1ª PARTE: TEORIA DE GRUPOS

TEMA 1º: GRUPOS CICLICOS. FUNCION DE EULER

1. DEFINICION (*)

Sea G un grupo y a un elemento de G. El conjunto

$$H = \{a^\lambda / \lambda \in \mathbb{Z}\}$$

sabemos que es un subgrupo de G. Si existe un elemento a de G de modo que H, definido como anteriormente, coincida con G decimos que G es un grupo cíclico y de a decimos que es un generador de G. Esto lo representamos así:

$$G = \langle a \rangle$$

Cabe preguntarse si existen grupos cíclicos de cualquier orden. La respuesta es afirmativa.

$(\mathbb{Z}; +)$ es un grupo cíclico infinito generado por 1 (ó -1), pues

$$\mathbb{Z} = \{\lambda \cdot 1 / \lambda \in \mathbb{Z}\} \ (= \{\mu \cdot (-1) / \mu \in \mathbb{Z}\})$$

Consideremos en el grupo S_n de las permutaciones de orden n el ciclo de longitud n $\sigma = (1, 2, \ldots, n)$. El ciclo σ genera un grupo cíclico de orden n: $\langle \sigma \rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$.

2. ESTUDIO DE $(\mathbb{Z}; +)$ Y SUS SUBGRUPOS

Hemos dicho anteriormente que $(\mathbb{Z}; +)$ es un grupo cíclico infinito generado por 1 o -1. En adelante consideraremos para grupos cíclicos en $\mathbb{Z}$ generadores positivos.

2.1. PROPOSICION: Todo subgrupo S de $\mathbb{Z}$ es cíclico infinito.

Demostr.: Sea a el menor de los enteros positivos perteneciente a $S - \{0\}$. Vamos a probar que $S = \langle a \rangle = \{\lambda a / \lambda \in \mathbb{Z}\}$.

Que $\langle a \rangle \subset S$ es trivial por ser S subgrupo.

Probemos que $S \subset \langle a \rangle$

Sea $s \in S$. Dados los enteros s y a existen $k, r \in \mathbb{Z}$ tal que

$$s = ka + r, \quad 0 \leq r < a.$$

Como $s \in S$ y $a \in S$ se tiene que $r = s - ka \in S$, pues S es subgrupo de $\mathbb{Z}$. Siendo a el menor de los enteros positivos de S y r un entero positivo menor que a perteneciente a S debe ser $r = 0$. Luego $s = ka$, por

(*) Se utilizará ...

tanto $s \in \langle a \rangle$. En definitiva: $S = \langle a \rangle$.
Luego S es un grupo cíclico. Que es infinito es trivial.

2.2. PROPOSICION: La intersección de dos subgrupos de $\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$ generado por el mínimo común múltiplo de los generadores de los subgrupos. Es decir
dados $a, b \in \mathbb{Z}$, $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$ siendo $m = mcm(a,b)$.

Demostr.: $\langle a \rangle \cap \langle b \rangle$ es un subgrupo de $\mathbb{Z}$ como intersección de dos subgrupos de $\mathbb{Z}$. En virtud de la proposición anterior,

$$\exists\, m \in \mathbb{Z} \;/\; \langle m \rangle = \langle a \rangle \cap \langle b \rangle$$

Probemos que $m = mcm(a,b)$.
$m \in \langle m \rangle \Rightarrow m \in \langle a \rangle \wedge m \in \langle b \rangle$. Luego m es un múltiplo común de a y b.
Sea K un múltiplo común de a y b. Entonces:
$K \in \langle a \rangle \wedge K \in \langle b \rangle \Rightarrow K \in \langle m \rangle = \langle a \rangle \cap \langle b \rangle$
Luego K es múltiplo de m. Por tanto, m es el menor de los múltiplos comunes de a y b. csqd.

2.3. PROPOSICION: La suma de dos subgrupos de $\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$ generado por el máximo común divisor de los generadores de los subgrupos, es decir, dados $a, b \in \mathbb{Z}$
$\langle a \rangle + \langle b \rangle = \langle d \rangle$, siendo $d = mcd(a,b)$.

Demostr.: Recordemos que $\langle a \rangle + \langle b \rangle = \{ \lambda a + \mu b \;/\; \lambda, \mu \in \mathbb{Z} \}$ y que $\langle a \rangle + \langle b \rangle$ es el menor subgrupo que contiene a a y a b.
$\langle a \rangle + \langle b \rangle$, como subgrupo de $\mathbb{Z}$, está generado por un número entero δ: $\langle a \rangle + \langle b \rangle = \langle \delta \rangle$.
Probemos que $\delta = d$, siendo $d = mcd(a,b) = (a,b)$
Siendo d divisor común de a y b, $a = \lambda d$ y $b = \mu d$.
Luego $\langle a \rangle \subset \langle d \rangle$ y $\langle b \rangle \subset \langle d \rangle$ y, por tanto
$\langle \delta \rangle = \langle a \rangle + \langle b \rangle \subset \langle d \rangle$
Por otro lado, $\langle a \rangle + \langle b \rangle = \langle \delta \rangle \Rightarrow \langle a \rangle \subset \langle \delta \rangle$ y $\langle b \rangle \subset \langle \delta \rangle$, y tambien $a \in \langle \delta \rangle$ y $b \in \langle \delta \rangle$, lo cual significa que δ es un divisor común de a y b.
Siendo $d = mcd(a,b)$, se tiene que δ divide a d, o tambien $d \in \langle \delta \rangle$. Por otro modo $\langle d \rangle \subset \langle \delta \rangle$

Por tanto $\langle d \rangle = \langle \delta \rangle = \langle a \rangle + \langle b \rangle$. csqd.

2.4. PROPOSICION: IDENTIDAD DE BEZOUT

Dados dos números enteros a y b primos entre sí, es decir, con $mcd(a,b) = (a,b) = 1$, existen dos números enteros u y n tales que $ua + nb = 1$

Demostración: Siendo $(a,b) = 1$, según la proposición anterior
$\langle a \rangle + \langle b \rangle = \langle 1 \rangle = \mathbb{Z}$
Por tanto, $1 \in \langle a \rangle + \langle b \rangle$.
Luego $\exists u, n \in \mathbb{Z} \;/\; 1 = ua + nb$. csqd. (*)

3. Grupos cíclicos isomorfos. Automorfismos de un grupo cíclico.

3.1. TEOREMA: Dos grupos cíclicos del mismo orden son isomorfos.

Demostr.: • CASO INFINITO: Demostraremos que todo grupo cíclico G infinito es isomorfo a $\mathbb{Z}$, con lo cual quedará probado que todos los grupos cíclicos infinitos son isomorfos.
Sea a un generador de G. Definimos la aplicación

$$h: \mathbb{Z} \longrightarrow G, \quad \lambda \longmapsto a^\lambda$$

con el convenio $a^0 = e$, siendo e el elemento neutro de G.
h es un homomorfismo, trivialmente. Además es inyectiva, pues $a^\lambda = a^\mu \Leftrightarrow \lambda = \mu$, por definición de grupo cíclico infinito. (Alg. I, T. 8).
Además es sobre, pues todo elemento de G es una potencia entera de a. Por tanto, $\mathbb{Z} \simeq G$.
• CASO FINITO: Sean $G_1 = \langle a_1 \rangle$ y $G_2 = \langle a_2 \rangle$ dos grupos cíclicos finitos de orden n: $o(G_1) = o(G_2) = n$. Definimos la aplicación:

$$h: G_1 \longrightarrow G_2, \quad a_1 \longmapsto a_2$$

cumpliendo la condición de linealidad: $h(a_1^\lambda) = [h(a_1)]^\lambda = a_2^\lambda$
h es homomorfismo por construcción.
Además h es sobre pues $\forall y = a_2^\lambda \in G_2, \; \exists x = a_1^\lambda \in G_1 \;/\; h(x) = y$.
Siendo G_1 y G_2 conjuntos finitos del mismo orden, h es biyectiva. En definitiva, h es un isomorfismo. csqd.

3.2. TEOREMA: Dado un grupo cíclico G existen tantos automorfismos en G como generadores tenga.

Demostr.: Probamos primeramente que la imagen de un generador a de G por un automorfismo h de G es un generador de G. Habrá que probar que $G = \langle h(a) \rangle$.
Siendo $h: G \to G$, como $a \in G$ se tiene que $h(a) \in G$.
Como G es grupo $\langle h(a) \rangle \subset G$. Veamos que $G \subset \langle h(a) \rangle$.
Sea $u \in G$. Siendo h sobre, existe $v \in G$ tal que $u = h(v)$
Dado $v \in G = \langle a \rangle$, existe $\lambda \in \mathbb{Z}$ tal que $v = a^\lambda$. Entonces
$u = h(v) = h(a^\lambda) = [h(a)]^\lambda$, que prueba que $u \in \langle h(a) \rangle$.
Luego la imagen de un generador por un automorfismo es un generador.

De aquí deducimos que si $a_1, a_2, \ldots, a_n$ son generadores de un grupo cíclico G, los únicos automorfismos posibles son:

$$h_1: G \to G,\ a_1 \mapsto a_1 \quad , \quad h_2: G \to G,\ a_1 \mapsto a_2 \quad , \ldots , \quad h_n: G \to G,\ a_1 \mapsto a_n$$

Se puede pensar que el automorfismo $h': G \to G$ con $h'(a_2) = a_3$ es distinto de los anteriores, pero esto no es cierto, pues la imagen de $a_1 \in G = \langle a_2 \rangle$ es un generador de G, es decir, $h'(a_1) \in \{a_1, a_2, \ldots, a_n\}$ con lo cual h' coincide con uno de los anteriores. Por tanto, hay como máximo n automorfismos.
Veamos que $h_1, h_2, \ldots, h_n$ son automorfismos, con lo cual quedará probado el teorema. Como sabemos h_i se define así:

$$h_i: G \to G,\quad a_1 \mapsto a_i,\quad a_1^\lambda \mapsto h_i(a_1^\lambda) = [h_i(a_1)]^\lambda = a_i^\lambda$$

Se prueba fácilmente, con esta definición, que h_i es un automorfismo. c.s.q.d.

3.3. PROPOSICION: a) Todo subgrupo de un grupo cíclico es cíclico.
b) La imagen homomorfa de un grupo cíclico es cíclico. En particular todo grupo cociente de un grupo cíclico es cíclico.

Demostr.: a) Sea $G = \langle a \rangle$ un grupo cíclico. Definimos la aplicación

$$h: \mathbb{Z} \twoheadrightarrow G,\quad \lambda \mapsto a^\lambda$$

h es, trivialmente, homomorfismo y sobre (la flecha $\twoheadrightarrow$ indica que es suprayectiva).
Sea S un subgrupo de 6. Siendo h homomorfismo, $h^{-1}(S)$ es subgrupo de $\mathbb{Z}$. Como todo subgrupo de $\mathbb{Z}$ es cíclico, existe $d \in \mathbb{Z}$ tal que $h^{-1}(S) = \langle d \rangle$
Siendo h sobre, $S = h(h^{-1}(S)) = h(\langle d \rangle) =$
$= h(\{\lambda d / \lambda \in \mathbb{Z}\}) = \{h(\lambda d) / \lambda \in \mathbb{Z}\} = \{a^{\lambda d} / \lambda \in \mathbb{Z}\} = \langle a^d \rangle$
que prueba que S es un subgrupo cíclico.

b) Sea $6 = \langle a \rangle$ un grupo cíclico, 6' un grupo y $h: 6 \longrightarrow 6'$ un homomorfismo. Probemos que h(6) es un grupo cíclico. h(6) es grupo pues h es homomorfismo.
Probemos que $h(6) = \langle h(a) \rangle$
$\forall x \in \langle h(a) \rangle, \exists \lambda \in \mathbb{Z} / x = [h(a)]^\lambda = h(a^\lambda)$
Dado $\lambda \in \mathbb{Z}$, $a^\lambda \in 6$, luego $h(a^\lambda) = x \in h(6)$ y también $\langle h(a) \rangle \subset h(6)$. Probemos que $h(6) \subset \langle h(a) \rangle$.
$\forall x \in 6, \exists \lambda \in \mathbb{Z} / x = a^\lambda$, luego $h(x) = h(a^\lambda) = [h(a)]^\lambda \in \langle h(a) \rangle$.
Luego, h(6) es cíclico.
En particular, dado un subgrupo H de un grupo cíclico 6 podemos considerar el grupo cociente 6/H (no se ha exigido a H que sea subgrupo normal para que tenga sentido considerar 6/H pues, siendo todo grupo cíclico abeliano, H es ya normal).
El homomorfismo canónico $p: 6 \longrightarrow 6/H$ es sobre. Entonces según lo anterior $6/H = p(6)$ es cíclico. csqd.

4. Generadores de un grupo cíclico.

* CASO INFINITO: Si 6 es un grupo cíclico infinito es isomorfo a $\mathbb{Z}$. Sea φ_6 este isomorfismo. Como los generadores de $\mathbb{Z}$ son 1 y -1, los generadores de un grupo cíclico infinito 6 son dos, $\varphi_6(1)$ y $\varphi_6(-1)$.

* CASO FINITO:

4.1. TEOREMA: Sea $6 = \langle a \rangle$ un grupo cíclico finito de orden N, $|6| = o(6) = N$. Entonces:
a) El subgrupo $\langle a^k \rangle$ con $k < N$ coincide con $\langle a^d \rangle$, siendo $d = mcd(k, N)$
b) $\langle a^k \rangle = 6$ si y solo si $mcd(k, N) = 1$, es decir si k y N son primos entre sí.

Demostr.: a) Como d divide a k, $\langle a^k \rangle \subset \langle a^d \rangle$. Pues
$k = pd \Rightarrow \forall a^{\lambda k} \in \langle a^k \rangle, a^{\lambda k} = a^{\lambda p d} \in \langle a^d \rangle$.

Además, siendo $d = mcd(K,N)$, según Proposición 2.3, $\langle d \rangle = \langle K \rangle + \langle N \rangle$. Luego $\exists \lambda, \mu \in \mathbb{Z} / d = \lambda K + \mu N$.
Entonces $a^d = a^{\lambda K + \mu N} = a^{\lambda K} \cdot a^{\mu N} = a^{\lambda K}$, pues $a^N = e$.
Luego $a^d \in \langle a^K \rangle$ y por tanto $\langle a^d \rangle \subset \langle a^K \rangle$.
En definitiva $\langle a^d \rangle = \langle a^K \rangle$.

b) $\overset{N}{\Rightarrow}$ Supongamos que $d = mcd(K,N) > 1$.
Entonces, si $N = du$, como $\langle a^d \rangle = \{e, a^d, a^{2d}, \dots, a^{(n-1)d}\}$ (*) se tendría que, por ejemplo, $a^{d-1} \notin \langle a^d \rangle$. Como $\langle a^d \rangle = \langle a^K \rangle$ y $a^{d-1} \in G$, se contradice la hipótesis de que $G = \langle a^K \rangle$.
Debe ser entonces $d = (K,N) = 1$.
$\overset{S}{\Leftarrow}$ Si $(K,N) = 1$, $\langle a^K \rangle = \langle a^1 \rangle = G$. c.s.q.d.

4.2. COROLARIO: Sea G un grupo cíclico de orden N. Para cada divisor d de N existe un único subgrupo de orden d.

Demostr.: Si d divide a N, existe $u \in \mathbb{Z}$ tal que $N = d \cdot u$
Entonces $o(a^u) = d$, pues d es el menor natural tal que $(a^u)^d = a^N = e$, y por tanto $o(\langle a^u \rangle) = d$. Luego, existe al menos un subgrupo de G de orden d. Veamos que es único.
Supongamos que K es otro subgrupo de G de orden d.
Según proposición 3.3, K es cíclico. Luego $\exists r \in \mathbb{Z} / K = \langle a^r \rangle$.
Sea $s = mcd(r,N)$. Entonces $K = \langle a^s \rangle$.
Como $s | N$, $\exists t \in \mathbb{Z} / N = s \cdot t$. Entonces $o(\langle a^s \rangle) = t$ y también $o(K) = t$. Luego $t = d$.
Siendo $(N = du = st) \wedge (t = d) \Rightarrow (s = u)$
Luego $K = \langle a^r \rangle = \langle a^s \rangle = \langle a^u \rangle$. c.s.q.d.

5. Anillos $\mathbb{Z}_n$: Clases residuales módulo n.

Decimos que dos números enteros a y b son congruentes módulo n cuando al efectuar las divisiones euclídeas de a y b por n dan el mismo resto. La congruencia de números enteros módulo n es una relación de equivalencia y divide a $\mathbb{Z}$ en clases de equivalencia llamadas clases residuales módulo n. El conjunto cociente lo denotamos por $\mathbb{Z}_n$. Los elementos de $\mathbb{Z}_n$ los denotamos por letras con una raya encima. Cada elemento de $\mathbb{Z}_n$ es una clase

(*) Recordar de Alg I que si G es un grupo y $a \in G$, con $o(a) = d$, el grupo

residual módulo n, que son de la siguiente forma:
dado $K \in \mathbb{Z}$, $\overline{K} = \{K + \lambda n / \lambda \in \mathbb{Z}\} = K + \langle n \rangle$
Luego $\mathbb{Z}_n = \{\overline{0} = \langle n \rangle, \overline{1} = 1 + \langle n \rangle, \overline{2} = 2 + \langle n \rangle, \ldots, \overline{(n-1)} = (n-1) + \langle n \rangle\}$
Si recordamos que la relación de equivalencia R inducida por el ideal $\langle n \rangle$ en $\mathbb{Z}$ se define $x R y \Leftrightarrow x - y \in \langle n \rangle$, tenemos que $\mathbb{Z}_n$ es, precisamente, el anillo cociente $\mathbb{Z}/\langle n \rangle$.
La adición y el producto vienen definidos en el anillo cociente como sigue:
$$\overline{u} + \overline{v} = \overline{u+v} \quad , \quad \overline{u} \cdot \overline{v} = \overline{uv}$$
Denotaremos por $\mathbb{Z}_n^*$ el conjunto de las unidades de $\mathbb{Z}_n$; recordemos que $\overline{u} \in \mathbb{Z}_n^*$ sii $\exists \overline{v} \in \mathbb{Z}_n / \overline{u} \cdot \overline{v} = \overline{1}$.
$\mathbb{Z}_n^*$ es un grupo multiplicativo.
En adelante tomaremos como representante canónico de una clase residual módulo n al entero positivo y menor que n de dicha clase.

5.1. PROPOSICION: Un elemento $\overline{u}$ de $\mathbb{Z}_n$ es una unidad si y solo si u y n son primos entre sí, siendo $u \in \overline{u}$ y $0 < u < n$, es decir:
$$\overline{u} \in \mathbb{Z}_n^* \iff (u, n) = 1.$$

Demostr.: $\Rightarrow$| Si $\overline{u} \in \mathbb{Z}_n^*$, $\exists \overline{v} \in \mathbb{Z}_n / \overline{u} \cdot \overline{v} = \overline{1}$
O también, como $\overline{u} \cdot \overline{v} = \overline{uv}$, $uv \equiv 1 \pmod{n}$.
Luego $uv = 1 + Kn$, con $K \in \mathbb{Z}$.
De aquí deducimos que u y n deben ser primos, pues si existe $p \in \mathbb{Z}$ tal que $p \mid u$ y $p \mid n$ se tiene que $p \mid (uv - Kn)$ y, por tanto, $p \mid 1$. Luego $(u, n) = 1$
$\Leftarrow$| Si $(u, n) = 1$, por la identidad de Bezout, existen $r, s \in \mathbb{Z}$ tales que $ru + sn = 1$. Luego $ru = 1 - sn$, y también $ru \equiv 1 \pmod{n}$, o lo que es lo mismo, $\overline{r}\,\overline{u} = \overline{1}$, que prueba que $\overline{u} \in \mathbb{Z}_n^*$. cqfd.

6. FUNCION DE EULER

DEFINICION: La función de Euler es una aplicación $\varphi: \mathbb{N} \longrightarrow \mathbb{N}$ que asocia a cada natural n el cardinal del conjunto de naturales distintos de cero, primos con n y menores que n.
Es decir,
$$\varphi: \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \longmapsto \varphi(n) = \operatorname{card}\left(\{x \in \mathbb{N}^* / x < n \wedge (x, n) = 1\}\right)$$
siendo $\mathbb{N}^* = \mathbb{N} - \{0\}$.

De la proposición 5.1. se deduce que $\varphi(n)$ es el orden del grupo $\mathbb{Z}_n^*$, es decir: $\varphi(n) = o(\mathbb{Z}_n^*)$.

* CALCULO DE $\varphi(n)$:

a) CASO EN QUE $n = p^\alpha$, con p primo y $\alpha > 0$; téngase en cuenta que si $\alpha = 0$, $n = p^0 = 1$ y $\varphi(1) = 1$.

Los números que no son primos con p^α son los múltiplos de p, es decir, los números no primos con p^α y menores que él son los números de la forma kp con $k \in \{1, 2, 3, \dots, p^{\alpha-1}\}$. Los restantes naturales comprendidos entre 1 y p^α -distintos de kp con $k \in \{1, \dots, p^{\alpha-1}\}$- son primos con p^α y menores que él. Como hay $n = p^\alpha$ naturales y, de ellos, $p^{\alpha-1}$ naturales no son primos con n, tenemos que

$$\varphi(n) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p}\right).$$

b) CASO GENERAL: Sea $n \in \mathbb{N}$ y $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ su descomposición en factores primos. Probaremos que

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \cdots \varphi(p_n^{\alpha_n}) \qquad (I)$$

con lo cual, según lo anterior, tenemos que $\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) =$

$= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_1}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$, y en definitiva

$$\boxed{\varphi(n) = n \cdot \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)}$$

Para demostrar (I), probaremos que si m y n son enteros positivos con $(m, n) = 1$, entonces $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ y de aquí (I) se obtiene por recurrencia.

Sabemos que $\varphi(n) = o(\mathbb{Z}_n^*)$. Se trata de probar, entonces, que $o(\mathbb{Z}_{mn}^*) = o(\mathbb{Z}_m^*) \times o(\mathbb{Z}_n^*)$

Dados los anillos $\mathbb{Z}_m$ y $\mathbb{Z}_n$, podemos considerar el anillo producto $\mathbb{Z}_m \times \mathbb{Z}_n$. Probemos entonces el siguiente

6.1. Lema: Si m y n son primos entre sí, $\mathbb{Z}_{mn}$ y $\mathbb{Z}_m \times \mathbb{Z}_n$ son anillos isomorfos, es decir

si $(m, n) = 1$, $\quad \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

Demostr.: Denotaremos por $\overline{\lambda}_m$ y $\overline{\lambda}_n$ las clases residuales módulos m y n, respectivamente, de representante el entero λ.

Definimos la aplicación:

$$\theta: \mathbb{Z} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$
$$\lambda \longmapsto (\overline{\lambda}_m, \overline{\lambda}_n)$$

Veamos que θ es un homomorfismo de anillos:

- $\theta(\lambda+\mu) = (\overline{(\lambda+\mu)_m}, \overline{(\lambda+\mu)_n}) = (\bar{\lambda}_m + \bar{\mu}_m, \bar{\lambda}_n + \bar{\mu}_n) =$
$= (\bar{\lambda}_m, \bar{\lambda}_n) + (\bar{\mu}_m, \bar{\mu}_n) = \theta(\lambda) + \theta(\mu)$

- $\theta(\lambda\mu) = (\overline{(\lambda\mu)_m}, \overline{(\lambda\mu)_n}) = (\bar{\lambda}_m \bar{\mu}_m, \bar{\lambda}_n \bar{\mu}_n) =$
$= (\bar{\lambda}_m, \bar{\lambda}_n) \cdot (\bar{\mu}_m, \bar{\mu}_n) = \theta(\lambda) \cdot \theta(\mu)$.

Veamos ahora cual es $\operatorname{Ker}\theta$:

$[\lambda \in \operatorname{Ker}\theta] \Leftrightarrow [\theta(\lambda) = (\bar{0}_m, \bar{0}_n)] \Leftrightarrow [\lambda \equiv 0 (\operatorname{mod} m) \wedge \lambda \equiv 0 (\operatorname{mod} n)]$

Esto último equivale a que λ sea múltiplo común de m y n. Siendo m y n primos entre sí, sabemos que λ es múltiplo común de m y n si y solo si λ es múltiplo de mn. En definitiva, $\lambda \in \operatorname{Ker}\theta$ si y solo si λ es múltipo de mn, es decir: $\lambda \in \operatorname{Ker}\theta \Leftrightarrow \lambda \in \langle mn \rangle$. Luego $\operatorname{Ker}\theta = \langle mn \rangle$.

En virtud del primer teorema de isomorfía de anillos

$$\theta(\mathbb{Z}) \simeq \mathbb{Z}/\operatorname{Ker}\theta.$$

Luego $\theta(\mathbb{Z}) \simeq \mathbb{Z}/\langle mn \rangle = \mathbb{Z}_{mn}$ (II)

Por tanto, $\operatorname{card}(\theta(\mathbb{Z})) = \operatorname{card}(\mathbb{Z}_{mn}) = m \times n$

Como $o(\mathbb{Z}_m \times \mathbb{Z}_n) = o(\mathbb{Z}_m) \times o(\mathbb{Z}_n) = m \times n$, se tiene que $\operatorname{card}(\theta(\mathbb{Z})) = \operatorname{card}(\mathbb{Z}_m \times \mathbb{Z}_n)$. Luego $\theta(\mathbb{Z}) = \mathbb{Z}_m \times \mathbb{Z}_n$ (III)

En definitiva, según (II) y (III):

$$\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}. \quad \text{csqd.}$$

Sea φ el isomorfismo entre $\mathbb{Z}_{mn}$ y $\mathbb{Z}_m \times \mathbb{Z}_n$. Dicho isomorfismo conserva las propiedades de los anillos; luego:

$$(\mathbb{Z}_m \times \mathbb{Z}_n)^* = \varphi(\mathbb{Z}_{mn}^*) \quad \text{(IV)}$$

Veamos ahora que $(\mathbb{Z}_m \times \mathbb{Z}_n)^* = \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ (V)

$(\bar{u}, \bar{v}) \in (\mathbb{Z}_m \times \mathbb{Z}_n)^* \Leftrightarrow \exists (\bar{u}', \bar{v}') \in \mathbb{Z}_m \times \mathbb{Z}_n / (\bar{u}, \bar{v}) \cdot (\bar{u}', \bar{v}') = (\bar{u}\cdot\bar{u}', \bar{v}\cdot\bar{v}') = (\bar{1}_m, \bar{1}_n)$

$\Leftrightarrow [\exists \bar{u}' \in \mathbb{Z}_m / \bar{u}\cdot\bar{u}' = \bar{1}_m] \wedge [\exists \bar{v}' \in \mathbb{Z}_n / \bar{v}\cdot\bar{v}' = \bar{1}_n] \Leftrightarrow$

$\Leftrightarrow \bar{u} \in \mathbb{Z}_m^* \wedge \bar{v} \in \mathbb{Z}_n^* \Leftrightarrow (\bar{u}, \bar{v}) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

Según (IV) y (V), $\varphi(\mathbb{Z}_{mn}^*) = \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

Siendo φ isomorfismo, $o(\mathbb{Z}_{mn}^*) = o(\varphi(\mathbb{Z}_{mn}^*))$

Luego: $o(\mathbb{Z}_{mn}^*) = o(\mathbb{Z}_m^* \times \mathbb{Z}_n^*) = o(\mathbb{Z}_m^*) \times o(\mathbb{Z}_n^*)$

O bien: $\varphi(m \times n) = \varphi(m) \times \varphi(n)$, como queríamos probar.

Por recurrencia se prueba que $\varphi(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = \prod_{i=1}^{r} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$

siendo $p_1, \ldots, p_r$ números primos.

TEMA 2º: OPERACION DE UN GRUPO EN UN CONJUNTO

1. DEFINICIONES. EJEMPLOS.

DEFINICION: Sea $\mathcal{G}$ un grupo y E un conjunto. Decimos que $\mathcal{G}$ opera en E si existe una aplicación

$$\cdot : \mathcal{G} \times E \longrightarrow E$$
$$(\alpha, a) \longmapsto \alpha \cdot a$$

que verifica las propiedades:

P.1) Asociatividad mixta: $\forall \alpha, \beta \in \mathcal{G}, \forall a \in E, (\alpha\beta)\cdot a = \alpha \cdot (\beta \cdot a)$.

P.2) Si ε es el elemento neutro de $\mathcal{G}$, $\varepsilon \cdot a = a$, $\forall a \in E$.

1.1. TEOREMA: Es condición necesaria y suficiente para que un grupo $\mathcal{G}$ opere en un conjunto E que exista un homomorfismo entre $\mathcal{G}$ y el conjunto $\mathcal{J}(E)$ de las biyecciones de E.

Demostr.: $\Rightarrow$ Supongamos que $\mathcal{G}$ opera en E. Definimos la aplicación

$$\phi : \mathcal{G} \longrightarrow \mathcal{J}(E)$$
$$\alpha \longmapsto \phi(\alpha) = f_\alpha$$

siendo $f_\alpha : E \longrightarrow E$, $a \longmapsto \alpha \cdot a$

Que f_α es aplicación es trivial. f_α es inyectiva, pues si $\alpha \cdot a = \alpha \cdot b \Rightarrow \alpha^{-1}\cdot(\alpha \cdot a) = \alpha^{-1}\cdot(\alpha \cdot b) \Rightarrow (\alpha^{-1}\alpha)\cdot a = (\alpha^{-1}\alpha)\cdot b \Rightarrow$
$\Rightarrow \varepsilon \cdot a = \varepsilon \cdot b \Rightarrow a = b$.

Además es sobre, pues dado $b \in E$, $\exists\, a = \alpha^{-1}\cdot b \in E$ / $f_\alpha(a) = \alpha(\alpha^{-1}b) = b$.

Luego, efectivamente, $f_\alpha \in \mathcal{J}(E)$, $\forall \alpha \in \mathcal{G}$.

Además ϕ es homomorfismo, pues

$\forall \alpha, \beta \in \mathcal{G}$, $\phi(\alpha\beta) = f_{\alpha\beta} = f_\alpha \circ f_\beta = \phi(\alpha) \circ \phi(\beta)$.

$\Leftarrow$ Sea $\phi : \mathcal{G} \longrightarrow \mathcal{J}(E)$, $\alpha \longmapsto f_\alpha$ el homomorfismo de $\mathcal{G}$ en $\mathcal{J}(E)$.

Queremos que $\mathcal{G}$ opere en E. Para ello definimos:

$$\cdot : \mathcal{G} \times E \longrightarrow E$$
$$(\alpha, a) \longmapsto \alpha \cdot a = f_\alpha(a)$$

Que $\cdot$ es aplicación es trivial. Veamos que verifica P.1) y P.2)

P.1.) $(\alpha\beta)\cdot a = f_{\alpha\beta}(a) = (f_\alpha \circ f_\beta)(a) = f_\alpha[f_\beta(a)] = \alpha \cdot (\beta \cdot a)$

P.2.) $\varepsilon \cdot a = f_\varepsilon(a) = (f_{\alpha^{-1}} \circ f_\alpha)(a) = (f_{\alpha^{-1}} \circ f_\alpha)(a) = 1_E(a) = a$

Se prueba fácilmente que $f_{\alpha^{-1}} = f_\alpha^{-1}$.

DEFINICION: Dado un elemento a de un conjunto E sobre el que opera un grupo $\mathcal{G}$ definimos la órbita o trayectoria de a como el conjunto $O_a = \{\alpha \cdot a / \alpha \in \mathcal{G}\}$.
La órbita de un elemento de E es un subconjunto de E.

DEFINICION: Sea $\mathcal{G}$ un grupo que opera en un conjunto E. Definimos el estabilizador de un elemento $a \in E$ como el conjunto
$$\Sigma_a = \{\alpha \in \mathcal{G} / \alpha \cdot a = a\}$$
El estabilizador de un elemento de E es un subconjunto de $\mathcal{G}$.

1.1. TEOREMA: a) El estabilizador de un elemento de un conjunto E en el que opera un grupo $\mathcal{G}$ es un subgrupo de $\mathcal{G}$.
b) El índice de Σ_a coincide con el cardinal de la órbita de a.
c) Si $\mathcal{G}$ es de orden finito, entonces $\text{card}(O_a)$ divide al orden del grupo $\mathcal{G}$.

Demostr.: a) Sea $a \in E$. Entonces $\Sigma_a \neq \emptyset$, pues el neutro ϵ de $\mathcal{G}$ pertenece a Σ_a.
Ademas $\forall \alpha, \beta \in \Sigma_a$, $\alpha \cdot \beta \in \Sigma_a$, pues $(\alpha\beta)\cdot a = \alpha \cdot (\beta \cdot a) = \alpha \cdot a = a$.
y tambien, $\forall \alpha \in \Sigma_a$, $\alpha^{-1} \in \Sigma_a$, pues $\alpha \cdot a = a \Rightarrow \alpha^{-1} \cdot (\alpha \cdot a) = \alpha^{-1} \cdot a \Rightarrow$
$\Rightarrow (\alpha^{-1}\alpha)\cdot a = \alpha^{-1} \cdot a \Rightarrow a = \alpha^{-1} \cdot a$.
Luego Σ_a es subgrupo de $\mathcal{G}$.
b) La igualdad $\alpha_1 \cdot a = \alpha \cdot a$ equivale, trivialmente, a que $\alpha^{-1} \cdot (\alpha_1 \cdot a) = a$ y tambien $(\alpha^{-1}\alpha_1)\cdot a = a$.
Luego $\alpha^{-1}\alpha_1 \in \Sigma_a$ y por tanto, $\alpha_1 \in \alpha\,\Sigma_a$
Es decir, α_1 está en la misma clase a la izquierda que α en la descomposición de $\mathcal{G}$ en clases a la izquierda relativas al subgrupo Σ_a. En conclusión, podemos enunciar que la trayectoria O_a de un elemento a de E se corresponde biyectivamente al conjunto de las clases a la izquierda de $\mathcal{G}$ relativas al estabilizador Σ_a de a. En consecuencia, el índice de Σ_a, que como sabemos es el cardinal del conjunto cociente de clases a la izquierda $\mathcal{G}/\Sigma_a$, coincide con el cardinal de O_a. Es decir: $i(\Sigma_a) = \text{card}(O_a)$.
c) En virtud del teorema de Lagrange, $o(\mathcal{G}) = o(\Sigma_a)\, i(\Sigma_a)$
Siendo $i(\Sigma_a) = \text{card}(O_a)$, queda probado que $\text{card}(O_a)$ divide a $o(\mathcal{G})$. c.s.q.d.

* Podemos definir en E una relación de equivalencia $\mathcal{R}$ del siguiente modo: $a \mathcal{R} b \iff b \in O_a$.
Se ve claramente que las clases de equivalencia son las órbitas. A estas clases se les llama clases de transitividad. En consecuencia E admite una partición por órbitas.

DEFINICION: Una operación de un grupo en un conjunto E se dice que es transitiva cuando
$$\forall a \in E,\ O_a = E.$$
Es decir, existe en E una única clase de transitividad
La definición anterior equivale a pedir que
$$\forall a, b \in E,\ \exists \alpha \in \mathbb{Z} / \alpha \cdot a = b$$

* EJEMPLOS DE GRUPOS OPERANDO EN UN CONJUNTO:

Ejemplo 1º: Sea G un grupo. Entonces G opera en sí mismo por traslaciones a la izquierda. Siendo $\cdot$ la ley de G definimos:
$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (a, x) &\longmapsto a \cdot x \end{aligned}$$
Que G opera en G es trivial, pues la ley de G verifica la propiedad asociativa y existe en G elemento neutro. Tenemos entonces el homomorfismo correspondiente:
$$\begin{aligned} \Phi : G &\longrightarrow \mathcal{J}(G) \\ a &\longmapsto \gamma_a \end{aligned}$$
donde γ_a, como sabemos, se define como sigue:
$$\begin{aligned} \gamma_a : G &\longrightarrow G \\ x &\longmapsto \gamma_a(x) = ax \end{aligned}$$
Fácilmente se comprueba que Φ es inyectiva ($\gamma_a = \gamma_b, \forall x \in G, \gamma_a(x) = \gamma_b(x)$; en particular, $\gamma_a(\varepsilon) = \gamma_b(\varepsilon)$, o bien $a = b$). Por tanto $G \simeq \Phi(G)$, es decir, G es isomorfo al grupo de las traslaciones a la izquierda.
Como consecuencia de esto obtenemos el siguiente:

1.2. TEOREMA: (DE CAYLEY)
Todo grupo finito G de orden n es isomorfo a un subgrupo del grupo S_n de las permutaciones de n elementos.

Demostr.: Siendo G un grupo finito de orden n, $\mathcal{J}(G)$ es isomorfo a S_n. Según lo dicho anteriormente, G es isomorfo a $\Phi(G)$, y $\Phi(G)$, como subgrupo de $\mathcal{J}(G)$, es isomorfo a un subgrupo de S_n. Luego G es isomorfo a un subgrupo de S_n, c.s.q.d.

El teorema de Cayley permite extender las propiedades de los subgrupos de S_n a los grupos finitos de orden n.

DEFINICION: Dado un subconjunto S de un grupo G, definimos el normalizador de S como el conjunto

$$N_S = \{g \in G / gSg^{-1} = S\}$$

Fácilmente se prueba que N_S es subgrupo de G. Además, evidentemente, si S es subgrupo, S es normal en N_S, y N_S es el mayor subgrupo de G en el cual S es normal.

