Z}$ y $Sub(\mathbb{Z}) = \{n\mathbb{Z} : n \geq 0\}$ 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 $d|n$ 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 $H =< x^s >$.
4. (Identificación de subgrupos) Denotemos por $Div(n)$ a los divisores de n. La aplicación

$$f : Div(n) \to Sub(C_n)$$

tal que

$$d \mapsto < x^{n/d} >$$

es una biyección.
5. (Relación de inclusión) Sean $d_1, d_2 \in Div(n)$.

$$< a^{n/d_1} > \leq < a^{n/d_2} > \iff d_1|d_2$$

Demostración. 1. El isomorfismo es trivial. Para ver que los subgrupos de $\mathbb{Z}$ son precisamente los múltiplos de los números naturales, puede consultarse [**?**] página 58. La relación de orden es similar a la que se deducía en los retículos de ideales principales puestos en correspondencia con el retículos de enteros ordenados por divisibilidad.

2. Por la proposición sobre las propiedades del orden de un elemento, tenemos que $ord(x^{n/d}) = \frac{ord(x)}{mcd(n,n/d)} = \frac{n}{n/d} = d$. Sabíamos además que $d = ord(x^{n/d}) = |\langle x^{n/d}\rangle|$, de donde el grupo cíclico generado por $x^{n/d}$ tiene precisamente, d elementos.
3.
4.

□

4. Grupos cociente, teoremas de isomorfía y producto directo de grupos

4.1. Subgrupos normales

Definición 4.1 (Subgrupo normal). Sea N un subgrupo de un grupo G.
N es normal en G $\iff \forall a \in G. aN = Na$
en cuyo caso escribiremos $N \lhd G$.

Ejemplo 4.1.
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 $< (12) > \not\trianglelefteq S_3$.
4. El subgrupo de las rotaciones de D_3 es normal en D_3.

Proposición 4.1 (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 3.1. 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 $ah_1h_2^{-1}a^{-1} \in aHa^{-1}$. □

Teorema 4.1 (Condición de normalidad). Sea N un subgrupo de un grupo G.
$N \lhd G \iff aNa^{-1} = N \; \forall a \in G \iff aNa^{-1} \leq N \; \forall a \in G$
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 $f : N \to aN$ tal que $f(n) = an$ es biyectiva.

$\Rightarrow$ Si $N \lhd G$ 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. □

Ejemplo 4.2. 1. Si $f : G \to G'$ es un homomorfismo entonces $Ker(f) \trianglelefteq G$.

En efecto, sea $a \in G$ y $n \in Ker(f)$ entonces $ana^{-1} \in Ker(f)$ 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 2.4 $\alpha\beta\alpha^{-1} = \alpha(ij)(kl)\alpha^{-1} = \alpha(ij)\alpha^{-1}\alpha(kl)\alpha^{-1} = (\alpha(i)\alpha(j))(\alpha(k)\alpha(l)) \in K$ 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 4.2 (Condición de normalidad para subgrupos finitamente generados). Si $N =< x_1, ..., x_r > \leq G$ entonces $N \lhd G \iff ax_ia^{-1} \in N \, \forall a \in G$ con $i = 1, ...r$.

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

$\Rightarrow$ Por el criterio 4.1 $aNa^{-1} \leq N \, \forall a \in G$ de donde claramente $ax_ia^{-1} \in N \, \forall a \in G$.

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

Para empezar, si $x_i \in \{x_1, ..., x_r\}$ 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 $ax_1^{n_1}...x_r^{n_r}a^{-1} \in N$ para lo que basta introducir a y a^{-1} entre cada potencia x_i. □

Ejemplo 4.3. $A_n \trianglelefteq S_n \, \forall n \geq 2$.

Basta utilizar que A_n es el *kernel* del morfismo signatura sobre S_n

Teorema 4.2 (Extensión del teorema de correspondencia entre subgrupos y homomorfismos). Sea $f : G_1 \to G_2$ 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 4.1.

