Tema 3.- Subgrupos. Generadores. Retículos

Definición

Dados los grupos G y H, se dice que H es un subgrupo de G, $H < G$, si H es un subconjunto de G y la aplicación de inclusión $H \to G$ es un homomorfismos de grupos.

Proposición

Sea G un grupo y $\emptyset \neq H \subset G$. Entonces:

1.- Son equivalentes:

$i)$ $H < G$

$ii)$ Se verifican las condiciones:

$$a) \forall x, y \in H \Longrightarrow xy \in H \quad b) \, 1 \in H \quad c) \forall x \in H \Longrightarrow x^{-1} \in H$$

$iii) \forall x, y \in H \Longrightarrow xy^{-1} \in H$

2.- En el caso de que G sea finito entonces son equivalentes:

$i)$ $H < G$

$ii)$ $\forall x, y \in H \Longrightarrow xy \in H$

Proposición

Sea $f: G \to G'$ un homomorfismo de grupos. Entonces:

$i)$ Si $H < G \Longrightarrow f_*(H) = \{f(x) \setminus x \in H\} < G'$.

$ii)$ Si $H < G \Longrightarrow f^*(H') = \{x \in G \setminus f(x) \in H'\} < G$.

En particular se tiene que $Im(f) = f_*(G) < G'$ y $Kerf = f^*(1) < G$

Proposición

Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de un grupo G. Entonces

$$\bigcap_{i \in I} H_i < G$$

Definición

Sea G un grupo y $S \subset G$. El subgrupo de G generado por S, denotado por $G = \langle S \rangle$, es la intersección de todos los subgrupos de G que contiene a S.

Proposición

Sea G un grupo, $S \subset G$ y $\langle S \rangle$ el subgrupo generado por S. Entonces:

$i)$ Si $S = \emptyset \Longrightarrow \langle S \rangle = 1$ el grupo trivial.

$ii)$ Si $S \neq \emptyset, \langle S \rangle$ es el conjunto de todos los elementos de G que se expresan como producto finito de elementos de S y de sus inversos, esto es,

$$\langle S \rangle = \{x_1^{\gamma_1} x_2^{\gamma_2} \dots x_n^{\gamma_n} \setminus n \geq 1 \ \ x_i \in S, \gamma_i = \pm 1 \ \forall i = 1, \dots, n\}$$

$iii)$ Si G es finito y $\emptyset \neq S \subset G$ entonces $\langle S \rangle$ es el conjunto de los elementos de G que se expresan como producto finito de elementos de S.

En el caso particular de que, siendo $S \subset G$, se tenga que $G = \langle S \rangle$ se dice que S *es un sistema de generadores* de G. Y si S es finito, se dice que G es *un grupo finitamente generado*, y si S es unitario, se dice que G es *cíclico*.

Definición

Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de un grupo G, se llama *compuesto de los subgrupos* H_i al subgrupo de G generado por el subconjunto $S = \bigcup_{i \in I} H_i$ y lo denotamos $\bigvee_{i \in I} H_i$. Por lo tanto, el compuesto es menor subgrupo de G que contiene a la unión de los H_i.

Un retículo de subgrupos es un grafo dirigido de subgrupos.

Definición

Sea G un grupo y $H, K < G$. Entonces se define

$$HK = \{hk \setminus h \in H, k \in K\} \subset G$$

Proposición

Sea G un grupo y $H, K < G$. Entonces

$$HK = H \vee K \ (y \ por \ tanto, HK \ es \ un \ subgrupo) \Leftrightarrow HK = KH$$

Definición (Clases laterales de un subgrupo en un grupo)

Sea G un grupo, Si $H < G$ se definen en G dos relaciones:

La relación $_{H}\sim$ por $y \ {}_{H}\sim x \Leftrightarrow x^{-1}y \in H$ y la relación $\sim_{H}$ por $y \sim_{H} x \Leftrightarrow yx^{-1} \in H$.

Ambas son de equivalencia:

La clase de equivalencia respecto de la primera es $xH = \{xh \setminus h \in H\}$ y se llama *clase lateral por la izquierda* de H en G definida por x. El correspondiente conjunto cociente

$$G/_{H}\sim = \{xH \setminus x \in G\}$$

La clase de equivalencia respecto de la segunda es $Hx = \{hx \setminus h \in H\}$ y se llama *clase lateral por la derecha* de H en G definida por x. El correspondiente conjunto cociente

$$G/\sim_H = \{Hx \setminus x \in G\}$$

Proposición

Sea G un grupo y $H < G$. Entonces:

$i)$ $\forall x \in G, x \in xH \;\; y \;\; x \in Hx$.