DEFINICION: Sea G un grupo. Definimos el centro de G como

$$Z(G) = \{g \in G / gx = xg, \forall x \in G\}$$

$Z(G)$ es subgrupo normal de G. Esto lo representamos así: $Z(G) \triangleleft G$.

1.3. PROPOSICION: Si el grupo cociente $G/Z(G)$ es cíclico, entonces G es abeliano.

Demostr.: Los elementos de $G/Z(G)$ son de la forma $a \cdot Z(G)$, $a \in G$. Si $G/Z(G)$ es cíclico, existe $a \in G$ tal que $G/Z(G) = \langle a \cdot Z(G) \rangle$. Sean, entonces, $x_1, x_2 \in G$. Las clases de $G/Z(G)$ constituyen una partición de G. Luego, x_1 y x_2 son elementos de unas clases de $G/Z(G)$. Por tanto, $\exists K_1, K_2 \in \mathbb{Z} / x_1 \in (a\,Z(G))^{K_1} \wedge x_2 \in (a \cdot Z(G))^{K_2}$

Pero $(a \cdot Z(G))^{K_1} = a^{K_1} \cdot Z(G)$. Luego:

$x_1 \in a^{K_1} \cdot Z(G)$ y $x_2 \in a^{K_2} \cdot Z(G)$.

Entonces, $\exists c_1, c_2 \in Z(G) / x_1 = a^{K_1} \cdot c_1 \wedge x_2 = a^{K_2} \cdot c_2$

Entonces, $x_1 x_2 = a^{K_1} c_1 \cdot a^{K_2} \cdot c_2 = a^{K_1} a^{K_2} c_1 c_2 = a^{K_1+K_2} c_1 c_2 =$

$= a^{K_2+K_1} c_2 c_1 = a^{K_2} a^{K_1} c_2 c_1 = a^{K_2} c_2 a^{K_1} c_1 = x_2 \cdot x_1$, y esto cualesquiera que sean $x_1, x_2 \in G$. Luego G es abeliano y, por tanto, $G = Z(G)$. c.s.q.d.

1.4. COROLARIO: El índice del centro de un grupo G no puede ser un número primo distinto de 1.

Demostr.: Supongamos que $i(Z(G)) = p$, siendo p primo.

– Veamos que todo grupo finito de orden primo es cíclico: Sea G un grupo de orden primo p; sea $a \in G - \{e\}$. El orden de un elemento siempre es divisor de $o(G)$, pues $o(a) = o(\langle a \rangle)$ y $\langle a \rangle$ es subgrupo de G. Si $o(a) \mid o(G)$, siendo p primo se tiene que $o(a) = 1$ ó $o(a) = p$; siendo e el único elemento de orden 1, debe ser $o(a) = p$. Luego $o(\langle a \rangle) = o(G) \Rightarrow G = \langle a \rangle$.

Si $i(Z(G)) = p$, $o(G/Z(G)) = p$. Luego $G/Z(G)$ es cíclico y, según lo visto en el pá-

Ejemplo 2º: Operación de un grupo en sí mismo por conjugación.
Sea G un grupo. Definimos la aplicación:

$$*: G \times G \longrightarrow G$$
$$(g, x) \longmapsto g * x = g x g^{-1}$$

Fácilmente se comprueba que $*$ verifica las propiedades P.1.) y P.2).
Luego G opera en sí mismo mediante $*$. Se dice que G opera en G por conjugación. El homomorfismo inducido por $*$ es:

$$\phi: G \longrightarrow \mathcal{I}(G)$$
$$g \longmapsto \gamma_g$$

siendo $\gamma_g: G \longrightarrow G$
$x \longmapsto \gamma_g(x) = g x g^{-1}$

Se comprueba fácilmente que γ_g es un automorfismo de G. A estos automorfismos se les llama internos.
La órbita de un elemento a es: $C_a = \{g * a / g \in G\} = \{g a g^{-1} / g \in G\}$.

1.5. Teorema: Sea G un grupo que opera en sí mismo por conjugación. Entonces, el cardinal de la órbita de un elemento $a \in G$ es igual al índice del normalizador del elemento a (también llamado centralizador de a), es decir, $\text{card}(C_a) = i(N_a)$.

Demostr.: El estabilizador de a es: $\Sigma_a = \{g \in G / g * a = a\} = \{g \in G / g a g^{-1} = a\} = N_a$

Como $\text{card}(C_a) = i(\Sigma_a)$ y $\Sigma_a = N_a$, queda probado el teorema.

Además si G es de orden finito, $\text{card}(C_a)$ divide a $o(G)$. (Th. 1.1. c)).

* Ecuacion de las clases de Frobenius:

1.6. Lema: Sea G un grupo que opera en sí mismo por conjugación. Entonces, dado $a \in G$, $C_a = \{a\}$ si y solo si $a \in Z(G)$.

Demostr.: $\Rightarrow$] $C_a = \{g a g^{-1} / g \in G\}$.
Si $C_a = \{a\}$, se tiene que $(\forall g \in G, g a g^{-1} = a) \Rightarrow (g a = a g, \forall g \in G)$.
Luego $a \in Z(G)$.
$\Leftarrow$] Si $a \in Z(G)$, $C_a = \{g a g^{-1} / g \in G\} = \{a g g^{-1} / g \in G\} = \{a\}$. c.q.d.

Sabemos que en un conjunto E en el que opera un grupo G se induce una partición por órbitas. En el caso de que un grupo G opere

en sí mismo por conjugación, las órbitas se llaman clases de conjugación.

1.7. TEOREMA: (Fórmula de las clases de Frobenius)

El orden de un grupo finito G, que opera en sí mismo por conjugación, coincide con el orden de $Z(G)$ más unos ciertos sumandos d_i que verifican que $1 < d_i$ y $d_i \mid o(G)$. Es decir:

$$o(G) = o(Z(G)) + \sum d_i, \quad 1 < d_i, \ d_i \mid o(G).$$

Demostr.: G admite una partición por clases de conjugación. Las clases de conjugación de los elementos del centro tienen un solo elemento, según el lema anterior, y son las únicas que tienen un solo elemento. Las restantes clases tendrán d_i elementos; luego $1 < d_i$. Además, el cardinal de la órbita de un elemento divide a $o(G)$ (Th. 1.1.). Luego $d_i \mid o(G)$. Entonces: $o(G) = o(Z(G)) + \sum d_i$, $1 < d_i$, $d_i \mid o(G)$. c.s.q.d.

1.8. COROLARIO: El centro de un p-grupo G es no trivial: $Z(G) \neq \{e\}$. (*)

Demostr.: $p^\alpha = o(G) = o(Z(G)) + \sum d_i$, $d_i \mid p^\alpha$, $1 < d_i$.

Siendo p primo, si $d_i \mid p^\alpha$, d_i debe ser múltiplo de p: $p \mid d_i$.

Si fuese $Z(G) = \{e\}$, $p^\alpha = 1 + \sum d_i$, lo cual es imposible, pues $(1 = p^\alpha - \sum d_i) \wedge (p \mid p^\alpha) \wedge (p \mid \sum d_i) \Rightarrow p \mid 1$,

que es absurdo, pues p es primo, $p \neq 1$.

1.9. COROLARIO: Todo grupo G de orden p^2, con p primo, es abeliano.

Demostr.: Siendo $Z(G)$ subgrupo de G, por el teorema de Lagrange, $o(Z(G))$ divide a $o(G) = p^2$.

Entonces $o(Z(G))$ puede ser 1, p ó p^2.

1 no puede ser, pues G es un p-grupo y, por tanto, $Z(G) \neq \{e\}$.

Si $o(Z(G)) = p$, siendo $O(G) = o(Z(G)) \cdot i(Z(G))$, debería ser $i(Z(G)) = p$. Pero, según COROLARIO 1.4., el índice del centro de un grupo no puede ser primo. Debe ser, entonces, $o(Z(G)) = p^2$.

Luego $Z(G) = G$, que prueba que G es abeliano. c.s.q.d.

1.10. PROPOSICION: a) Sea G un grupo. Entonces G opera por conjugación sobre $P(G)$.

b) G opera por conjugación en el conjunto $\mathcal{T}$ de los subgrupos de G.

Demostr.: a) $* : G \times \mathcal{P}(G) \longrightarrow \mathcal{P}(G)$

$(g, H) \longmapsto g * H = gHg^{-1}$

Evidentemente, $\forall g \in G$, $gHg^{-1} \in \mathcal{P}(G)$. Veamos que $*$ verifica las propiedades P.1.) y P.2.):

P.1.) $\forall g_1, g_2 \in G$, $\forall H \in \mathcal{P}(G)$, $(g_1 g_2) * H = (g_1 g_2) H (g_1 g_2)^{-1} =$

$= g_1 (g_2 H g_2^{-1}) g_1^{-1} = g_1 (g_2 * H) g_1^{-1} = g_1 * (g_2 * H)$

P.2.) $\forall H \in \mathcal{P}(G)$, $\varepsilon * H = \varepsilon H \varepsilon^{-1} = H$.

b) Se demuestra de manera análoga a a). Solo queda comprobar que $\forall g \in G$, $\forall S \in \mathcal{S}$, $g * S = g S g^{-1} \in \mathcal{S}$, pero esto es trivial si tenemos en cuenta que

$\gamma_g : G \longrightarrow G$

$x \longmapsto \gamma_g(x) = gxg^{-1}$

es un automorfismo de G y transforma subgrupos en subgrupos. Luego, siendo S subgrupo, $\gamma_g(S) = g S g^{-1}$ es subgrupo de G. c.s.q.d.

Obsérvese que la órbita de un elemento H de $\mathcal{P}(G)$ es:

$C_H = \{ g * H / g \in G \} = \{ gHg^{-1} / g \in G \}$ y el estabilizador es:

$\Sigma_H = \{ g \in G / g * H = H \} = \{ g \in G / gHg^{-1} = H \}$, que, por tanto, coincide con el normalizador de H, N_H. Entonces, según el teorema 1.1., $i(N_H) = \text{card}(C_H)$, y si G es finito $\text{card}(C_H) \mid o(G)$.

TEMA 3º: EL GRUPO DE LAS PERMUTACIONES S_n

1. INTRODUCCION. DEFINICION

Según el TEOREMA DE CAYLEY demostrado en el tema anterior, todo grupo finito de orden n es isomorfo a un subgrupo del grupo S_n de las permutaciones de n elementos. Para estudiar las propiedades de los grupos finitos de orden n es suficiente, por tanto, estudiar los subgrupos de S_n.

1.1. PROPOSICION: Sea E un conjunto. Llamamos $\mathcal{J}(E)$ al conjunto de las biyecciones de E en E. Entonces:

a) $(\mathcal{J}(E), \circ)$ es grupo.

b) Si E y E' son grupos con el mismo cardinal, entonces los grupos $\mathcal{J}(E)$ y $\mathcal{J}(E')$ son isomorfos.

Demostr.: a) Que $(\mathcal{J}(E), \circ)$ es grupo es trivial, pues la composición de dos biyecciones es una biyección; la composición de biyecciones es asociativa; el elemento neutro es i_E, la identidad en E y cada biyección f admite la biyección simétrica f^{-1} con $f \circ f^{-1} = f^{-1} \circ f = i_E$.

b) Si $\text{card}(E) = \text{card}(E')$, existe una biyección $\phi: E \to E'$. Definimos una aplicación φ de $\mathcal{J}(E)$ en $\mathcal{J}(E')$ que a cada biyección $f: E \to E$ le asocia $\varphi(f): E' \xrightarrow{\phi^{-1}} E \xrightarrow{f} E \xrightarrow{\phi} E'$ que es una biyección de E' en E'

Veamos que φ es homomorfismo:

$\varphi(g \circ f) = \phi \circ g \circ f \circ \phi^{-1} = \phi \circ g \circ \phi^{-1} \circ \phi \circ f \circ \phi^{-1} = \varphi(g) \circ \varphi(f)$.

- φ es inyectiva: Veamos que $\text{Ker}\,\varphi = \{i_E\}$. Si $\varphi(f) = i_{E'} \Rightarrow$
$\Rightarrow \phi \circ f \circ \phi^{-1} = i_{E'} \Rightarrow f = \phi^{-1} \circ i_{E'} \circ \phi = i_E$. Luego $\text{Ker}\,\varphi = \{i_E\}$.
- φ es sobre: $\forall g \in \mathcal{J}(E')$, $\exists f = \phi^{-1} \circ g \circ \phi \in \mathcal{J}(E)$ / $\varphi(f) =$
$= \phi \circ \phi^{-1} \circ g \circ \phi \circ \phi^{-1} = g$.

Luego $\mathcal{J}(E) \cong \mathcal{J}(E')$. c.s.q.d.

DEFINICION: Llamamos S_n al grupo de las biyecciones (grupo simétrico) de un conjunto de n elementos.

El conjunto de n elementos más sencillo es $E = \{1, 2, \ldots, n\}$. Tomaremos entonces S_n como el grupo de las biyecciones de dicho conjunto. Un elemen-

to σ de S_n se llama una permutación y se representa por

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

2. Ciclos

Definición Se llama ciclo de longitud m en S_n a una permutación σ que verifica que

$\exists \{i_1, i_2, \dots, i_m\} \subset E$ / $\sigma(i_k) = i_{k+1}$ si $1 \le k \le m-1$, $\sigma(i_m) = i_1$ y $\sigma(i_p) = i_p$ si $m+1 \le p \le n$

Un ciclo de longitud m deja invariantes $n-m$ elementos y los m elementos restantes los transforma de modo que a cada elemento le asocia el siguiente y al último de ellos le asocia el primero. (*)

El ciclo anterior lo representamos de la forma:

$$\sigma = (i_1, i_2, \dots, i_m)$$

Definición: (Transposición). Se llama transposición a un ciclo de longitud 2.

$$\tau_{ij} = (i, j) = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

Definición: (ciclos disjuntos) Dos ciclos σ_1 y σ_2 son disjuntos si

$$(\forall i \in E,\ \sigma_1(i) \neq i \Rightarrow \sigma_2(i) = i) \wedge (\forall j \in E,\ \sigma_2(j) \neq j \Rightarrow \sigma_1(j) = j)$$

Es decir, cuando el conjunto de elementos que se mueven por σ_1 y el conjunto de elementos que se mueven por σ_2 son disjuntos.

Evidentemente, si σ_1 y σ_2 son dos ciclos disjuntos, conmutan, es decir (σ_1 y σ_2 disjuntos) $\Rightarrow (\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1)$, pues si

$(\sigma_1(i) = i) \wedge (\sigma_2(i) = i) \Rightarrow (\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i)) = \sigma_1(i) = i = (\sigma_2 \circ \sigma_1)(i)$

$(\sigma_1(i) = j) \wedge (\sigma_2(i) = i) \Rightarrow (\sigma_1 \circ \sigma_2)(i) = \sigma_1(i) = j = (\sigma_2 \circ \sigma_1)(i)$, pues j se mueve por σ_1 y, por tanto, no se mueve por σ_2. El caso en que $\sigma_1(i) = i$ y $\sigma_2(i) = j$ es análogo al anterior. El caso $\sigma_1(i) \neq i$ y $\sigma_2(i) \neq i$ no se puede dar por ser los ciclos disjuntos.

21. Proposición: Un ciclo de longitud m es un elemento de orden m en el grupo S_n: $\sigma = (i_1, \dots, i_m) \Rightarrow o(\sigma) = m$.

Demostr.: Si $\sigma = (i_1, i_2, \dots, i_m)$ se tiene

$\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\dots$, $\sigma(i_{m-1}) = i_m$, $\sigma(i_m) = i_1$

$\sigma^2(i_1) = i_3$, $\sigma^2(i_2) = i_4$, $\dots$, $\sigma^2(i_{m-1}) = i_1$, $\sigma^2(i_m) = i_2$

. . . . . .

(*) . . . . . .

$\sigma^k(i_1)=i_{k+1}, \sigma^k(i_2)=i_{k+2}, \ldots, \sigma^k(i_{m-k})=i_m, \sigma^k(i_{m-k+1})=i_1, \ldots, \sigma^k(i_m)=i_k$

$\sigma^{m-1}(i_1)=i_m, \sigma^{m-1}(i_2)=i_1, \ldots, \sigma^{m-1}(i_{m-1})=i_{m-2}, \sigma^{m-1}(i_m)=i_{m-1}$

$\sigma^m(i_1)=i_1, \sigma^m(i_2)=i_2, \ldots, \sigma^m(i_{m-1})=i_{m-1}, \sigma^m(i_m)=i_m$.

Luego m es el menor natural tal que σ^m coincide con la identidad ($\sigma^m = i_E$ pues $\forall p \in \{1,\ldots,m\}$, $\sigma^m(i_p)=i_p$ y $\forall i \in E-\{i_p / 1\le p\le m\}$, $\sigma^m(i)=i$). Luego $o(\sigma)=m$. c.s.q.d.

Se deduce de lo anterior que el subgrupo de S_n engendrado por un ciclo σ de longitud m es $\langle\sigma\rangle = \{i_E, \sigma, \sigma^2, \ldots, \sigma^{m-1}\}$.

2.2. TEOREMA: Toda permutación $\sigma \in S_n$ admite una descomposición en producto de ciclos disjuntos de longitud mayor o igual que 2, y esta descomposición es única salvo el orden en que aparecen escritos los ciclos, es decir, dada una permutación $\sigma \in S_n$, existen ciclos disjuntos $\alpha_1, \alpha_2, \ldots, \alpha_r$ tal que $\sigma = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_r$, con $\text{long}\,\alpha_i \ge 2$, $\forall i \in \{1,\ldots,r\}$. (*)

Demostr.: Consideremos el subgrupo H de S_n generado por la permutación σ, es decir, $H = \langle\sigma\rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{q-1}\}$, siendo $q = o(\sigma)$. (**)

Hacemos operar H sobre el conjunto $E=\{1,2,\ldots,n\}$ mediante la operación:

$$* : H \times E \longrightarrow E$$
$$(\sigma^k, i) \longmapsto \sigma^k * i = \sigma^k(i)$$

Fácilmente se comprueba que, efectivamente, H opera en E por $*$. Como sabemos, E admite, entonces, una partición por órbitas. Dado un elemento $i \in E$, la órbita asociada a i es: $O_i = \{i, \sigma(i), \sigma^2(i), \ldots, \sigma^{q-1}(i)\}$. Este conjunto no está bien escrito, pues puede haber elementos que se repitan (p.ej. en el caso en que i sea invariante por σ, es decir, $\sigma(i)=i$, la órbita del elemento i se reduciría a $\{i\}$). Supongamos que $\text{card}(O_i)=s$, entonces $O_i = \{i, \sigma(i), \sigma^2(i), \ldots, \sigma^{s-1}(i)\}$ (son los s primeros elementos pues en cuanto $\sigma^k(i)=i$ se tiene $\sigma^{k+1}(i)=\sigma(i)$, que ya está entre los s primeros). E, como hemos dicho, admite una partición por órbitas, es decir, si tenemos r órbitas $\{O_j\}_{j=1}^r$

$$E = \bigcup_{j=1}^{r} O_j \quad \text{con} \quad O_i \cap O_j = \phi \quad \text{si } i \ne j.$$

Consideremos la restricción de σ a cada órbita O_i:

$$\sigma/_{O_i} = \begin{pmatrix} i, \sigma(i), \sigma^2(i), \ldots, \sigma^{s-2}(i), \sigma^{s-1}(i) \\ \sigma(i), \sigma^2(i), \sigma^3(i), \ldots, \sigma^{s-1}(i), \quad i \end{pmatrix} \quad \text{y a } \ldots$$

(*) En adelante la composición $\alpha_1 \circ \alpha_2$ de dos ciclos o transposiciones la denota-

Luego la restricción de σ a cada órbita O_i es un ciclo. Definimos, entonces, para cada órbita O_i,

$$\alpha_i : E \longrightarrow E$$
$$x \longmapsto \alpha_i(x) = \begin{cases} = \sigma|_{O_i}(x) & \text{si } x \in O_i \\ = x & \text{si } x \in E - O_i \end{cases} \quad (I)$$

Por tanto, α_i es un ciclo en S_n.

Veamos que si $i \neq j$, entonces α_i y α_j son disjuntos. Si $i \neq j$, tenemos que $O_i \cap O_j = \emptyset$, luego el conjunto de elementos no invariantes por α_i y el conjunto de elementos no invariantes por α_j son disjuntos; luego α_i y α_j son disjuntos. La longitud de estos ciclos es mayor o igual que 2, pues si long $\alpha_k = 1$ estamos en el caso $O_k = \{k\}$ y α_k sería la identidad en E. Luego, si tenemos r órbitas no unitarias $O_1, O_2, \ldots, O_r$, a la vista de (I) podemos escribir que

$$\sigma = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_r$$

Antes de ver que la descomposición es única demostraremos el siguiente

2.2.1. Lema: Sean α y β dos ciclos en S_n de modo que $\exists i \in E$ tal que $\alpha(i) \neq i$ y además $\forall p \geq 1$, $\alpha^p(i) = \beta^p(i)$. Entonces $\alpha = \beta$.

demostr: Sea $\alpha = (i_1, \ldots, i_k, \ldots, i_m)$, con $i_k = i$. Entonces α lo podemos escribir también del siguiente modo: $\alpha = (i_k = i, i_{k+1}, \ldots, i_m, i_1, \ldots, i_{k-1})$. Entonces, $\alpha(i) = i_{k+1}$, $\alpha^2(i) = i_{k+2}$, $\ldots$, $\alpha^{m-k}(i) = i_m$, $\ldots$, $\alpha^{m-1}(i) = i_{k-1}$

Por tanto, $\alpha = (i, \alpha(i), \alpha^2(i), \ldots, \alpha^{m-1}(i))$.

Siendo $\forall p \geq 1$, $\alpha^p(i) = \beta^p(i)$ se tiene que long α = long β.

Análogamente, el ciclo β lo podemos representar en la forma $\beta = (i, \beta(i), \beta^2(i), \ldots, \beta^{m-1}(i))$. Como $\beta(i) = \alpha(i), \ldots, \beta^{m-1}(i) = \alpha^{m-1}(i)$, se tiene que $\alpha = \beta$. c.s.q.d.

→ (CONTINUA DEMOSTRACION DEL TEOREMA): Veamos que la descomposición de una permutación como producto de ciclos disjuntas de longitud mayor o igual que 2 es única. Supongamos que σ admite dos descomposiciones: $\sigma = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_r$ y $\sigma = \beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_s$.

Dado el ciclo α_1, siendo long $\alpha_1 \geq 2$, existe $i \in E$ tal que $\alpha_1(i) \neq i$. Entonces, como $\alpha_2, \ldots, \alpha_r$ son disjuntos con α_1, se verifica que i es invariante por $\alpha_2, \ldots, \alpha_r$. Luego $\sigma(i) = \alpha_1(i) \neq i$.

Siendo $\sigma(i) \neq i$ y $\sigma = \prod_{j=1}^{s} \beta_j$, por ser los ciclos $\{\beta_j\}_{j=1}^{s}$ disjuntos dos a dos, se ha de verificar que $\exists k_1 \in \{1, \ldots, s\} / \beta_{k_1}(i) \neq i$.

Luego $\sigma(i) = \beta_{k_1}(i)$. Por tanto, $\alpha_1(i) = \beta_{k_1}(i)$

Además $\forall p \geq 1$, $\sigma^p(i) = \sigma^{p-1}(\sigma(i)) = \sigma^{p-1}(\alpha_1(i)) =$
$= \sigma^{p-2}(\sigma(\alpha_1(i))) = \sigma^{p-2}(\alpha_1(\sigma(i))$ pues α_1 conmuta con σ ya que σ es un producto de ciclos disjuntos con α_1
Luego $\forall p \geq 1$, $\sigma^p(i) = \sigma^{p-2}(\alpha_1(\alpha_1(i))) = \sigma^{p-2}(\alpha_1^2(i)) = \ldots = \alpha_1^p(i)$
Analogamente, $\sigma^p(i) = \beta_{k_1}^p(i)$. Luego $\forall p \geq 1$, $\alpha_1^p(i) = \beta_{k_1}^p(i)$
En virtud del lema tenemos que, $\alpha_1 = \beta_{k_1}$.
Razonando analogamente con $\alpha_2, \ldots, \alpha_r$ obtenemos que
$\forall j \in \{1, \ldots, r\}$, $\exists\, k_j \in \{1, \ldots, s\}$ / $\alpha_j = \beta_{k_j}$

Deducimos de aquí que $\{\alpha_1, \ldots, \alpha_r\} \subset \{\beta_1, \ldots, \beta_s\}$
Procediendo ahora con $\beta_1, \ldots, \beta_s$ como hemos hecho con $\alpha_1, \ldots, \alpha_r$ obtendríamos que $\{\beta_1, \ldots, \beta_s\} \subset \{\alpha_1, \ldots, \alpha_r\}$. Luego $\{\alpha_1, \ldots, \alpha_r\} = \{\beta_1, \ldots, \beta_s\}$ que prueba que la descomposición de σ en ciclos disjuntos de longitud mayor o igual que dos es única, salvo el orden de los factores. c.s.q.d.

2.3. PROPOSICION: Sea $\sigma \in S_n$ y $\alpha = (i_1, \ldots, i_m)$ un ciclo. Entonces

$$\sigma \alpha \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_m)).$$

Demostr.: Sea $i \in E$, Supongamos en un primer caso que i es de la forma $i = \sigma(i_k)$ con $k \in \{1, \ldots, m\}$.
Entonces: $(\sigma \alpha \sigma^{-1})(i) = (\sigma \alpha \sigma^{-1})(\sigma(i_k)) = (\sigma \alpha)(i_k) =$
$= \sigma(\alpha(i_k)) = \begin{cases} = \sigma(i_{k+1}) & \text{si } 1 \leq k < m \\ = \sigma(i_1) & \text{si } k = m \end{cases}$
Veamos como actua el ciclo $(\sigma(i_1), \ldots, \sigma(i_m))$ sobre i:
$(\sigma(i_1), \ldots, \sigma(i_m))(i) = (\sigma(i_1), \ldots, \sigma(i_m))(\sigma(i_k)) =$
$= \begin{cases} = \sigma(i_{k+1}) & \text{si } 1 \leq k < m \\ = \sigma(i_1) & \text{si } k = m \end{cases}$
Luego si $i = \sigma(i_k)$, $1 \leq k \leq m$, $\sigma \alpha \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_m))$.
Supongamos ahora que $i \neq \sigma(i_k)$, $\forall k \in \{1, \ldots, m\}$. Entonces $\sigma^{-1}(i) \neq i_k$, $\forall k \in \{1, \ldots, m\}$, pues σ^{-1} es inyectiva.
Entonces, como α solo mueve los elementos $i_1, \ldots, i_m$, se tiene que $(\sigma \alpha \sigma^{-1})(i) = \sigma[\alpha(\sigma^{-1}(i))] = \sigma[\sigma^{-1}(i)] = i$
Por otro lado $(\sigma(i_1), \ldots, \sigma(i_m))(i) = i$, pues el ciclo $(\sigma(i_1), \ldots, \sigma(i_m))$ solo mueve a los elementos $\{\sigma(i_k)\}_{k=1}^m$ e $i \neq \sigma(i_k)$, $\forall k \in \{1, \ldots, m\}$.
En cualquier caso, $\sigma \alpha \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_m))$. c.s.q.d.

DEFINICION: Dos permutaciones σ_1 y σ_2 se dicen conjugadas si $\exists\, \gamma \in S_n$ / $\sigma_2 = \gamma \sigma_1 \gamma^{-1}$.

De la proposición anterior se deduce que dos ciclos conjugados tienen la misma longitud.

Diremos que dos permutaciones τ_1 y τ_2 de estructuras cíclicas respectivas $\prod_{i=1}^{r} \alpha_i$ y $\prod_{j=1}^{s} \beta_j$ tienen la misma estructura cíclica si $r = s$ y mediante una permutación conveniente de los índices j podemos conseguir que $\text{long}\ \alpha_i = \text{long}\ \beta_i$. Ejemplo: En S_8 las permutaciones $(1,2)\cdot(3,4,5)$ y $(4,5)(1,3,7)$ tienen la misma estructura cíclica.

2.4. TEOREMA: Dos permutaciones son conjugadas si y solo si tienen la misma estructura cíclica.

Demostr.: $\Rightarrow$ Si τ_1 y τ_2 son permutaciones conjugadas, existe $\gamma \in S_n$ tal que $\tau_2 = \gamma \tau_1 \gamma^{-1}$.

Supongamos que $\tau_1 = \prod_{i=1}^{r} \alpha_i$ y $\tau_2 = \prod_{i=1}^{s} \beta_i$

Entonces $\gamma \tau_1 \gamma^{-1} = \gamma \alpha_1 \alpha_2 \dots \alpha_{r-1} \alpha_r \gamma^{-1} = \gamma \alpha_1 \gamma^{-1} \cdot \gamma \alpha_2 \gamma^{-1} \cdot \dots \cdot \gamma \alpha_{r-1} \gamma^{-1} \cdot \gamma \alpha_r \gamma^{-1} =$
$= \prod_{i=1}^{r} (\gamma \alpha_i \gamma^{-1})$

Por la proposición 2.3, si $\alpha_i = (j_{1i}, \dots, j_{mi})$, entonces $\gamma \alpha_i \gamma^{-1} = (\gamma(j_{1i}), \dots, \gamma(j_{mi}))$.
Siendo $\tau_2 = \gamma \tau_1 \gamma^{-1} = \prod_{i=1}^{r} (\gamma \alpha_i \gamma^{-1})$ y $\tau_2 = \prod_{i=1}^{s} \beta_i$ se verifica que $r = s$ y $\beta_i = \gamma \alpha_i \gamma^{-1} = (\gamma(j_{1i}), \dots \gamma(j_{mi}))$. Evidentemente: $\text{long}\ \beta_i = \text{long}\ \alpha_i$.
Veamos que si $i \neq K$, β_i y β_K son disjuntos. Siendo $i \neq K$, los ciclos $\alpha_i = (j_{1i}, \dots, j_{mi})$ y $\alpha_K = (j_{1K}, \dots, j_{pK})$ no tienen ningún elemento común. Siendo γ una permutación, es inyectiva y a elementos distintos asocia elementos distintos; luego los ciclos $\beta_i = (\gamma(j_{1i}), \dots, \gamma(j_{mi}))$ y $\beta_K = (\gamma(j_{1K}), \dots, \gamma(j_{pK}))$ no tienen ningún elemento común; luego son disjuntos.

Por tanto, τ_1 y τ_2 tienen la misma estructura cíclica.

$\Leftarrow$ Sean $\tau_1 = \prod_{i=1}^{r} \alpha_i$ y $\tau_2 = \prod_{i=1}^{r} \beta_i$, con $\text{long}\ \alpha_i = \text{long}\ \beta_i$, $1 \leq i \leq r$.

Supongamos que $\alpha_i = (j_1, j_2, \dots, j_{m_i})$ y $\beta_i = (j'_1, j'_2, \dots, j'_{m_i})$

y esto para cada $i \in \{1, \dots, r\}$.

Hacemos $\gamma(j_1) = j'_1$, $\gamma(j_2) = j'_2$, $\dots$, $\gamma(j_{m_i}) = j'_{m_i}$, y esto para cada $i \in \{1, \dots, r\}$. De este modo obtenemos una biyección de E_1, conjunto de elementos movidos por τ_1, en E'_1, conjunto de elementos que son movidos por τ_2: $\gamma/_{E_1} : E_1 \longrightarrow E'_1$. Sea E_2 el conjunto de elementos invariantes por τ_1 y E'_2 el conjunto de elementos invariantes por τ_2. Como τ_1 y τ_2 tienen la misma estructura cíclica se tiene, trivialmente, que $\text{card}(E_2) = \text{card}(E'_2)$.

existe una biyección de E_2 en E_2'. Prolongando entonces la biyección γ/E_1 a $E = E_1 \cup E_2$, obtenemos una biyección $\gamma \in S_n$, y además según hemos construido γ/E_1, se tiene que $\sigma_2 = \gamma \sigma_1 \gamma^{-1}$. c.s.q.d.

2.5. TEOREMA: Las transposiciones constituyen un sistema generador de S_n.

Demostr.: Toda permutación se descompone en producto de ciclos. Probemos que todo ciclo se puede expresar como producto de transposiciones, con lo cual quedará probado que toda permutación se puede escribir como producto de transposiciones. Consideremos el ciclo $(1,2,\dots,k)$. Evidentemente admite la siguiente descomposición:

$$(1,2,\dots,k) = (1,k)\cdot(1,k-1)\cdot\dots\cdot(1,3)\cdot(1,2)$$

pues: $(1,2) = \begin{pmatrix} 1 & 2 & 3 & \dots & k-2 & k-1 & k \\ 2 & 1 & 3 & \dots & k-2 & k-1 & k \end{pmatrix}$

$(1,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & k-2 & k-1 & k \\ 2 & 3 & 1 & 4 & \dots & k-2 & k-1 & k \end{pmatrix}$

. . . . . .

$(1,k-2)\dots(1,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & \dots & k-2 & k-1 & k \\ 2 & 3 & 4 & \dots & 1 & k-1 & k \end{pmatrix}$

$(1,k-1)(1,k-2)\dots(1,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & \dots & k-2 & k-1 & k \\ 2 & 3 & 4 & \dots & k-1 & 1 & k \end{pmatrix}$

$(1,k)(1,k-1)\dots(1,2) = \begin{pmatrix} 1 & 2 & 3 & \dots & k-2 & k-1 & k \\ 2 & 3 & 4 & \dots & k-1 & k & 1 \end{pmatrix} = (1,2,\dots,k)$ c.s.q.d.

Sin embargo, esta descomposición no tiene porque ser única.
Contraejemplo: En S_4, $(1,3) = (4,1)(4,3)(4,1) = (2,1)(2,3)(2,1)$

Interesa encontrar sistemas generadores irreducibles. Recordemos que en un grupo G un sistema de generadores $\{x_i\}_{i=1}^k$ es irreducible si $\forall j \in \{1,\dots,k\}$, $\langle G - \{x_j\} \rangle \neq G$.

2.6. TEOREMA: a) Las transposiciones $(1,2),(2,3),\dots,(n-1,n)$ constituyen un sistema de generadores irreducible de S_n.
b) Si $n>2$, la transposición $\tau=(1,2)$ y el ciclo $\sigma=(1,2,\dots,n)$ constituyen un sistema de generadores irreducible de S_n.

Demostr.: a) Según el teorema anterior toda permutación de S_n se puede expresar como producto de transposiciones. Es suficiente probar entonces que toda transposición (i,j) (*) se puede expresar como producto de transposiciones de la forma $(k,k+1)$, $1 \leq k < n$.

Para efectuar la transposición (i,j) llevamos j al lugar $i+1$ mediante las transposiciones sucesivas $(j-1,j),(j-2,j-1),\dots,(i+1,i+2)$. Una vez que j está en el lugar $i+1$ efectuamos la transposición $(i,i+1)$ y j e i permutan sus lugares. A continuación llevamos i al lugar que ocupaba j primitivamente mediante las transposiciones $(i+1,i+2),(i+2,i+3),\dots,(j-1,j)$. Luego:

$$(i,j)=(j-1,j)(j-2,j-1)\dots(i+1,i+2)(i,i+1)(i+1,i+2)\dots(j-2,j-1)(j-1,j).$$

Luego $\Sigma=\{(i,i+1)/\ 1\le i<n\}$ es un sistema de generadores de S_n.

Probemos que es irreducible. Si a Σ le quitamos la transposición $(i,i+1)$ $\Sigma'=\Sigma-\{(i,i+1)\}$ ya no genera a S_n, pues, por ejemplo, la transposición $(i,i+1)$ no se puede expresar como producto de transposiciones de $\Sigma'=\{(1,2),\dots,(i-1,i),(i+1,i+2),\dots,(n-1,n)\}$; tampoco se puede expresar como producto de transposiciones de Σ' una transposición de la forma (k,ℓ) con $k\in\{1,2,\dots,i\}$ y $\ell\in\{i+1,\dots,n\}$, pues no podemos efectuar la transposición $(i,i+1)$.

b) Para ver que $\{\tau,\sigma\}$, $\tau=(1,2)$ y $\sigma=(1,2,\dots,n)$, generan S_n probaremos que toda transposición de la forma $(i,i+1)$, $1\le i<n$, se puede expresar como producto de potencias de τ y σ.

Tenemos que $\sigma(1)=2$, $\sigma^2(1)=\sigma(\sigma(1))=\sigma(2)=3$, $\sigma^3(1)=\sigma(\sigma^2(1))=\sigma(3)=4$, $\sigma^4(1)=5,\dots,\sigma^{i-1}(1)=i$.

Análogamente $\sigma^{i-1}(2)=\sigma^{i-1}(\sigma(1))=\sigma^i(1)=i+1$

Entonces, según PROPOSICION 2.3,

$$\sigma^{i-1}\cdot\tau\cdot(\sigma^{i-1})^{-1}=\sigma^{i-1}\cdot(1,2)\cdot(\sigma^{i-1})^{-1}=(\sigma^{i-1}(1),\sigma^{i-1}(2))=(i,i+1).$$

Veamos que es irreducible. Trivialmente, si $2<n$, entonces $2<n!$. Siendo τ un ciclo de longitud 2 se tiene que $o(\langle\tau\rangle)=2<n!=o(S_n)$. Luego $\langle\tau\rangle\neq S_n$. Por tanto, $\{\tau\}$ no es sistema generador de S_n si $n>2$.