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 $f(h) \in G_2$ 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 $ghg^{-1} = f(g_1)f(h_1)f(g_1)^{-1} = f(g_1h_1g_1^{-1}) \in f(H_1)$ ya que $H_1 \trianglelefteq G_1$.

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

4.2. Grupo cociente

Definición 4.2 (Grupo cociente). Sea G un grupo y $N \lhd G$ 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 4.4. 1. Si G es abeliano entonces G/N es abeliano para cualquier subgrupo N de G.

Definición 4.3 (Proyección canónica). La aplicación $p : G \to G/N$ tal que $p(a) = aN$ es un epimorfismo llamado proyección canónica.

Proposición 4.3 (Retículo de subgrupos del grupo cociente). Sea G un grupo y $N \lhd G$ entonces se verifica:

1. Si $H \leq G$ y $N \leq H$ entonces $N \lhd H$ 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 $N \lhd G$ entonces necesariamente es normal en todo subgrupo contenido en G. Obsérvese que esto no quiere decir que la normalidad sea transitiva es decir que $H_1 \lhd H_2 \lhd H_3$ no quiere decir que $H_1 \lhd H_3$. Un buen ejemplo de esto se tiene en D_4 con $\{1, s\} \lhd \{1, s, r^2, r^2 s\} \lhd D_4$ pero $\{1, s\} \not\lhd D_4$.

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. □

4.3. Teoremas de isomorfismo

Proposición 4.4 (Teorema de factorización de un homomorfismo mediante la proyección canónica). Sea $f : G \to G'$ un homomorfismo de grupos y sea $N \trianglelefteq G$ con $N \leq Ker(f)$ entonces existe un único homomorfismo $\bar{f} : G/N \to G'$ 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 $g : G/N \to G'$ 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). $Ker(\bar{f}) = \{xN \in G/N : \bar{f}(xN) = f(x) = 1\} = Ker(f)/N$ 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. □

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 4.3 (Primer teorema de isomorfismo). Sea $f : G \to G'$ un homomorfismo de grupos entonces $G/Ker(f) \cong Img(f)$ mediante el isomorfismo $aKer(f) \mapsto f(a)$.

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

Corolario 4.1 (Fórmula de las dimensiones). Sea $f : G \to G'$ un homomorfismo con G un grupo finito entonces $|G| = |Ker(f)||Im(f)|$.

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

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

Teorema 4.4 (Segundo teorema de isomorfismo o del doble cociente). Sea G un grupo y $N \trianglelefteq G$.
Sea $H \in Sub(G)$ 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.

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

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

Claramente $H \subseteq Ker(f)$. Veamos la otra inclusión. Si $x \in Ker(f) \Rightarrow xN \in H/N$ 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 $G/H = G/Ker(f) \equiv Img(f) = (G/N)/(H/N)$. □

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 4.5 (Tercer teorema de isomorfismo). Sea G un grupo y $H, K \leq Sub(G)$ siendo $K \trianglelefteq G$. Entonces:
1. $HK = KH$ y por tanto $HK \in Sub(G)$ 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 3.5, se tiene que $HK \in Sub(G)$ y claramente $K \trianglelefteq HK$.

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

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

Además,

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

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. □

4.4. Producto directo

4.4.1. Producto directo de grupos

Definición 4.4 (Producto directo de grupos). Dados $G_1, ..., G_n$ grupos su producto directo es el conjunto:

$$G_1 \times ... \times G_n = \{(x_1, ..., x_n) : x_i \in G_i, 1 \leq i \leq n\}$$

junto con la operación producto componente a componente:

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n')$$

Lo denotaremos por $\prod_{k=1}^{n} G_k$.

Definición 4.5 (Proyecciones e inyecciones canónicas). La proyección canónica sobre la i-ésima componente es la aplicación $p_i : \prod_{k=1}^{n} G_k \to G_i$ tal que $p_i((x_1, ..., x_n)) = x_i$. Claramente, las proyecciones canónicas son epimorfismos.