$ii)$ $\forall x \in G$, los conjuntos H, xH, Hx son biyectivos.

$iii)$ Los conjuntos cociente $G/_H\sim$ y $G/\sim_H$ de clases laterales son biyectivos.

Definición

El cardinal del conjunto $G/_H\sim$ (o del conjunto $G/\sim_H$ que es el mismo) se llama *índice* de H en G, y se denota por $[G:H]$.

Teorema de Lagrange

Sea G un grupo finito y $H < G$. Entonces $|H|$ divide a $|G|$ y se tiene que:

$$|G| = [G:H]|H|$$

Corolario

El orden de cualquier elemento de un grupo finito divide al orden del grupo.

Corolario

Si G un grupo finito y $H, K < G$ son subgrupos de G tales que $K < H < G$ entonces

$$[G:K] = [G:H][H:K]$$

Lema

Si G es un grupo finito de orden primo entonces G es cíclico.

Lema

Sea G es un grupo y $x \in G$ con $o(x) = n$. Entonces $x^k = 1 \Leftrightarrow {}^n/_k$.

Lema

Sea G es un grupo y $x \in G$. Entonces:

$i)$ Si $o(x) = \infty$ todas las potencias de x son elementos distintos de G.

$ii)$ Si $o(x) = n$ entonces $\langle x \rangle = \{1, x, \dots, x^{n-1}\}$ y tiene que $x^i = x^j \Leftrightarrow {}^n/_{i-j}$.

Proposición

Sea G un grupo y $a \in G$. Existe entonces un único homomorfismo de grupos $\varphi_a: Z \to G \setminus \varphi_a(1) = a$ y $Im\varphi_a = \{a^n \setminus n \in Z\} = \langle a \rangle$.

Teorema

Si G un grupo cíclico entonces $G \cong Z$ o bien $G \cong Z_n$ para algún n.

Proposición

Si G un grupo cíclico, $G = \langle a \rangle$ y $o(a) = n$ entonces para cada $^m/_n$ existe un único subgrupo cíclico $\langle a^{n/m} \rangle$.

Proposición

Sea G un grupo y $a \in G$ con $o(a) = n$. Entonces, si $k > 0$ se tiene que $\langle a^k \rangle = \langle a^d \rangle$ con $d = mcd(n, k)$ y $o(a^k) = {}^n/_d$.

Corolario

Si G un grupo y $a \in G$ con $o(a) = n$ se tiene que $\langle a^i \rangle = \langle a^j \rangle \Leftrightarrow mcd(n, i) = mcd(n, j)$.

Corolario

Sea $G = \langle a \rangle$ con $o(a) = n$. Entonces se tiene que $G = \langle a^k \rangle \Leftrightarrow mcd(n, k) = 1$. Y en consecuencia, el número de generadores de G es $\varphi(n)$, con φ la función de Euler.

Orden	Nº de grupos	abelianos	No abelianos
1	1	$\{1\}$	ninguno
2	1	C_2	ninguno
3	1	C_3	ninguno
4	2	$C_4; C_2 \oplus C_2$	ninguno
5	1	C_5	ninguno
6	2	C_6	D_3
7	1	C_7	ninguno
8	5	$C_8; C_4 \oplus C_2; C_2 \oplus C_2 \oplus C_2$	D_4, Q_2
9	2	$C_9; C_3 \oplus C_3$	ninguno
10	2	C_{10}	D_5
11	1	C_{11}	ninguno
12	5	$C_{12}; C_6 \oplus C_2$	D_6, Q_3, A_4
13	1	C_{13}	ninguno
14	2	C_{14}	D_7
15	3	C_{15}	ninguno

Ejercicio 1

Describir todos los elementos de los grupos alternados A_n, consistentes en las permutaciones pares de S_n correspondiente, para $n = 2, 3$ y 4.