Análogamente, siendo $\text{long}\,\sigma=n$, $o(\langle\sigma\rangle)=n<n!=o(S_n)$ si $n>2$.

Luego $\{\sigma\}$ tampoco genera a S_n, que prueba que $\{\tau,\sigma\}$ es un sistema generador irreducible de S_n. c.s.q.d.

2.7. PROPOSICION: Si $n>2$, el centro de S_n es $Z(S_n)=\{i_E\}$

Demostr.: Sea $\gamma\in Z(S_n)$. Consideremos la transposición $(i,j)\in S_n$.

Entonces $\gamma(i,j)=(i,j)\gamma$ y también $\gamma(i,j)\gamma^{-1}=(i,j)$

Pero $\gamma(i,j)\gamma^{-1}=(\gamma(i),\gamma(j))$. Luego $(\gamma(i),\gamma(j))=(i,j)$

Debe ser entonces: $[\gamma(i)=i\ \wedge\ \gamma(j)=j]\ \vee\ [\gamma(i)=j\ \wedge\ \gamma(j)=i]$

Si fuese $\gamma(i)=i$, como esto lo podemos hacer para cada $i\in\{1,2,\dots,n\}$ habría que $\gamma=i_E$. Probemos que no puede ser $\gamma(i)=j\ \wedge\ \gamma(j)=i$

Como $n>2$, $\exists l \in E-\{i,j\}$. Entonces $\gamma(i,l)\gamma^{-1}=(i,l)$ y también $\gamma(i,l)\gamma^{-1}=(\gamma(i),\gamma(l))$. Luego sería $(\gamma(i),\gamma(l))=(i,l)$.
Si suponemos que $\gamma(i)=j$ llegamos a una contradicción pues se tendría que $(\gamma(i),\gamma(l))=(j,\gamma(l))$ que no puede ser igual a (i,l), pues $(j,\gamma(l))$ mueve a j y (i,l) lo deja invariante. Por tanto, $\forall i\in E$, $\gamma(i)=i$. Luego $\gamma=i_E$. c.s.q.d.

3. Signatura de una permutación

Consideremos el grupo multiplicativo $\{-1,1\}$. Definimos una aplicación

$$\pi: S_n \longrightarrow \{-1,1\}$$
$$\sigma \longmapsto \pi(\sigma)=\prod_{j>i}\frac{\sigma(j)-\sigma(i)}{j-i}$$

Veamos que π está bien definida, es decir, que $\forall \sigma\in S_n$, $\pi(\sigma)\in\{-1,1\}$.
Veremos que dada una fracción $\frac{\sigma(j)-\sigma(i)}{j-i}$ del producto, existe una fracción y solo una que tiene de numerador $\sigma(k)-\sigma(p)=\varepsilon(j-i)$ con $\varepsilon=\pm 1$ y otra fracción que tiene por denominador $k'-p'=\varepsilon[\sigma(j)-\sigma(i)]$
Dado el denominador $j-i$, existen $k,p\in E$ tales que $\sigma(k)=j$ y $\sigma(p)=i$, y k y p son únicos por ser σ biyectiva. Entonces existe en el producto una fracción de la forma $\frac{\sigma(k)-\sigma(p)}{\varepsilon(k-p)}$ según sea $k>p$ o $k<p$.
En cualquier caso al efectuar el producto se simplifican $\sigma(k)-\sigma(p)$ y $j-i$ y queda 1 o -1 según el valor de ε. Análogamente, cada numerador se simplifica con uno y solo un denominador. En cualquier caso $\pi(\sigma)\in\{-1,1\}$.

DEFINICION: Decimos que una permutación σ es de clase par si $\pi(\sigma)=1$ y diremos que es de clase impar si $\pi(\sigma)=-1$. A $\pi(\sigma)$ se le llama signatura de σ.

DEFINICION: Diremos que dos elementos $i,j\in E$ forman inversión respecto a una permutación σ si se verifica que $i<j$ y $\sigma(i)>\sigma(j)$.

3.1. PROPOSICION: Sea $\sigma\in S_n$ y i_σ el número de inversiones de σ. Entonces $\pi(\sigma)=(-1)^{i_\sigma}$.

Demostr: Siendo $\pi(\sigma)=\prod_{j>i}\frac{\sigma(j)-\sigma(i)}{j-i}$

Hay tantos factores negativos como veces sea $\sigma(j)<\sigma(i)$, es decir, tantos como inversiones tenga σ. Como $\pi(\sigma)\in\{-1,1\}$ será $\pi(\sigma)=(-1)^{i_\sigma}$. c.s.q.d

3.2. PROPOSICION: π es un homomorfismo de S_n en $\{-1,1\}$.

Demostr. $\pi(\sigma_1\sigma_2)=\prod_{j>i}\frac{(\sigma_1\sigma_2)(j)-(\sigma_1\sigma_2)(i)}{j-i}=\prod_{j>i}\frac{(\sigma_1\sigma_2)(j)-(\sigma_1\sigma_2)(i)}{\sigma_2(j)-\sigma_2(i)}\cdot\prod_{j>i}\frac{\sigma_2(j)-\sigma_2(i)}{j-i}=$

$$= \prod_{j>i} \frac{\sigma_1[\sigma_2(j)] - \sigma_1[\sigma_2(i)]}{\sigma_2(j) - \sigma_2(i)} \cdot \prod_{j>i} \frac{\sigma_2(j) - \sigma_2(i)}{j - i}$$

Si probamos que $\prod_{j>i} \frac{\sigma_1[\sigma_2(j)] - \sigma_1[\sigma_2(i)]}{\sigma_2(j) - \sigma_2(i)} = \prod_{\sigma_2(j)>\sigma_2(i)} \frac{\sigma_1[\sigma_2(j)] - \sigma_1[\sigma_2(i)]}{\sigma_2(j) - \sigma_2(i)}$ (I)

el problema estaría resuelto. Siendo σ_2 una biyección de E en E los conjuntos $\{(\sigma_2(j), \sigma_2(i)) / \sigma_2(j) > \sigma_2(i)\}$ y $\{(j,i) / j > i\}$ son iguales. Luego los dos productos de (I) tienen el mismo número de factores. Veamos que cada factor del primer producto está en el segundo. Consideremos el factor $\frac{\sigma_1[\sigma_2(j)] - \sigma_1[\sigma_2(i)]}{\sigma_2(j) - \sigma_2(i)}$ con $j>i$.

Si $\sigma_2(j) > \sigma_2(i)$, este factor se encuentra en el segundo producto.
Si $\sigma_2(j) < \sigma_2(i)$, como $\frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} = \frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{\sigma_2(i) - \sigma_2(j)}$, también está en el segundo producto. Luego se verifica la igualdad (I).

Entonces, $\prod_{j>i} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} = \Pi(\sigma_1)$ y $\prod_{j>i} \frac{\sigma_2(j) - \sigma_2(i)}{j - i} = \Pi(\sigma_2)$

y, por tanto, $\Pi(\sigma_1 \sigma_2) = \Pi(\sigma_1) \cdot \Pi(\sigma_2)$. c.s.q.d.

3.3 Proposición: La aplicación $\Pi: S_n \longrightarrow \{-1, 1\}$ es sobre, es decir, en S_n hay permutaciones pares e impares, si $n>1$.

Demostr.: Una permutación par es la identidad en E, pues

$$\Pi(i_E) = \prod_{j>i} \frac{i_E(j) - i_E(i)}{j - i} = \prod_{j>i} \frac{j - i}{j - i} = 1$$

Toda transposición es de clase impar. Sea $\tau = (i,j)$, $(i<j)$.
Si $k, p < i$, k y p no forman inversión respecto de τ, pues $\tau(k) = k$ y $\tau(p) = p$. Análogamente, si $k, p > j$, tampoco forman inversión. Si $k \leq i$, k e i tampoco forman inversión, y si $k > j$ k y j tampoco forman inversión, pues $\tau(k) = k > j > i = \tau(j)$
Sea $k \in E$ tal que $i < k \leq j$. Entonces como $\tau(i) = j$ y $\tau(k) = k$ o $\tau(k) = i$, se tiene que $\tau(i) > \tau(k)$. Luego k e i forman inversión. Tenemos, entonces, $j - i$ inversiones (las que forman los elementos $j, i+1, i+2, \ldots, j-1$ con i). Ya hemos contado también la inversión de i con j pues hemos supuesto $i < k \leq j$. Veamos ahora las inversiones que forma j con los k tales que $i < k < j$.
Siendo $\tau(k) = k$ y $\tau(j) = i$, se tiene que j forma inversión con k.
De aquí obtenemos, entonces, $j - i - 1$ inversiones (las que forman $i+1, i+2, \ldots, j-1$). Luego $i_\tau = (j-i) + (j-i-1) = 2(j-i) - 1$

4. El grupo alternado A_n

Según hemos visto anteriormente, la aplicación π que a cada permutación hace corresponder el 1 o el -1 según sea par o impar es un homomorfismo de S_n en $\{-1, 1\}$. Veamos cuál es $\operatorname{Ker}\pi$

$\operatorname{Ker}\pi = \{\sigma \in S_n / \pi(\sigma) = 1\}$. Es decir, $\operatorname{Ker}\pi$ es el conjunto de permutaciones de S_n de clase par. A $\operatorname{Ker}\pi$ lo denotaremos por A_n. Entonces A_n es un subgrupo normal de S_n que llamamos grupo alternado.

Por el 1er Teorema de Isomorfía de grupos $S_n/\operatorname{Ker}\pi$ es isomorfo a $\pi(S_n)$. Siendo π sobre, $\pi(S_n) = \{-1, 1\}$. Luego

$$i(A_n) = o\left(S_n/A_n\right) = o(\pi(S_n)) = o(\{-1,1\}) = 2$$

Entonces, $o(A_n) = \dfrac{o(S_n)}{i(A_n)} = \dfrac{n!}{2}$

que demuestra que de las $n!$ permutaciones, la mitad son de clase par y la otra mitad de clase impar.

4.1. PROPOSICION: El número de transposiciones en que se descompone una permutación es siempre de la misma clase, es decir, par si $\pi(\sigma) = 1$ e impar si $\pi(\sigma) = -1$. (*)

Demostr.: Sea $\sigma = \prod_{i=1}^{h} \alpha_i$, siendo α_i transposiciones.

Entonces $\pi(\sigma) = \pi\left(\prod_{i=1}^{h} \alpha_i\right) = \prod_{i=1}^{h} \pi(\alpha_i) = (-1)^h$, pues la signatura de cualquier transposición es -1. Entonces, si $\pi(\sigma) = 1$, debe ser h par y si $\pi(\sigma) = -1$, h será impar. c.s.q.d.

DEFINICION: Un grupo se dice simple si no admite subgrupos normales propios.

Antes de demostrar un teorema muy importante en Teoría de Galois, vamos a demostrar dos lemas preliminares:

Lema 1: Si $n \geq 3$, A_n está generado por los 3-ciclos (ciclos de longitud 3).

Demostr.: Veamos que el producto de dos transposiciones se puede expresar como producto de 3-ciclos.

- Supongamos que las transposiciones tienen un elemento común:

Se comprueba que $(i,j)(j,p) = (i,j,p)$

(*) Sólo hemos demostrado la descomposición de una permutación como producto de transposiciones

- Si las transposiciones (i,j) y (k,p) no tienen ningún elemento común, siendo $(i,j)^2 = i_E$ cualquiera que sea la transposición tenemos $(i,j)(k,p) = (i,j)(j,k)(j,k)(k,p) = (i,j,k)\cdot(j,k,p)$.

Luego un producto de dos transposiciones se puede sustituir por un 3-cido equivalente o por un producto de dos 3-cidos.

Entonces, si $\sigma \in A_n$, σ se puede descomponer como un producto par de transposiciones. Agrupando estas transposiciones de dos en dos, queda probado que σ se puede descomponer en producto de 3-cidos, que prueba que los 3-cidos generan A_n. c.s.q.d.

Lema 2: Si $n \geq 5$ y H es un subgrupo normal de A_n, las proposiciones siguientes son equivalentes:

a) H contiene un producto de dos transposiciones disjuntas.

b) H contiene un 3-cido (cido de longitud 3).

c) $H = A_n$

Demostr.: **a) $\Rightarrow$ b)** Supongamos que H contiene a $\alpha = (i,j)(k,p)$ donde (i,j) y (k,p) son disjuntas.

Siendo $n \geq 5$, $\exists \ell \in E - \{i,j,k,p\}$. Sea $\sigma = (\ell, i, j)$. Entonces $\sigma \in A_n$, por ser un 3-cido. Como $\alpha \in H$ y $H \triangleleft A_n$ (H es subgrupo normal de A_n), $\sigma\alpha\sigma^{-1} \in H$. Pero $\sigma\alpha\sigma^{-1} = \sigma(i,j)(k,p)\sigma^{-1} =$
$= (\sigma(i), \sigma(j))\cdot(\sigma(k), \sigma(p)) = (j,\ell)(k,p)$. Luego $(j,\ell)(k,p) \in H$

Si $\alpha = (i,j)(k,p) \in H$, siendo H subgrupo, $\alpha^{-1} = [(i,j)(k,p)]^{-1} = (k,p)^{-1}(i,j)^{-1} =$
$= (k,p)(i,j) \in H$.

Luego $\sigma\alpha\sigma^{-1}\alpha^{-1} \in H$; pero $\sigma\alpha\sigma^{-1}\alpha^{-1} = (j,\ell)(k,p)(k,p)(i,j) =$
$= (j,\ell)(i,j) = (\ell,j)(j,i) = (\ell,j,i)$.

Luego H contiene un 3-cido.

b) $\Rightarrow$ c) Veamos que si H contiene un 3-cido (i,j,k) también contiene a cualquier otro 3-cido (r,s,t).

Sea $\sigma \in S_n$ tal que $\sigma(i) = r$, $\sigma(j) = s$ y $\sigma(k) = t$.

Si $\sigma \in A_n$, siendo $H \triangleleft A_n$, $\sigma(i,j,k)\sigma^{-1} \in H$.

Pero $\sigma(i,j,k)\sigma^{-1} = (\sigma(i), \sigma(j), \sigma(k)) = (r,s,t)$ que prueba que $(r,s,t) \in H$.

Supongamos que σ es de clase impar; siendo $n \geq 5$, $\exists u, n \in E - \{i,j,k\}$.

Siendo σ impar, como (u,n) es una transposición, también es impar; luego $\tau = \sigma(u,n)$ es de clase par, pues $\pi(\tau) = \pi(\sigma(u,n)) = \pi(\sigma)\cdot\pi(u,n) = (-1)(-1) = 1$.

Luego $\tau \in A_n$. Siendo $H \triangleleft A_n$, $\tau(i,j,k)\tau^{-1} \in H$.

Como $u, n \notin \{i,j,k\}$, (u,n) y (i,j,k) son disjuntos y, por tanto, con-

mutan. Luego $\tau(i,j,k)\tau^{-1} = [\sigma(m,n)](i,j,k)[\sigma(m,n)]^{-1} =$
$= \sigma(m,n)(i,j,k)(m,n)^{-1}\sigma^{-1} = \sigma(m,n)(i,j,k)(m,n)\sigma^{-1} =$
$= \sigma(i,j,k)(m,n)(m,n)\sigma^{-1} = \sigma(i,j,k)\sigma^{-1} = (r,s,t) \in H$.
Por tanto, H contiene a todos los ciclos de longitud 3 y, siendo subgrupo, contiene al grupo generado por los 3-ciclos, que es A_n. Luego $H = A_n$.

c) $\Rightarrow$ a) Sean i, j, k y ℓ cuatro elementos distintos dos a dos de E, que existen pues $n \geq 5$. Sea $\sigma = (i,j)(k,\ell)$. Entonces $\sigma \in A_n$ pues $\pi(\sigma) = \pi((i,j)) \cdot \pi((k,\ell)) = (-1)(-1) = 1$.
Luego, siendo $H = A_n$, $\sigma \in H$, que prueba que H contiene un producto de dos transposiciones disjuntas. c.s.q.d.

4.2. TEOREMA: Si $n \geq 5$, el grupo alternado A_n es simple.

Demostr.: Sea H un subgrupo normal de A_n no trivial, es decir, $H \neq \{i_E\}$. Se trata de probar que $H = A_n$.
Si $H \neq \{i_E\}$, $\exists \alpha \in H / \alpha \neq i_E$. Sea $\alpha = \prod_{i=1}^{r} \alpha_i$ la descomposición de α como producto de ciclos disjuntos; siendo disjuntos estos ciclos conmutan. Podemos suponer entonces que $\text{long}(\alpha_1) \leq \ldots \leq \text{long}(\alpha_r)$.
Consideraremos cuatro casos:
1er caso: $\text{long}(\alpha_r) > 3$. Sea $\alpha_r = (i_1, \ldots, i_m)$ con $m > 3$.
Sea $\sigma = (i_1, i_2, i_3)$. Siendo $\text{long}(\sigma) = 3$, $\sigma \in A_n$.
Como $H \triangleleft A_n$, $\sigma\alpha\sigma^{-1} \in H$.
El ciclo σ solo mueve elementos de α_r; los elementos de los ciclos $\alpha_1, \ldots, \alpha_{r-1}$ permanecen invariantes por σ, ya que $\alpha_1, \ldots \alpha_{r-1}$ son disjuntos con α_r. Entonces, $\forall i \in \{1, \ldots, r-1\}$, $\sigma\alpha_i\sigma^{-1} = \alpha_i\sigma\sigma^{-1} = \alpha_i$. Entonces:
$\sigma\alpha\sigma^{-1} = \sigma\alpha_1\alpha_2\cdots\alpha_{r-1}\alpha_r\sigma^{-1} =$
$= \sigma\alpha_1\sigma^{-1}\sigma\alpha_2\sigma^{-1}\cdot\ldots\cdot\sigma\alpha_{r-1}\sigma^{-1}\cdot\sigma\alpha_r\sigma^{-1} = \alpha_1\alpha_2\cdots\alpha_{r-1}(\sigma\alpha_r\sigma^{-1}) =$
$= \left(\prod_{i=1}^{r-1}\alpha_i\right)(\sigma\alpha_r\sigma^{-1})$

Pero $\sigma\alpha_r\sigma^{-1} = \sigma(i_1, i_2, i_3, i_4, \ldots, i_m)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \sigma(i_3), \sigma(i_4), \ldots, \sigma(i_m)) =$
$= (i_2, i_3, i_1, i_4, \ldots, i_m)$, pues $\sigma = (i_1, i_2, i_3)$
Luego $\sigma\alpha\sigma^{-1} = \alpha_1\alpha_2\ldots\alpha_{r-1}(i_2, i_3, i_1, i_4, \ldots, i_m)$
Entonces $\alpha^{-1}\sigma\alpha\sigma^{-1} = (\alpha_1\alpha_2\cdots\alpha_{r-1}\alpha_r)^{-1}\alpha_1\alpha_2\cdots\alpha_{r-1}\cdot(i_2, i_3, i_1, i_4, \ldots, i_m) =$
$= \alpha_r^{-1}\alpha_{r-1}^{-1}\cdots\alpha_2^{-1}\alpha_1^{-1}\alpha_1\alpha_2\cdots\alpha_{r-1}(i_2, i_3, i_1, i_4, \ldots, i_m) = \alpha_r^{-1}(i_2, i_3, i_1, i_4, \ldots, i_m)$

Si $\alpha_r = (i_1, i_2, i_3, \ldots, i_{m-1}, i_m)$, $\alpha_r(i_1) = i_2$, $\alpha_r(i_2) = i_3, \ldots, \alpha_r(i_{m-1}) = i_m$, entonces
$i_{m-1} = \alpha_r^{-1}(i_2)$, $i_{m-2} = \alpha_r^{-1}(i_3)$, $\ldots$, $i_2 = \alpha_r^{-1}(i_{m-1})$, $i_1 = \alpha_r^{-1}(i_m)$, y por tanto $\alpha_r^{-1} = (i_m, i_{m-1}, \ldots, i_3, i_2, i_1)$

Entonces $\alpha^{-1}\tau\alpha\tau^{-1} = (i_m, i_{m-1}, \dots, i_2, i_1)(i_2, i_3, i_1, i_4, \dots, i_m) =$
$= (i_1, i_3, i_m)$ (I)

por lo siguiente:

$(\alpha^{-1}\tau\alpha\tau^{-1})(i_1) = \alpha^{-1}[\tau\alpha\tau^{-1}(i_1)] = \alpha^{-1}(i_4) = i_3$

$(\alpha^{-1}\tau\alpha\tau^{-1})(i_2) = \alpha^{-1}[\tau\alpha\tau^{-1}(i_2)] = \alpha^{-1}(i_3) = i_2$

$(\alpha^{-1}\tau\alpha\tau^{-1})(i_3) = \alpha^{-1}[\tau\alpha\tau^{-1}(i_3)] = \alpha^{-1}(i_1) = i_m$

$(\alpha^{-1}\tau\alpha\tau^{-1})(i_m) = \alpha^{-1}[\tau\alpha\tau^{-1}(i_m)] = \alpha^{-1}(i_2) = i_1$

Comprobar que $\forall k \in \{4,5,\dots,m-2,m-1\}$, $\alpha^{-1}\tau\alpha\tau^{-1}(i_k) = i_k$. Entonces:

$$\alpha^{-1}\tau\alpha\tau^{-1} = \begin{pmatrix} i_1 & i_3 & i_m & i_2 & i_4 & \dots & i_{m-1} \\ i_3 & i_m & i_1 & i_2 & i_4 & \dots & i_{m-1} \end{pmatrix} = (i_1, i_3, i_m)$$

Como $\tau\alpha\tau^{-1} \in H$ y $\alpha^{-1} \in H$, pues H es subgrupo, tenemos que $\alpha^{-1}\tau\alpha\tau^{-1} \in H$. Luego H es un subgrupo normal de A_n y contiene un 3-ciclo. Entonces, por el lema 2 debe ser $H = A_n$.

2º caso: $\text{long}(\alpha_r) = 3$ y $\text{long}(\alpha_{r-1}) = 3$.

Sea $\alpha_r = (i_1, i_2, i_3)$ y $\alpha_{r-1} = (i_4, i_5, i_6)$.

Tomemos $\tau = (i_2, i_3, i_4)$. Entonces τ es un 3-ciclo y, por tanto, $\tau \in A_n$.

Como $H \trianglelefteq A_n$, $\tau\alpha\tau^{-1} \in H$. Además: ($H$ subgrupo) $\wedge$ ($\alpha \in H$) $\Rightarrow$ ($\alpha^{-1} \in H$).

Entonces $\alpha^{-1}\tau\alpha\tau^{-1} \in H$.

τ solo mueve elementos de α_{r-1} y α_r; luego $\forall k \in \{1,\dots,r-2\}$, $\tau\alpha_k\tau = \alpha_k$.

Entonces: $\alpha^{-1}\tau\alpha\tau^{-1} = \alpha_r^{-1}\alpha_{r-1}^{-1}\cdots\alpha_2^{-1}\alpha_1^{-1}\alpha_1\alpha_2\cdots\alpha_{r-2}\,\tau\alpha_{r-1}\tau^{-1}\,\tau\alpha_r\tau^{-1} =$

$= \alpha_r^{-1}\alpha_{r-1}^{-1}\,\tau\alpha_{r-1}\tau^{-1}\,\tau\alpha_r\tau^{-1} = (i_1, i_2, i_3)^{-1}(i_4, i_5, i_6)^{-1}(\tau(i_4), \tau(i_5), \tau(i_6))(\tau(i_1), \tau(i_2), \tau(i_3)) =$

$= (i_3, i_2, i_1)(i_6, i_5, i_4)(i_2, i_5, i_6)(i_1, i_3, i_4) =$

$\overset{(*)}{=} \begin{pmatrix} i_1 & i_2 & i_4 & i_3 & i_6 & i_5 \\ i_2 & i_4 & i_3 & i_6 & i_1 & i_5 \end{pmatrix} = (i_1, i_2, i_4, i_3, i_6)$

Entonces $(i_1, i_2, i_4, i_3, i_6) \in H$. Por tanto, H contiene un ciclo de longitud mayor que 3. Entonces, por el primer caso H debe contener un 3-ciclo, y por tanto, será $H = A_n$.

3er caso: $\text{long}(\alpha_r) = 3$ y $\alpha_1, \dots, \alpha_{r-1}$ son transposiciones (2-ciclos).

Sea $\alpha_r = (i_1, i_2, i_3)$. Si $\alpha \in H$, $\alpha^2 \in H$, pues H es subgrupo.

Pero $\alpha^2 = \alpha_1\alpha_2\cdots\alpha_r\,\alpha_1\alpha_2\cdots\alpha_r = \alpha_1^2\alpha_2^2\cdots\alpha_{r-1}^2\alpha_r^2$ (**)

Siendo $\alpha_1, \dots, \alpha_{r-1}$ transposiciones tenemos que $\alpha_1^2 = \dots = \alpha_{r-1}^2 = i_E$.

Luego $\alpha^2 = \alpha_r^2$. Pero α_r es un 3-ciclo; luego $o(\alpha_r) = 3$, es decir $\alpha_r^3 = i_E \Rightarrow \alpha_r^2 = \alpha_r^{-1}$. Por tanto, $\alpha^2 = \alpha_r^2 = \alpha_r^{-1} = (i_3, i_2, i_1) \in H$

(*) $\alpha^{-1}\tau\alpha\tau^{-1}(i_1) = i_2$ pues si llamamos $\beta_1 = (i_3, i_2, i_1)$, $\beta_2 = (i_6, i_5, i_4)$, $\beta_3 = (i_2, i_5, i_6)$, $\beta_4 = (i_1, i_3, i_4)$ tenemos $\alpha^{-1}\tau\alpha\tau^{-1} = \beta_1\beta_2\beta_3\beta_4$ y entonces $\alpha^{-1}\tau\alpha\tau^{-1}(i_1) = \beta_1\beta_2\beta_3\beta_4(i_1) = i_2$ pues $\beta_4(i_1) = i_3$, β_3 y β_2 no mueven i_3 y $\beta_1(i_3) = i_2$, es decir $\beta_1\beta_2\beta_3\beta_4(i_1) = \beta_1\beta_2\beta_3(i_3) = \beta_1\beta_2(i_3) = \beta_1(i_3) = i_2$

(**) Esta última igualdad es cierta, porque siendo los ciclos disjuntos, conmutan.

Luego H contiene un 3-ciclo. Siendo $H \triangleleft A_n$ debe ser $H = A_n$.

4º caso: $\alpha_1, \alpha_2, \dots, \alpha_r$ son transposiciones.

Sean $\alpha_r = (i_1, i_2)$ y $\alpha_{r-1} = (i_3, i_4)$. Sea $\sigma = (i_2, i_3, i_4)$

Análogamente a los casos anteriores $\alpha^{-1}\sigma\alpha\sigma^{-1} \in H$.

Pero $\alpha^{-1}\sigma\alpha\sigma^{-1} = \alpha_r^{-1}\alpha_{r-1}^{-1}\cdots\alpha_1^{-1}\alpha_1\cdots\alpha_{r-2}\sigma\alpha_{r-1}\sigma^{-1}\sigma\alpha_r\sigma^{-1} =$

$= \alpha_r^{-1}\alpha_{r-1}^{-1}(\sigma\alpha_{r-1}\sigma^{-1})(\sigma\alpha_r\sigma^{-1}) \overset{(*)}{=} \alpha_r\alpha_{r-1}(\sigma\alpha_{r-1}\sigma^{-1})(\sigma\alpha_r\sigma^{-1}) =$

$= (i_1, i_2)(i_3, i_4)(\sigma(i_3), \sigma(i_4))(\sigma(i_1), \sigma(i_2)) = (i_1, i_2)(i_3, i_4)(i_4, i_2)(i_1, i_3) =$

$= \begin{pmatrix} i_1 & i_4 & i_2 & i_3 \\ i_4 & i_1 & i_3 & i_2 \end{pmatrix} = (i_1, i_4)(i_2, i_3)$

Luego H contiene un producto de dos transposiciones disjuntas. Siendo $H \triangleleft A_n$, en virtud del lema 2 tenemos que $H = A_n$.

Luego, en cualquier caso, $H = A_n$. c.s.q.d.

4.3. TEOREMA: Si $n \geq 5$, A_n es el único subgrupo normal propio de S_n.

Demostr.: Sea H un subgrupo normal no trivial de S_n. Entonces $H \cap A_n$ es subgrupo normal de A_n, pues

$\forall g \in A_n, \forall x \in H \cap A_n$, $gxg^{-1} \in H \cap A_n$ ya que $g, x \in A_n \Rightarrow gxg^{-1} \in A_n$ y $(H \triangleleft S_n) \wedge (g \in A_n \subset S_n) \wedge (x \in H) \Rightarrow gxg^{-1} \in H$.

Si $H \cap A_n \triangleleft A_n$, siendo A_n simple debe ser $H \cap A_n = A_n$ o bien $H \cap A_n = \{i_E\}$.

1er caso: $H \cap A_n = A_n$.

Entonces $A_n \subset H$; luego $i(H) \leq i(A_n) = 2$. Luego $i(H) = 1$ o $i(H) = 2$

Si $i(H) = 1 \Rightarrow S_n/H = \{\bar{1}\}$ donde $\bar{1}$ es el neutro del grupo cociente. Si $S_n/H = \{\bar{1}\}$, debe ser $H = S_n$.

Si $i(H) = 2$, como $A_n \subset H$ y $i(A_n) = i(H)$, por el teorema de Lagrange debe ser $H = A_n$.

2º caso: $H \cap A_n = \{i_E\}$.

Probemos por reducción al absurdo que $o(H) > 2$. Supongamos que fuese $o(H) = 2$. Entonces H es cíclico. Sea $H = \langle\alpha\rangle$, $\alpha \neq i_E$. Debe ser $\alpha^2 = i_E$. Sea $\alpha = \alpha_1 \cdots \alpha_r$ la descomposición de la permutación α como producto de ciclos disjuntos.

Entonces $\alpha^2 = \alpha_1^2 \cdot \alpha_2^2 \cdots \alpha_r^2 = i_E$; siendo α_i disjunto con α_j, $\forall i \neq j$, debe ser $\alpha_i^2 = i_E$, $\forall i \in \{1, \dots, r\}$. Por tanto, α_i es una transposición.

a) Supongamos que α es una transposición, $\alpha = (i, j)$.

Veamos que H no puede ser, entonces, normal en S_n.
Sea $\sigma \in S_n$ tal que $\sigma(i)=k$, $\sigma(j)=l$, con $k \neq l$ y $k,l \notin \{i,j\}$.
Entonces $\sigma\alpha\sigma^{-1}=(k,l) \notin H$.
b) Supongamos entonces que $\alpha=(i,j)(k,l)(s,t)\ldots$; tengamos en cuenta que α no puede se producto de dos transposiciones, pues las permutaciones de H deben ser impares, excepto i_E, pues $H \cap A_n=\{i_E\}$.
Tenemos $\sigma \in S_n$ tal que: $\sigma(i)=k, \sigma(j)=s, \sigma(k)=i, \sigma(l)=t, \sigma(s)=j, \sigma(t)=l$ dejando fijos los restantes elementos de E.
Entonces $\sigma\alpha\sigma^{-1}=(\sigma(i),\sigma(j))(\sigma(k),\sigma(l))(\sigma(s),\sigma(t))\ldots =$
$=(k,s)(i,t)(j,l)\ldots$
y ésta no pertenece a H, pues $\sigma\alpha\sigma^{-1} \neq i_E$ (trivial) y $\sigma\alpha\sigma^{-1} \neq \alpha$, pues $\sigma\alpha\sigma^{-1}(i)=t$ y $\alpha(i)=j$.

No puede ser entonces $o(H)=2$. Será, por tanto, $o(H)>2$.
Luego $\exists \alpha_1, \alpha_2 \in H / i_E \neq \alpha_1 \neq \alpha_2 \neq i_E$.
Siendo $H \cap A_n=\{i_E\}$ tenemos que $\pi(\alpha_1)=\pi(\alpha_2)=-1$.
Siendo H subgrupo, $\alpha_1^2 \in H$. Como $\pi(\alpha_1^2)=(-1)(-1)=1$, debe ser $\alpha_1^2=i_E$. Por otro lado $\pi(\alpha_1\alpha_2)=(-1)(-1)=1$. Análogamente, $\alpha_1\alpha_2=i_E$.
Hemos llegado a una contradicción, pues por un lado $\alpha_1^{-1}=\alpha_1$ y por otro $\alpha_1^{-1}=\alpha_2$. Luego no puede darse el caso $H \cap A_n=\{i_E\}$.
Se da entonces el 1er caso y queda probado que, si H es subgrupo normal propio de S_n, entonces $H=A_n$. c.s.q.d.

TEMA 4º: TEOREMAS DE SYLOW

1. Producto de dos subgrupos

DEFINICION: Sea G un grupo y H y K dos subgrupos de G. Definimos el producto de los subgrupos H y K como el conjunto

$$H\cdot K = \{hk \,/\, h\in H \wedge k\in K\}$$

En general, $H\cdot K$ no será subgrupo de G. Vamos a dar una condición necesaria y suficiente para que $H\cdot K$ sea subgrupo, pero antes demostraremos el siguiente:

1.1. LEMA: Sea G un grupo. Definimos $S^- = \{x^{-1}\in G \,/\, x\in S\}$, siendo $S\subset G$.
Entonces, S es subgrupo de G si y solo si $S^- = S$ y $S\cdot S = S$

Demostr: $\Rightarrow$ Si S es subgrupo, $\forall x\in S,\ x^{-1}\in S \Rightarrow (x^{-1})^{-1}\in S^- \Rightarrow x\in S^-$
Luego $S\subset S^-$. Analogamente, $\forall x\in S^-,\ x^{-1}\in S \Rightarrow (x^{-1})^{-1} = x\in S$. Luego $S^-\subset S$
Ademas $[\forall x,y\in S,\ x\cdot y\in S] \Rightarrow S\cdot S\subset S$
y $[\forall x\in S,\ x = x\cdot e\in S\cdot S] \Rightarrow S\subset S\cdot S$
$\Rightarrow S\cdot S = S$

$\Leftarrow$ (S es subgrupo de G) $\Leftrightarrow$ ($\forall x,y\in S,\ xy^{-1}\in S$)
Siendo $S = S^-$, $\forall y\in S,\ y^{-1}\in S$. Luego
$\forall x,y\in S,\ x,y^{-1}\in S \Rightarrow xy^{-1}\in S$, pues $S\cdot S = S$. c.s.q.d.

1.2. PROPOSICION: Sea G un grupo y H y K subgrupos de G. Es condición necesaria y suficiente para que $H\cdot K$ sea subgrupo de G que $HK = KH$.

Demostr: $\Rightarrow$ Si HK es subgrupo, $(HK)^- = HK$.
Pero $(HK)^- = \{(hk)^{-1} \,/\, h\in H \text{ y } k\in K\} = \{k^{-1}h^{-1} \,/\, h\in H \text{ y } k\in K\}$
Luego $(HK)^- = K^-H^-$
Siendo H y K subgrupos, $H^- = H$ y $K^- = K$. Entonces:
$HK = K^-H^- = KH$

$\Leftarrow$ Veamos que si $HK = KH$, entonces $(HK)^- = HK$ y $(HK)(HK) = HK$.
$(HK)^- = K^-H^- = KH = HK$
$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = H\cdot K$, pues H y K son subgrupos y, por tanto, $HH = H$ y $KK = K$. c.s.q.d.

Veamos algunos ejemplos en el que el producto de dos subgrupos es un subgrupo.

EJEMPLOS: ① Si H y K son subgrupos de un grupo G tales que H está contenido en el normalizador de K, entonces HK es subgrupo de G.
Si $H\subset N(K) \Rightarrow (\forall h\in H,\ hKh^{-1} = K) \Rightarrow (\forall h\in H,\ hK = Kh) \Rightarrow (HK = KH) \Rightarrow$
$\Rightarrow$ (HK es subgrupo de G)

② Si H es subgrupo normal de G (ó K, no necesariamente ambos) entonces HK es subgrupo de G.

Si $H \triangleleft G \Rightarrow N(H) = G$. Como $K \subset G = N(H)$, según ①, HK es subgrupo de G.

1.3. PROPOSICION: Sean $H_1, H_2, \dots, H_n$ subgrupos de G. Entonces si $\forall i \in \{2, \dots, n\}$, $(H_1 \cdots H_{i-1})\, H_i = H_i \cdot (H_1 \cdots H_{i-1})$ se verifica que $H_1 \cdot H_2 \cdots H_n$ es subgrupo de G.

Demostr: Procederemos por inducción sobre el número de subgrupos:
- Si $i=2$, por hipótesis $H_1 H_2 = H_2 H_1$; luego $H_1 H_2$ es subgrupo de G.
- Si $H_1 \cdots H_{n-1}$ es subgrupo de G, siendo H_n subgrupo y verificándose por hipótesis que $(H_1 \cdots H_{n-1}) H_n = H_n (H_1 \cdots H_{n-1})$, tenemos que $H_1 \cdots H_{n-1} \cdot H_n$ es subgrupo de G. c.s.q.d.

1.4. COROLARIO: Si los subgrupos $H_1, \dots, H_n$ conmutan dos a dos, el producto $H_1 \cdots H_n$ es subgrupo de G.

La demostración es trivial si tenemos en cuenta que la condición de que $H_p H_q = H_q H_p$, $\forall p, q \in \{1, \dots, n\}$ implica que $\forall i \in \{2, \dots, n\}$, $(H_1 \cdots H_{i-1}) H_i = H_i (H_1 \cdots H_{i-1})$.