La inyección canónica desde la j-ésima componente es la aplicación $u_j : G_j \to \prod_{k=1}^{n} G_k$ tal que $u_j(x) = (1, ..., x, ..., 1)$ 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 4.5. 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 4.5 (Factores del producto). Sean $G_1, ..., G_n$ grupos y $G = \prod_{k=1}^{n} G_k$.
1. $G_j \cong Img(u_j)$ 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. $\prod_{k=1, k\neq j}^{n} G_k \cong Ker(p_j)$ e identificando $\prod_{k=1, k\neq j}^{n} G_k$ con $Ker(p_j)$ 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 $Img(u_j) \cong G_j$. Considerando el homomorfismo $\phi : G \to G_1 \times ... \times G_{j-1} \times G_{j+1} \times ... \times G_n$ tal que $\phi((g_1, ..., g_n)) = (g_1, ..., g_{j-1}, g_{j+1}, ..., g_n)$ se tendrá que $Ker(\phi) = G_j$ 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 $Ker(p_j) = \{(g_1, ..., g_{j-1}, 1, g_{j+1}, ..., g_n) : g_j \in G_j \; \forall j \neq i\}$ y la aplicación $\phi : Ker(p_j) \to \prod_{k=1, k\neq j}^{n} G_k$ tal que $\phi((g_1, ..., 1, ..., g_n)) = (g_1, ..., g_n)$.

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

En resumen, tenemos que formalmente se identificará

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

y

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

4.4.2. Producto directo de homomorfismos

Definición 4.6. Sean $f_i : G_i \to H_i$ homomorfismos de grupos con $i = 1, ..., n$. El homomorfismo producto es

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

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

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 4.6 (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 $i = 1, ..., n$.
2. $\prod f_i$ es monomorfismo (respectivamente epimorfismo, isomorfismo) $\iff$ f_i es monomorfismo (respectivamente epimorfismo, isomorfismo) $\forall i = 1, ..., n$.

Consideremos ahora el monomorfismo

$$\phi : Aut(G_1) \times ... \times Aut(G_n) \to Aut(G_1 \times ... \times G_n)$$

tal que

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

.

Teorema 4.6 (Caracterización del producto directo). Sean $G_1, ..., G_n$ grupo finitos.
1. $|\prod_{i=1}^{n} G_i| = \prod_{i=1}^{n} |G_i|$.
2. $ord((x_1, ..., x_n)) = mcm(ord(x_1), ..., ord(x_n))$.
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. $\prod_{i=1}^{n} Aut(G_i) \cong Aut(\prod_{i=1}^{n} G_i)$ y el isomorfismo es ϕ.

4.4.3. Producto directo interno

Definición 4.7 (Producto directo interno). Sea G un grupo, $H, K \leq G$ y $\lambda : H \times K \to G$ tal que $\lambda((h,k)) = hk$.

G es producto directo interno de H y K si λ es un isomorfismo. Esto permite reconocer G como producto directo (externo) de dos de sus subgrupos.

Teorema 4.7 (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 $g = hk$

Generalizamos para n subgrupos.

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

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

Teorema 4.8 (Condiciones de producto directo interno). Son equivalentes:
1. ϕ es un isomorfismo.
2. $H_i \trianglelefteq G$ $\forall i = 1, ..., n$, $\prod_{i=1}^{n} H_i = G$ y $(H_1 ... H_{i-1}) \cap H_i = \{1\}$ $\forall i = 2, ..., n$.
3. $h_i h_j = h_j h_i$ $\forall h_i \in H_i$ $\forall h_j \in H_j$ $\forall i \neq j$, $G = H_1 \vee ... \vee H_n$,$(H_1 ... H_{i-1}) \cap H_i$ $\forall i = 2, ..., n$.
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 $g \in G$ $\exists! h_1 \in H_1, ..., h_n \in H_n$ tal que $g = h_1 ... h_n$.