Solución

Ejercicio 2

Sea $D_n = \langle r, s / \ s^2 = 1 \ \ r^n = 1 \ \ sr = r^{n-1}s \rangle$. Demostrar que el subgrupo de D_n generado por los elementos $\{r^j s, r^k s\}$ es todo el grupo D_n siempre que

$$0 \leq j < k < n \text{ y } mcd(k-j, n) = 1$$

Solución

Ejercicio 3

1.- Demostrar que el subgrupo de $SL_2(Z_3)$ generado por los elementos

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

es isomorfo al grupo cuaternio Q_2.

2.- Demostrar que $SL_2(Z_3)$ y S_4 son dos grupos de orden 24 que no son isomorfos.

Pista: Demostrar que S_4 no puede contener a ningún subgrupo isomorfo a Q_2.

Solución

Ejercicio 4

Razonar que un subconjunto no vacío $X \subseteq G$ de un grupo G es un subgrupo de G si y solo si, $X = \langle X \rangle$.

Solución

Ejercicio 5

Sean $a, b \in G$ dos elementos de un grupo que conmutan entre sí, esto es, para los que $ab = ba$, y de manera que sus órdenes son primos relativos, esto es, $mcd\big(o(a), o(b)\big) = 1$.

1.- Razonar que $\langle a \rangle \cap \langle b \rangle = 1$.

2.- Demostrar que $o(ab) = o(a)o(b)$.

Solución

Ejercicio 6

Encontrar un grupo G y elementos $a, b \in G$ tales que sus órdenes sean primos relativos, pero para los que no se verifique la igualdad $o(ab) = o(a)o(b)$ del ejercicio anterior.

Solución

Ejercicio 7

Sea G un grupo y $a, b \in G$ dos elementos de orden finito. ¿Es ab necesariamente de orden finito?

Solución

Ejercicio 8

En el grupo S_3 se considera el conjunto

$$H = \{Id, (1 \quad 2 \quad 3), (1 \quad 3 \quad 2)\}$$

1.- Demostrar que H es un subgrupo de S_3.

2.- Describir las diferentes clases de S_3 módulo H.

Solución

Ejercicio 9

1.- Demostrar que si $H \leq G$ es un subgrupo, entonces $[G:H] = |G|$ si y solo sí, $H = \{1\}$, mientras que $[G:H] = 1$ si y solo sí, $H = G$.

2.- Demostrar que si se tienen subgrupos $G_2 \leq G_1 \leq G$ entonces

$$[G:G_2] = [G:G_1][G_1:G_2]$$

3.- Demostrar que si se tiene una cadena descendiente de subgrupos de la forma

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$$

Entonces

$$|G| = \prod_{i=0}^{r-1} [G_i:G_{i+1}]$$

Solución

Ejercicio 10

1.- Demostrar que si G es un grupo de orden 4, entonces se tiene que o bien G es cíclico, o bien es isomorfo al grupo de Klein.

Solución

2.- Demostrar que si G es un grupo de orden 6, entonces se tiene que o bien G es cíclico, o bien es isomorfo al grupo D_3.

Solución

Ejercicio 11

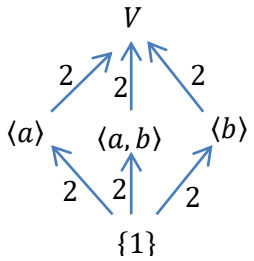
Describir los retículos de subgrupos de los siguientes grupos:

$i)$ el grupo V de Klein $ii)$ el grupo simétrico S_3 $iii)$ el grupo diédrico D_4

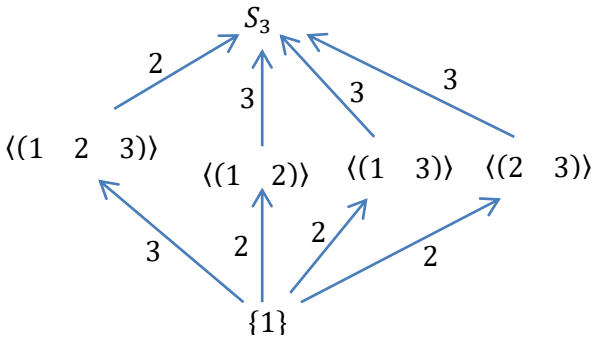
$iv)$ el grupo cuaternio Q_2 $v)$ el grupo alternado A_4