2. TEOREMAS DE ISOMORFIA.

2.1. PROPOSICION: a) Sean G y G' dos grupos y $f: G \to G'$ un homomorfismo. Entonces:

$$G/\mathrm{Ker}\, f \simeq \mathrm{Im}\, f$$

b) Un subgrupo H de un grupo G es normal en G si y solo si H es el núcleo de un homomorfismo de G en otro grupo.

Demostr: a) Definimos una aplicación φ como sigue:

$$\varphi: G/\mathrm{Ker}\, f \longrightarrow \mathrm{Im}\, f$$
$$x \cdot \mathrm{Ker}\, f \longmapsto f(x)$$

- φ está bien definida: $x\,\mathrm{Ker}\, f = y\,\mathrm{Ker}\, f \Rightarrow x^{-1} y\,\mathrm{Ker}\, f = \mathrm{Ker}\, f \Rightarrow$
$\Rightarrow x^{-1} y \in \mathrm{Ker}\, f \Rightarrow x^{-1} y \in \mathrm{Ker}\, f \Rightarrow f(x^{-1} y) = e' \Rightarrow f(x^{-1}) f(y) = e' \Rightarrow f(x) = f(y)$.
- φ es homomorfismo: $\varphi[(x\,\mathrm{Ker}\, f)(y\,\mathrm{Ker}\, f)] = \varphi[(xy)\,\mathrm{Ker}\, f] = f(xy) = f(x) f(y)$.
- φ es inyectiva: $f(x) = f(y) \Rightarrow \begin{cases} f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \mathrm{Ker}\, f \\ f(x^{-1}y) = e' \Rightarrow x^{-1}y \in \mathrm{Ker}\, f \end{cases} \Rightarrow$

$$\Rightarrow \begin{cases} x \in y\,\mathrm{Ker}\, f \\ y \in x\,\mathrm{Ker}\, f \end{cases} \Rightarrow \begin{cases} x\,\mathrm{Ker}\, f \subset y\,\mathrm{Ker}\, f \\ y\,\mathrm{Ker}\, f \subset x\,\mathrm{Ker}\, f \end{cases} \Rightarrow x\,\mathrm{Ker}\, f = y\,\mathrm{Ker}\, f.$$

- φ es sobre: $\forall y \in \mathrm{Im}\, f$, $\exists x \in G / y = f(x)$. Dado $x \in G$, $x\,\mathrm{Ker}\, f \in G/\mathrm{Ker}\, f$. Además $\varphi(x\,\mathrm{Ker}\, f) = f(x) = y$.

b) $\Rightarrow$| Si $H \lhd G$, podemos considerar el grupo cociente G/H. La aplicación canónica $p: G \longrightarrow G/H$, $x \longmapsto xH$ es un homomorfismo y

Se verifica que $\operatorname{Ker} p = H$.

$\Leftarrow$| Si H es el núcleo de un homomorfismo $h: G \to G'$, H es un subgrupo normal de G. c.s.q.d.

2.2. TEOREMA: (Teorema fundamental del homomorfismo de grupos)

Sea $f: G \longrightarrow G'$ un homomorfismo suprayectivo. Entonces, f induce una biyección entre los subgrupos de G que contienen a $\operatorname{Ker} f$ y los subgrupos de G'. Además, si H es un subgrupo de G que contiene a $\operatorname{Ker} f$ se verifica que H es normal en G si y solo si $f(H)$ es normal en G'. (*)

Demostr: * La aplicación inducida por f hará corresponder a cada subgrupo H de G con $H \supset \operatorname{Ker} f$ el subgrupo de G' $f(H)$.

- Esta aplicación inducida es inyectiva: Sean H_1 y H_2 subgrupos de G que contienen a $\operatorname{Ker} f$. Probaremos que si $f(H_1) = f(H_2)$ entonces $H_1 = H_2$.

Probemos antes que si $H \supset \operatorname{Ker} f$ entonces $f^{-1}[f(H)] = H$.

Siempre se verifica que $H \subset f^{-1}[f(H)]$.

Sea entonces $x \in f^{-1}[f(H)]$. Entonces, $\exists h \in H / f(x) = f(h) \Rightarrow f(xh^{-1}) = e'$

Luego $xh^{-1} \in \operatorname{Ker} f$. Como $H \supset \operatorname{Ker} f$, $xh^{-1} \in H \Rightarrow xh^{-1}h \in H \Rightarrow x \in H$.

Se tiene, en definitiva, que $f^{-1}[f(H)] = H$.

Por tanto, $f(H_1) = f(H_2) \Rightarrow f^{-1}[f(H_1)] = f^{-1}[f(H_2)] \Rightarrow H_1 = H_2$.

- La aplicación inducida por f es sobre: Sea H' subgrupo de G'.

Entonces $H = f^{-1}(H')$ es subgrupo de G, pues la contraimagen de un subgrupo por un homomorfismo es un subgrupo.

Además, $e' \in H' \Rightarrow f^{-1}(\{e'\}) \subset f^{-1}(H') \Leftrightarrow \operatorname{Ker} f \subset H$

Veamos que $f(H) = H'$.

Siendo f sobre, $f(H) = f[f^{-1}(H')] = H'$

** Sabemos (por TEOREMA 10.1, TEMA 7º, ALGEBRA I) que si H es subgrupo normal de G, entonces $f(H)$ es subgrupo normal de $\operatorname{Im} f = G'$ (pues f es sobre).

Probemos, entonces, que si $f(H) \lhd G' \Rightarrow H \lhd G$.

Si $f(H) \lhd G' \Rightarrow f^{-1}(f(H)) \lhd G$. Pero, en este caso y como consecuencia de que $H \supset \operatorname{Ker} f$, $f^{-1}(f(H)) = H$. Luego $H \lhd G$. c.s.q.d.

De este teorema vamos a sacar un corolario muy importante que nos dice como son los subgrupos en el grupo cociente G/N siendo $N \lhd G$.

2.3. COROLARIO: Sea G un grupo y N un subgrupo normal de G. Entonces la aplicación canónica $p: G \twoheadrightarrow G/N$ induce una biyección entre los subgrupos de G que contienen a N y los subgrupos de G/N. Además, si H es un subgrupo de G que contiene a N, $(H/N \lhd G/N) \Leftrightarrow (H \lhd G)$

La demostración es trivial si tenemos en cuenta que p es un homomorfismo suprayectivo de G en el grupo cociente G/N, que si H es un subgrupo que contiene a N entonces $p(H) = H/N$ y que $N = \operatorname{Ker} p$.
El hecho de que la aplicación inducida sea sobre implica que si H' es un subgrupo de G/N, H' es de la forma H/N donde H es un subgrupo de G que contiene a N.
El hecho de que la aplicación inducida sea inyectiva implica que si $H_1/N = H_2/N$ entonces $H_1 = H_2$, siempre que $H_1 \supset N$ y $H_2 \supset N$.

2.4.: 1er TEOREMA DE ISOMORFIA:

Sea G un grupo y H y K subgrupos normales de G de modo que $H \supset K$. Entonces

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

Demostr.: Consideremos la aplicación

$$\theta: G/K \longrightarrow G/H$$
$$xK \longmapsto \theta(xK) = xH$$

- θ está bien definida: es decir $xK = yK \Rightarrow xH = yH$

$$xK = yK \Rightarrow \begin{cases} x \in yK \\ y \in xK \end{cases} \Rightarrow \begin{cases} x \in yH \\ y \in xH \end{cases} \quad \text{pues } K \subset H$$

Entonces $\begin{cases} xH \subset yH \\ yH \subset xH \end{cases} \Rightarrow xH = yH$

- θ es homomorfismo suprayectivo: $\forall x, y \in G$, $\theta[(xK)(yK)] = \theta[(xy)K] = (xy)H = (xH)(yH)$. θ es sobre, trivialmente.
- Veamos que $\operatorname{Ker}\theta = H/K$:
  $\operatorname{Ker}\theta = \{xK \in G/K \,/\, \theta(xK) = xH = H\}$ y $H/K = \{hK / h \in H\}$.
  Si $xK \in \operatorname{Ker}\theta \Rightarrow xH = H \Rightarrow xe \in H \Rightarrow x \in H \Rightarrow xK \in H/K$
  Si $xK \in H/K \Rightarrow x \in H \Rightarrow xH = H \Rightarrow xK \in \operatorname{Ker}\theta$.
  $\Rightarrow \operatorname{Ker}\theta = H/K$.
- Siendo θ sobre, $\operatorname{Im}\theta = G/H$

Como $\operatorname{Im}\theta \simeq \frac{G/K}{\operatorname{Ker}\theta}$ se tiene que $G/H \simeq \frac{G/K}{H/K}$. c.q.d.

2.5. 2º TEOREMA DE ISOMORFIA:

Sea G un grupo y H y K dos subgrupos de G tales que $H \subset N(K)$. (*)
Entonces:
a) $H \cap K$ es subgrupo normal de H
b) K es subgrupo normal de HK.
c) $H \cdot K/K \simeq H/H\cap K$

Demostr.: a) Hay que probar que $\forall h \in H$, $h(H\cap K)h^{-1} \subset H\cap K$.
Dado $h\in H$, $\forall x \in H\cap K$, $x\in H \wedge x\in K \Rightarrow hxh^{-1}\in H \wedge hxh^{-1}\in K$ pues $H\subset N(K)$. Luego $\forall h\in H, \forall x\in H\cap K$, $hxh^{-1}\in H\cap K$.
Por tanto $H\cap K \lhd H$.

b) Que HK es subgrupo de G es claro pues $H\subset N(K)$ (ejemplo ①).
Veamos que $K \lhd HK$ o lo que es equivalente que $HK \subset N(K)$
Si $H\subset N(K) \Rightarrow HK \subset N(K)\cdot K \subset N(K)\cdot N(K)$ ya que todo conjunto está contenido en su normalizador. Siendo $N(K)$ subgrupo, $N(K)\cdot N(K) = N(K)$
Luego $HK \subset N(K)$.

c) Definimos la aplicación

$$\begin{aligned} p: H &\longrightarrow HK/K \\ h &\longmapsto p(h) = hK \end{aligned}$$

Está bien definida, pues $\forall h\in H$, $h\in HK$
- p es homomorfismo, pues $\forall h,h'\in H$, $p(hh') = (hh')K = (hK)(h'K) = p(h)p(h')$
- p es sobre, pues si $gK \in HK/K$, existen $h\in H$ y $c\in K$ tal que $g = hc$. Entonces, como $cK = K$, $p(h) = hK = hcK = gK$.
- $\operatorname{Ker} p = H\cap K$, pues siendo $\operatorname{Ker} p = \{h\in H / hK = K\}$ se tiene que
$(x\in \operatorname{Ker} p) \Leftrightarrow [(xK = K) \wedge (x\in H)] \Rightarrow [(x\in K)\wedge(x\in H)] \Rightarrow [x\in H\cap K]$
$(x\in H\cap K) \Rightarrow [(x\in H)\wedge(xK = K)] \Rightarrow [x\in \operatorname{Ker} p]$.

Entonces siendo $H/\operatorname{Ker} p \simeq \operatorname{Im} p$, e $\operatorname{Im} p = HK/K$ se tiene que:

$$H/H\cap K \simeq HK/K \quad \text{c.s.q.d.}$$

3. TEOREMAS DE SYLOW

DEFINICIONES: ① Si p es un número primo, se llama un p-grupo a un grupo G de orden p^n, con $n\geq 0$. (**)
② Sea p un número primo y G un grupo. Se dice que H es un p-subgrupo de G si H es subgrupo de G y H es un p-grupo.

(a) Aquí podríamos imponer la condición de que K sea subgrupo normal de G, pero esta

si $o(H) = p^K$, $K \geq 0$.

③ p-Subgrupos de Sylow: Sea G un grupo finito y p un número primo. Se dice que H es un p-subgrupo de Sylow de G si $o(H) = p^n$, y p^n es la mayor potencia de p que divide a $o(G)$.

3.1. PROPOSICION: Si G es un grupo finito abeliano y p es un número primo que divide a $o(G)$, entonces en G existe al menos un elemento de orden p.

Demostr.: Si $p = 1$, el teorema es trivial, pues e es un elemento de orden 1.
Supongamos que $o(G) = n = mp$ y $p \neq 1$.
Procederemos por inducción sobre m:
- Si $m = 1$, el orden de G sería el número primo p, por tanto, G debe ser cíclico (pues dado $a \in G - \{e\}$ se tiene que $\langle a \rangle$ es subgrupo de G, con $o(\langle a \rangle) \geq 2$; entonces $(o(\langle a \rangle) \mid o(G) = p) \wedge (p \text{ primo}) \Rightarrow o(\langle a \rangle) = o(G)$).
Si $G = \langle a \rangle$, entonces a es un elemento de orden p.
- Supongamos que, cualquiera que sea el grupo G' de orden Kp con $K < m$, existe en G' un elemento de orden p.
Sea G un grupo de orden mp ($m \geq 2$). Entonces G admite un subgrupo propio H, pues una condición necesaria y suficiente para que G no admita subgrupos propios (Problema 2, Tema 1) es que G sea cíclico de orden primo, y mp no es primo. Entonces, $o(H) < o(G)$.
Si $p \mid o(H)$, por hipótesis de inducción, existe en H un elemento de orden p, y, por tanto, existe en G un elemento de orden p.
Si p no$\mid o(H)$, siendo $o(G) = o(H)\, i(H)$ (*), se tiene que $p \mid i(H)$, es decir, $p \mid o(G/H)$.
Como $o(H) > 1$, $o(G/H) < o(G)$. Entonces, por hipótesis de inducción, existe en G/H un elemento $\bar{x}$ de orden p.
Si $\bar{x} \in G/H$, $x \in G$. Supongamos que $o(x) = r$. Entonces $x^r = e$ y también $\bar{x}^r = \overline{x^r} = \bar{e}$.
Como $o(\bar{x}) = p \wedge \bar{x}^r = \bar{e}$ debe ser $p \mid r$.
Sea K el subgrupo cíclico de G engendrado por x: $K = \langle x \rangle$
Entonces $o(K) = r$. Luego $p \mid o(K)$. Según COROLARIO 4.2 (Tema 1º) dado un grupo cíclico de orden N, para cada divisor d de N existe un único subgrupo de orden d, y, por tanto, un único elemento de orden d. Luego siendo K cíclico, $o(K) = r$ y $p \mid r$, existe un elemento y en K, y por tanto

en 6, que es de orden p. csqd.

3.2. TEOREMA: (*) Sea 6 un grupo finito de orden n. Sea p un número primo tal que $p^r \mid o(6)$; entonces existe en 6 un subgrupo de orden p^r.

Demostr.: Procederemos por inducción sobre n.

* Si n = 1, el teorema es trivial, pues sería $6 = \{e\}$. Podríamos haber puesto la condición de que p sea distinto de 1; en este caso la inducción empezaría para n = 2, pero el teorema seguiría siendo cierto trivialmente, pues si $p^r \mid 2 \Rightarrow p^r = 1$ o $p^r = 2$, y $\{e\}$ y 6 son subgrupos de 6.

* Supongamos que todo grupo finito 6' de orden menor que n, admite un subgrupo de orden p^r si $p^r \mid o(6')$. Probaremos que si $o(6) = n$ y $p^r \mid n$ entonces 6 admite un subgrupo de orden p^r.

  - Si 6 no admite subgrupos propios, entonces o(6) sería primo. Como $p^r \mid o(6)$ y o(6) es primo debe ser $o(6) = p$ y $r = 1$. Entonces, 6 admite un subgrupo de orden p^1: el propio 6.

  - Supongamos que 6 admite al menos un subgrupo propio. Consideraremos dos subcasos:

  a) 6 admite un subgrupo propio H tal que $p^r \mid o(H)$. Entonces, siendo $o(H) < o(6)$, por hipótesis de inducción, existe en H un subgrupo de orden p^r. Luego, 6 admite un subgrupo de orden p^r.

  b) Cualquiera que sea H subgrupo propio de 6, p^r no $\mid o(H)$. Entonces, cualquiera que sea H, como $o(6) = o(H)\, i(H)$, $p^r \mid o(6)$ y p^r no $\mid o(H)$, debe ser p divisor de i(H) (no podemos asegurar que $p^r \mid i(H)$ pues puede ser que $p^{r-1} \mid o(H)$).

Aplicando la ecuación de las clases de Frobenius (si 6 opera sobre sí mismo por conjugación) tenemos que:

$$o(6) = o(Z(6)) + \sum d_i$$

donde los d_i, si existen, verifican que $1 < d_i$, $d_i \mid o(6)$ y además d_i es el índice del normalizador de un elemento $x_i \in 6$ (pues $i(N_{x_i}) = o(C_{x_i})$).

Según lo dicho anteriormente, siendo N_{x_i} subgrupo de 6, $p \mid d_i = i(N(x_i))$

Como además, $p \mid o(6)$, se tiene que $p \mid o(Z(6))$

Pero Z(6) es un subgrupo abeliano de 6. Entonces, por la PROPOSICION 3.1, existe en Z(6) un elemento x de orden p.

Sea $K = \langle x \rangle \subset Z(6)$. Trivialmente $\langle x \rangle$ es subgrupo normal

de G, pues $\langle x\rangle \in Z(G)$ y $\forall g\in G, \forall x^k\in\langle x\rangle$, $g x^k g^{-1} = x^k g g^{-1} = x^k$.
Consideremos entonces el grupo cociente $G/\langle x\rangle$.

$$o(G/\langle x\rangle) = \frac{o(G)}{o(\langle x\rangle)} = \frac{n}{p} < n.$$

Como $p^r \mid o(G) = n \;\wedge\; o(G/\langle x\rangle) = \frac{n}{p} \Rightarrow p^{r-1} \mid o(G/\langle x\rangle)$.
Por hipótesis de inducción, existe en $G/\langle x\rangle$ un subgrupo $\overline{H}$ de orden p^{r-1}. Según corolario 2.3, $\overline{H}$ es de la forma $\overline{H} = H/\langle x\rangle$, siendo H un subgrupo de G que contiene a $\langle x\rangle$.
Luego, como $o(H) = o(\overline{H})\, o(\langle x\rangle) = p^{r-1} p = p^r$, queda probado el teorema. ■

3.3. TEOREMA: (de Cauchy)

> Si p es un número primo que divide al orden de un grupo finito G, existe en G un elemento de orden p.

Demostr.: Por el teorema 3.2, existe en G un subgrupo H de orden p. Siendo p primo, H es cíclico. Si $H = \langle x\rangle$, $o(x) = o(\langle x\rangle) = p$. c.s.q.d.

3.4. TEOREMA: (2° y 3^{er} teoremas de Sylow)

> Sea G un grupo finito y p un número primo que divide a $o(G)$.
> a) Si H es un p-subgrupo de G, H está contenido en un p-subgrupo de Sylow.
> b) 2° teorema de Sylow: Todos los p-subgrupos de Sylow de G son conjugados.
> c) 3^{er} teorema de Sylow: El número de p-subgrupos de Sylow que existen en G es congruente con 1 módulo p, y divisor de $o(G)$.

Demostr.: a) En virtud del teorema 3.2 y como consecuencia de que $p \mid o(G)$, siempre existe en G un p-subgrupo "maximal", es decir, un p-subgrupo de Sylow. Sea, entonces, P un p-subgrupo de Sylow de G.
Se comprueba fácilmente que G opera por conjugación en el conjunto $\mathcal{S}$ de los p-subgrupos de Sylow de G:

$$\begin{aligned} G \times \mathcal{S} &\longrightarrow \mathcal{S} \\ (g, P_1) &\longmapsto g P_1 g^{-1} \end{aligned}$$

(Esta aplicación está bien definida pues gP_1g^{-1} es la imagen de P_1 por un automorfismo interno de G y por tanto $o(gP_1g^{-1}) = o(P_1)$).
Consideremos la órbita de P en $\mathcal{S}$ por acción de G:

$$O_P = \{gPg^{-1} / g\in G\} \qquad (I)$$

Entonces $\operatorname{card}(O_P) = i(N(P))$. $N(P)$ es un subgrupo de G que

contiene a P. Luego $o(P) \mid o(N(P))$. Si $o(P) = p^n$, debe existir $K \in \mathbb{N}$ tal que $o(N(P)) = K \cdot p^n$. Como P es un p-subgrupo de Sylow, p^n es la mayor potencia de p que divide a $o(6)$. Entonces, K y p deben ser primos entre sí, pues de lo contrario, como $K p^n \mid o(6)$, existiría una potencia de p mayor que p^n que divide a $o(6)$ (pues si $(K,p) > 1$, siendo p primo, debe ser $p \mid K$). Por tanto, $(K,p) = 1$.
Análogamente $i(N(P))$ no es divisible por p ($o(N(P)) \cdot i(N(P)) = o(6)$).
Por tanto, p no $\mid$ card (O_P). (II)

Sea, entonces, H un p-subgrupo cualquiera de 6. Se prueba fácilmente que H opera por conjugación en el conjunto O_P:

$$H \times O_P \longrightarrow O_P$$
$$(h, gPg^{-1}) \longmapsto hgPg^{-1}h^{-1}$$

Entonces, el conjunto O_P (órbita de P en $\mathcal{S}$ por acción del grupo 6) admite una partición por órbitas S_i, $i \in J$, por acción del grupo H:

$$O_P = \bigcup_{i \in J} S_i$$

Como las órbitas son disjuntas dos a dos, $\text{card}(O_P) = \sum_{i \in J} \text{card}(S_i)$ (III)

Para cada $i \in J$, card (S_i) coincide con el índice del normalizador de un elemento de O_P en H y, por tanto, card $(S_i) = i_H(K_i)$ siendo K_i un subgrupo de H (el normalizador en H de un elemento de O_P es subgrupo de H). Siendo H un p-subgrupo de 6 ($o(H) = p^r$) el índice de cualquier subgrupo de H, divisor de $o(H)$, debe ser ó 1 ó una potencia de p. Pero card (O_P) no es divisible por p, según (II), luego, en virtud de (III), debe existir $i \in J$ tal que p no $\mid$ card (S_i), y, en consecuencia, $\exists i \in J$ / card $(S_i) = 1$.

Sea S una de estas órbitas: $S = \{P'\}$, donde $P' \in O_P$.
Si $P' \in O_P$, $\exists g \in 6$ / $P' = gPg^{-1}$. Luego P' es un p-subgrupo de Sylow de 6, por ser conjugado de P; (obsérvese, (I), que O_P es el conjunto de subgrupos conjugados de P).
Siendo $S = \{hP'h^{-1} / h \in H\} = \{P'\}$ debe ser $hP'h^{-1} = P'$, $\forall h \in H$. Luego: $H \subset N(P')$. Entonces, por el segundo teorema de isomorfía:

$$\frac{H \cdot P'}{P'} \simeq \frac{H}{H \cap P'}$$

Como P' es un p-subgrupo de 6 y $o(H \cap P') \mid o(P')$ (pues $H \cap P'$ es subgrupo de P') se tiene que $H \cap P'$ es un p-subgrupo de 6 (pues p primo).
Siendo H un p-subgrupo de 6, el grupo cociente $\frac{H}{H \cap P'}$ que

tiene de orden $\frac{o(H)}{o(H\cap P')}$ es un p-grupo. Luego HP'/P' es un p-grupo, por ser isomorfo a $H/H\cap P'$. Como $o(HP') = o(P')\cdot o(HP'/P')$ tenemos que HP' es un p-subgrupo de 6.

Además $HP' \supset P'$; luego, siendo P' un p-subgrupo de Sylow (maximal) y HP' un p-subgrupo de 6, debe ser $HP' = P'$.

Luego $H \subset HP' = P'$.

Por tanto, H está contenido en un p-subgrupo de Sylow, pues P', como conjugado de P, es un p-subgrupo de Sylow.

b) Sean P y H p-subgrupos de Sylow de 6. Siendo H p-subgrupo y P un p-subgrupo de Sylow, haciendo las mismas consideraciones que en a), tenemos que $H \subset P'$, donde P' es un p-subgrupo de Sylow conjugado de P. Siendo H un p-subgrupo de Sylow de 6 y $H \subset P'$ debe ser $H = P'$, pues P' es p-subgrupo de 6. Por tanto P y H son conjugados.

c) Sea P un p-subgrupo de Sylow de 6. Consideremos la órbita O_P de P en $\mathcal{S}$ por acción del grupo 6. Según (I), O_P contiene los p-subgrupos de Sylow conjugados de P. Según b), todos los p-subgrupos de Sylow son conjugados; luego O_P contiene todos los p-subgrupos de Sylow de 6 y, recíprocamente, todo elemento de O_P es un p-subgrupo de Sylow de 6.

Haciendo operar por conjugación el grupo P sobre O_P, obtenemos una partición de O_P por órbitas C_i, $i \in I$, y, de modo análogo a (III) tenemos que: $\text{card}(O_P) = \sum_{i\in I} \text{card}(C_i)$, donde $\text{card}(C_i)$ o es 1 o es una potencia de p. Si probamos que solo existe una clase de conjugación C_i de cardinal 1 quedará probado que $\text{card}(O_P) \equiv 1 \pmod p$ y, por tanto, el 3er teorema de Sylow, pues $\text{card}(O_P)$ es el número de p-subgrupos de Sylow de 6, y además, $\text{card}(O_P)$ divide a $o(6)$ (TEHA 2°, Teorema 1.1).

Evidentemente, $P \in O_P$. La órbita de P en O_P por acción de P es

$$O_P(P) = \{ p P p^{-1} / p \in P \} = \{P\}$$

Por tanto, existe al menos una órbita en O_P de cardinal 1. Veamos que no existe ninguna más. Supongamos que existe otra órbita unitaria en O_P: $S = \{P'\}$. Análogamente a como se hizo en a), $P \subset N(P')$ (observar que ahora $H = P$). $N(P')$ es un grupo, cuyo orden es divisible por P ya que P' es un p-subgrupo de Sylow de 6 y $o(P') \mid o(N(P'))$.

Además P y P' son subgrupos de $N(P')$ y, aun más, P y P' son p-subgrupos de Sylow del grupo $N(P')$, pues $P, P' \subset N(P')$ y P y P' son p-subgrupos de Sylow de G. Aplicando el segundo teorema de Sylow al grupo $N(P')$ tenemos que todos los p-subgrupos de Sylow de $N(P')$ son conjugados en $N(P')$. Luego:

$$\exists g \in N(P') \;/\; P = gP'g^{-1}.$$

Pero si $g \in N(P')$, $gP'g^{-1} = P'$. Luego $P = P'$, que prueba que sólo hay una órbita de cardinal 1 en O_P.

En consecuencia, y como se indicó anteriormente, $\text{card}(O_P) \equiv 1 \pmod p$. c.s.q.d.

3.5. PROPOSICION: Sea G un p-grupo y H un subgrupo propio de G. Entonces $H \neq N(H)$.

Demostr.: Siendo G un p-grupo, el centro de G es no trivial (COROLARIO 1.8, TEMA 2°). Consideraremos, entonces, dos casos:

a) $Z(G) \not\subset H$. Entonces, existe al menos un elemento $x \in Z(G)$ tal que $x \notin H$. Pero el centro de un grupo está siempre contenido en el normalizador de cualquier subgrupo, pues $\forall z \in Z(G), \forall S$ subgrupo de G, $zSz^{-1} = zz^{-1}S = S$. Por tanto, $x \in N(H) - H$, que prueba que $H \neq N(H)$.

b) $Z(G) \subset H$. Supongamos que $o(G) = p^n$. Procederemos por inducción sobre n. Para $n = 1$ la proposición no tiene sentido pues si $o(G) = p$, G no admite subgrupos propios. Comenzaremos la inducción para $n = 2$.

- Si $n = 2$, $o(G) = p^2$; entonces G es abeliano (COROLARIO 1.9, Tema 2°) y, por tanto, todo subgrupo de G es normal en G. Entonces:

$$H \lhd G \Rightarrow N(H) = G \Rightarrow N(H) \neq H, \text{ pues } H \text{ es subgrupo propio de } G.$$

- Supongamos que el teorema es cierto para todo p-grupo de orden menor que p^n. Siendo $Z(G) \lhd G$, podemos considerar el grupo cociente $G/Z(G)$, que es un p-grupo pues G lo es y $Z(G)$ es un p-subgrupo de G, ya que todo subgrupo de un p-grupo es p-subgrupo.

Además $o(G/Z(G)) < o(G)$, pues $Z(G)$ es no trivial.

Si $H \supset Z(G)$, podemos considerar el grupo cociente $H/Z(G)$, que es subgrupo propio de $G/Z(G)$, pues siendo $H \neq G$ y $H \supset Z(G)$, en virtud de COROLARIO 2.3, $H/Z(G) \neq G/Z(G)$.

Entonces, por hipótesis de inducción, $N(H/Z(G)) \neq H/Z(G)$.

Si probamos que $N(H/Z(G)) = N(H)/Z(G)$ quedará probado que $N(H)/Z(G) \neq H/Z(G)$ y de aquí deduciríamos que $N(H) \neq H$, en virtud de la biyección que existe entre los subgrupos de G que contienen a $Z(G)$ y

los subgrupos de $G/Z(G)$ (COROLARIO 2.3), como fueremos probar.
Veamos entonces que $N(H/Z(G)) = N(H)/Z(G)$.
$H/Z(G) = \{hZ(G) / h\in H\}$; $N(H/Z(G)) = \{gZ(G)\in G/Z(G) / [gZ(G)][H/Z(G)][gZ(G)]^{-1} = H/Z(G)\} =$
$= \{qZ(G)\in G/Z(G) / qZ(G)\cdot hZ(G)\cdot g^{-1}Z(G)\in H/Z(G), \forall h\in H\} =$
$= \{qZ(G)\in G/Z(G) / qhq^{-1}Z(G)\in H/Z(G), \forall h\in H\}$.

Por otro lado, $N(H) = \{g\in G / gHg^{-1} = H\}$, luego:
$N(H)/Z(G) = \{gZ(G)\in G/Z(G) / gHg^{-1} = H\} = \{gZ(G)\in G/Z(G) / ghg^{-1}\in H, \forall h\in H\}$.

Entonces $qZ(G)\in N(H/Z(G)) \Leftrightarrow qhq^{-1}Z(G)\in H/Z(G), \forall h\in H \Leftrightarrow$
$\Leftrightarrow qhq^{-1}\in H, \forall h\in H \Leftrightarrow qZ(G)\in N(H)/Z(G)$.
Por tanto $N(H/Z(G)) = N(H)/Z(G)$ y, como se indicó anteriormente, $N(H)\neq H$. c.q.d.

3.6. TEOREMA: 1er teorema de Sylow.

> Sea G un grupo finito de orden $p^n\cdot K$ con $(p,K)=1$. Para cada $r\leq n$ existe un subgrupo de G de orden p^r. Además, si H es un subgrupo de orden p^r, $r<n$, existe un subgrupo K de G tal que $H\subset K$, $o(K) = p^{r+1}$ y H es normal en K.

Demostr.: La primera parte es el teorema 3.2.
Siendo H un p-subgrupo de G, está contenido en un p-subgrupo de Sylow P de G. Como $(p,K)=1$, y $o(G) = p^n\cdot K$ se verifica que $o(P) = p^n$.
Siendo $r<n$, H es subgrupo propio de P. Entonces, por la proposición anterior, H es distinto del normalizador de H en P: $H\neq N_P(H)$
Vamos a encontrar un subgrupo K de G que verifique $H\subset K\subset N_P(H)$ y $o(K) = p^{r+1}$, con lo cual quedará probado el teorema pues $K\subset N_P(H) \Rightarrow H\lhd K$.
Siendo H normal en su normalizador $N_P(H)$, $N_P(H)/H$ es un grupo no trivial, pues $H\neq N_P(H)$. Además este grupo cociente es un p-grupo, pues $o(H) = p^r \mid o(N_P(H))$ y $o(N_P(H)) \mid o(P) = p^n$.
Como $p \mid o(N_P(H)/H)$, según el teorema de Cauchy, existe en $N_P(H)/H$ un elemento de orden p, y, por tanto, existe un subgrupo $\bar{K}$ de orden p. Según COROLARIO 2.3, $\bar{K}$ es de la forma: $\bar{K} = \frac{K}{H}$, donde K es un subgrupo de $N_P(H)$ que contiene a H.
Luego $o(K) = o(\bar{K})\, o(H) = p\cdot p^r = p^{r+1}$ y $H\subset K\subset N_P(H)$. c.q.d.

3.7. TEOREMA: a) Si H es un subgrupo propio de un p-grupo G, H está contenido en un subgrupo K propio maximal, es decir, tal que si $o(G) = p^n$ entonces $o(K) = p^{n-1}$. (*)

b) Todo subgrupo propio maximal de un p-grupo G es normal en G.

Demostr: a) Si H es subgrupo propio de G y $o(G) = p^n$ se tiene que $o(H) = p^r$ con $r < n$. Por la proposición anterior, existe un subgrupo H_1 de orden p^{r+1} tal que $H \subset H_1$. Si $r+1 = n-1$, el teorema está probado. Si $r+1 < n-1$, existe un subgrupo H_2 de orden p^{r+2} tal que $H_1 \subset H_2$. Si $r+2 = n-1$, el teorema está probado; si no procediendo de este modo obtenemos un subgrupo $K = H_{n-1-r}$ de orden $p^{r+n-1-r} = p^{n-1}$ tal que $H \subset K$. y K ya es un subgrupo propio maximal.

b) Si K es un subgrupo propio maximal de un grupo G de orden p^n, $o(K) = p^{n-1}$. Entonces, por la proposición 3.5. $K \neq N(K)$.

Como $K \subset N(K)$ y $o(N(K)) \mid o(G)$ debe ser $N(K) = G$. Luego $K \lhd G$. csqd.

3.8. TEOREMA: Sea G un p-grupo y K un subgrupo normal de G de orden p. Entonces $K \subset Z(G)$.

Demostr: Siendo K un subgrupo de orden primo p, es cíclico, pues dado $a \in K - \{e\}$, $o(a) \neq 1 \wedge o(a) \mid p \Rightarrow o(a) = p \Rightarrow K = \langle a \rangle = \{e, a, \dots, a^{p-1}\}$.

La clase de conjugación del elemento a es:

$$C_a = \{ gag^{-1} / g \in G \}.$$

Siendo $K \lhd G$, $gKg^{-1} = K$, $\forall g \in G$.

Luego $\forall g \in G$, $gag^{-1} \in \{a, a^2, \dots, a^{p-1}\}$, pues si $gag^{-1} = e \Rightarrow a = e$.

Por tanto, $\operatorname{card} C_a \leq p-1$. Luego p no $\mid \operatorname{card} C_a$.

Pero $\operatorname{card} C_a = i(N(a))$. Luego p no $\mid i(N(a))$.

Siendo $N(a)$ subgrupo del p-grupo G, $o(N(a))$ e $i(N(a))$ son potencias de p. Como p no $\mid i(N(a))$ debe ser $i(N(a)) = 1$.

Entonces, $\operatorname{card} C_a = 1$. Como $a \in C_a$ se verifica que $C_a = \{a\}$.

Luego $\forall g \in G$, $gag^{-1} = a \Rightarrow \forall g \in G$, $ga = ag$.

En definitiva, $a \in Z(G)$ y, por tanto, $K \subset Z(G)$. csqd.

TEMA 5º: PRODUCTO DIRECTO DE GRUPOS.

1. Producto y producto directo de grupos

- **DEFINICION:** Sea $(G_i)_{i\in I}$ una familia de grupos. Sea G el producto cartesiano de los G_i : $G = \prod_{i\in I} G_i$. Definimos en G la siguiente ley de composición: si $x=(x_i)_{i\in I}$ e $y=(y_i)_{i\in I}$, definimos $xy=(x_iy_i)_{i\in I}$. Esta ley dota a G de estructura de grupo, trivialmente. Diremos que G es el grupo producto de los G_i, $i\in I$.

  Sea $G' = \{(x_i)_{i\in I} \in G / x_i = e_i, \forall i \in I - \{i_1,\dots,i_n\}\}$ siendo e_i el neutro de G_i, es decir, los elementos de G' son los elementos de G que tienen, como máximo, un número finito de coordenadas distintas del elemento neutro. Trivialmente, G' es un subgrupo de G. Decimos que G' así definido es el producto directo (o coproducto) de los grupos G_i y escribiremos:

$$G' = \coprod_{i\in I} G_i.$$

  Cuando las operaciones de los grupos son aditivas, el coproducto se llama suma directa y se escribe: $G' = \bigoplus_{i\in I} G_i$.

  Si el conjunto de índices I es finito, el producto y el producto directo coinciden, trivialmente. En este caso se escribe el producto directo por $G_1 \times G_2 \times \dots \times G_n$ si la ley es multiplicativa y $G_1 \oplus G_2 \oplus \dots \oplus G_n$ si la ley es aditiva. (*)

- **DEFINICION:** Sea G un grupo y $(G_i)_{i\in I}$ una familia de subgrupos de G. Diremos que G es producto directo de esta familia de subgrupos si la aplicación:

$$\Phi : \coprod_{i\in I} G_i \longrightarrow G$$

$$x=(x_i)_{i\in I} \longmapsto \prod_{i\in I} x_i$$

  es un isomorfismo de grupos.

  Nota: Φ está bien definida ya que $\prod_{i\in I} x_i$ no será nunca un producto infinito, que no hemos definido en G, ya que los x_i son el elemento neutro de G salvo, a lo sumo, un número finito de ellos.

  Veamos a continuación dos caracterizaciones de un grupo como producto directo de una familia de subgrupos suyos.