5. Grupos solubles

5.1. Grupos simples y series normales

Definición 5.1 (Serie normal y refinamiento). Dado un grupo G, una serie normal de G es una sucesión finita de grupos de la forma

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

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 $H_i \trianglelefteq\!\!\!\!\neq H_{i+1}\, i = 0, 1, ..., n-1$. En este caso diremos que la longitud de la serie es n (esto es, G no se cuenta).

Supongamos una serie normal

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

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 5.1. 1. $\{1\} \trianglelefteq A_4 \trianglelefteq S_4$
2. $\{1\} \trianglelefteq K \trianglelefteq S_4$
3. $\{1\} \trianglelefteq K \trianglelefteq A_4 \leq S_4$ 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 5.2 (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 5.3 (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 5.2. 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 impropios.

$\Rightarrow$ 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 $< x >$ será normal en G. Como G es simple, necesariamente $G =< x >$, 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 5.1 (Condición de factores simples). Sea $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_n = G$ una serie normal.

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

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 $H_{i-1} \trianglelefteq K \trianglelefteq H_i$. 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 $H_i/H_{i-1} \neq \{1\} \implies H_{i-1} \trianglelefteq H_i$.

Supongamos ahora que $\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq ... \trianglelefteq K_m = G$ 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 $H_{r-1} \trianglelefteq K_l \trianglelefteq K_{l+1} = H_r$ de donde $K_l/H_{r-1} \trianglelefteq H_r/H_{r-1}$ y K_l/H_{r-1} es no trivial. Como H_r/H_{r-1} es simple llegamos a una contradicción. □

Ejemplo 5.3. 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 $\{0\} = t_1\mathbb{Z} \trianglelefteq ... \trianglelefteq t_{n-1}\mathbb{Z} \trianglelefteq \mathbb{Z}$, 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 5.2 (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

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

de modo que la serie

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

es una serie de composición para G. □

Ejemplo 5.4. La serie de composición del grupo no tiene por qué ser única. Así $\{1\} \trianglelefteq\!\!\!\!< < r^2 > \trianglelefteq\!\!\!\!< < r > \trianglelefteq D_4$ y si $K =< r^2, s >$ es uno de los subgrupos de Klein tenemos $\{1\} \trianglelefteq\!\!\!\!< < s > \trianglelefteq K \trianglelefteq D_4$. 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 5.4 (Series equivalentes). Dadas dos series normales de G,

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

y

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_n = G$$

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 $i = 1, ..., n$.

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.

Proposición 5.1 (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. □

Proposición 5.2 (Consecuencia del tercer teorema de isomorfía). Sea G un grupo. $A,B,C\leq G$ y $B\trianglelefteq A$. Entonces se verifica:
i) $B\cap C\trianglelefteq A\cap C$ 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 3.5 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 $B\leq A$. □

Proposición 5.3 (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 3.5 y el teorema 4.1).

Aplicamos el apartado ii) del lema 5.2 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. □

Teorema 5.3 (Lema de refinamiento de Schreier (1928)). Dos series de un grupo G admiten refinamientos equivalentes.

Demostración. Sean

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

y

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

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

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

y

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

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.

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

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

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

Cuya longitud es nm. □

Teorema 5.4 (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. □

Definición 5.5 (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 Fact(G).

5.2. Grupos solubles

Definición 5.6 (Grupo soluble). Un grupo G es soluble si tiene una serie normal:

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

cuyos factores G_i/G_{i-1} con $i = 1, ..., n$ son abelianos.

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

Ejemplo 5.5. Todo grupo abeliano es soluble ya que $\{1\} \trianglelefteq G$ es una serie normal y además $G/\{1\} = G$ es abeliano.

Teorema 5.5 (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 $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ una serie normal para G cuyos cocientes G_i/G_{i-1} son abelianos con $i = 1, ..., n$.