Solución

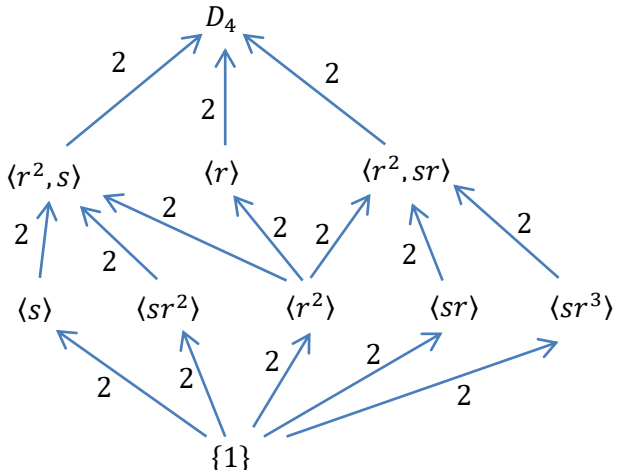
$i)$ el grupo V de Klein



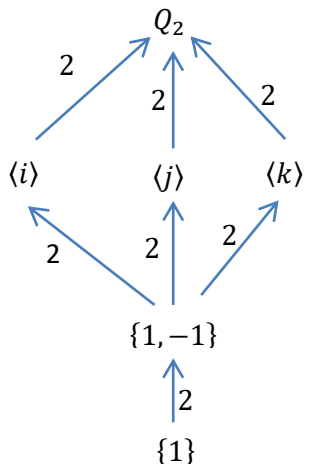
$ii)$ el grupo simétrico S_3



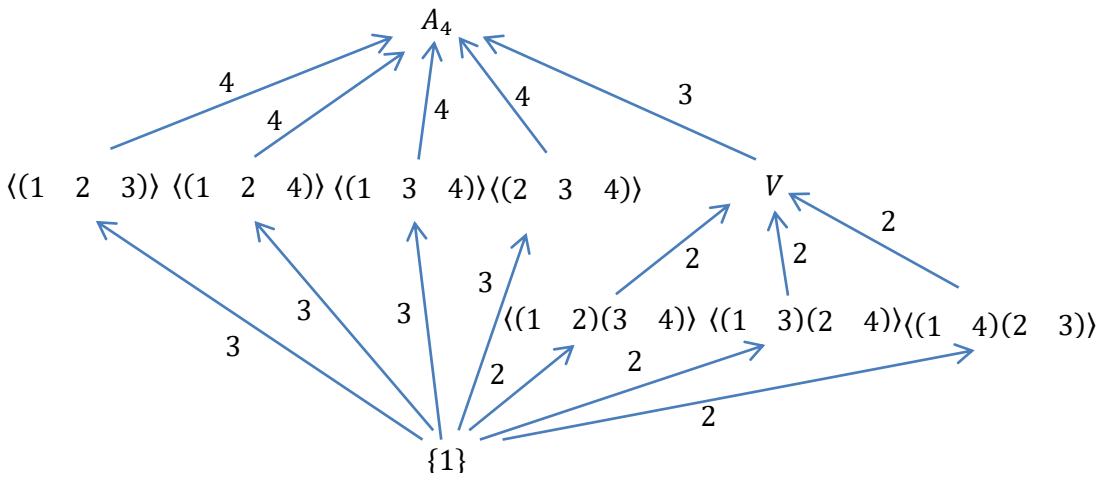
$iii)$ el grupo diédrico D_4



iv) el grupo cuaternio Q_2



v) el grupo alternado A_4



Ejercicio 12

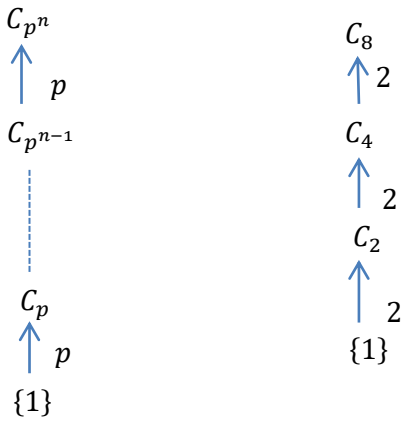
Describe el retículo de subgrupos del grupo cíclico

$$\boldsymbol{C_{p^n} = \langle x \setminus x^{p^n} = 1 \rangle}$$

Siendo p un número primo. En particular, describe el retículo de subgrupos del grupo cíclico

$$\boldsymbol{C_8 = \langle x \setminus x^8 = 1 \rangle}$$

Solución



Ejercicio 13

Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es

si y solo sí, $G = G_p$ es un grupo cíclico de orden primo.