1.1. TEOREMA: Sea G un grupo y $(G_i)_{i\in I}$ una familia de subgrupos de G. Las condiciones siguientes son equivalentes:

a) G es producto directo de los subgrupos G_i, $i\in I$.

b) (1) $\forall i\in I$, $G_i \lhd G$, (2) $G = \langle \bigcup_{i\in I} G_i \rangle$, (3) $\forall k\in I$, $G_k \cap \langle \bigcup_{i\neq k} G_i \rangle = \{1\}$.

c) i) Si $i\neq j$ se verifica que $\forall x\in G_i$, $\forall y\in G_j$, $xy = yx$.

ii) Para cada $x\in G-\{1\}$, existe un único $I_x = \{i_1,\dots,i_n\}\subset I$, $I_x\neq\emptyset$, y para estos índices unos únicos elementos $x_{i_1},\dots,x_{i_n}$ tales que $x_{i_k}\in G_{i_k}-\{1\}$, $\forall k\in\{1,\dots,n\}$ y con $x = x_{i_1}\cdot x_{i_2}\cdot\dots\cdot x_{i_n}$.

Demostr.: a) $\Rightarrow$ b) | Si G es producto directo de los subgrupos G_i, existe un isomorfismo $\phi: (x_i)_{i\in I}\in \coprod_{i\in I} G_i \longrightarrow \prod_{i\in I} x_i \in G$.

(1) Sea $G_i' = \{(x_j)_{j\in I}\in \coprod_{j\in I} G_j \;/\; x_j = 1 \text{ si } j\neq i\}$

Veamos que $G_i' \lhd \coprod_{j\in I} G_j$: dado $x=(x_j)_{j\in I}\in G_i'$ e $y\in \coprod_{j\in I} G_j$

$yxy^{-1} = (y_j x_j y_j^{-1})_{j\in I}$, siendo $y_j x_j y_j^{-1} = 1$ si $j\neq i$, pues $x_j = 1$, e $y_i x_i y_i^{-1}\in G_i$. Luego $yxy^{-1}\in G_i'$.

Trivialmente, $G_i = \phi(G_i')$. Siendo ϕ isomorfismo y $G_i' \lhd \coprod_{j\in I} G_j$ se verifica que $G_i \lhd \phi(\coprod_{j\in I} G_j) = G$.

(2) Evidentemente, $\langle \bigcup_{i\in I} G_i \rangle \subset G$. Veamos que $G\subset \langle \bigcup_{i\in I} G_i \rangle$.

Sea $x\in G$. Siendo ϕ sobre, existe $y\in \coprod_{i\in I} G_i$ tal que $x = \phi(y)$.

Sean $y_{i_1},\dots,y_{i_k}$ las coordenadas de y que son distintas de 1. Entonces, $x = \phi(y) = y_{i_1}\cdots y_{i_k}$, con $y_{i_r}\in G_{i_r}\subset \bigcup_{i\in I} G_i$. Luego $x\in \langle \bigcup_{i\in I} G_i \rangle$. Por tanto, $G = \langle \bigcup_{i\in I} G_i \rangle$.

(3) Sea $x\in G_k \cap \langle \bigcup_{i\neq k} G_i \rangle$. Si $x\in G_k$, $x = x_k$ y si $x\in \langle \bigcup_{i\neq k} G_i \rangle$, $x = x_{i_1}\cdots x_{i_n}$, siendo $i_1,\dots,i_n$ distintos de k.

Sea $y = (y_i)_{i\in I}\in \coprod_{i\in I} G_i$ definido como sigue: $y_k = x_k$ e $y_i = 1$ si $i\neq k$.

Sea $z = (z_i)_{i\in I}$ definido así: $z_{i_1} = x_{i_1}, \dots, z_{i_n} = x_{i_n}$, $z_i = 1$ si $i\notin\{i_1,\dots,i_n\}$.

Entonces $\phi(y) = \phi(z) = x$. Siendo ϕ inyectiva debe ser $y = z$.

Luego $y_k = z_k$. Como $z_k = 1$, pues $k\notin\{i_1,\dots,i_n\}$, e $y_k = x_k$ se tiene que $x_k = 1$. Luego $x = 1$. Por tanto, $G_k \cap \langle \bigcup_{i\neq k} G_i \rangle = \{1\}$.

b) $\Rightarrow$ c) | i) Sean $x\in G_i$, $y\in G_j$ con $i\neq j$. Se trata de ver que $xy = yx$ o bien, que $xyx^{-1}y^{-1} = 1$.

Como $y\in G_j$ y $G_j \lhd G$ se tiene que $xyx^{-1}\in G_j$; como $y\in G_j$ se tiene que $xyx^{-1}y^{-1}\in G_j$. Además $x\in G_i$ y $G_i \lhd G \Rightarrow yx^{-1}y^{-1}\in G_i$.

Luego $xyx^{-1}y^{-1} \in G_i$. Por tanto, $xyx^{-1}y^{-1} \in G_i \cap G_j < G_i \cap \langle \bigcup_{j \neq i} G_j \rangle = \{1\}$.
En definitiva, $xyx^{-1}y^{-1} = 1$, como queríamos probar.

ii) Sea $x \in G - \{1\}$. Por (2), $x = x_{i_1} \cdots x_{i_n}$; podemos considerar los índices $i_1, \ldots, i_n$ distintos dos a dos, pues si no lo fueran, por i) podemos conmutar los factores y agruparlos en un único elemento del subgrupo G_i correspondiente; también podemos suponer los $x_{i_r} \neq 1$, pues de haber alguno igual a 1 se puede suprimir. Sea entonces $I_x = \{i_1, \ldots, i_n\}$.
Veamos que es único: Supongamos que $x = y_{j_1} \cdots y_{j_p}$, con $j_l \neq j_t$ si $l \neq t$. Entonces $1 = xx^{-1} = x_{i_1} \cdots x_{i_n} y_{j_p}^{-1} \cdots y_{j_1}^{-1}$. (I)
Sea $J_x = \{j_1, \ldots, j_p\}$ y $K_x = I_x \cup J_x = \{k_1, \ldots, k_s\}$.
Conmutando convenientemente los elementos de (I) podemos escribir: $1 = z_{k_1} \cdots z_{k_s}$. Entonces $z_{k_1} = z_{k_s}^{-1} \cdots z_{k_2}^{-1}$.
Luego $z_{k_1} \in G_{k_1} \cap \langle \bigcup_{i \neq k_1} G_i \rangle = \{1\} \Rightarrow z_{k_1} = 1$.
Entonces: $1 = z_{k_2} \cdots z_{k_s}$ y, del mismo modo, $z_{k_2} = 1$. Analogamente, $\forall l \in \{1, \ldots, s\}$, $z_{k_l} = 1$.
Por definición de z_{k_l}, se verifica que $z_{k_l} = x_{k_l}$, ó $z_{k_l} = y_{k_l}$ ó $z_{k_l} = x_{k_l} y_{k_l}^{-1}$. Siendo $z_{k_l} = 1$, $x_{i_r} \neq 1$, $\forall r \in \{1, \ldots, n\}$ y $y_{j_t} \neq 1$, $\forall t \in \{1, \ldots, p\}$, debe ser $z_{k_l} = x_{k_l} y_{k_l}^{-1}$, $\forall l \in \{1, \ldots, s\}$.
Deducimos de esto que $\forall r \in \{1, \ldots, n\}$, $\exists t \in \{1, \ldots, p\} / i_r = j_t$ y, del mismo modo, $\forall t \in \{1, \ldots, p\}$, $\exists r \in \{1, \ldots, n\} / j_t = i_r$. Debe ser entonces $I_x = J_x$.
Además $z_{k_l} = 1 \Rightarrow x_{k_l} = y_{k_l}$, como se quería demostrar.

c) $\Rightarrow$ a) Se trata de probar que la aplicación $\phi : (x_i)_{i \in I} \in \coprod_{i \in I} G_i \longmapsto \prod_{i \in I} x_i \in G$ es un isomorfismo.

- ϕ es homomorfismo: $\forall \bar{x} = (x_i)_{i \in I}$, $\bar{y} = (y_i)_{i \in I} \in \coprod_{i \in I} G_i$, $\phi(\bar{x}\bar{y}) = \phi[(x_i)_{i \in I}(y_i)_{i \in I}] = \phi[(x_i y_i)_{i \in I}] = \prod_{i \in I}(x_i y_i) \overset{i)}{=} \prod_{i \in I} x_i \cdot \prod_{i \in I} y_i = \phi(\bar{x}) \cdot \phi(\bar{y})$.

- ϕ es inyectivo: Si $\bar{x} = (x_i)_{i \in I}$ e $\bar{y} = (y_i)_{i \in I}$ son tales que $\phi(\bar{x}) = \phi(\bar{y}) = g \in G$, se tiene, supuesto que $x_{i_1}, \ldots, x_{i_n}$ e $y_{j_1}, \ldots, y_{j_p}$ son las coordenadas distintas de 1 de $\bar{x}$ e $\bar{y}$, respectivamente, que:
$g = \phi(\bar{x}) = x_{i_1} \cdots x_{i_n}$ y $g = \phi(\bar{y}) = y_{j_1} \cdots y_{j_p}$. Entonces, según ii) $n = p$, $\{i_1, \ldots, i_n\} = \{j_1, \ldots, j_n\}$ y, mediante una permutación adecuada de los índices, podemos hacer $x_{i_1} = y_{i_1}, \ldots, x_{i_n} = y_{i_n}$. Como además $\forall i \in I - \{i_1, \ldots, i_n\}$, $x_i = y_i = 1$ se verifica que $\bar{x} = \bar{y}$.

- ϕ es sobre: Según ii), todo elemento $x \in G$ admite una única descomposición de la forma $x = x_{i_1} \cdots x_{i_n}$. Sea $y = (y_i)_{i \in I}$ definido

por: $y_{i_1} = x_{i_1}, \dots, y_{i_n} = x_{i_n}$, $y_i = 1$ si $i \notin \{i_1, \dots, i_n\}$. Entonces $y \in \coprod_{i \in I} G_i$ y se tiene que $\phi(\bar{y}) = x$. Luego ϕ es sobre. c.s.q.d.

NOTA: Sea $(G_i)_{i \in I}$ una familia de subgrupos de un grupo G. Si G es producto directo de estos subgrupos existe un isomorfismo entre G y $\coprod_{i \in I} G_i$. Este isomorfismo nos permite, desde el punto de vista algebraico, identificar dichos grupos y escribir, por tanto, $G = \coprod_{i \in I} G_i$ y considerar $(x_i)_{i \in I} = \prod_{i \in I} x_i$.

Para el caso particular en que I sea finito podemos enunciar un teorema análogo al anterior:

1.2. TEOREMA: Sea G un grupo y $\{G_i\}_{i=1}^n$ una familia finita de subgrupos de G. Las proposiciones siguientes son equivalentes:

a) G es producto directo de los G_i, es decir, $G = G_1 \times G_2 \times \dots \times G_n$.

b) (1) $\forall i \in \{1, \dots, n\}$, $G_i \lhd G$, (2) $G = G_1 \cdot G_2 \cdot \dots \cdot G_n$, (3) $\forall i \in \{2, \dots, n\}$, $(G_1 \cdots G_{i-1}) \cap G_i = \{1\}$.

c) i) G_i y G_j conmutan elemento a elemento si $i \neq j$.
ii) Cada elemento $x \in G$ admite una única descomposición de la forma $x = x_1 \cdot x_2 \cdot \dots \cdot x_n$, $x_i \in G_i$.

d) i) G_i y G_j conmutan elemento a elemento si $i \neq j$.
ii') Dados $x_1, x_2, \dots, x_n$, con $x_i \in G_i$, si $x_1 x_2 \cdots x_n = 1$, entonces $x_1 = \dots = x_n = 1$. (*)

Demostr.: La demostración de las implicaciones a) $\Rightarrow$ b) y b) $\Rightarrow$ c) y c) $\Rightarrow$ a) es totalmente análoga a las correspondientes implicaciones del teorema anterior. Probemos que, verificándose i), ii) $\Leftrightarrow$ ii') con lo cual quedará demostrado el teorema.

ii) $\Rightarrow$ ii') Trivialmente, $1 = 1 \cdot 1 \cdot \overset{n}{\dots} \cdot 1$. Si $1 = x_1 \cdots x_n$, por ii) se verificará que $x_1 = 1, \dots, x_n = 1$.

ii') $\Rightarrow$ ii) Si $x = x_1 \cdots x_n$ y $x = y_1 \cdots y_n \Rightarrow 1 = x_1 \cdots x_n y_n^{-1} \cdots y_1^{-1} \overset{i)}{\Rightarrow}$

$\Rightarrow 1 = (x_1 y_1^{-1})(x_2 y_2^{-1}) \cdots (x_n y_n^{-1}) \overset{ii')}{\Rightarrow} x_1 y_1^{-1} = 1, \dots, x_n y_n^{-1} = 1 \Rightarrow x_1 = y_1, \dots, x_n = y_n$.

1.3. COROLARIO: Si un grupo finito G es producto directo de una familia finita de subgrupos suyos $\{G_i\}_{i=1}^n$, entonces

$$o(G) = o(G_1) \cdot o(G_2) \cdot \dots \cdot o(G_n)$$

Demostr.: Si G es producto directo de sus subgrupos $G_1, \dots, G_n$, entonces G es isomorfo a $G_1 \times G_2 \times \dots \times G_n$. En particular, tienen el mismo número de elementos; como $o(G_1 \times G_2 \times \dots \times G_n) = o(G_1) \cdot o(G_2) \cdot \dots \cdot o(G_n)$ se verifica que $o(G) = o(G_1) \cdot o(G_2) \cdot \dots \cdot o(G_n)$. c.s.q.d.

1.4. PROPOSICION: Sea $(G_i)_{i\in I}$ una familia de grupos y H_i un subgrupo normal de G_i, para cada $i\in I$. Entonces:

a) $\dfrac{\prod_{i\in I} G_i}{\prod_{i\in I} H_i} \simeq \prod_{i\in I} (G_i/H_i)$

b) $\dfrac{\coprod_{i\in I} G_i}{\coprod_{i\in I} H_i} \simeq \coprod_{i\in I} (G_i/H_i)$

Demostr.: a) Consideremos la siguiente aplicación:

$$\varphi: \prod_{i\in I} G_i \longrightarrow \prod_{i\in I} (G_i/H_i)$$
$$(x_i)_{i\in I} \longmapsto (x_i H_i)_{i\in I}$$

Probemos que φ es un homomorfismo sobre:

- φ es homomorfismo: $\varphi[(x_i)_{i\in I}(y_i)_{i\in I}] = \varphi[(x_i y_i)_{i\in I}] = ((x_i y_i)H_i)_{i\in I} = ((x_i H_i)(y_i H_i))_{i\in I} = (x_i H_i)_{i\in I}\cdot(y_i H_i)_{i\in I} = \varphi[(x_i)_{i\in I}]\cdot\varphi[(y_i)_{i\in I}]$.
- φ es sobre: Dado $\bar z \in \prod_{i\in I}(G_i/H_i)$, existe $(x_i)_{i\in I}\in\prod_{i\in I} G_i$ / $\bar z = (x_i H_i)_{i\in I}$. Entonces $\bar z = \varphi[(x_i)_{i\in I}]$.

Veamos que $\operatorname{Ker}\varphi = \prod_{i\in I} H_i$.

$(x_i)_{i\in I}\in\operatorname{Ker}\varphi \Leftrightarrow (x_i H_i)_{i\in I} = \bar 1 = (H_i)_{i\in I} \Leftrightarrow \forall i\in I,\ x_i H_i = H_i \Leftrightarrow$
$\Leftrightarrow \forall i\in I,\ x_i\in H_i \Leftrightarrow (x_i)_{i\in I}\in\prod_{i\in I} H_i$. Luego $\operatorname{Ker}\varphi = \prod_{i\in I} H_i$.

Siendo φ sobre: $\varphi(\prod_{i\in I} G_i) = \prod_{i\in I}(G_i/H_i)$. Según PROPOSICION 2.1 (Tema 4°):

$$\Big(\prod_{i\in I} G_i\Big)\Big/\Big(\prod_{i\in I} H_i\Big) \simeq \prod_{i\in I}(G_i/H_i)$$

b) Consideremos la aplicación

$$\psi: \coprod_{i\in I} G_i \longrightarrow \coprod_{i\in I} (G_i/H_i)$$
$$(x_i)_{i\in I} \longmapsto (x_i H_i)_{i\in I}$$

Trivialmente $\psi = \varphi_{|\coprod_{i\in I} G_i}$. Veamos que está bien definida, es decir, que si $(x_i)_{i\in I}\in\coprod_{i\in I} G_i$ entonces $\psi[(x_i)_{i\in I}] = (x_i H_i)_{i\in I}\in\coprod_{i\in I}(G_i/H_i)$

Si $(x_i)_{i\in I}\in\coprod_{i\in I} G_i$, $x_i = e_i$ (neutro de G_i) excepto para un número finito de índices. Entonces, $x_i H_i = H_i$ (neutro de G_i/H_i) excepto para un número finito de índices, que prueba que $(x_i H_i)_{i\in I}\in\coprod_{i\in I}(G_i/H_i)$.

ψ es sobre, pues dado $\bar z\in\coprod_{i\in I}(G_i/H_i)$, $\exists (x_i)_{i\in I}\in\prod_{i\in I} G_i$ / $\bar z = (x_i H_i)_{i\in I}$ (*);

Sean $i_1,\dots,i_n$ los índices para los cuales $x_{i_r} H_{i_r} \neq H_{i_r}$, y los únicos que verifican esto. Sea $\bar y = (y_i)_{i\in I}\in\coprod_{i\in I} G_i$ definido por $y_{i_r} = x_{i_r}$, $1\le r\le n$, $y_i = e_i$ si $i\in I - \{i_1,\dots,i_n\}$. Entonces $\psi(\bar y) = \bar z$.

Siendo $\psi = \psi|_{\coprod_{i\in I} G_i}$ y $\operatorname{Ker}\psi = \prod_{i\in I} H_i$ se prueba fácilmente que

$\operatorname{Ker}\psi = \prod_{i\in I} H_i \cap \coprod_{i\in I} G_i = \coprod_{i\in I} H_i$.

Según PROPOSICION 2.1. (Tema 4º): $\dfrac{\coprod_{i\in I} G_i}{\coprod_{i\in I} H_i} \simeq \psi\left(\coprod_{i\in I} G_i\right) = \coprod_{i\in I} \left(G_i/H_i\right)$. c.s.q.d.

* Si el conjunto de índices I es finito, $I=\{1,\dots,n\}$, la proposición anterior dice que:

$$\frac{G_1 \times G_2 \times \dots \times G_n}{H_1 \times H_2 \times \dots \times H_n} \simeq \frac{G_1}{H_1} \times \frac{G_2}{H_2} \times \dots \times \frac{G_n}{H_n}$$

1.5. COROLARIO: Si G es producto directo de dos subgrupos H y K, entonces

$$G/H \simeq K.$$

Demostr: Siendo $H \simeq H \times \{1\}$

$$G/H = H\times K/H \simeq \frac{H\times K}{H\times\{1\}} \simeq \frac{H}{H} \times \frac{K}{\{1\}} \simeq \frac{K}{\{1\}} \simeq K. \quad \text{c.s.q.d.}$$

OBSERVACION: Para grupos cíclicos y grupos abelianos utilizaremos notación aditiva.

1.6. PROPOSICION: Sean n y m números enteros positivos primos entre sí. Entonces G es un grupo cíclico de orden $n\times m$ si y solo si G es suma directa de dos grupos cíclicos de órdenes n y m, respectivamente.

Demostr.: $\Rightarrow$] Sea G un grupo cíclico de orden $n\times m$. Según COROLARIO 4.2, Tema 1:
$[n \mid o(G)]$ y $[G$ cíclico$] \Rightarrow [\exists x \in G / o(x)=n]$. Análogamente:
$[m \mid o(G)]$ y $[G$ cíclico$] \Rightarrow [\exists y \in G / o(y)=m]$.
Sea $H = \langle x\rangle + \langle y\rangle = \{\lambda x + \mu y / \lambda,\mu \in \mathbb{Z}\}$. Entonces H es subgrupo de G.
Veamos que G es suma directa de $\langle x\rangle$ e $\langle y\rangle$. Siendo G cíclico, es abeliano. Luego $\langle x\rangle$ e $\langle y\rangle$ son subgrupos normales de G.
Además $\langle x\rangle \cap \langle y\rangle = \{0\}$: Sea $z \in \langle x\rangle \cap \langle y\rangle$, entonces
$o(z) \mid o(x) \wedge o(z) \mid o(y) \Rightarrow o(z) \mid mcd(n,m) \Rightarrow o(z)=1 \Rightarrow z=0$.
Si probamos, por último, que $H=G$ quedará probado, por TEOREMA 1.2 que G es suma directa de $\langle x\rangle$ e $\langle y\rangle$. Según lo probado anteriormente, $H = \langle x\rangle \oplus \langle y\rangle$. Según COROLARIO 1.3, $o(H) = o(\langle x\rangle)\, o(\langle y\rangle) = n\cdot m$.
Luego, $[o(H)=o(G)]$ y $[H$ subgrupo de $G] \Rightarrow H=G$. Luego
$G = \langle x\rangle \oplus \langle y\rangle$.

$\Leftarrow$] Supongamos que $G = \langle x\rangle \oplus \langle y\rangle$, con $o(x)=n$, $o(y)=m$ y $(n,m)=1$.
Observar que $\langle x\rangle$ e $\langle y\rangle$ no tienen porque ser subgrupos de G. En principio G es un conjunto de pares de la forma $(\lambda x, \mu y)$, $\lambda,\mu \in \mathbb{Z}$.
Si $o(x)=n \Rightarrow o(x,0)=n$, y $o(y)=m \Rightarrow o(0,y)=m$.
Entonces $n\cdot m\,(x,y) = (n\cdot m\, x, n\cdot m\, y) = (0,0)$ / $o(x,y) \mid$

Veamos que $nm \mid o(x,y)$, y quedará visto que $o(x,y) = nm$.
Si $K \in \mathbb{Z}$ verifica que $K(x,y) = (0,0)$ se tiene que:
$(Kx, Ky) = (0,0) \Rightarrow Kx = 0 \wedge Ky = 0 \Rightarrow n \mid K \wedge m \mid K \Rightarrow$
$\Rightarrow mcm(n,m) \mid K$. Siendo $(n,m) = 1$, $mcm(n,m) = nm$.
Luego $nm \mid K$. En particular, $K = o(x,y)$ verifica que $K(x,y) = (0,0)$.
Luego $nm \mid o(x,y)$. Por tanto, $o(x,y) = nm$.
Siendo $o(G) = o(\langle x \rangle \oplus \langle y \rangle) = o(\langle x \rangle) \cdot o(\langle y \rangle) = n \cdot m$, se verifica que $o(\langle (x,y) \rangle) = o(G)$. Como $\langle (x,y) \rangle$ es subgrupo de G, debe ser $G = \langle (x,y) \rangle$ (*) c.s.q.d.

1.7. COROLARIO: Sea G un grupo finito de orden n y $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la descomposición de n en producto de factores primos. Entonces, G es cíclico si y solo si es suma directa de r grupos cíclicos de órdenes $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$, respectivamente.

Demostración: Procederemos por inducción sobre r.
- Si $r = 2$, siendo $p_1^{\alpha_1}$ y $p_2^{\alpha_2}$ primos entre sí, pues p_1 y p_2 son primos, por el teorema anterior, G es cíclico sii es suma directa de dos grupos cíclicos de órdenes $p_1^{\alpha_1}$ y $p_2^{\alpha_2}$.
- Supuesto que todo grupo G' de orden $p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$ es cíclico sii es suma directa de grupos cíclicos de órdenes $p_1^{\alpha_1}, \ldots, p_{r-1}^{\alpha_{r-1}}$, probemos que si G es tal que $o(G) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, entonces G es cíclico si y solo si es suma directa de r grupos cíclicos de órdenes $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$.
Siendo $mcd(p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}, p_r^{\alpha_r}) = 1$, G es cíclico sii es suma directa de dos grupos cíclicos G' y G_r de órdenes respectivos $p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$ y $p_r^{\alpha_r}$, $G = G' \oplus G_r$. Siendo $o(G') = p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$, G' es cíclico sii es suma directa de $r-1$ grupos cíclicos de órdenes $p_1^{\alpha_1}, \ldots, p_{r-1}^{\alpha_{r-1}}$, $G' = G_1 \oplus \ldots \oplus G_{r-1}$. Luego G es cíclico sii es suma directa de r grupos cíclicos de órdenes respectivos $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$, $G = G_1 \oplus \ldots \oplus G_r$.
c.s.q.d

TEMA 6º: GRUPOS ABELIANOS

1. Grupos p-primarios

DEFINICION: Un grupo G se dice p-primario, siendo p un número primo, si para cada $x \in G$, $o(x)$ es una potencia de p.

1.1. PROPOSICION: Sea G un grupo finito. Entonces, G es p-primario si y solo si G es un p-grupo.

Demostr.: $\Rightarrow$| Sea q un número primo tal que $q \mid o(G)$. Siendo G finito, existe un elemento x de G tal que $o(x)=q$. Siendo G un grupo p-primario, $o(x)$ es potencia de p. Como q es primo debe ser $p=q$. Luego, el único número primo que divide a $o(G)$ es p, lo cual prueba que G es un p-grupo.

$\Leftarrow$| Si G es un p-grupo, $o(G)=p^n$. Entonces, como para cada $x \in G$, $o(x) \mid o(G)$ se tiene que $o(x) \mid p^n$ y, siendo p primo, se verifica que $o(x)$ es potencia de p. csqd.

2. Descomposición de un grupo abeliano finito p-primario como suma directa de grupos cíclicos

2.1. PROPOSICION: Toda suma directa de grupos cíclicos es un grupo abeliano.

Demostr.: Sea $G = \bigoplus_{i \in I} \langle x_i \rangle$. Siendo la suma directa, los grupos $\langle x_i \rangle$ y $\langle x_j \rangle$ conmutan elemento a elemento si $i \neq j$. Si $i=j$, siendo $\langle x_i \rangle$ abeliano, los elementos de $\langle x_i \rangle$ conmutan. Luego, dos elementos cualesquiera de G conmutan, lo cual significa que G es abeliano. csqd.

2.2. TEOREMA: Sea G un grupo abeliano finito. Entonces G es suma directa de sus subgrupos de Sylow. (*)

Demostr.: Sea $n = o(G)$. Entonces, por Teorema 3.2. (Tema 4º), para cada número primo p que divide a n existe un p-subgrupo de Sylow $S(p)$. Además es único, ya que siendo los p-subgrupos de Sylow de G conjugados, si S' es otro p-subgrupo de Sylow existe $x \in G$ tal que $xS'x^{-1} = S(p)$. Pero G es abeliano, luego todos sus subgrupos son normales y, por tanto, $xS'x^{-1} = S'$. En definitiva, $S' = S(p)$.

Sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la descomposición de n en factores primos.

Probemos que $G = S(p_1) \oplus \ldots \oplus S(p_r)$.

Sea $H = S(p_1) + \ldots + S(p_r)$. Veamos que estas sumas son directas.

Para cada $i \in \{1, \ldots, r\}$, $S(p_i) \lhd H$ ya que $H \subset G$ y $S(p_i) \lhd G$ (G abeliano).

Además, $\forall i \in \{1,\dots,r-1\}$, $S(p_1)+\dots+S(p_i) \cap S(p_{i+1}) = \{0\}$, pues si $x \in S(p_1)+\dots+S(p_i) \cap S(p_{i+1}) \Rightarrow \begin{cases} x = x_1+\dots+x_i, \ x_t \in S(p_t) \\ x \in S(p_{i+1}) \Rightarrow o(x) = p_{i+1}^k \end{cases}$.

Entonces $p_1^{\alpha_1}\dots p_i^{\alpha_i} \cdot x = p_1^{\alpha_1}\dots p_i^{\alpha_i} x_1 + \dots + p_1^{\alpha_1}\dots p_i^{\alpha_i} x_i = 0$ ya que $x_t \in S(p_t)$ y $o(x_t) \mid p_t^{\alpha_t}$.

Entonces $o(x) \mid p_1^{\alpha_1}\dots p_i^{\alpha_i}$. Siendo $o(x)$ una potencia de p_{i+1} y p_{i+1} primo con $p_1^{\alpha_1}\dots p_i^{\alpha_i}$, se verifica que $o(x)=1$, ya que $o(x) \mid mcd(p_1^{\alpha_1}\dots p_i^{\alpha_i}, p_{i+1}^k) = 1$. Por tanto $x=0$.

Luego, según TEOREMA 1.2. (TEMA 5°), $H = S(p_1) \oplus \dots \oplus S(p_r)$.

Como $o(H) = o(S(p_1))\cdots o(S(p_r)) = p_1^{\alpha_1}\cdots p_r^{\alpha_r} = n = o(G)$ se verifica que $H = G$, y, por tanto, $G = \bigoplus_{i=1}^{r} S(p_i)$. c.s.q.d.

2.3. Lema: Sea G un grupo abeliano p-primario. Sean $y_1,\dots,y_t$ elementos de G tales que $\langle y_1,\dots,y_t\rangle = \langle y_1\rangle \oplus \dots \oplus \langle y_t\rangle$. Entonces:

a) Si para cada $i \in \{1,\dots,t\}$, $y_i = p z_i$ con $z_i \in G$, entonces $\langle z_1,\dots,z_t\rangle = \langle z_1\rangle \oplus \dots \oplus \langle z_t\rangle$.

b) Sea, para cada $i \in \{1,\dots,t\}$, $k_i \in \mathbb{Z}$ tal que $k_i y_i \neq 0$. Entonces, $\langle k_1 y_1,\dots,k_t y_t\rangle = \langle k_1 y_1\rangle \oplus \dots \oplus \langle k_t y_t\rangle$.

Demostr.: a) Siendo G abeliano, $\langle z_i\rangle$ y $\langle z_j\rangle$ conmutan elemento a elemento. Si probamos que $\sum_{i=1}^{t} n_i z_i = 0 \Rightarrow \forall i \in \{1,2,\dots,t\}$, $n_i z_i = 0$, quedará probado, según teorema 1.2. aptdo d (Tema 5), que G es suma directa de los grupos cíclicos $\langle z_1\rangle,\dots,\langle z_t\rangle$. (*)

Si $\sum_{i=1}^{t} n_i z_i = 0 \Rightarrow p\sum_{i=1}^{t} n_i z_i \overset{(*)}{=} \sum_{i=1}^{t} n_i (p z_i) = 0 \Rightarrow \sum_{i=1}^{t} n_i y_i = 0 \Rightarrow \forall i \in \{1,\dots,t\}$, $n_i y_i = 0$ pues $\langle y_1,\dots,y_t\rangle = \langle y_1\rangle \oplus \dots \oplus \langle y_t\rangle$. Siendo G un grupo p-primario, para cada $i \in \{1,\dots,t\}$, existe $e_i \geq 1$ tal que $o(y_i) = p^{e_i}$.

Siendo $n_i y_i = 0$ se deduce que $p^{e_i} \mid n_i$, $\forall i$, es decir, $\forall i$, $\exists k_i \in \mathbb{Z} / n_i = k_i p^{e_i}$.

Entonces, $0 = \sum_{i=1}^{t} n_i z_i = \sum_{i=1}^{t} k_i p^{e_i} z_i \overset{e_i \geq 1}{=} \sum_{i=1}^{t} k_i p^{e_i - 1} p z_i = \sum_{i=1}^{t} k_i p^{e_i - 1} y_i \Rightarrow$

$\Rightarrow \forall i, 1 \leq i \leq t$, $k_i p^{e_i - 1} y_i = 0$

Como $n_i z_i = k_i p^{e_i - 1} y_i$, $\forall i$, se verifica que $\forall i \in \{1,\dots,t\}$, $n_i z_i = 0$.

Luego $\langle z_1,\dots,z_t\rangle = \langle z_1\rangle \oplus \dots \oplus \langle z_t\rangle$.

b) Procederemos del mismo modo que en a).

$\sum_{i=1}^{t} n_i (k_i y_i) = 0 \Rightarrow \sum_{i=1}^{t} (n_i k_i) y_i = 0$. Como los y_i son "linealmente independientes", $\forall i \in \{1,\dots,t\}$, $(n_i k_i) y_i = 0 \Rightarrow \forall i, 1 \leq i \leq t$, $n_i (k_i y_i) = 0$.

Luego, y como queríamos probar,

$$\langle k_1 y_1,\dots,k_t y_t\rangle = \langle k_1 y_1\rangle \oplus \dots \oplus \langle k_t y_t\rangle.$$

2.4. Lema: Si en un grupo abeliano G todo elemento distinto de 0 es de orden p, entonces G es un espacio vectorial sobre el cuerpo $\mathbb{Z}_p$, (*) donde la multiplicación por escalares se define como sigue:

$$\mathbb{Z}_p \times G \longrightarrow G$$
$$(\bar{K}, x) \longmapsto \bar{K}x = Kx, \text{ siendo } K \in \bar{K}. (\dagger)$$

Además, si G es finito, $\{x_1, \dots, x_n\} \subset G$ es base de G sobre $\mathbb{Z}_p$ si y solo si G es suma directa de los grupos cíclicos $\langle x_1\rangle, \dots, \langle x_n\rangle$.

Demostr.: • Veamos que la ley externa definida anteriormente está bien definida, es decir, que si $\bar{K}_1 = \bar{K}_2$, $K_1, K_2 \in \mathbb{Z}$, entonces $K_1 x = K_2 x$.

$\bar{K}_1 = \bar{K}_2 \Rightarrow K_2 \equiv K_1 \pmod p \Rightarrow \exists s \in \mathbb{Z} / K_2 = K_1 + sp$.

Entonces, $K_2 x = (K_1 + sp)x = K_1 x + spx = K_1 x$, pues $px = 0$, ya que todo elemento de G es de orden p. Probemos que se verifican las propiedades de la ley externa de los espacios vectoriales:

- $\forall x \in G$, $\bar{1}x = 1x = x$
- $\forall \bar{K}_1, \bar{K}_2 \in \mathbb{Z}_p$, $\forall x \in G$, $(\bar{K}_1 \bar{K}_2)x = \overline{K_1 K_2}\, x = (K_1 K_2)x = K_1(K_2 x) = \bar{K}_1(\bar{K}_2 x)$.
- $\forall \bar{K}_1, \bar{K}_2 \in \mathbb{Z}_p$, $\forall x \in G$, $(\bar{K}_1 + \bar{K}_2)x = \overline{K_1 + K_2}\, x = (K_1 + K_2)x = K_1 x + K_2 x = \bar{K}_1 x + \bar{K}_2 x$.
- $\forall \bar{K} \in \mathbb{Z}_p$, $\forall x, y \in G$, $\bar{K}(x+y) = K(x+y) = Kx + Ky = \bar{K}x + \bar{K}y$.

• $\Rightarrow$ Supongamos que $\mathcal{B} = \{x_1, \dots, x_n\}$ es base de G sobre $\mathbb{Z}_p$. Veamos que $G = \langle x_1\rangle \oplus \dots \oplus \langle x_n\rangle$.

Que $G = \langle x_1\rangle + \dots + \langle x_n\rangle$ es trivial pues $\mathcal{B}$ es base de G sobre $\mathbb{Z}_p$, y todo $x \in G$ se puede escribir en la forma: $x = \sum_{i=1}^{n} \bar{K}_i x_i = \sum_{i=1}^{n} K_i x_i$.

Veamos que los x_i son linealmente independientes.

Si $\sum_{i=1}^{n} n_i x_i = 0 \Rightarrow \sum_{i=1}^{n} \bar{n}_i x_i = 0$. Siendo $\{x_i\}_{i=1}^{n}$ base de G, debe ser $\forall i \in \{1, \dots, n\}$, $\bar{n}_i = \bar{0}$; luego $\forall i \in \{1, \dots, n\}$, n_i es múltiplo de p. Siendo los elementos de G de orden p se tiene entonces que $n_i x_i = 0$, $\forall i \in \{1, \dots, n\}$.

Luego $G = \bigoplus_{i=1}^{n} \langle x_i\rangle$

$\Leftarrow$ Supongamos que $G = \bigoplus_{i=1}^{n} \langle x_i\rangle$. Veamos que $\mathcal{B} = \{x_1, \dots, x_n\}$ es base de G sobre $\mathbb{Z}_p$. $\mathcal{B}$ es sistema de generadores pues $G = \sum_{i=1}^{n} \langle x_i\rangle$, y $x = \sum_{i=1}^{n} K_i x_i = \sum_{i=1}^{n} \bar{K}_i x_i$. Veamos que $\mathcal{B}$ es libre.

Si $\sum_{i=1}^{n} \bar{n}_i x_i = 0 \Rightarrow \sum_{i=1}^{n} n_i x_i = 0 \Rightarrow n_i x_i = 0$, $\forall i \in \{1, \dots, n\}$, pues G es suma directa de los subgrupos $\langle x_i\rangle$.

Luego, siendo $o(x_i) = p$, n_i es múltiplo de p, $1 \le i \le n$.

Por tanto, $n_i \equiv 0 \pmod p \Rightarrow \bar{n}_i = \bar{0}$, $\forall i \in \{1, \dots, n\}$. c.q.d.

Veamos a continuación un teorema importante.

2.5. TEOREMA: Si G es grupo abeliano finito p-primario, admite una descomposición como suma directa de grupos cíclicos.

Demostr.: Siendo G finito y p-primario es un p-grupo (PROPOSICION 11). Luego $o(G)$ es una potencia de p. Supongamos que $o(G)=p^{m+1}$. Entonces $p^{m+1}G=\{0\}$. Probaremos el teorema por inducción sobre m.