Por el teorema de Jordan-Hölder dicha serie admite un refinamiento que es una serie de composición $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_m = G$. 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 $G_{j-1} \trianglelefteq H_{r-1} \not\trianglelefteq H_r \trianglelefteq G_j$ 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. □

Ejemplo 5.6. S_2 es un grupo abeliano y por tanto es soluble. Se verifica que $Fact(S_2) = \{C_2\}$.
En S_3 tenemos la serie de composición $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ de donde $Fact(S_3) = \{C_2, C_3\}$ 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 $Fact(S_4) = \{C_2, C_3, C_2, C_2\}$ y por tanto S_4 es un grupo soluble.

Proposición 5.4 (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 $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ con G_i/G_{i-1} abeliano. Vamos a ver que $\{1\} = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq ... \trianglelefteq G_n \cap H = G$ 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 $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ con G_i/G_{i-1} abeliano. Entonces claramente (revisar notas) $G_iN \trianglelefteq G_{i+1}N$ y la serie $\{1\} = G_0N/N \trianglelefteq G_1N/N \trianglelefteq ... \trianglelefteq G_nN/N = G/N$ nos dirá que G/N es abeliano.

En efecto, $\frac{G_iN/N}{G_{i-1}N/N} \cong \frac{G_iN}{G_{i-1}N} \cong \frac{G_i}{G_i \cap G_{i-1}N} \cong \frac{G_i/G_{i-1}}{\frac{G_i \cap G_{i-1}N}{G_{i-1}}}$. 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 $\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_r = N$ con N_i/N_{i-1} abeliano. Como G/N es soluble existe otra serie $\{1\} = G_0/N \trianglelefteq G_1/N \trianglelefteq ... \trianglelefteq G_n/N = G/N$ con $(G_i/N)/(G_{i-1}/N) \cong G_i/G_{i-1}$ abeliano.

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

Corolario 5.1 (Solubilidad de los grupos diédricos). D_n es un grupo soluble $\forall n \geq 3$.

Demostración. Consideremos $N =< r >$. 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. □

Teorema 5.6 (Teorema de Abel). A_n es un grupo simple $\forall n \geq 5$.

Corolario 5.2 (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. □

Definición 5.7 (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

$$[G:G] := < \{[x,y] : x,y \in G\} >$$

Proposición 5.5 (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 $f : G \to A$ es un homomorfismo y A es abeliano entonces $[G,G] \leq Ker(f)$.
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 $[x,y] \in Ker(f)$.
5. $\Leftarrow$ Si $[G:G] \triangleleft N$ entonces $(xN)(yN) = (xy)N = [x,y]yxN = yxN = (yN)(xN)$.
$\Rightarrow$ Si G/N es abeliano entonces $[G:G] \leq Ker(p) = N$ donde p es la proyección canónica. □

Definición 5.8 (Derivado y serie derivada de un grupo). Dado un grupo G, el n-ésimo derivado de G es por recurrencia:
$G^0 := G$
$G^1 := [G,G]$
$G^{n+1} := [G^n, G^n]$ $n \geq 1$

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

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

llamada serie derivada del grupo G cuyos factores son abelianos.

Teorema 5.7 (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 $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ 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. $\square$

6. G-conjuntos y p-grupos

6.1. G-conjuntos

Definición 6.1 (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 $G \times X \to X$ tal que $(g,x) \mapsto g_x$ cumpliendo dos condiciones:

1. $1_x = x \ \forall x \in X$.
2. $(g_1 g_2)_x = g_{1_{g_{2_x}}} \ \forall g_1, g_2 \in X$ 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 6.1 (Representación asociada a una acción). Dar una acción de G sobre X equivale a dar un homomorfismo $G \to S(X)$.

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

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

Definición 6.2 (Núcleo de una acción, acción fiel). Definimos el núcleo de una acción como el núcleo de su homomorfismo representante ϕ esto es $Ker(\phi) = \{g \in G : \phi(g) = id_X\} = \{g \in G : g_x = x \ \forall x \in X\}$.

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

Ejemplo 6.1. 1. Dados G y X arbitrarios, la acción trivial es $G \times X \to X$ tal que $g_x = x \ \forall g \in G$ y $\forall x \in X$. La representación asociada es el homomorfismo trivial de G a $S(X)$.