Solución

Ejercicio 14

Describir los retículos de subgrupos de los grupos cíclicos

$$\boldsymbol{C_6 = \langle x \setminus x^6 = 1 \rangle} \quad \boldsymbol{y} \quad \boldsymbol{C_{12} = \langle x \setminus x^{12} = 1 \rangle}$$

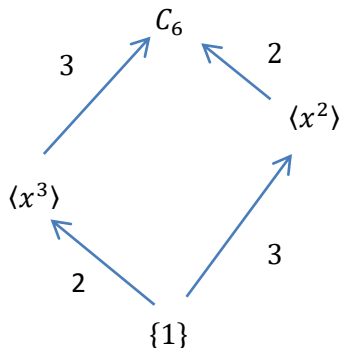
Solución

Para $C_6 = \langle x \setminus x^6 = 1 \rangle$ es de orden 6, entonces $H \leq C_6 \Longrightarrow {|H|}/{|C_6|} \Longrightarrow |H| = 1,2,3,6$

Todo subgrupo de un grupo cíclico es cíclico. Sea $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$

Para $|H| = 1 \Longrightarrow H_1 = \{1\}$. Para $|H| = 2 \Longrightarrow H_2 = \langle x^3 \rangle$. Para $|H| = 3 \Longrightarrow H_3 = \langle x^2 \rangle$.

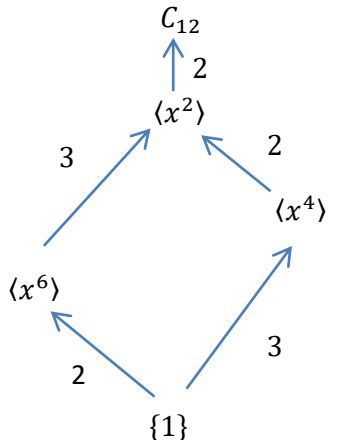
Para $|H| = 6 \Longrightarrow H = C_6$.



Para $C_{12} = \langle x \setminus x^{12} = 1 \rangle$ es de orden 12, entonces $H \leq C_{12} \Longrightarrow {|H|}/{|C_{12}|} \Longrightarrow |H| = 1,2,3,6,12$

Para $|H| = 1 \Longrightarrow H_1 = \{1\}$. Para $|H| = 2 \Longrightarrow H_2 = \langle x^6 \rangle$. Para $|H| = 3 \Longrightarrow H_3 = \langle x^4 \rangle$.

Para $|H| = 6 \Longrightarrow H = \langle x^2 \rangle$. Para $|H| = 12 \Longrightarrow H = C_{12}$.



Ejercicio 15

Se considera el grupo cíclico C_{136} de orden 136, con generador t, ¿Qué relación hay entre los subgrupos $H_1 = \langle t^{48}, t^{72} \rangle$ y $H_2 = \langle t^{46} \rangle$?

Solución

Ejercicio 16

Demostrar que el grupo de unidades Z_7^x es un grupo cíclico.

Solución

Ejercicio 17

Sea G un grupo y sea $C_n = \langle x \setminus x^n = 1 \rangle$ el grupo cíclico de orden n. Demostrar que:

1.- Si $\theta: C_n \to G$ es un homomorfismo de grupos, con $\theta(x) = g$, entonces $o(g)/n$ y $\theta(x^k) = g^k \ \forall k \in \{0, 1, \dots, n-1\}$.

Solución

2.- Para cada $g \in G$ tal que $o(g)/n$, existe un único homomorfismo de grupos $\theta_g: C_n \to G$ tal que $\theta_g(x) = g$.

Solución

3.- Si $g \in G$ es tal que $o(g)/n$, entonces el homomorfismo θ_g es monomorfismo si y solo sí $o(g) = n$.

Solución

4.- Existe un isomorfismo de grupos

$$U(Z_n) \cong Aut(C_n)$$

dado por $r \to f_r$ para cada $r = 1, \dots, n$ con $mcd(r, n) = 1$, donde el automorfismo f_r se define mediante $f_r(x) = x^r$. En particular, $Aut(C_n)$ es un grupo abeliano de orden $\varphi(n)$.

Solución

Ejercicio 18

1.- Describir explícitamente el grupo de automorfismos $Aut(C_8)$.

2.- Demostrar que $Aut(C_8)$ es isomorfo al grupo de Klein.

Solución