- Si $m=0$, $pG=\{0\}$. En este caso todos los elementos de $G-\{0\}$ serían de orden p y, según lema 2.4, G sería espacio vectorial sobre $\mathbb{Z}_p$. Siendo G finito, admite una base $\{x_1,\dots,x_n\}$ y, en consecuencia, $G=\langle x_1\rangle\oplus\dots\oplus\langle x_n\rangle$.

- Supongamos que todo grupo finito abeliano H que verifique $p^mH=\{0\}$ se puede descomponer como suma directa de grupos cíclicos. Probemos, con esta hipótesis de inducción, que siendo $p^{m+1}G=\{0\}$ se verifica que G se puede expresar como suma directa de grupos cíclicos.

Sea $H=pG=\{px\in G / x\in G\}$. H es subgrupo de G, pues $\forall u,v\in H$, $\exists x,y\in G / u=px \wedge v=py$. Entonces, $u-v=px-py=p(x-y)\in H$.

Además $p^mH=p^{m+1}G=\{0\}$. Entonces, por hipótesis de inducción:

$$H=\langle y_1\rangle\oplus\dots\oplus\langle y_t\rangle \qquad (I)$$

Los elementos de H son de la forma px, $x\in G$. Por tanto, dados $y_1,\dots,y_t\in H$ existen $z_1,\dots,z_t\in G$ tales que $y_i=pz_i$, $\forall i\in\{1,\dots,t\}$. (II)

Entonces, según lema 2.3, $L=\langle z_1,\dots,z_t\rangle=\langle z_1\rangle\oplus\dots\oplus\langle z_t\rangle$.

Sea $G(p)=\{x\in G / px=0\}$. Trivialmente, $G(p)$ es subgrupo de G.

Veamos que $G=L+G(p)$.

Dado $x\in G$, $px\in H$. Entonces, según (I), $\exists\{n_i\}_{i=1}^t\subset\mathbb{Z} / px=\sum_{i=1}^t n_iy_i$, y, según (II), $px=\sum_{i=1}^t n_ipz_i=p\sum_{i=1}^t n_iz_i \Rightarrow p(x-\sum_{i=1}^t n_iz_i)=0$.

Luego $x-\sum_{i=1}^t n_iz_i\in G(p)$.

Por tanto, $x=\sum_{i=1}^t n_iz_i+(x-\sum_{i=1}^t n_iz_i)\in L+G(p)$, pues $\sum_{i=1}^t n_iz_i\in L$ y $x-\sum_{i=1}^t n_iz_i\in G(p)$.

Veamos que esta suma no es directa. Supongamos que $o(y_i)=k_i$, $1\le i\le t$. Siendo G p-primario, $o(y_i)=p^{\alpha_i}$ con $\alpha_i\ge 1$ ya que $y_i\neq 0$. Entonces, $k_iz_i\in L=\langle z_1,\dots,z_t\rangle$. Además $o(k_iz_i)=p$, pues $pk_iz_i=k_ipz_i=k_iy_i=0$, y $k_iz_i\neq 0$ ya que si $k_iz_i=0 \Rightarrow p^{\alpha_i-1}y_i=p^{\alpha_i-1}pz_i=p^{\alpha_i}z_i=k_iz_i=0 \Rightarrow o(y_i)=p^{\alpha_i-1}$, en contra de que $o(y_i)=p^{\alpha_i}$. Luego $o(k_iz_i)\mid p$ y $o(k_iz_i)\neq 1 \Rightarrow o(k_iz_i)=p$, pues p es primo.

Entonces $\forall i\in\{1,\dots,t\}$, $k_iz_i\in L\cap G(p)$. Luego $L\cap G(p)\neq\{0\}$

se tiene que $\langle K_1 z_1, \dots, K_t z_t \rangle = \langle K_1 z_1 \rangle \oplus \dots \oplus \langle K_t z_t \rangle$. (III)

Por definición, los elementos de $G(p) - \{0\}$ son de orden p. Entonces $G(p)$ es un espacio vectorial sobre el cuerpo $\mathbb{Z}_p$. De (III) se deduce que los $K_i z_i$, $1 \le i \le t$, son linealmente independientes en $G(p)$. Siendo G finito, $G(p)$ es de dimensión finita; luego el sistema libre $\{K_i z_i\}_{i=1}^t$ se puede prolongar a una base de $G(p)$

$$\mathcal{B} = \{K_1 z_1, \dots, K_t z_t, x_1, \dots, x_s\} \quad (IV).$$

En particular, $\{x_j\}_{j=1}^s$ es un sistema libre en $G(p)$ y, en consecuencia, $\langle x_1, \dots, x_s \rangle = \langle x_1 \rangle \oplus \dots \oplus \langle x_s \rangle$. Sea $H = \langle x_1, \dots, x_s \rangle$.

Probemos que $G = L \oplus H$, con lo cual quedará terminada la demostración, ya que L y H son sumas directas de grupos cíclicos.

- $L \cap H = \{0\}$: Sea $x \in L \cap H$, entonces $x = \sum_{i=1}^t a_i z_i = \sum_{j=1}^s b_j x_j$

$x \in H \subset G(p) \Rightarrow px = 0$; luego $\sum_{j=1}^s b_j p x_j = 0 \Rightarrow \sum_{i=1}^t a_i p z_i = 0 \Rightarrow$

$\Rightarrow \sum_{i=1}^t a_i y_i = 0 \Rightarrow a_i y_i = 0$, $1 \le i \le t$, pues los y_i son linealmente independientes. Entonces, siendo $K_i = o(y_i)$, $K_i \mid a_i$, $\forall i \in \{1, \dots, t\}$. Sea $a_i = K_i c_i$, $1 \le i \le t$.

Entonces, $\sum_{i=1}^t c_i K_i z_i = \sum_{j=1}^s b_j x_j \Rightarrow \sum_{i=1}^t c_i K_i z_i - \sum_{j=1}^s b_j x_j = 0$. (V)

Pero según (IV), $\mathcal{B} = \{K_i z_i\}_{i=1}^t \cup \{x_j\}_{j=1}^s$ es base de $G(p)$. Entonces, de (V) se deduce que: $c_i K_i z_i = 0$, $1 \le i \le t$, $b_j x_j = 0$, $1 \le j \le s$. Luego $x = \sum_{j=1}^s b_j x_j = 0$.

- $L + H = G$: Sea $x \in G$, entonces $px \in H$. De (I) deducimos que

$$\exists \{n_i\}_{i=1}^t \subset \mathbb{Z} / px = \sum_{i=1}^t n_i y_i$$

Entonces $px = \sum_{i=1}^t n_i p z_i \Rightarrow p\left(x - \sum_{i=1}^t n_i z_i\right) = 0$.

Luego, por definición de $G(p)$, $x - \sum_{i=1}^t n_i z_i \in G(p)$.

Siendo $G(p) = \langle K_1 z_1 \rangle \oplus \dots \oplus \langle K_t z_t \rangle \oplus \langle x_1 \rangle \oplus \dots \oplus \langle x_s \rangle$, existen $s_1, \dots, s_t, r_1, \dots, r_s \in \mathbb{Z}$ tales que $x - \sum_{i=1}^t n_i z_i = \sum_{i=1}^t s_i K_i z_i + \sum_{k=1}^s r_k x_k$

Por tanto, $x = \sum_{i=1}^t (n_i + s_i K_i) z_i + \sum_{k=1}^s r_k x_k$.

Como $\sum_{i=1}^t (n_i + s_i K_i) z_i \in L$ y $\sum_{k=1}^s r_k x_k \in H$, se tiene que $x \in L + H$.

En definitiva, $G = L \oplus H = \langle z_1 \rangle \oplus \dots \oplus \langle z_t \rangle \oplus \langle x_1 \rangle \oplus \dots \oplus \langle x_s \rangle$. c.s.g.d.

2.6. TEOREMA: (de la estructura primaria de un grupo abeliano finito).

> Un grupo finito G es abeliano si y solo si es suma directa (finita) de grupos cíclicos primarios (*)

Demostr.: $\Rightarrow$] Si G es un grupo abeliano finito, por teorema 2.5 es suma

directa de sus subgrupos de Sylow $\{S_p\}_{p\in P}$ siendo P el conjunto de los números primos, distintos de 1 que dividen a $o(G)$. Para cada p, S_p es un p-subgrupo y, por tanto, p-primario ya que S_p es finito. Luego, para cada p, S_p es un grupo abeliano finito y p-primario y, por tanto, en virtud del teorema 2.5, S_p es suma directa de grupos cíclicos. En definitiva, G es suma directa de grupos cíclicos, que son primarios ya que el orden de uno cualquiera de estos grupos cíclicos divide al orden de un S_p, que es un p-grupo.

$\Leftarrow$ Si G es suma directa finita de grupos cíclicos primarios (no es necesario que sean primarios) es abeliano según PROPOSICIÓN 2.1. c.s.q.d.

2.7. COROLARIO: (Estructura canónica de un grupo abeliano finito).

a) Sea G un grupo abeliano finito. Entonces G es suma directa de grupos cíclicos $\sigma(u_1),\dots,\sigma(u_s)$ donde $u_i = o(\sigma(u_i))$ y $u_i \mid u_{i-1}$, $2\le i\le s$: $G = \sigma(u_1)\oplus\dots\oplus\sigma(u_s)$

b) Si G es finito, G es abeliano si y solo si G admite una estructura canónica, es decir, si se descompone como suma directa de grupos cíclicos de la forma del aptado a).

Demostr.: a) Si G es abeliano finito, G es suma directa de grupos cíclicos primarios, según el teorema anterior. Para cada primo p_i divisor de $o(G)$ consideremos un sumando cíclico de orden maximal, es decir, tomamos para cada p_i un grupo cíclico de la descomposición de G de orden $p_i^{e_i}$, siendo ésta la mayor potencia de p_i que aparece en el conjunto de los órdenes de los grupos cíclicos citados. Sea $\sigma(p_i^{e_i})$ el sumando considerado para cada p_i. Si tenemos r primos, $p_1,\dots,p_r$ distintos de 1 que dividen a $o(G)$, llamamos

$$\sigma(u_1) = \bigoplus_{i=1}^{r} \sigma(p_i^{e_i})$$

Entonces, por COROLARIO 1.7, $\sigma(u_1)$ es cíclico y $u_1 = o(\sigma(u_1)) = \prod_{i=1}^{r} p_i^{e_i}$

Si H_1 es la suma directa de los grupos cíclicos de la descomposición primaria de G, salvo los sumandos de $\sigma(u_1)$ se tiene que:

$$G = \sigma(u_1)\oplus H_1$$

Análogamente, en la estructura primaria de H_1 seleccionamos para cada p_i un sumando cíclico de orden maximal: $\sigma(p_i^{f_i})$; trivialmente $\forall i\in\{1,\dots,r\}$, $f_i\le e_i$. Sea $\sigma(u_2) = \bigoplus_{i=1}^{r}\sigma(p_i^{f_i})$, con $u_2 = o(\sigma(u_2)) = \prod_{i=1}^{r} p_i^{f_i}$ (Eventualmente, algún $p_i^{f_i}$ puede ser igual a 1). Entonces u_2 divide a u_1. Si H_2 es la suma directa de los grupos cíclicos que

$G = \sigma(u_1) \oplus \sigma(u_2) \oplus H_2$.

Así sucesivamente, en un número s finito de pasos llegamos a que G se puede descomponer en la forma

$G = \sigma(u_1) \oplus \sigma(u_2) \oplus \ldots \oplus \sigma(u_s)$ donde $\sigma(u_i)$ son cíclicos, y $u_i \mid u_{i-1}$, $2 \leq i \leq s$.

b) $\Rightarrow$| Trivial por a)

$\Leftarrow$| Si G admite una estructura canónica, es suma directa de unos ciertos grupos cíclicos y, por tanto, G es abeliano. c.s.q.d.

Antes de probar que la descomposición primaria de un grupo G abeliano finito es única, en el sentido de que dos descomposiciones primarias de G tienen el mismo número de sumandos de cada orden, veamos unos lemas preliminares.

2.8. Lema: Si G es un grupo abeliano finito elemental, es decir, un grupo en el que todo elemento distinto de 0 es de orden p, o lo que es equivalente, tal que $p \cdot G = \{0\}$, entonces dos descomposiciones de G en suma directa de grupos cíclicos tienen el mismo número de sumandos, los cuales serán de orden p, trivialmente.

Demostr.: Si $pG = \{0\}$, por Lema 2.4, G es un espacio vectorial sobre $\mathbb{Z}_p$. Siendo G de dimensión finita, admite una base $\mathcal{B} = \{x_1, \ldots, x_n\}$. Pero $\mathcal{B} = \{x_1, \ldots, x_n\}$ es base de G sobre $\mathbb{Z}_p$ si y solo si $G = \bigoplus_{i=1}^{n} \langle x_i \rangle$. Luego G es suma directa de los grupos cíclicos $\langle x_1 \rangle, \ldots, \langle x_n \rangle$.

Si G admite otra descomposición como suma directa de grupos cíclicos $G = \langle y_1 \rangle \oplus \ldots \oplus \langle y_r \rangle$, entonces $\{y_1, \ldots, y_r\}$ es base de G. Dos bases tienen siempre el mismo número de elementos; luego $r = n$. c.s.q.d.

DEFINICION: Si H es un grupo abeliano elemental, llamamos $d(H)$ al número de sumandos de cualquier estructura primaria de H, que sabemos que es único para cada H grupo abeliano elemental, según el teorema anterior.

2.9. Lema: Si G es una suma directa de b copias (*) de grupos cíclicos de órdenes p^k, entonces

$\forall n \leq K$, $d\left(\frac{p^n G}{p^{n+1} G}\right) = b$

Demostr.: Sea $G = \langle a_1 \rangle \oplus \ldots \oplus \langle a_b \rangle$ con $o(a_i) = p^K$, $1 \leq i \leq b$.

Trivialmente $\frac{p^n G}{p^{n+1} G}$ es un grupo, pues $p^{n+1} G = p(p^n G)$ que es subgrupo de $p^n G$ y normal pues G es abeliano, por ser suma directa de grupos cíclicos. Veamos que $\frac{p^n G}{p^{n+1} G}$ es elemental

para que tenga sentido hablar de $d(p^n G/p^{n+1}G)$.

$\forall z \in p^n G/p^{n+1}G$, $\exists x \in G / z = p^n x + p^{n+1}G$. Entonces:

$pz = p(p^n x + p^{n+1}G) \overset{(*)}{=} p^{n+1}x + p^{n+1}G = p^{n+1}G = \bar{0}$ ya que $p^{n+1}G$ es el neutro de $p^nG/p^{n+1}G$. Luego los elementos de $p^nG/p^{n+1}G$ distintos de $\bar{0}$ son de orden p, que prueba que $p^nG/p^{n+1}G$ es elemental.

Veamos ahora que $p^nG = \langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle$, $\forall n < K$.

Siendo $n<K \Rightarrow p^n < p^K = o(\langle a_i\rangle)$, $1 \le i \le b$. Entonces, $n<K \Rightarrow p^n a_i \neq 0$.

Luego, según Lema 2.3, siendo $G = \langle a_1, \dots, a_b\rangle = \langle a_1\rangle \oplus \dots \oplus \langle a_b\rangle$ pues siempre $\langle a_1\rangle \oplus \dots \oplus \langle a_b\rangle \subset \langle a_1, \dots, a_b\rangle$, se verifica que

$$\langle p^n a_1, \dots, p^n a_b\rangle = \langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle.$$

Siempre se tiene $p^nG \supset \langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle$, pues si $x \in \bigoplus_{i=1}^{b} \langle p^n a_i\rangle \Rightarrow x = \sum_{i=1}^{b} p^n n_i a_i = p^n \sum_{i=1}^{b} n_i a_i \in p^nG$.

Además $p^nG \subset \langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle$, pues $x \in G \Rightarrow x = \sum_{i=1}^{b} n_i a_i \Rightarrow$
$\Rightarrow p^n x = p^n \sum_{i=1}^{b} n_i a_i = \sum_{i=1}^{b} n_i p^n a_i \in \langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle$.

Luego $p^nG = \langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle$.

Análogamente $p^{n+1}G = \langle p^{n+1}a_1\rangle \oplus \dots \oplus \langle p^{n+1}a_b\rangle$ si $n+1<K$.

En este caso:

$$(I)\quad \frac{p^nG}{p^{n+1}G} = \frac{\langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle}{\langle p^{n+1}a_1\rangle \oplus \dots \oplus \langle p^{n+1}a_b\rangle} \simeq \frac{\langle p^n a_1\rangle}{\langle p^{n+1}a_1\rangle} \oplus \dots \oplus \frac{\langle p^n a_b\rangle}{\langle p^{n+1}a_b\rangle}$$

en virtud de la PROPOSICION 1.4. Tema 5º. Cada sumando directo de los anteriores es un grupo cíclico: $\dfrac{\langle p^n a_i\rangle}{\langle p^{n+1}a_i\rangle} = \langle p^n a_i + \langle p^{n+1}a_i\rangle\rangle$ trivialmente (PROPOSICION 3.3, Tema 1º), y además, todos son de orden p, pues $p(p^n a_i + \langle p^{n+1}a_i\rangle) =$
$= p^{n+1}a_i + \langle p^{n+1}a_i\rangle = \langle p^{n+1}a_i\rangle = \bar{0}$.

Luego, según (I), $\dfrac{\langle p^n a_1\rangle}{\langle p^{n+1}a_1\rangle} \oplus \dots \oplus \dfrac{\langle p^n a_b\rangle}{\langle p^{n+1}a_b\rangle}$ es una descomposición primaria de $p^nG/p^{n+1}G$ como suma directa de grupos cíclicos.

Siendo $p^nG/p^{n+1}G$ elemental, $d(H)$ es constante y coincide con el número de sumandos en (I), es decir: $d(H) = b$, siendo $H = p^nG/p^{n+1}G$. (Esto se basa en el aptdo b) del lema siguiente).

Si $n+1 = K \Rightarrow p^{n+1}a_i = 0$, $1 \le i \le b$. Entonces $p^{n+1}G \neq \{0\}$.

Entonces $p^nG/p^{n+1}G \simeq p^nG = \langle p^n a_1\rangle \oplus \dots \oplus \langle p^n a_b\rangle$.

que son sumandos cíclicos. Siendo $p^nG/p^{n+1}G$ elemental, se tiene

$$d(p^nG/p^{n+1}G) = b. \qquad \text{c.s.q.d.}$$

2.10. LEMA: a) Sean H y K dos grupos abelianos elementales ($pH=pK=\{0\}$) y $G = H \oplus K$. Entonces G es elemental y $d(G) = d(H) + d(K)$. Este resultado es válido para una suma directa finita de grupos abelianos elementales.

b) Sea G un grupo elemental y H un grupo isomorfo a G. Entonces H es elemental y $d(H) = d(G)$.

Demostr.: a) $\forall x \in G$, $\exists (x_H, x_K) \in H \times K / x = x_H + x_K$.

Entonces $px = p(x_H + x_K) = px_H + px_K = 0 + 0 = 0$. Luego G es elemental.

Si $H = \bigoplus_{i=1}^{n_H} \langle h_i \rangle$ y $K = \bigoplus_{i=1}^{n_K} \langle k_i \rangle$ se tiene que $d(H) = n_H$ y $d(K) = n_K$. Siendo $G = H \oplus K$, $G = \left(\bigoplus_{i=1}^{n_H} \langle h_i \rangle\right) \oplus \left(\bigoplus_{j=1}^{n_K} \langle k_j \rangle\right)$.

El número de sumandos en esta descomposición cíclica de G es $n_H + n_K = d(H) + d(K)$. Siendo G elemental, el número de sumandos de cualquier descomposición cíclica de G es invariante; luego:

$$d(G) = d(H) + d(K).$$

Fácilmente se generaliza este resultado para un número finito de sumandos $G = H_1 \oplus \dots \oplus H_n$.

b) Si G es elemental, existe un número primo p tal que $pG = \{0\}$.

$\forall h \in H$, $\exists g \in G / \phi(g) = h$, siendo ϕ el isomorfismo que existe, por hipótesis, entre G y H. Entonces, $ph = p\phi(g) = \phi(pg) = \phi(0) = 0$

Luego $pH = \{0\}$ que prueba que H es elemental. Tiene, entonces, sentido hablar de $d(H)$.

Sea $G = \langle g_1 \rangle \oplus \dots \oplus \langle g_n \rangle$. Siendo G elemental, $d(G) = n$.

Sea $h_i = \phi(g_i)$, $1 \le i \le n$. Veamos que $H = \langle h_1 \rangle \oplus \dots \oplus \langle h_n \rangle$, con lo cual, siendo H elemental, quedará visto que $d(H) = n = d(G)$.

- $\langle h_i \rangle$ y $\langle h_j \rangle$ conmutan elemento a elemento: $\forall a_i, a_j \in \mathbb{Z}$, $a_i h_i + a_j h_j = a_i \phi(g_i) + a_j \phi(g_j) =$
$= \phi(a_i g_i + a_j g_j) = \phi(a_j g_j + a_i g_i) = a_j h_j + a_i h_i$.

- $\sum_{i=1}^{n} a_i h_i = 0 \Rightarrow \sum_{i=1}^{n} a_i \phi(g_i) = 0 \Rightarrow$

$\Rightarrow \phi\left(\sum_{i=1}^{n} a_i g_i\right) = 0 \Rightarrow \sum_{i=1}^{n} a_i g_i = 0$, pues ϕ es inyectiva y $\ker \phi = \{0\}$.

Entonces, siendo $G = \bigoplus_{i=1}^{n} \langle g_i \rangle$, debe ser $a_i g_i = 0$, $1 \le i \le n$.

Luego $a_i h_i = \phi(a_i g_i) = 0$, $1 \le i \le n$.

Por tanto, $H = \bigoplus_{i=1}^{n} \langle h_i \rangle$ y $d(H) = n = d(G)$. c.s.q.d.

2.11. LEMA: Sea $G = \bigoplus_{i=1} C_i$ una descomposición de un grupo finito abeliano p-primario G como suma directa de grupos cíclicos. Entonces $d(p^n G / p^{n+1} G)$ es el número de sumandos cíclicos que tienen orden mayor o igual a p^{n+1}.

Demostr.: Si G es p-primario es un p-grupo y, por tanto, los C_i son p-grupos. Sea B_k la suma directa de los sumandos C_i que tienen órdenes igual a p^k. Entonces $G = B_1 \oplus B_2 \oplus \dots \oplus B_t$.

Luego $p^n G = p^n B_1 \oplus p^n B_2 \oplus \dots \oplus p^n B_n \oplus p^n B_{n+1} \oplus \dots \oplus p^n B_t$ (*)

Como los sumandos cíclicos de $B_1, B_2, \dots, B_n$ son de órdenes respectivos $p, p^2, \dots, p^n$ se tiene que $p^n B_1 = p^{n-1} p B_1 = p^{n-1}\{0\} = \{0\}, \dots, p^n B_n = \{0\}$.

Luego $p^n G = p^n B_{n+1} \oplus \dots \oplus p^n B_t$.

Análogamente $p^{n+1} G = p^{n+1} B_{n+2} \oplus \dots \oplus p^{n+1} B_t$.

Entonces:
$$\frac{p^n G}{p^{n+1} G} \simeq p^n B_{n+1} \oplus \frac{p^n B_{n+2}}{p^{n+1} B_{n+2}} \oplus \dots \oplus \frac{p^n B_t}{p^{n+1} B_t} \quad (I)$$

Como $\frac{p^n G}{p^{n+1} G}$ es elemental y cada uno de los sumandos directos del segundo miembro de (I) son abelianos y elementales, se tiene que:
$$d\left(\frac{p^n G}{p^{n+1} G}\right) = d(p^n B_{n+1}) + d\left(\frac{p^n B_{n+2}}{p^{n+1} B_{n+2}}\right) + \dots + d\left(\frac{p^n B_t}{p^{n+1} B_t}\right)$$

Sea b_i el nº de sumandos cíclicos C_i que hay en B_i. Entonces $d(p^n B_{n+1}) = b_{n+1}$, pues ninguno de los sumandos cíclicos de B_{n+1} se anulan al multiplicarlos por p^n ya que son de orden p^{n+1}.

B_{n+2} es suma de b_{n+2} copias de sumandos cíclicos de orden p^{n+2}. Como $n < n+2$, según lema 2.9, $d\left(\frac{p^n B_{n+2}}{p^{n+1} B_{n+2}}\right) = b_{n+2}$.

Así sucesivamente, $d\left(\frac{p^n B_t}{p^{n+1} B_t}\right) = b_t$. Luego:
$$d\left(p^n G / p^{n+1} G\right) = b_{n+1} + b_{n+2} + \dots + b_t$$
que prueba que $d\left(p^n G / p^{n+1} G\right)$ es el número de sumandos cíclicos de orden mayor o igual que p^{n+1}. c.s.q.d.

DEFINICION: Sea G un grupo abeliano finito p-primario. Llamamos
$$U(n, G) = d\left(\frac{p^{n-1} G}{p^n G}\right) - d\left(\frac{p^n G}{p^{n+1} G}\right)$$

2.12. PROPOSICION: Si G es un grupo abeliano finito p-primario, $U(n, G)$ es un invariante de G y coincide con el número de sumandos de orden p^n que hay en cualquier descomposición primaria de G.

Demostr.: Trivial por lema 2.11.

(*) La demostración de esta igualdad es análoga a la del lema 2.3 b).

Deducimos de esto que en el caso de que G sea p-primario, dos descomposiciones primarias de G tienen el mismo número de sumandos de cada orden. Probaremos esto para cualquier grupo abeliano finito.

2.13. TEOREMA: Sea G un grupo abeliano finito. Entonces dos descomposiciones primarias de G tienen el mismo número de sumandos de cada orden.

Demostr.: Si $p_1, \dots, p_r$ son los primos que dividen a $o(G)$, según teorema 2.7, G es suma directa de sus subgrupos de Sylow: $G = \bigoplus_{i=1}^{r} S_{p_i}$ y en teorema 2.6 obteníamos una descomposición primaria de G a partir de estos subgrupos de Sylow. Cualquier descomposición primaria de G obtenida a partir de los p_i-subgrupos de Sylow tiene el mismo número de sumandos de cada orden, pues S_{p_i} son grupos p_i-primarios y, por lo dicho anteriormente como consecuencia inmediata de PROPOSICIÓN 2.12, toda descomposición primaria de S_{p_i} como suma directa de grupos cíclicos tiene el mismo número de sumandos de cada orden p_i^k; como todos los sumandos directos de G cíclicos de orden p_i^k son también sumandos del correspondiente S_{p_i} queda visto que cualquier descomposición primaria de G como suma directa de grupos cíclicos obtenida a partir de los p_i-subgrupos de Sylow tiene el mismo número de sumandos de cada orden.

Probemos, entonces, que cualquier descomposición primaria de G se puede obtener a partir de sus subgrupos de Sylow y el teorema quedará demostrado.

Sea $G = \oplus C_j$ una descomposición primaria de G como suma directa de grupos cíclicos. Para cada p_i^{mmo} divisor de $o(G)$ sea S'_{p_i} la suma directa de los sumandos C_j cuyos órdenes son potencias de p_i. Entonces, $G = S'_{p_1} \oplus \dots \oplus S'_{p_r}$. Veamos que $S'_{p_i} = S_{p_i}$, es decir, que S'_{p_i} es una descomposición primaria de S_{p_i} y el teorema quedará probado. Antes veremos que $S'_{p_i} = \{x \in G / o(x) \text{ es potencia de } p_i\}$. Sea $x \in G$ tal que $o(x) = p_i^{\alpha}$. Si $x \in G$, $x = x_1 + \dots + x_r$, $x_j \in S'_{p_j}$. Entonces $p_i^{\alpha} x = p_i^{\alpha} x_1 + \dots + p_i^{\alpha} x_r = 0$. Como $G = \bigoplus_{i=1}^{r} S'_{p_i}$, debe ser $p_1^{\alpha} x_1 = \dots = p_r^{\alpha} x_r = 0$. Si $j \neq i$, $p_i^{\alpha} x_j = 0 \Rightarrow x_j = 0$, pues si fuese $x_j \neq 0$ y $p_i^{\alpha} x_j = 0 \Rightarrow p_i^{\alpha}$ es múltiplo de $o(x_j)$ que es una potencia de p_j, lo cual es absurdo pues p_j y p_i son números primos distintos y ninguna potencia de p_j divide a otra potencia de p_i. En definitiva, $i \neq j \Rightarrow x_j = 0$. Luego: $x = x_i \in S'_{p_i}$. Además $S'_{p_i} \subset \{x \in G / o(x) \text{ es potencia de } p_i\}$ pues si $x \in S_{p_i}$, se escribe

como suma de unos elementos $x_{i_1}, \dots, x_{i_t}$ que tienen de orden una potencia de p_i; luego $o(x)$ es potencia de p_i.

Veamos ahora que $S'_{p_i} = S_{p_i}$.

$S'_{p_i} \subset S_{p_i}$ pues S'_{p_i} es un grupo p_i-primario finito y, por tanto, un p_i-grupo. Luego, este p_i-grupo está contenido en el p_i-subgrupo de Sylow correspondiente.

Además $S_{p_i} \subset S'_{p_i}$ porque siendo S_{p_i} un p_i-grupo, todo elemento de S_{p_i} tiene de orden una potencia de p_i.

Luego los sumandos cíclicos que se encontraban en S'_{p_i} son una descomposición primaria de S_{p_i} y, en consecuencia, como se indicó anteriormente, cualquier descomposición primaria de G tiene el mismo número de sumandos de cada orden. c.s.q.d.

2.14. TEOREMA: Sean G y H grupos abelianos finitos. Entonces G y H son isomorfos si y solo si admiten descomposiciones primarias del mismo tipo, es decir, con el mismo número de sumandos de cada orden.

Demostración: - 1º caso: Supongamos que G y H son p-primarios.

Veamos que $G \simeq H \iff U(n,G) = U(n,H)$ para cada n.

Si $G \simeq H$ entonces $\frac{p^n G}{p^{n+1} G} \simeq \frac{p^n H}{p^{n+1} H}$ trivialmente.

Luego $d\left(\frac{p^n G}{p^{n+1} G}\right) = d\left(\frac{p^n H}{p^{n+1} H}\right)$

Esto es válido para cada n; luego, por definición de $U(n,G)$ y $U(n,H)$, se tiene que $U(n,G) = U(n,H)$.

Recíprocamente, si $U(n,G) = U(n,H)$, G y H admiten descomposiciones primarias con el mismo número de sumandos de cada orden.

Siempre podemos definir un isomorfismo φ_i entre dos sumandos, uno C_i de G y otro C'_i de H, del mismo orden. Estos isomorfismos se pueden extender a un isomorfismo $\phi: G = \oplus C_i \longrightarrow H = \oplus C'_i$ definido por $\phi(x_1 + \dots + x_n) = \phi(x_1) + \dots + \phi(x_n)$ siendo $\phi_{|C_i} = \varphi_i$.

Luego $G \simeq H$

- 2º caso: (Caso General) $\Rightarrow$ Si $G \simeq H$, $S_{p_i} \simeq S'_{p_i}$ siendo S_{p_i} un p_i-subgrupo de Sylow de G y S'_{p_i} un p_i-subgrupo de Sylow de H, pues si $f: G \to H$ es un isomorfismo, $f(S_{p_i}) \subset S'_{p_i}$, ya que si $x \in S_{p_i}$, $o(x) = p_i^{\alpha} \Rightarrow p_i^{\alpha} f(x) = f(p_i^{\alpha} x) = f(0) = 0 \Rightarrow o(f(x)) \mid p_i^{\alpha} \Rightarrow$ $\Rightarrow o(f(x))$ es potencia de p_i y, por tanto, $f(x) \in S'_{p_i}$. Además, como f es biyectiva, $o(G) = o(H)$ y si p_i^n es la mayor potencia de p_i que divide a $o(G)$ ($o(S_{p_i}) = p_i^n$) entonces p_i^n es la mayor potencia de p_i que divide a $o(H)$ (y, por tanto, $o(S'_{p_i}) = p_i^n$). Luego: $f(S_{p_i}) = S'_{p_i}$

to $f|_{S_{p_i}}$ es un isomorfismo entre S_{p_i} y S'_{p_i}. Luego $G \simeq H \Rightarrow S_{p_i} \simeq S'_{p_i}$. Recíprocamente, si $f_i : S_{p_i} \longrightarrow S'_{p_i}$ es un isomorfismo, para cada i, como $G = \bigoplus_{i=1}^{r} S_{p_i}$ y $H = \bigoplus_{i=1}^{r} S'_{p_i}$, los isomorfismos f_i se pueden extender a un isomorfismo $f : G \to H$, es decir, de modo que $f|_{S_{p_i}} = f_i$. Luego $G \simeq H \iff S_{p_i} \simeq S'_{p_i}$, $1 \le i \le r$.

El número de sumandos de cada orden p_i^n en G es igual a $U(n, S_{p_i})$, pues si $i \neq j$, un p_j-subgrupo no puede dar lugar a sumandos de orden p_i^n, pues p_i y p_j son primos y distintos. Entonces, si $G \simeq H \Rightarrow$ $\Rightarrow S_{p_i} \simeq S'_{p_i}$, $1 \le i \le r$, y de aquí, por el primer caso, siendo los S_{p_i} y S'_{p_i} p_i-primarios, se deduce que $U(n, S'_{p_i}) = U(n, S_{p_i})$ y, en consecuencia, $U(n, G) = U(n, H)$.

$\Leftarrow$ Si $U(n, G) = U(n, H)$, entonces $U(n, S_{p_i}) = U(n, S'_{p_i})$, $1 \le i \le r$. Razonando del mismo modo que antes, $S_{p_i} \simeq S'_{p_i}$, $1 \le i \le r$ y, por tanto, $G \simeq H$. c.s.q.d.

2.15. TEOREMA: Sea G un grupo abeliano finito y $\sigma(u_1) \oplus \dots \oplus \sigma(u_s)$ y $\sigma(n_1) \oplus \dots \oplus \sigma(n_t)$ dos estructuras canónicas de G; entonces $s = t$ y $u_i = n_i$, $1 \le i \le s$.

Demostr.: Veamos que u_1 es el exponente de G, es decir, que es el más pequeño de los enteros positivos u tales que $ux = 0$, $\forall x \in G$. Dado $x \in G$, existen $x_1, \dots, x_s$, con $x_i \in \sigma(u_i)$, tal que $x = x_1 + \dots + x_s$. Entonces $u_1 x = u_1 x_1 + u_1 x_2 + \dots + u_1 x_s$. Siendo $\sigma(u_i)$ un grupo cíclico de orden u_i, $o(x_i) \mid u_i$. Además, por ser $\sigma(u_1) \oplus \dots \oplus \sigma(u_s)$ una estructura canónica de G, $u_i \mid u_{i-1}$, $2 \le i \le s$. Entonces $u_i \mid u_1$, $1 \le i \le s$ y, en consecuencia, $o(x_i) \mid u_1$. Luego, $u_1 x_i = 0$, $\forall i \in \{1, \dots, s\}$. Luego $u_1 x = 0$ y, por tanto, $u_1 \in \{m \in \mathbb{N} / mx = 0, \forall x \in G\}$. Veamos que u_1 es el mínimo de este conjunto. Sea a_1 un generador de $\sigma(u_1)$, es decir, $\sigma(u_1) = \langle a_1 \rangle$. Entonces, $o(a_1) = o(\langle a_1 \rangle) = u_1$. Por definición de $o(a_1)$, u_1 es el más pequeño natural u tal que $ua_1 = 0$. Luego, si $m \in \mathbb{Z}^+$ y $mx = 0$, $\forall x \in G$, entonces, $ma_1 = 0 \Rightarrow u_1 \mid m \Rightarrow u_1 \le m$. Por tanto, u_1 es el exponente de G. Análogamente, partiendo de la estructura canónica $\sigma(n_1) \oplus \dots \oplus \sigma(n_t)$ de G llegamos a que n_1 es el exponente de G. Por la definición, el exponente de G, es un invariante de G y es único. Entonces, $u_1 = n_1$. Si $H_1 = \sigma(u_2) \oplus \dots \oplus \sigma(u_s)$ y $K_1 = \sigma(n_2) \oplus \dots \oplus \sigma(n_t)$, $G = \sigma(u_1) \oplus H_1$ y $G = \sigma(n_1) \oplus K_1$. A partir de estas dos sumas directas de G obtenemos dos descomposiciones primarias de G que tendrán el mismo número de sumandos

de cada orden. Además $\sigma(u_1) \cong \sigma(n_1)$, pues son dos grupos cíclicos del mismo orden, luego tienen el mismo número de sumandos de cada orden (Teorema 2.14) y, en consecuencia, H_1 y K_1 tienen el mismo número de sumandos de cada orden; luego $H_1 \cong K_1$, por teorema 2.14. Siendo H_1 y K_1 isomorfos, tienen el mismo exponente, trivialmente. Como $H_1 = \sigma(u_2) \oplus \ldots \oplus \sigma(u_s)$ y $K_1 = \sigma(n_2) \oplus \ldots \oplus \sigma(n_t)$, razonando análogamente a como se hizo antes, $\exp(H_1) = u_2$ y $\exp(K_1) = n_2$. Luego, $u_2 = n_2$. Razonando de este modo, si suponemos $s \leq t$, llegamos a que $u_1 = n_1, u_2 = n_2, \ldots, u_s = n_s$. Entonces, no puede ser $s < t$, pues siendo $\sigma(u_1) \cong \sigma(n_1), \ldots, \sigma(u_s) \cong \sigma(n_s)$, si fuese $s < t$, se tendría $\sigma(n_{s+1}) = \ldots = \sigma(n_t) = \{0\}$, y supusimos que en una estructura canónica de un grupo no hay sumandos directos triviales. Luego $s = t$ y $u_i = n_i$, $1 \leq i \leq s$. c.s.q.d.