2. La restricción de una acción $\phi : G \times X \to X$ a un subgrupo $H \leq G$ es también una acción $\phi' : H \times X \to X$ 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 $S_n \times X \to X$ 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 $G \times X^n \to X^n$ tal que $(\sigma, (x_1, ..., x_n)) \mapsto (x_{\sigma^{-1}(1)}, ..., x_{\sigma^{-1}(n)})$. 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 $G \times G \to G$ 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 $G \times G \to G$ 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 $X = Sub(G)$. Consideremos la acción $G \times Sub(G) \to Sub(G)$ tal que $(g,H) \mapsto gHg^{-1}$. Claramente $Ker(\phi) = \{g \in G : gH = Hg \ \forall Sub(G)\}$. Obsérvese que es una generalización de la acción por conjugación.

Teorema 6.1 (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 translación 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. □

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 $\forall x, y \in X . O(x) = O(y)$, 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 6.2 (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 translación. 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:

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

7. Clasificación de grupos abelianos finitos

Teorema 7.1 (Descomposición cíclica primaria de un grupo abeliano finito). Sea A un grupo abeliano finito con $|A| = \prod_{i=1}^{k} p_i^{r_i}$ entonces:

$$A \cong \prod_{i=1}^{k} \prod_{j=1}^{t_i} C_{p_i}^{n_{ij}}$$

donde para cada i se tiene que $n_{i1} \geq n_{i2} \geq n_{it_i} \geq 1$ y $n_{i1} + n_{i2} + \ldots + n_{it_i} = r_i$. A los $p_i^{n_{ij}}$ se les llama divisores elementales del grupo A.

Corolario 7.1. Dos grupos abelianos finitos son isomorfos si y sólo si tienen los mismos divisores elementales.

Ejemplo 7.1. Grupos de orden 360 salvo isomorfismo.

Teorema 7.2 (Descomposición cíclica de un grupo abeliano finito). Sea A un grupo abeliano finito, entonces:

$$A \cong \prod C_{d_i}$$

donde d_i son enteros positivos tales que $|A| = \prod d_i$ y $\forall j \leq i . d_i | d_j$. Además esta descomposición es única.

A los valores d_i se les llama factores invariantes del grupo A.

8. Apéndice

8.1. Clasificación de los grupos de orden menor o igual que 15

Los grupos de orden primo $p \in \{2,3,5,7,9,11,13\}$ son isomorfos a C_p.

Los grupos de orden p^2 son abelianos luego son isomorfos a C_{p^2} o $C_p \times C_p$.

En consecuencia los grupos de orden 4,9 también están clasificados.

Proposición 8.1. Sea p un primo con $p > 2$ y G un grupo con $|G| = 2p$ entonces $G \cong C_{2p}$ o $G \cong D_p$.

8.2. Producto semidirecto de grupos

Proposición 8.2 (Definición del producto semidirecto). Sean H, K dos grupos y sea $\theta : K \to Aut(H)$ un homomorfismo de grupos. Sabemos del tema 6 que este homomorfismo representa una acción $K \times H \to H$ definida por $k \star h = \theta(k)(h)$.

$H \times K$ con el producto definido como $(h_1, k_1)(h_2, k_2) = (h_1(k_1 \star h_2), k_1 k_2)$ es un grupo que llamaremos producto semidirecto de H por K relativo a θ y denotaremos por $H \rtimes_\theta K$.

Teorema 8.1 (Producto semidirecto interno). Sean $H, K \leq G$ verificando:

1. $H \trianglelefteq G$
2. $HK = G$
3. $H \cap K = \{1\}$

Sea $\theta : K \to Aut(H)$ dada por $\theta(k)(h) = khk^{-1}$ donde la operación producto es la del grupo G. Entonces:

$$H \rtimes_\theta K \cong G$$

En cuyo caso diremos que G es producto semidirecto interno de H y K.

Parte II.
Ejercicios