2.16. TEOREMA: Dos grupos abelianos finitos G y H son isomorfos si y solo si admiten estructuras canónicas del mismo tipo, es decir, que si $G = \sigma(u_1) \oplus \ldots \oplus \sigma(u_s)$ y $H = \sigma(n_1) \oplus \ldots \oplus \sigma(n_t)$, entonces $s = t$ y $u_i = n_i$.

Demostr: $\Rightarrow$| Veamos que si $f: G \to H$ es isomorfismo entonces $\exp(G) = \exp(H)$. Por el mismo razonamiento hecho en el teorema anterior, $u_1 = \exp(G)$ y $n_1 = \exp(H)$. Entonces $u_1 = \min\{u \in \mathbb{Z}^+ / ug = 0, \forall g \in G\}$ y $n_1 = \min\{n \in \mathbb{Z}^+ / nh = 0, \forall h \in H\}$.

Siendo f y f^{-1} isomorfismos podemos escribir:

$\forall h \in H, u_1 h = u_1 f(g) = f(u_1 g) = f(0) = 0 \Rightarrow u_1 \in \{n \in \mathbb{Z}^+ / nh = 0, \forall h \in H\} \Rightarrow n_1 \leq u_1$.

$\forall g \in G, n_1 g = n_1 f^{-1}(h) = f^{-1}(n_1 h) = f^{-1}(0) = 0 \Rightarrow n_1 \in \{u \in \mathbb{Z}^+ / ug = 0, \forall g \in G\} \Rightarrow u_1 \leq n_1$

Luego $u_1 = n_1$. Razonando análogamente a como se hizo en el teorema anterior se prueba que G y H admiten estructuras canónicas del mismo tipo.

$\Leftarrow$| Si $G = \sigma(u_1) \oplus \ldots \oplus \sigma(u_s)$ y $H = \sigma'(u_1) \oplus \ldots \oplus \sigma'(u_s)$ donde $\sigma(u_i)$ y $\sigma'(u_i)$ son grupos cíclicos de orden u_i, entonces $\sigma(u_i) \cong \sigma'(u_i)$, $1 \leq i \leq s$. Sea $f_i: \sigma(u_i) \to \sigma'(u_i)$, $1 \leq i \leq s$, estos isomorfismos. Prolonguemos estos isomorfismos a G:

$$f: \sigma(u_1) \oplus \ldots \oplus \sigma(u_s) \longrightarrow \sigma'(u_1) \oplus \ldots \oplus \sigma'(u_s)$$
$$g_1 + \ldots + g_s \longmapsto f(g_1) + \ldots + f(g_s)$$

siendo $f(g_i) = f_i(g_i)$, $1 \leq i \leq s$. Entonces, f es isomorfismo fácilmente. Luego, $G \cong H$. c.s.q.d.

TEMA 7º: GRUPOS LIBRES

1. Definición. Existencia de grupos libres.

DEFINICION: Sea G un grupo y X un subconjunto de G. Diremos que G es libre sobre X si para toda aplicación f de X en un grupo cualquiera H existe un único homomorfismo $h: G \longrightarrow H$ haciendo conmutativo el diagrama siguiente:

donde i es la inyección canónica, es decir, tal que $h(x)=f(x)$, $\forall x \in X$.
Se dice tambien que X es base de G.

Antes de probar la existencia de grupos libres veremos algunas definiciones más.

- Dado un conjunto X siempre existe otro conjunto X' disjunto con X y del mismo cardinal que él. Si, por ejemplo, $X=\{x_i\}_{i\in I}$ podemos tomar $X'=\{(x_i,i)\}_{i\in I}$. Trivialmente, $X\cap X'=\emptyset$ y $\operatorname{card} X=\operatorname{card} X'$.
Además, siempre podemos considerar otro conjunto unitario $X''=\{1\}$ de modo que $1\notin X\cup X'$, pues de lo contrario, $X\cup X'$ contendrían todos los elementos que se pueden concebir lo cual es absurdo.
Se dice, entonces, que el conjunto $X\cup X'\cup X''$ es un alfabeto sobre X y los elementos de dicha unión se llaman letras.
- Sea S el conjunto de las sucesiones de letras, $S=\{(a_1,a_2,\dots,a_n,\dots)\}$. Diremos que un elemento w de S es una palabra si existe $K\in\mathbb{N}$ tal que $\forall m>K$, $a_m=1$.
A la sucesión $(1,1,\dots,1,\dots)$ se llama palabra vacía.
- Siendo $\operatorname{card} X=\operatorname{card} X'$, existe una biyección f de X en X'. A la imagen por f de un elemento x de X lo denotaremos por x^{-1} y si $x'\in X'$ denotamos por x'^{-1} a la imagen de x' por f^{-1}. Entonces:

DEFINICION: Una palabra w diremos que es reducida si se verifica que, si $w=(a_1,a_2,\dots,a_n,\dots)$, entonces $a_{i+1}\neq a_i^{-1}$ y además si para un cierto k natural $a_k=1$, entonces $a_m=1$, $\forall m>K$.

Entonces, haciendo el convenio $x^1=x$, $\forall x\in X\cup X'$, una palabra reducida la podemos escribir en la forma

$$w=x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}, \text{ con } \varepsilon_i=\pm 1,\ x_i\in X\cup X' \text{ y además}$$

$x_{i+1}^{\varepsilon_{i+1}}\neq x_i^{-\varepsilon_i}$, $1\leq i\leq n-1$.

Llamamos W al conjunto de las palabras reducidas.

1.1. TEOREMA: Dado un conjunto cualquiera X no vacío existe un grupo libre F tal que $F \supset X$ y X es base de F, es decir, tal que F es libre sobre X.

Demostración: Sea X' un conjunto disjunto con X y con el mismo cardinal que él. Sea $X'' = \{1\}$ de modo que X, X' y X'' satisfacen las consideraciones hechas anteriormente. Del mismo modo llamamos W al conjunto de las palabras reducidas sobre X. Para cada $x \in X$ definimos dos aplicaciones $|x|$ y $|x^{-1}|$, que representamos abreviadamente por $|x^\varepsilon|^{(\varepsilon = \pm 1)}$, del siguiente modo:

$$|x^\varepsilon| : W \longrightarrow W$$

$$x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \longmapsto |x^\varepsilon|(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) = \begin{cases} = x^\varepsilon x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} & \text{si } x^\varepsilon \neq x_1^{-\varepsilon_1} \\ = x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} & \text{si } x^\varepsilon = x_1^{-\varepsilon_1} \end{cases}$$

- $|x^\varepsilon|$ está bien definida: podría haber "problemas" si una misma palabra reducida w admitiese dos expresiones distintas $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ e $y_1^{\varepsilon'_1} \cdots y_m^{\varepsilon'_m}$, pero como $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} = (x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n}, 1, 1, \ldots)$ e $y_1^{\varepsilon'_1} \cdots y_m^{\varepsilon'_m} = (y_1^{\varepsilon'_1}, \ldots, y_m^{\varepsilon'_m}, 1, 1, \ldots)$, si $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} = y_1^{\varepsilon'_1} \cdots y_m^{\varepsilon'_m}$ debe ser $m = n$ y $x_1^{\varepsilon_1} = y_1^{\varepsilon'_1}, \ldots, x_n^{\varepsilon_n} = y_n^{\varepsilon'_n}$. Por tanto, una palabra reducida admite una única expresión reducida, y portanto, $|x^\varepsilon|$ está bien definida.
- Si representamos por $|x^\varepsilon| \cdot |y^{\varepsilon'}|$ la composición de dos aplicaciones de este tipo tenemos que $\forall x \in X$, $|x|\,|x^{-1}| = |x^{-1}| \cdot |x| = \mathbb{1}_W$, pues dada $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \in W$, si $x^{-1} \neq x_1^{-\varepsilon_1}$, tenemos que:
$|x|\,|x^{-1}|(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) = |x|(x^{-1} x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ y si $x^{-1} = x_1^{-\varepsilon_1}$, entonces $|x| \cdot |x^{-1}|(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}) = |x|(x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}) = x x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$, pues $x^{-1} = x_1^{-\varepsilon_1} \Rightarrow x = x_1^{\varepsilon_1}$.
Luego $|x| \cdot |x^{-1}|$ es la identidad en W. Análogamente, $|x^{-1}| \cdot |x| = \mathbb{1}_W$.
En consecuencia, para todo $x \in X \cup X'$, $|x|$ es una biyección de W en W, es decir, $|x| \in \mathcal{J}(W)$, y $|x^{-1}| = |x|^{-1}$
Consideremos en $\mathcal{J}(W)$ el subconjunto $X_0 = \{|x| \,/\, x \in X\}$, y sea F_0 el subgrupo de $\mathcal{J}(W)$ generado por X_0. Los elementos de F_0 son composiciones finitas de elementos de X_0, es decir, si $\varphi = |x_1^{\varepsilon_1}| \cdot |x_2^{\varepsilon_2}| \cdots |x_n^{\varepsilon_n}|$ pertenece a F_0 se verifica que: $\varepsilon_i = \pm 1$ y $|x_i^{\varepsilon_i}| \neq |x_{i+1}^{-\varepsilon_{i+1}}|$ y $x_i \neq 1$.
Veamos que cada elemento $\varphi \in F_0$ admite una única expresión de este tipo
Supongamos que $\varphi = |x_1^{\varepsilon_1}| \cdots |x_n^{\varepsilon_n}| = |y_1^{\varepsilon'_1}| \cdots |y_m^{\varepsilon'_m}|$; entonces,
$|x_1^{\varepsilon_1}| \cdots |x_n^{\varepsilon_n}|(1) = |y_1^{\varepsilon'_1}| \cdots |y_m^{\varepsilon'_m}|(1) \Rightarrow |x_1^{\varepsilon_1}| \cdots |x_{n-1}^{\varepsilon_{n-1}}|(x_n^{\varepsilon_n}) = |y_1^{\varepsilon'_1}| \cdots |y_m^{\varepsilon'_m}|(1) \Rightarrow$
$\Rightarrow |x_1^{\varepsilon_1}| \cdots |x_{n-2}^{\varepsilon_{n-2}}|(x_{n-1}^{\varepsilon_{n-1}} x_n^{\varepsilon_n}) = |y_1^{\varepsilon'_1}| \cdots |y_{m-2}^{\varepsilon'_{m-2}}|(y_{m-1}^{\varepsilon'_{m-1}} y_m^{\varepsilon'_m})$ pues $x_{n-1}^{\varepsilon_{n-1}} \neq x_n^{\varepsilon_n}$

queda que $x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n} = y_1^{\varepsilon'_1}\cdots y_m^{\varepsilon'_m}$ y, por tanto, $x_1^{\varepsilon_1}=y_1^{\varepsilon'_1}, \dots, x_n^{\varepsilon_n}=y_m^{\varepsilon'_m}$ y $m=n$ pues la expresión de una palabra reducida es única. Luego la expresión de φ como composición de elementos $|x_1^{\varepsilon_1}|,\dots,|x_n^{\varepsilon_n}|$ con $\varepsilon_i=\pm 1$ y $x_i^{\varepsilon_i}\neq x_{i+1}^{-\varepsilon_{i+1}}$ es única.

- Veamos ahora que F_0 es libre sobre X_0. Queremos ver que cualquiera que sea el grupo G y cualquiera que sea la aplicación $f: X_0 \to G$, existe un único homomorfismo $h: F_0 \to G$ haciendo conmutativo el diagrama

$$\begin{array}{ccc} X_0 & \xrightarrow{i} & F_0 \\ & \searrow^{f} & \downarrow h \\ & & G \end{array}$$

es decir, de modo que $\forall |x| \in X_0$, $f(|x|) = h(|x|)$. Si h debe ser homomorfismo, para una aplicación $|x_1^{\varepsilon_1}|\cdots|x_n^{\varepsilon_n}| \in F_0$ se debe verificar:

$$h(|x_1^{\varepsilon_1}|\cdots|x_n^{\varepsilon_n}|) = h(|x_1^{\varepsilon_1}|)\cdots h(|x_n^{\varepsilon_n}|) = h(|x_1|^{\varepsilon_1})\cdots h(|x_n|^{\varepsilon_n}) =$$
$$= [h(|x_1|)]^{\varepsilon_1}\cdots[h(|x_n|)]^{\varepsilon_n} = [f(|x_1|)]^{\varepsilon_1}\cdots[f(|x_n|)]^{\varepsilon_n}.$$

Luego de haber un homomorfismo de F_0 en G será de esta forma:

$$h(|x_1^{\varepsilon_1}|\cdots|x_n^{\varepsilon_n}|) = [f(|x_1|)]^{\varepsilon_1}\cdots[f(|x_n|)]^{\varepsilon_n}.$$

Veamos ahora que h, así definido, es ~~homomorfismo~~ homomorfismo

Sean $\varphi_1, \varphi_2 \in F_0$, tal que $\varphi_1 \neq \varphi_2^{-1}$, pues si $\varphi_1 = \varphi_2^{-1}$, es $\varphi_1\varphi_2 = \mathbb{1}_W$ y entonces $h(\varphi_1\varphi_2) = h(\varphi_1)\cdot h(\varphi_2)$ trivialmente. Supongamos que $\varphi_1 = |x_1^{\varepsilon_1}|\cdots|x_n^{\varepsilon_n}|$ y $\varphi_2 = |y_1^{\varepsilon'_1}|\cdots|y_k^{\varepsilon'_k}|$. Puede ocurrir que $x_n^{\varepsilon_n} = y_1^{-\varepsilon'_1}$ en cuyo caso, al componer φ_1 con φ_2 (yuxtaponerlos) habría que suprimir dichos términos; supongamos que $\varphi_1\varphi_2$ admite una expresión reducida de la forma $|x_1^{\varepsilon_1}|\cdots|x_s^{\varepsilon_s}|\,|y_{n-s}^{\varepsilon'_{n-s}}|\cdots|y_k^{\varepsilon'_k}|$, pues $\varphi_1\varphi_2 \neq \mathbb{1}_W$. Entonces

$$h(\varphi_1\varphi_2) = [f(|x_1|)]^{\varepsilon_1}\cdots[f(|x_s|)]^{\varepsilon_s}[f(|y_{n-s}|)]^{\varepsilon'_{n-s}}\cdots[f(|y_k|)]^{\varepsilon'_k}. \quad (I)$$

donde faltan los términos centrales que se anularon al componer φ_1 y φ_2. Veamos que $|x_s^{\varepsilon_s}| = |y_1^{-\varepsilon'_1}| \Rightarrow [f(|x_s|)]^{\varepsilon_s} = [f(|y_1|)]^{-\varepsilon_1}$, con lo cual, al componer $h(\varphi_1)$ con $h(\varphi_2)$ quedará la misma expresión (I) y $h(\varphi_1\varphi_2) = h(\varphi_1)h(\varphi_2)$, como queríamos probar:

$$|x_s^{\varepsilon_s}| = |y_1^{-\varepsilon'_1}| \Rightarrow f(|x_s^{\varepsilon_s}|) = f(|y_1^{-\varepsilon'_1}|) \Rightarrow [f(|x_s|)]^{\varepsilon_s} = [f(|y_1|)]^{-\varepsilon_1}.$$

Por tanto, existe un homomorfismo $h: F_0 \to G$ y es único, que prueba que F_0 es libre sobre X_0.

- Queremos construir un grupo libre F sobre X. Probaremos que F es W con la ley de composición "yuxtaposición" de palabras reducidas. Veamos que existe una biyección entre F_0 y F. Consideremos la aplicación:

$$\phi: F_0 \longrightarrow F = W$$
$$|x_1^{\varepsilon_1}|\cdots|x_n^{\varepsilon_n}| \longmapsto |x_1^{\varepsilon_1}|\cdots|x_n^{\varepsilon_n}|(1) = x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n}$$

ϕ es biyectiva, pues elementos distintos de F_0 tienen imágenes distintas (la expresión reducida de los elementos de F_0 es única), elementos distintos de F tienen orígenes distintos en F_0 y todo elemento de F tiene contraimagen.

Podemos transportar por ϕ la estructura de F_0 a F de modo que ϕ sea isomorfismo. (*) Tenemos entonces en F una estructura de grupo isomorfa a F_0; siendo F_0 libre sobre X_0, $F = \phi(F_0)$ es libre sobre $\phi(X_0)$, pero $\phi(|x|) = |x|(1) = x$, $\forall x \in X$. Luego $\phi(X_0) = X$ y F es libre sobre X.

Queda ver que la ley inducida en F por la ley de F_0, a través de ϕ, es, precisamente, la "yuxtaposición" de palabras reducidas, con lo cual $F = W$ con la "yuxtaposición" de palabras será el grupo libre asociado a X. Pero:

$$[x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}] \cdot [y_1^{\varepsilon'_1} \dots y_k^{\varepsilon'_k}] = \phi(|x_1^{\varepsilon_1}| \dots |x_n^{\varepsilon_n}|) \cdot \phi(|y_1^{\varepsilon'_1}| \dots |y_k^{\varepsilon'_k}|) =$$

$$= \phi\left[\left(|x_1^{\varepsilon_1}| \dots |x_n^{\varepsilon_n}|\right)\left(|y_1^{\varepsilon'_1}| \dots |y_k^{\varepsilon'_k}|\right)\right] = \phi\left[|x_1^{\varepsilon_1}| \dots |x_s^{\varepsilon_s}| |y_{n-s}^{\varepsilon'_{n-s}}| \dots |y_k^{\varepsilon'_k}|\right] =$$

$= x_1^{\varepsilon_1} \dots x_s^{\varepsilon_s} y_{n-s}^{\varepsilon'_{n-s}} \dots y_k^{\varepsilon'_k}$, que ya es una palabra reducida puesto que $|x_1^{\varepsilon_1}| \dots |x_s^{\varepsilon_s}| |y_{n-s}^{\varepsilon'_{n-s}}| \dots |y_k^{\varepsilon'_k}| \in F_0$ ya que se han suprimido los términos centrales que verificaban: $x_{s_1}^{\varepsilon_n} = y_1^{-\varepsilon_1}$, $x_{s_1-1}^{\varepsilon_{n-1}} = y_2^{-\varepsilon_2}$, $\dots$, $x_{s+1}^{\varepsilon_{s+1}} = y_{n-s-1}^{-\varepsilon'_{n-s-1}}$ y siendo $x_s^{\varepsilon_s} \neq y_{n-s}^{-\varepsilon'_{n-s}}$.

Por tanto, la ley de grupo en F es la "yuxtaposición". Luego, W es el grupo libre sobre X. c.s.q.d.

- El inverso de un elemento $x \in X \cup X'$ es x^{-1} ya que, por definición de yuxtaposición, $x x^{-1} = 1$.
- Si $\text{card}(X) > 1$, el grupo libre sobre X no es abeliano, pues para que $ab = ba$, $a, b \in X$, debe ser $(a, b, 1, 1, \dots) = (b, a, 1, 1, \dots)$ y esto sucede si $a = b$ o $a = b^{-1}$.
- Veamos cuál es el grupo libre engendrado por un elemento: $X = \{a\}$. Los elementos del grupo libre engendrado por X son de la forma a^n, $n \in \mathbb{Z}$. Siendo $a^m \neq a^n$ si $m \neq n$, pues $a^m = (a, a, \overset{m}{\dots}, a, 1, \dots)$ y $a^n = (a, a, \overset{n}{\dots}, a, 1, \dots)$, se deduce que $F \simeq \mathbb{Z}$.
- Deducimos de aquí que todos los grupos libres son infinitos y no abelianos, salvo el caso en que X es unitario.

1.2. PROPOSICION: Todo grupo es isomorfo al cociente de un grupo libre.

Demostr.: Sea G un grupo. Consideremos el grupo libre F de base G. Sea $i: G \to F$ la inyección canónica y 1_G la identidad en G. Entonces, dado el grupo G, existe un único homomorfismo $h: F \to G$ que hace conmutativo el diagrama:

$$\begin{array}{ccc} G & \xrightarrow{i} & F \\ & {\scriptstyle 1_G}\searrow \quad \swarrow{\scriptstyle h} & \\ & G & \end{array}$$

es decir, tal que $\forall x \in G$, $h(x) = 1_G(x) = x$. Trivialmente, h es sobre, pues dado $x \in G$ existe $y = x \in F$ / $h(y) = x$.

Luego $G \simeq F/\mathrm{Ker}\,h$. c.s.q.d.

2. Presentación de un grupo

DEFINICION: Diremos que $(X|\Delta)$ es una presentación de un grupo G si se verifica lo siguiente:

- X es un conjunto no vacío que llamaremos conjunto de generadores de G.
- Δ es un conjunto de relaciones $\{r_j = 1 / j \in J\}$.
- Si F es el grupo libre de base X, el conjunto $\{r_j / j \in J\}$ es un subconjunto de F.
- Si H es el mínimo subgrupo normal de F que contiene al conjunto $\{r_j / j \in J\}$, G es isomorfo a F/H. (*)

Ejemplo: Sea $X = \{a, b\}$ y F el grupo libre de base X. Consideremos el subconjunto de F siguiente: $\{a^3b^2, a^{-1}b\}$. Sea H la clausura normal de dicho subconjunto, es decir, el mínimo subgrupo normal H de F que contiene a $\{a^3b^2, a^{-1}b\}$. Entonces, el grupo de la presentación $(\{a, b\} \mid a^3b^2 = 1, a^{-1}b = 1)$ es F/H, o cualquier grupo isomorfo a él. La notación $a^3b^2 = 1$ es debida a que, como $a^3b^2 \in H$, $a^3b^2 H = H$, y H es el elemento neutro de F/H.

TEMA 8º: GRUPOS ABELIANOS INFINITOS

1. GRUPOS ABELIANOS LIBRES

DEFINICION: Sea S un conjunto no vacio. Definimos el grupo abeliano libre determinado por S como un par (F, f), donde F es un grupo abeliano y $f: S \to F$ una aplicación satisfaciendo la sifuiente propiedad universal:

"Si f' es una aplicación arealquiera de S en un grupo abeliano cualquiera G, existe un único homomorfismo $h: F \to G$ tal que $h \circ f = f'$, es decir, que hace conmutativo el diagrama:

$$\begin{array}{ccc} S & \xrightarrow{f} & F \\ & \searrow^{f'} \quad \swarrow_{h} & \\ & G & \end{array}$$

1.1. TEOREMA: (de existencia de un grupo abeliano libre).

Sea S un conjunto no vacío. Entonces, existe un grupo abeliano libre determinado por S.

Demostr.: Sea $\mathbb{Z}^{<S>}$ el conjunto de las aplicaciones $f: S \to \mathbb{Z}$ con soporte finito, es decir, tales que $f(s) = 0$, para todas las s de S, excepto, posiblemente, para un número finito de ellos. Definimos la suma de dos elementos de $\mathbb{Z}^{<S>}$ como: $(f+g)(s) = f(s) + g(s)$. Trivialmente, $\mathbb{Z}^{<S>}$ con esta ley de composición interna es un grupo abeliano.

Denotaremos, para cada $s \in S$, con $1 \cdot s$ la aplicación de S en $\mathbb{Z}$ que asocia a s el 1, y a los restantes elementos de S el cero.

Probemos que $\mathbb{Z}^{<S>} = \bigoplus_{s \in S} <1 \cdot s>$

Como $(1 \cdot s + 1 \cdot s)(s) = 1 \cdot s(s) + 1 \cdot s(s) = 1+1 = 2, \ldots, (1 \cdot s + \overset{n}{\ldots} + 1 \cdot s)(s) = n, \ldots$ tenemos que $o(1 \cdot s)$ es infinito. Luego $<1 \cdot s>$ es cíclico infinito y, por tanto, isomorfo a $\mathbb{Z}$.

Sea $\varphi \in \mathbb{Z}^{<S>}$. Entonces, $\varphi(s) = 0$, $\forall s \in S - \{s_1, \ldots, s_n\}$.

Sea $\varphi(s_i) = k_i$, $i \in \{1, \ldots, n\}$. Entonces, trivialmente

$$\varphi = \sum_{i=1}^{n} k_i s_i$$

siendo $k_i \cdot s_i : S \longrightarrow \mathbb{Z}$

$$\begin{array}{l} s_i \longmapsto k_i \\ s \longmapsto 0, \text{ si } s \neq s_i. \end{array}$$

Luego $k_i \cdot s_i \in <1 \cdot s_i>$, y, en consecuencia, $\varphi \in \bigoplus_{s \in S} <1 \cdot s>$

A fin de no utilizar subíndices podemos poner $\varphi = \sum K_s \cdot s$, que es una suma finita. Entonces φ admite una expresión única de este tipo, pues si $\varphi = \sum K'_s \cdot s$, se tiene que $\sum K_s \cdot s - \sum K'_s \cdot s$ es la función idénticamente nula; de acuerdo con la definición de suma en $\mathbb{Z}^{\prime}\langle S\rangle$, y dado a que es abeliano, podemos poner: $\sum (K_s - K'_s)\, s \equiv 0$. Entonces, por definición de las aplicaciones $K \cdot s$, debe ser $K_s = K'_s$, como queríamos ver.

Veamos ahora que $(\mathbb{Z}\langle S\rangle, f)$ es un grupo abeliano libre determinado por S, siendo f la aplicación:

$$\begin{aligned} f: S &\longrightarrow \mathbb{Z}\langle S\rangle \\ s &\longmapsto f(s) = 1 \cdot s \end{aligned}$$

Sea G un grupo abeliano cualquiera y $f': S \to G$ una aplicación tenemos que ver que existe un único homomorfismo $h: \mathbb{Z}\langle S\rangle \to G$ tal que $h \circ f = f'$. Un elemento de $\mathbb{Z}\langle S\rangle$ es una suma finita de la forma $\sum n_s \cdot s$. Definimos, entonces, $h(\sum n_s \cdot s) = \sum n_s \cdot f'(s)$. Probemos que h es homomorfismo, y que es único:

$$h\left(\sum n_s \cdot s + \sum K_s \cdot s\right) = h\left(\sum (n_s + K_s)\cdot s\right) = \sum (n_s + K_s)\cdot f'(s) \overset{(1)}{=}$$
$$= \sum n_s f'(s) + \sum K_s \cdot f'(s) = h\left(\sum n_s \cdot s\right) + h\left(\sum K_s \cdot s\right).$$

La igualdad (1) es cierta pues G es abeliano.

Además h hace conmutativo el diagrama, pues:

$$\forall s \in S,\ (h \circ f)(s) = h(f(s)) = h(1 \cdot s) = f'(s)$$

Falta ver que h es único. Sea $h': \mathbb{Z}\langle S\rangle \longrightarrow G$ un homomorfismo haciendo conmutativo el diagrama

$$\begin{array}{ccc} S & \xrightarrow{f} & \mathbb{Z}\langle S\rangle \\ & {\scriptstyle f'} \searrow \quad \swarrow {\scriptstyle h'} & \\ & G & \end{array}$$

Un elemento de $\mathbb{Z}\langle S\rangle$ es de la forma, $\sum n_s \cdot s$, siendo ésta una suma finita y los s, elementos de S. Entonces, siendo h' homomorfismo, $h'(\sum n_s \cdot s) = \sum h'(n_s \cdot s)$

Para cada uno de estos s, $n_s \cdot s = 1 \cdot s + \overset{n_s}{\cdots} + 1 \cdot s$. Luego, $h'(n_s \cdot s) = n_s\, h'(1 \cdot s)$. Como h' hace conmutativo el diagrama, se tiene $h'(1 \cdot s) = h'(f(s)) = f'(s)$. Luego

$$h'\left(\sum n_s \cdot s\right) = \sum n_s \cdot f'(s) = h\left(\sum n_s \cdot s\right).$$

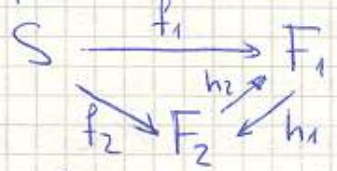
Por tanto, h es único y, como se indicó anteriormente, $(\mathbb{Z}\langle S\rangle, f)$

es un grupo abeliano libre determinado por S. c.s.q.d.

OBSERVACIONES: La aplicación $f: S \to \mathbb{Z}\langle S\rangle$ definida anteriormente es inyectiva, pues si $s, s' \in S$, $s \neq s' \Rightarrow 1\cdot s \neq 1\cdot s'$, por definición de $1\cdot s$ y $1\cdot s'$. En general, si (F, f) es un grupo abeliano libre determinado por S, $f: S \to F$ es inyectiva y, aunque, S en principio no es una parte de F, mediante esta inyección podemos identificar S con $f(S) \subset F$ y considerar, por tanto, S como una parte de F. (*)

12. PROPOSICION: Dos grupos abelianos libres determinados por el mismo conjunto S son isomorfos.

Demostr: Sean (F_1, f_1) y (F_2, f_2) dos grupos abelianos libres determinados por S. Consideremos el diagrama siguiente:



Siendo (F_1, f_1) grupo abeliano libre sobre S, F_2 un grupo abeliano y f_2 una aplicación de S en F_2, existe un único homomorfismo $h_1: F_1 \to F_2$ haciendo conmutativo el diagrama, es decir, tal que $h_1 \circ f_1 = f_2$. (I)

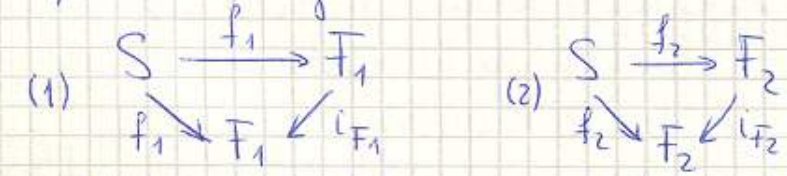
Análogamente, siendo (F_2, f_2) grupo abeliano libre determinado por S, F_1 un grupo abeliano y f_1 una aplicación de S en F_1 existe un único homomorfismo $h_2: F_2 \to F_1$ tal que $h_2 \circ f_2 = f_1$ (II).

De (I) y (II) obtenemos lo siguiente:

$f_2 = h_1 \circ f_1 = h_1 \circ (h_2 \circ f_2) = (h_1 \circ h_2) \circ f_2$ (III)

$f_1 = h_2 \circ f_2 = h_2 \circ (h_1 \circ f_1) = (h_2 \circ h_1) \circ f_1$ (IV)

De aquí no podemos deducir que $h_1 \circ h_2$ sea la identidad en F_2 ni $h_2 \circ h_1$ sea la identidad en F_1. Consideremos, para probarlo, los diagramas siguientes:



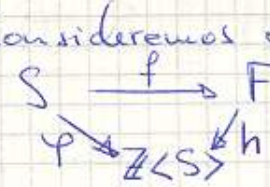
Para el primero existe un único homomorfismo de F_1 en F_1 haciendo conmutativo el diagrama, que es la identidad en F_1. Pero según (IV), $h_2 \circ h_1$ es un homomorfismo de F_1 en F_1 que hace conmutativo el diagrama (1). Debe ser entonces $h_2 \circ h_1 = i_{F_1}$.

tenemos que $h_1 \circ h_2 = i_{F_2}$
Por tanto, h_1 y h_2 son biyectivas. Luego h_1 es un isomorfismo de F_1 en F_2. c.s.q.d.

OBSERVACION: A la vista de este resultado podemos decir que el grupo abeliano libre determinado por un conjunto S es único, salvo isomorfismos. Llamaremos $F_{ab}(S)$ "al" grupo abeliano libre determinado por S. A modo de recíproco de lo dicho anteriormente, podemos decir que todo grupo isomorfo a $F_{ab}(S)$ es un grupo abeliano libre determinado por S, trivialmente.

1.3. PROPOSICION: Sea (F, f) un grupo abeliano libre determinado por un conjunto S no vacío. Entonces, f es inyectiva.

Demostr.: Consideremos el diagrama



Siendo F un grupo abeliano libre determinado por S, y $\mathbb{Z}\langle S\rangle$ un grupo abeliano y $\varphi: s \in S \longmapsto 1 \cdot s \in \mathbb{Z}\langle S\rangle$, existe un único homomorfismo $h: F \to \mathbb{Z}\langle S\rangle$, haciendo conmutativo el diagrama, es decir, tal que $h \circ f = \varphi$. Si f no fuese inyectiva, existirían $s_1, s_2 \in S$ tales que $s_1 \neq s_2$ y $f(s_1) = f(s_2)$. Entonces, $h(f(s_1)) = h(f(s_2))$, es decir, $\varphi(s_1) = \varphi(s_2)$. Entonces, φ no sería inyectiva, contra lo probado en la OBSERVACION al teorema 1.1. Luego f es inyectiva. c.s.q.d.

OBSERVACION: Como hemos dicho S se puede considerar contenido en el grupo abeliano libre $F_{ab}(S)$ determinado por S. Podemos, entonces, escribir $F_{ab}(S) = \bigoplus_{s \in S} \langle s\rangle$, pues $F_{ab}(S) \cong \mathbb{Z}\langle S\rangle$ y $\mathbb{Z}\langle S\rangle = \bigoplus_{s \in S} \langle 1 \cdot s\rangle$

DEFINICION: Diremos que un grupo abeliano G es un grupo abeliano libre si G es isomorfo al grupo abeliano libre determinado por un cierto conjunto S, $F_{ab}(S)$

1.4. PROPOSICION: Un grupo abeliano G es libre si y sólo si es suma directa de grupos cíclicos infinitos.

Demostr.: Si G es abeliano libre, $G \cong F_{ab}(S)$, para un cierto conjunto S. Siendo $F_{ab}(S) \cong \mathbb{Z}\langle S\rangle = \bigoplus_{s \in S} \langle 1 \cdot s\rangle$, existe un isomorfismo $\Phi: \mathbb{Z}\langle S\rangle \longrightarrow G$.
Entonces, $\mathbb{Z}\langle S\rangle = \bigoplus_{s \in S} \langle 1 \cdot s\rangle \Rightarrow G = \bigoplus_{s \in S} \langle \Phi(1 \cdot s)\rangle$
Además, siendo $\langle 1 \cdot s\rangle$ infinito, $\langle \Phi(1 \cdot s)\rangle$ es también infinito, pues

Ψ es isomorfismo.

Recíprocamente, si G es suma directa de grupos cíclicos infinitos, es isomorfo a $\mathbb{Z}^{(S)}$, para un cierto conjunto S, que es isomorfo a $Fab(S)$, grupo abeliano libre determinado por S, y, por tanto, G es un grupo abeliano libre determinado por S. c.s.q.d.

DEFINICION: Sea G un grupo abeliano libre. Diremos que un subconjunto $B=\{x_k \neq 0 / k\in K\}$ de G es base de G si $G=\bigoplus_{k\in K}\langle x_k\rangle$. (*)

1.5. PROPOSICION: Dos bases de un mismo grupo abeliano libre tienen el mismo cardinal.

Demostr.: Sea F un grupo abeliano libre y $B=\{x_i / i\in I\}$ y $B'=\{y_j / j\in J\}$ bases de F. Queremos probar $card(I)=card(J)$. Sea p un número primo. Entonces, pF es subgrupo de F (trivial) y es normal puesto que F es abeliano. Entonces F/pF es un grupo, cuyos elementos no nulos son de orden p, pues $\forall x\in F$, $p(x+pF)=px+pF=pF$, pues $px\in pF$, y pF es el neutro en F/pF. Según Lema 2.4, Tema 6º, podemos considerar F/pF como espacio vectorial sobre $\mathbb{Z}_p$. Sabemos que dos bases de un espacio vectorial, ya sea de dimensión finita o infinita, tienen el mismo cardinal. Probemos, entonces, que $\{x_i+pF / i\in I\}$ es base de F/pF.

Evidentemente, este conjunto constituye un sistema de generadores de F/pF, pues $\forall \bar{x}\in F/pF$, $\bar{x}=x+pF$ con $x\in F$. Entonces, $x=\sum n_i x_i$; luego $\bar{x}=\sum \bar{n}_i \bar{x}_i$, siendo $\bar{x}_i=x_i+pF$. Observar que $\sum n_i x_i$ es una suma finita, pues así son los elementos de $\bigoplus_{i\in I}\langle x_i\rangle$.

Probemos entonces que $\{x_i+pF / i\in I\}$ es un sistema libre, es decir, que si $\sum \bar{n}_i \bar{x}_i=0$, con $\bar{n}_i\in\mathbb{Z}_p$, entonces $\bar{n}_i=\bar{0}$, $\forall i$.

Si para cada $\bar{n}_i$ tomamos como representante $n_i\in\mathbb{Z}$ tal que $0\leq n_i\in p-1$, tenemos que si $\sum \bar{n}_i\bar{x}_i=\bar{0}$, entonces $(\sum n_i x_i)+pF=\bar{0}=pF \Rightarrow \sum n_i x_i\in pF$. Entonces, existe $x=\sum u_i x_i$ de F tal que $\sum n_i x_i = p\sum u_i x_i = \sum p u_i x_i$. Luego:

$\sum (n_i - p u_i)x_i = 0 \Rightarrow (n_i - p u_i)x_i = 0$, $\forall i$, pues F es suma directa de los $\langle x_i\rangle$. Por tanto, $n_i = p u_i$, $\forall i$ o, lo que es equivalente $n_i\equiv 0 \pmod p$ o bien $\bar{n}_i=\bar{0}$, $\forall i$.

Por tanto, $\bar{B}=\{\bar{x}_i=x_i+pF / i\in I\}$ es base de F/pF.

Análogamente, $\bar{B}'=\{\bar{y}_j=y_j+pF / j\in J\}$ es base de F/pF.

(*) Los elementos x_k son de orden infinito, pues según PROPOSICION 1.4, G grupo abeliano libre siendo t_i de orden infinito. Entonces $x\in G$, $x=\sum n_i t_i$ y $o(x)$ es infinito, pues si $n\sum n_i t_i=0 \Rightarrow \sum n n_i t_i=0 \Rightarrow n n_i t_i=0$, $\forall i$ (pues la suma es directa) y t_i serían de orden finito.

Por tanto, $\text{card}(\bar{\beta}) = \text{card}(\bar{\beta}')$ y, en consecuencia, $\text{card}(I) = \text{card}(J)$. c.s.q.d.

DEFINICIONES: Sea G un grupo. Dados dos elementos a y b de G definimos el conmutador de a y b como el elemento

$$[a,b] = aba^{-1}b^{-1} \in G.$$

Llamamos conjunto derivado de G al conjunto G' generado por los conmutadores $[a,b]$ cuando a y b recorren G:

$$G' = \langle \{ [a,b] / a,b \in G \} \rangle$$

1.6. PROPOSICION: Dado un grupo G, su conjunto derivado G' es subgrupo normal de G y es el menor de los subgrupos normales H de G tales que G/H es abeliano, es decir, $G' \triangleleft G$ y si H es subgrupo normal de G de manera que G/H es abeliano, entonces $H \supset G'$, y G/G' es abeliano.

Demostr.: • Si probamos que para cada conmutador $[a,b]$ y para cada $g \in G$, $g[a,b]g^{-1} \in G'$, quedará visto que $G' \triangleleft G$ ya que todo elemento de G' es producto de conmutadores y entre cada dos de ellos podemos "intercalar" $g^{-1}g$ y aplicar que $g[a,b]g^{-1} \in G'$, $\forall a,b \in G$. Veamos entonces que $g[a,b]g^{-1} \in G'$.

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gabg^{-1}a^{-1}g^{-1}b^{-1}bgb^{-1}g^{-1} =$$
$$= (ga)b(ga)^{-1}b^{-1} \cdot bgb^{-1}g^{-1} = [ga,b] \cdot [b,g]$$ que es un elemento de G'. Luego $G' \triangleleft G$.

• G/G' es abeliano: Se trata de ver que $\forall x,y \in G$, $xG' \cdot yG' = yG' \cdot xG'$. Dados $x,y \in G$, $[x,y] = xyx^{-1}y^{-1} \in G'$. Luego:

$$xyx^{-1}y^{-1}G' = G' \Longrightarrow xG'yG' \cdot x^{-1}G' \cdot y^{-1}G' = G' \Rightarrow$$
$$\Rightarrow xG'yG'x^{-1}G' = yG' \Rightarrow xG'yG' = yG'xG'.$$

• Sea $H \triangleleft G$ tal que G/H es abeliano. Entonces

$$\forall x,y \in G,\ xHyH = yHxH \Rightarrow \forall x,y \in G,\ xyx^{-1}y^{-1}H = H \Rightarrow$$
$$\Rightarrow \forall x,y \in G,\ [x,y] = xyx^{-1}y^{-1} \in H.$$

Luego $H \supset G'$. c.s.q.d.

1.7. TEOREMA: Un grupo abeliano A es libre si y solo si A es isomorfo a F/F' donde F es el grupo libre determinado por un cierto conjunto S y F' su conjunto derivado.

Demostr.: Si A es un grupo abeliano libre, entonces es isomorfo

a $F_{ab}(S)$, grupo abeliano libre determinado por un conjunto S. Sea F el grupo libre engendrado por S. Sea G un grupo abeliano cualquiera y f una aplicación cualquiera de S en G. Consideremos el diagrama siguiente:

(1)
$$\begin{array}{ccccc} S & \xrightarrow{i} & F & \xrightarrow{p} & F/F' \\ & \searrow^{f} & \downarrow h & \swarrow_{h'} & \\ & & G & & \end{array}$$

donde i es la inyección canónica de S en F y p la proyección canonica de F en el grupo cociente F/F'.

Probemos que existe un único homomorfismo h' de F/F' en G haciendo conmutativo el diagrama siguiente

(2)
$$\begin{array}{ccc} S & \xrightarrow{g} & F/F' \\ & \searrow^{f} \quad \swarrow_{h'} & \\ & G & \end{array}$$

donde $g = poi$, con lo cual $(F/F', g)$ será un grupo abeliano libre determinado por S y, por tanto, isomorfo a A.

Siendo F un grupo libre sobre S, existe un único homomorfismo $h: F \longrightarrow G$ tal que $hoi = f$.

Siendo h homomorfismo, $F/\mathrm{Ker}\,h \simeq h(F)$

Como $h(F)$ es subgrupo de G y G es abeliano, $h(F)$ es abeliano y, por tanto, $F/\mathrm{Ker}\,h$ es abeliano. Entonces, por la proposición anterior, $\mathrm{Ker}\,h \supset F'$.

Vamos a construir un homomorfismo $h': F/F' \longrightarrow G$. Los elementos de F/F' son de la forma $\bar{x} = x + F'$, $x \in F$. Definimos

$$h': \bar{x} = x + F' \in F/F' \longmapsto h'(\bar{x}) = h(x) \in G.$$

- h' está bien definido: Sean x_1 y x_2 dos representantes de la clase $\bar{x}$. Tenemos que ver que $h(x_1) = h(x_2)$. Si $x_1, x_2 \in \bar{x}$, entonces $x_1 - x_2 \in F'$. Como $F' \subset \mathrm{Ker}\,h$, $h(x_1 - x_2) = 0$. Luego $h(x_1) = h(x_2)$.
- h' es homomorfismo: $\forall \bar{x}, \bar{y} \in F/F'$, $h'(\bar{x} + \bar{y}) = h(x + y) = h(x) + h(y) = h'(\bar{x}) + h'(\bar{y})$
- h' hace conmutativo el diagrama (2), es decir, $h'og = f$: $\forall s \in S$, $(h'og)(s) = h'(g(s)) = h'(\bar{s}) = h(s) = f(s)$, pues $hoi = f$.

Probemos ahora que h' es único. Sea $h'': F/F' \longrightarrow G$ un homomorfismo que haga conmutativo el diagrama (2). Veamos que $h'' \equiv h'$. Dado $\bar{x} \in F/F'$, $\exists x \in F / \bar{x} = x + F'$. Si $x \in F$, x es una palabra (*) de la forma $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$. Entonces: $h''(\bar{x}) = h''(s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} + F') =$

(*) Observar que en F como grupo libre utilizamos notación multiplicativa y los elementos de F/F' los representamos por $x + F$ (notación aditiva)

$= h''[(s_1^{\varepsilon_1}+F')(s_2^{\varepsilon_2}+F')\dots(s_n^{\varepsilon_n}+F')] = [h''(s_1+F')]^{\varepsilon_1}\cdot\dots\cdot[h''(s_n+F')]^{\varepsilon_n}$

pues h'' es homomorfismo. Como hace conmutativo el diagrama (2) debe ser

$$h''(\bar{x}) = [f(s_1)]^{\varepsilon_1}\cdot\dots\cdot[f(s_n)]^{\varepsilon_n}$$

Como $s_1,\dots,s_n\in S$, $f(s_1)=h(s_1),\dots,f(s_n)=h(s_n)$. Luego:

$h''(\bar{x}) = [h(s_1)]^{\varepsilon_1}\cdot\dots\cdot[h(s_n)]^{\varepsilon_n} = h(s_1^{\varepsilon_1}\cdots s_n^{\varepsilon_n}) = h(x) = h'(\bar{x})$

y esto cualquiera que sea $\bar{x}\in F/F'$. Luego, $h''=h'$.

En consecuencia, $(F/F', g)$ es un grupo abeliano libre determinado por S, es decir $F/F'\simeq F_{ab}(S)\simeq A$. Luego A es isomorfo a F/F', donde F es el grupo libre engendrado por S.

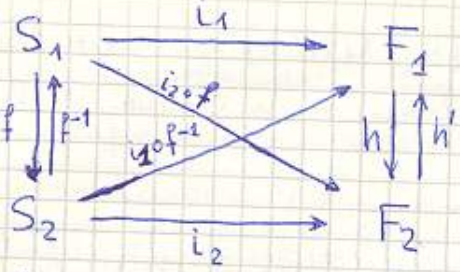
Recíprocamente, si A es isomorfo a F/F', donde F es un grupo libre sobre S, como F/F' es un grupo abeliano libre determinado por S, A es un grupo abeliano libre determinado por S. c.s.q.d.

1.8. COROLARIO: Sea F_1 un grupo libre determinado por S_1 y F_2 un grupo libre determinado por S_2. Entonces, F_1 es isomorfo a F_2 si y solo si $\text{card}(S_1) = \text{card}(S_2)$.

Demostr.: $\Rightarrow$ Supongamos que ϕ es un isomorfismo de F_1 en F_2. Entonces, F_1' es isomorfo a F_2' y F_1/F_1' es isomorfo a F_2/F_2'. (*)
Entonces, por el teorema anterior, F_1/F_1' es un grupo abeliano libre determinado por S_1 y F_2/F_2' es un grupo abeliano libre determinado por S_2. Además, siendo F_1/F_2' y F_2/F_2' isomorfos, son isomorfos al grupo abeliano libre $F_{ab}(S)$ determinado por un cierto conjunto S, es decir, existe un isomorfismo $\phi_1: F_1/F_1' \longrightarrow F_{ab}(S)$. Podemos suponer que S_1 está contenido en F_1/F_1', (en realidad, si $(F_1/F_1', g_1)$ es un grupo abeliano libre sobre S_1, siendo g_1 inyectiva podemos identificar S_1 con $g_1(S_1)$ que sí es una parte de F_1/F_1' y con el mismo cardinal que S_1). Entonces S_1 es una base de F_1/F_1' y, por tanto, $\phi_1(S_1)$ es una base de $F_{ab}(S)$. Análogamente, S_2 es base de F_2/F_2' y, por tanto, $\phi_2(S_2)$ es una base de $F_{ab}(S)$. Dos bases de un mismo grupo abeliano libre tienen el mismo cardinal, luego: $\text{card}(\phi_1(S_1)) = \text{card}(\phi_2(S_2))$ y, siendo ϕ_1 y ϕ_2 isomorfismos, $\text{card}(S_1) = \text{card}(S_2)$.

$\Leftarrow$ Si $\text{card}(S_1) = \text{card}(S_2)$, existe una biyección $f: S_1 \longrightarrow S_2$. Sean i_1 e i_2 las inyecciones canónicas de S_1 en F_1 y S_2 en F_2, respectivamente. Consideremos, entonces, el diagrama siguiente:

(*) En general un objeto $\dots$



Siendo F_1 libre, existe un único homomorfismo $h: F_1 \to F_2$ tal que $h \circ i_1 = i_2 \circ f$. Siendo F_2 libre, existe un único homomorfismo $h': F_2 \to F_1$ tal que $h' \circ i_2 = i_1 \circ f^{-1}$.

Entonces, como $h \circ i_1$ es la restricción de h a S_1, pues i_1 es la inyección canónica de S_1 en F_1, y siendo $(i_2 \circ f)(S_1) = S_2$, podemos escribir que $h|_{S_1}: S_1 \to S_2$ es la aplicación f. Análogamente, la aplicación $h'|_{S_2}: S_2 \to S_1$ es f^{-1}.

Queremos ver que $h \circ h' = \mathbb{1}_{F_2}$ y $h' \circ h = \mathbb{1}_{F_1}$, con lo cual h será biyectiva y, por tanto, F_1 y F_2 isomorfos.

Un elemento de F_2, grupo libre sobre S_2, es una palabra $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ con $x_1, \dots, x_n \in S_2$. Entonces:

$(h \circ h')(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) = h[h'(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n})] = h[h'(x_1)^{\varepsilon_1} \dots h'(x_n)^{\varepsilon_n}] =$

$= h[h'(x_1)]^{\varepsilon_1} \dots h[h'(x_n)]^{\varepsilon_n}$, pues h y h' son homomorfismos.

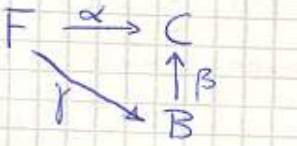
Pero, como $x_1, \dots, x_n \in S_2$, y h' sobre S_2 coincide con f^{-1} se tiene que: $h'(x_1) = f^{-1}(x_1), \dots, h'(x_n) = f^{-1}(x_n)$, que son elementos de S_1. Como h sobre S_1 coincide con f se tiene que:

$h[h'(x_1)] = f[f^{-1}(x_1)] = x_1, \dots, h[h'(x_n)] = f[f^{-1}(x_n)] = x_n$. Luego:

$(h \circ h')(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$, que prueba que $h \circ h' = \mathbb{1}_{F_2}$.

Análogamente, $h' \circ h = \mathbb{1}_{F_1}$. Luego, como se indicó anteriormente, h es un isomorfismo de F_1 en F_2. c.s.q.d.

1.9. TEOREMA: Sea $\beta: B \twoheadrightarrow C$ un homomorfismo sobre entre dos grupos abelianos B y C y $\alpha: F \to C$ un homomorfismo, donde F es un grupo abeliano libre. Entonces existe un homomorfismo $\gamma: F \to B$ tal que $\beta \circ \gamma = \alpha$, es decir, de modo que hace conmutativo el diagrama siguiente:



(*)

Demostr: Sea $\mathcal{B} = \{x_i \mid i \in I\}$ una base de F.

Dado $x_i \in \mathcal{B}$, $\alpha(x_i) \in C$. Siendo $\beta: B \to C$ sobre, para $\alpha(x_i)$ existe al menos un elemento de B cuya imagen por β es $\alpha(x_i)$. Tomamos uno de estos elementos que denotamos por b_i y definimos $\gamma(x_i) = b_i$.

Observar que al no ser b_i único, γ no tiene porqué ser única: para cada elemento $b \in B$ con $\beta(b) = \alpha(x_i)$, podemos definir una aplicación γ.

Vamos a extender la definición de γ para todo elemento de F. Un elemento x de F admite una expresión, y sólo una, como una suma finita de la forma $\sum n_i x_i$ (*). Definimos entonces:

$\gamma(x) = \gamma(\sum n_i x_i) \overset{\text{def}}{=} \sum n_i \gamma(x_i) = \sum n_i b_i$, pues $\gamma(x_i) = b_i$.

Que γ es un homomorfismo de F en B es trivial, por construcción de γ.

Probemos que $\beta \circ \gamma = \alpha$, es decir, que γ hace conmutativo el diagrama:

$(\beta \circ \gamma)(\sum n_i x_i) = \beta(\sum n_i \gamma(x_i)) = \beta(\sum n_i b_i) = \sum n_i \beta(b_i) = \sum n_i \alpha(x_i) =$
$= \alpha(\sum n_i x_i)$, pues $\beta(b_i) = \alpha(x_i)$, por definición de b_i.

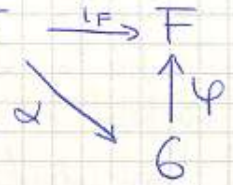
Luego $\beta \circ \gamma = \alpha$. c.s.q.d.

1.10. COROLARIO: Sea G un grupo abeliano y F un grupo abeliano libre. Sea $\varphi: G \twoheadrightarrow F$ un homomorfismo sobre. Entonces

$$G = \operatorname{Ker}\varphi \oplus S$$

donde $S \simeq F$.

Demostr.: Consideremos el diagrama siguiente



Por la propiedad proyectiva de los grupos abelianos libres, existe un homomorfismo $\alpha: F \to G$ tal que $\varphi \circ \alpha = i_F$.

Veamos que $G = \operatorname{Ker}\varphi \oplus \operatorname{Im}\alpha$ y que $\operatorname{Im}\alpha \simeq F$, con lo cual quedará terminada la demostración:

- $\forall x \in G$, $\exists x' \in \operatorname{Ker}\varphi$ y $x'' \in \operatorname{Im}\alpha$ / $x = x' + x''$:

  $\forall x \in G$, $x = [x - \alpha(\varphi(x))] + \alpha(\varphi(x))$

  Evidentemente $\alpha(\varphi(x)) \in \operatorname{Im}\alpha$. Veamos que $x - \alpha(\varphi(x)) \in \operatorname{Ker}\varphi$.

  $\varphi(x - \alpha(\varphi(x))) = \varphi(x) - \varphi[\alpha(\varphi(x))] = \varphi(x) - (\varphi\circ\alpha)(\varphi(x)) = \varphi(x) - i_F(\varphi(x)) =$
  $= \varphi(x) - \varphi(x) = 0$. Haciendo $x' = x - \alpha(\varphi(x))$ y $x'' = \alpha(\varphi(x))$ queda visto que $x = x' + x''$ con $x' \in \operatorname{Ker}\varphi$ y $x'' \in \operatorname{Im}\alpha$.

- $\operatorname{Ker}\varphi \cap \operatorname{Im}\alpha = \{0\}$: Sea $y \in \operatorname{Ker}\varphi \cap \operatorname{Im}\alpha$. Entonces, existe $x \in F$ tal que $y = \alpha(x)$ y $\varphi(y) = 0$. Luego $0 = \varphi(y) = \varphi(\alpha(x)) = (\varphi\circ\alpha)(x) = i_F(x) = x$.

  Por tanto, $x = 0 \Rightarrow y = \alpha(x) = 0$.

  En definitiva, $G = \operatorname{Ker}\varphi \oplus \operatorname{Im}\alpha$.

Además $G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$. Como φ es sobre, $\operatorname{Im}\varphi = F$. Luego $F \simeq G/\operatorname{Ker}\varphi$.

Por otra parte, como $G = \operatorname{Ker}\varphi \oplus \operatorname{Im}\alpha$ y $\operatorname{Ker}\varphi \simeq \operatorname{Ker}\varphi$ x 1.14 se tiene que

$$\frac{G}{\ker\varphi} \simeq \frac{\ker\varphi \oplus \mathrm{Im}\,\alpha}{\ker\varphi \times \{1\}} \simeq \frac{\ker\varphi}{\ker\varphi} \oplus \frac{\mathrm{Im}\,\alpha}{\{1\}} \simeq \mathrm{Im}\,\alpha .$$

Luego $F \simeq \mathrm{Im}\,\alpha$. c.s.q.d.

2. Teorema del subgrupo para grupos abelianos libres.

DEFINICION: Sea G un grupo abeliano libre. Se llama rango de G al cardinal de una base de G.

El concepto de rango de un grupo abeliano libre está bien definido en virtud de la PROPOSICION 1.5.

2.1. TEOREMA: (Teorema del subgrupo para grupos abelianos libres).

Sea G un grupo abeliano libre de rango finito n. Si H es un subgrupo de G entonces H es libre de rango menor o igual que n. Además existen dos bases $\mathcal{B}=\{u_1,\dots,u_n\}$ y $\mathcal{B}'=\{c_1u_1,\dots,c_mu_m\}$ de G y H, respectivamente, donde $c_i \in \mathbb{N}-\{0\}$ verificando que $c_i \mid c_{i+1}$, $\forall i \in \{1,\dots,m-1\}$. (*)

Demostr: Procederemos por inducción sobre $n = rg(G)$. Supondremos que el subgrupo H es distinto de $\{0\}$, pues si $H=\{0\}$ el teorema es trivial (H sería un grupo libre generado por 0).

* Si $rg(G)=1$, G es un grupo cíclico infinito: $G=\langle u\rangle \simeq \mathbb{Z}$. Por tanto, si H es un subgrupo de G, es cíclico infinito y generado por un elemento de G que será de la forma cu, $c\in\mathbb{Z}-\{0\}$. Siempre podemos considerar $c>0$, pues si c fuese negativo, siendo $G=\langle u\rangle=\langle -u\rangle$, tenemos que $H=\langle(-c)(-u)\rangle$ donde $-c>0$. Además, por la proposición 1.4., H es libre.

* Supongamos que el teorema es cierto para todo grupo abeliano libre de rango menor que n. Sea G un grupo abeliano libre de rango n y $H\neq\{0\}$ un subgrupo de G.

Consideremos el conjunto S de los números naturales distintos de cero para los cuales existe una base $\{a_1,\dots,a_n\}$ de G y unos enteros $\{c_i\}_{i=2}^n$ tales que $ca_1+\sum_{i=2}^n c_ia_i \in H$.

Veamos que $S\neq\emptyset$. Sea $\{a_1,\dots,a_n\}$ una base de G y sea $w\in H-\{0\}$. Entonces $w=\sum_{i=1}^n \lambda_i a_i$, $\lambda_i\in\mathbb{Z}$. Siendo $w\neq 0$, existe $i\in\{1,\dots,n\}$ tal que $\lambda_i\neq 0$. Podemos suponer que $\lambda_1\neq 0$, pues si $\{a_1,\dots,a_i,\dots,a_n\}$ es base de G, también es base de G $\{a_i,a_2,\dots,a_{i-1},a_1,\dots,a_n\}$. Entonces

$$w=\lambda_1a_1+\sum_{i=2}^n \lambda_ia_i$$

Además, podemos tomar $\lambda_1>0$, pues si fuese $\lambda_1<0$, podemos escribir $w=(-\lambda_1)(-a_1)+\sum_{i=2}^n \lambda_ia_i$, con $-\lambda_1>0$ y siendo $\{-a_1,a_2,\dots,a_n\}$ base de G, pues $\langle a_i\rangle=\langle -a_i\rangle$

Por tanto, $\lambda_1 \in S$. Luego $S \neq \emptyset$.
S, como subconjunto de $\mathbb{N}$, está bien ordenado, es decir, admite elemento mínimo. Sea $c_1 = \min S$; entonces $c_1 > 0$, pues $c_1 \in S \subset \mathbb{N} - \{0\}$.
Por definición de S, como $c_1 \in S$, existe una base $\{a_1, \dots, a_n\}$ de G y $\{k_i\}_{i=2}^n \subset \mathbb{Z}$ tales que $v_1 = c_1 a_1 + \sum_{i=2}^n k_i a_i \in H$.
Efectuemos la división euclídea de k_i por c_1:
dado $i \in \{2, \dots, n\}$, $k_i = q_i c_1 + r_i$ con $0 \leq r_i < c_1$, pues $c_1 > 0$.
Entonces, $v_1 = c_1 a_1 + \sum_{i=2}^n [q_i c_1 + r_i] a_i = c_1 [a_1 + \sum_{i=2}^n q_i a_i] + \sum_{i=2}^n r_i a_i$
Utilizaremos ahora un lema cuya demostración es trivial: "Si $\{a_1, \dots, a_n\}$ es una base de un grupo abeliano libre G y $w_1 = a_1 + \sum_{i=2}^n q_i a_i$ con $q_i \in \mathbb{Z}$ entonces $\{w_1, a_2, \dots, a_n\}$ es base de G".
Probemos que $r_i = 0$, $i \in \{2, \dots, n\}$. Si algun r_i fuese distinto de cero, consideremos la base de G siguiente $\{b_1, b_2, \dots, b_n\}$ siendo $b_1 = a_i$, $b_j = a_j$ si $j \neq i$, $j \neq 1$, y $b_i = w_1 = a_1 + \sum_{i=2}^n q_i a_i$. En esta base, v_1 se expresa así: $v_1 = r_i b_1 + (r_2 b_2 + \dots + r_i b_i + \dots + r_n b_n)$. Entonces, por definición de S, si $r_i \neq 0$, $r_i \in S$ y $r_i < c_1$, lo cual es absurdo, pues $c_1 = \min S$. Por tanto, $r_i = 0$, $i = 2, \dots, n$.
Luego, $v_1 = c_1 w_1$. Segun el lema anterior, $\mathcal{B} = \{w_1, a_2, \dots, a_n\}$ es base de G. Sea $K = \langle a_2, \dots, a_n \rangle$. Entonces, $rg(K) = n-1$, pues $\{a_2, \dots, a_n\}$ es base de K. Por hipótesis de inducción, el teorema es cierto para cualquier grupo abeliano libre de rango menor que n y, en particular, es cierto para K. Siendo $H \cap K$ un subgrupo de K, $H \cap K$ es libre de rango $m-1 \leq n-1 = rg(K)$ y, además, existe una base en K, $\{w_2, w_3, \dots, w_n\}$, y una base de $H \cap K$, $\{c_2 w_2, \dots, c_m w_m\}$ satisfaciendo que $c_i \in \mathbb{N} - \{0\}$ y $c_i | c_{i+1}$, $i = 2, \dots, n-1$.
Vamos a probar que $\{c_1 w_1, c_2 w_2, \dots, c_m w_m\}$ es base de H con lo cual quedará terminada la demostración, si probamos además que $c_1 | c_2$, pues $\{w_1, w_2, \dots, w_n\}$ es base de G, ya que $K = \bigoplus_{i=2}^n \langle w_i \rangle$ y $G = \langle w_1 \rangle \oplus K$. Veamos entonces que $\{c_i w_i\}_{i=1}^m$ es base de H.
- $\langle c_1 w_1 \rangle \cap \langle c_2 w_2, \dots, c_m w_m \rangle = \{0\}$, pues
$\langle c_1 w_1 \rangle \cap \langle c_2 w_2, \dots, c_m w_m \rangle \subset \langle w_1 \rangle \cap \langle w_2, \dots, w_n \rangle = \{0\}$, pues $\{w_1, \dots, w_n\}$ es base de G.
- $H = \langle c_1 w_1 \rangle + \langle c_2 w_2, \dots, c_m w_m \rangle$:
Que $\langle c_1 w_1 \rangle + \langle c_2 w_2, \dots, c_m w_m \rangle \subset H$ es trivial, pues $v_1 \in H$ y $v_1 = c_1 w_1$, y $\langle c_2 w_2, \dots, c_m w_m \rangle = H \cap K \subset H$.
Veamos que $H \subset \langle c_1 w_1 \rangle + \langle c_2 w_2, \dots, c_m w_m \rangle$.
Sea $x \in H$. Como $\mathcal{B} = \{w_1, a_2, \dots, a_n\}$ es base de G, $x = \lambda_1 w_1 + \sum_{i=2}^n \lambda_i a_i \in G$.

Si $\lambda_1 = 0$, $x \in H \cap K = \langle c_2 w_2, \dots, c_m w_m \rangle$ y es trivial que $x \in \langle c_1 w_1 \rangle + \langle c_2 w_2, \dots, c_m w_m \rangle$.

Si $\lambda_1 \neq 0$, $\lambda_1 = q_1 c_1 + r_1$, $0 \leq r_1 < c_1$. Luego

$x = q_1 c_1 w_1 + r_1 w_1 + \sum_{i=2}^{n} \lambda_i a_i \Rightarrow x - q_1 c_1 w_1 = r_1 w_1 + \sum_{i=2}^{n} \lambda_i a_i$.

Como $x \in H$ y $c_1 w_1 \in H$, $x - q_1 c_1 w_1 \in H$. Entonces, si fuese $r_1 \neq 0$, por definición de S, tendríamos que $r_1 \in S$ y $r_1 < c_1$, lo cual es absurdo, pues $c_1 = \min S$. Luego $r_1 = 0$.

Entonces, $x - q_1 c_1 w_1 = \sum_{i=2}^{n} \lambda_i a_i$, y también

$$x = q_1 c_1 w_1 + \sum_{i=2}^{n} \lambda_i a_i .$$

Como $q_1 c_1 w_1 \in \langle c_1 w_1 \rangle$ y $\sum_{i=2}^{n} \lambda_i a_i \in H \cap K$ (*) y $H \cap K = \langle c_2 w_2, \dots, c_m w_m \rangle$ se tiene que $x \in \langle c_1 w_1 \rangle + \langle c_2 w_2, \dots, c_m w_m \rangle$.

En definitiva, $H = \langle c_1 w_1 \rangle \oplus \langle c_2 w_2, \dots, c_m w_m \rangle$.

Pero $\langle c_2 w_2, \dots, c_m w_m \rangle = \langle c_2 w_2 \rangle \oplus \dots \oplus \langle c_m w_m \rangle$, pues $\{c_2 w_2, \dots, c_m w_m\}$ es base de $H \cap K$. Luego $\{c_1 w_1, \dots, c_m w_m\}$ es base de H.

Que H es libre es consecuencia inmediata de la PROPOSICION 1.4.

Veamos que $c_1 | c_2$ con lo cual quedará terminada la demostración.

Evidentemente, $c_2 w_2 - c_1 w_1 \in H$.

Sea $c_2 = q c_1 + r$, $0 \leq r < c_1$.

Entonces $c_2 w_2 - c_1 w_1 = q c_1 w_2 + r w_2 - c_1 w_1 = c_1(-w_1 + q w_2) + r w_2$.

Por el lema, si $u_1 = -w_1 + q w_2$, $\{u_1, w_2, \dots, w_n\}$ es base de G.

Luego, $c_2 w_2 - c_1 w_1$ se escribe como: $r w_2 + c_1 u_1 \in H$.

Entonces $r = 0$, pues si $r \neq 0$, $r \in S$ y $r < c_1$, lo cual es absurdo por definición de c_1. Luego $r = 0$ y, por tanto, $c_1 | c_2$. c.s.q.d.

3. Grupos abelianos de generación finita.

DEFINICION: Decimos que G es un grupo abeliano de generación finita si existen $x_1, \dots, x_n \in G$ tales que $G = \langle x_1 \rangle + \dots + \langle x_n \rangle$.

DEFINICION: (Subgrupo de torsión de un grupo abeliano).

Dado un grupo abeliano G definimos el subgrupo de torsión de G como el conjunto

$$tG = \{x \in G \mid o(x) \text{ es finito}\}.$$

Fácilmente se comprueba que tG es subgrupo de G.

3.1. LEMA: Supongamos que G es un grupo abeliano de generación finita; sea $S = \{x_1, \dots, x_n\}$ un sistema de generadores de G. Entonces $(F(S), f)$ el grupo abeliano libre determinado por S. Entonces G es isomorfo a $F(S)/H$ donde H es un subgrupo de $F(S)$.

Demostr.: Consideremos el diagrama siguiente

$$\begin{array}{ccc} S & \xrightarrow{f} & F(S) \\ & \searrow^{i} & \downarrow h \\ & & G \end{array}$$

donde i es la inyección canónica de S en G. Siendo $F(S)$ el grupo abeliano libre determinado por S y G un grupo abeliano, existe un único homomorfismo $h: F(S) \longrightarrow G$ haciendo conmutativo el diagrama, es decir, tal que $h \circ f = i$

Fácilmente se comprueba que h es sobre. Entonces

$$G = \operatorname{Im} h \simeq F(S)/\operatorname{Ker} h$$

Haciendo $H = \operatorname{Ker} h$ queda probado el lema.

3.2. TEOREMA: Un grupo abeliano G es de generación finita si y solo si $G = G_1 \oplus G_2$ donde G_1 es un grupo abeliano finito y G_2 un grupo abeliano libre de rango finito.

Además G_1 está unívocamente determinado por G, y se verifica que G_1 es el subgrupo de torsión de G: $G_1 = tG$.

Demostr.: $\Leftarrow$ Si $G = G_1 \oplus G_2$, siendo G_1 un grupo abeliano finito y G_2 un grupo abeliano libre de rango finito, el conjunto $S = G_1 \cup \mathcal{B}$, donde $\mathcal{B}$ es una base de G_2, es finito pues G_1 es finito y G_2 es de rango finito. Además, G está generado por S, pues todo elemento de G se escribe como suma de un elemento de G_1 y otro de G_2, y este último se escribe como "combinación lineal" de elementos de $\mathcal{B}$. (Siempre podemos considerar G_1 y G_2 como subgrupos de G, pues en el caso de que G sea el producto cartesiano de G_1 y G_2 siempre podemos identificar $G_1 = G_1 \times \{0\}$ y $G_2 = \{0\} \times G_2$).

$\Rightarrow$ Sea G un grupo abeliano de generación finita. Sea $S = \{x_1, \dots, x_n\}$ un sistema generador de G: $G = \langle x_1, \dots, x_n \rangle$. Entonces, por el lema anterior si $F(S)$ es el grupo abeliano libre determinado por S, $G \simeq F(S)/H$, donde H es subgrupo de $F(S)$. Según el teorema del subgrupo, existen $\mathcal{B} = \{u_1, \dots, u_n\}$ base de F y $\mathcal{B}' = \{c_1 u_1, \dots, c_m u_m\}$, $m \leq n$, base de H. Entonces:

$$G \simeq \frac{\langle u_1 \rangle \oplus \cdots \oplus \langle u_n \rangle}{\langle c_1 u_1 \rangle \oplus \cdots \oplus \langle c_m u_m \rangle} \simeq \frac{\langle u_1 \rangle}{\langle c_1 u_1 \rangle} \oplus \cdots \oplus \frac{\langle u_m \rangle}{\langle c_m u_m \rangle} \oplus \langle u_{m+1} \rangle \oplus \cdots \oplus \langle u_n \rangle$$

Pero $o\left(\frac{\langle u_1 \rangle}{\langle c_1 u_1 \rangle}\right) = c_1, \dots, o\left(\frac{\langle u_m \rangle}{\langle c_m u_m \rangle}\right) = c_m$ (*)

Sea $G_1' = \bigoplus_{i=1}^{m} \frac{\langle u_i \rangle}{\langle c_i u_i \rangle}$. Entonces G_1' es finito de orden $c_1 c_2 \dots c_m$.

Sea $G_2' = \langle u_{m+1} \rangle \oplus \dots \oplus \langle u_n \rangle$. Entonces, G_2' es un grupo abeliano libre (es suma directa de grupos cíclicos infinitos) y de rango finito $n-m$. Entonces, como $G \simeq G_1' \oplus G_2'$, si $\phi: G_1' \oplus G_2' \to G$ es un isomorfismo, llamando $G_1 = \phi(G_1')$ y $G_2 = \phi(G_2')$, podemos escribir $G = G_1 \oplus G_2$ donde G_1 es un grupo abeliano finito y G_2 un grupo abeliano libre de rango finito.

Veamos que $G_1 = tG$. Siendo G_1 un grupo finito, dado $x \in G_1$, $o(x) \mid o(G_1)$. Luego $o(x)$ es finito y, por tanto, $x \in tG$. Si $x \in tG$, $o(x)$ es finito y $x \in G$. Siendo $G = G_1 \oplus G_2$, $x = x_1 + x_2$ con $x_1 \in G_1$ y $x_2 \in G_2$. Si $o(x)$ es finito, existe $n \in \mathbb{N}$ tal que $nx = 0$. Entonces, $nx_1 + nx_2 = 0 \Rightarrow nx_1 = 0$ y $nx_2 = 0$, pues G es suma directa de G_1 y G_2. Siendo G_2 grupo abeliano libre, todo elemento de $G_2 - \{0\}$ es de orden infinito; como $nx_2 = 0$ y $x_2 \in G_2$ se deduce que $x_2 = 0$. Luego $x = x_1$ y, por tanto, $x \in G_1$. Luego $G_1 = tG$. c.s.q.d.

3.3. COROLARIO: Sea G un grupo abeliano de generación finita. Entonces $G = tG \oplus F$ donde F es un grupo abeliano libre isomorfo a $\frac{G}{tG}$.

Demostr.: Por el teorema anterior, $G = G_1 \oplus G_2$ siendo $G_1 = tG$ y $G_2 = F$ un grupo abeliano libre. Entonces, $G = tG \oplus F$ y, además $G/tG \cong \frac{tG \oplus F}{tG \times \{1\}} \simeq \frac{tG}{tG} \oplus F \simeq F$. c.s.q.d.

Deducimos, además, que si G es abeliano de generación finita, entonces G/tG es abeliano libre de rango finito.

3.4. TEOREMA: Un grupo abeliano G es de generación finita si y sólo si es una suma directa finita de grupos cíclicos primarios y grupos cíclicos infinitos. Además, el número de sumandos de cada orden es un invariante del grupo.

Demostr.: $\Rightarrow$ Si G es abeliano de generación finita, $G = G_1 \oplus G_2$ siendo G_1 un grupo abeliano finito y G_2 un grupo abeliano libre de rango finito. G_1, por ser abeliano finito, admite una descomposición como suma directa de grupos cíclicos primarios. G_2, como grupo abeliano libre, admite una descomposición como suma directa de grupos cíclicos infinitos (PROPOSICION 1.4.) y esta suma directa es finita pues G_2 es de rango finito. Además el número de sumandos de cada orden es un invariante de G, pues el número de sumandos de cada orden

da orden en G_1 es invariante en G_1 (la descomposición primaria de un grupo abeliano finito es "única"), y dos descomposiciones de G_2 como suma directa de grupos cíclicos infinitos tienen el mismo número de sumandos, pues dos bases de un grupo abeliano libre tienen el mismo cardinal.

$\Leftarrow$| Recíprocamente, si G es una suma directa finita de grupos cíclicos primarios y grupos cíclicos infinitos, agrupando los grupos cíclicos primarios obtenemos un grupo abeliano finito G_1, y agrupando los sumandos cíclicos infinitos obtenemos un grupo abeliano libre de rango finito (la suma directa es finita) que llamaremos G_2. Además $G = G_1 \oplus G_2$. Luego, G es abeliano de generación finita. c.s.q.