Ejercicios3-AII.pdf

jaliriop

Álgebra II

2º Grado en Matemáticas

Facultad de Ciencias
Universidad de Granada

Algebra II

Relación 3

Curso 2019-2020

Subgrupos. Generadores. Retículos. Grupos cíclicos

Ejercicio 1. Describir todos los elementos de los grupos alternados A_n, consistentes en las permutaciones pares del S_n correspondiente, para $n = 2$, $n = 3$ y $n = 4$.

Ejercicio 2. Sea $D_n = \langle r, s \mid s^2 = r^n = 1,\ sr = r^{n-1}s \rangle$ el grupo diédrico. 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 $0 \leq j < k < n$ y $m.c.d.(k - j, n) = 1$.

Ejercicio 3.

1. Demostrar que el subgrupo de $SL_2(\mathbb{Z}_3)$ generado por los elementos

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

es isomorfo al grupo cuaternio Q_2.

2. Demostrar que $SL_2(\mathbb{Z}_3)$ 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.)

Ejercicio 4. Razonar que un subconjunto no vacío $X \subseteq G$ de un grupo G es un subgrupo de G si, y sólo si, $X = \langle X \rangle$.

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, $m.c.d(o(a), o(b)) = 1$.

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

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

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.

Ejercicio 7. Sea G un grupo y $a, b \in G$ dos elementos de orden finito. ¿Es ab necesariamente de orden finito? (**Pista:** Considerar el grupo $GL_2(\mathbb{Q})$ y los elementos

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.)$$

Ejercicio 8. En el grupo S_3 se considera el conjunto

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

1. Demostrar que H es un subgrupo de S_3.

2. Describir las diferentes clases de S_3 módulo H.

Ejercicio 9.

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

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 descendente de subgrupos de la forma

$$G = G_0 \geq G_1 \geq \cdots \geq G_{r-1} \geq G_r,$$

entonces

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

4. Demostrar que si se tiene una cadena descendente de subgrupos de la forma

$$G = G_0 \geq G_1 \geq \cdots \geq G_{r-1} \geq G_r = 1,$$

entonces

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

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.

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 diédrico D_3.

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.


#ESTASREADYCOLACAO
ColaCao

Ejercicio 12. Describe el retículo de subgrupos del grupo cíclico

$$C_{p^n} = \langle x |\ x^{p^n} = 1\rangle,$$

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

$$C_8 = \langle x |\ x^8 = 1\rangle.$$

Ejercicio 13. Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es

$$\begin{array}{c} G \\ \uparrow \\ \{1\} \end{array}$$

si, y sólo si, $G = C_p$ es un grupo cíclico de orden primo.

Ejercicio 14. Describir los retículos de subgrupos de los grupos cíclicos $C_6 = \langle x |\ x^6 = 1\rangle$ y $C_{12} = \langle x |\ x^{12} = 1\rangle$.

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 $H_2 = \langle t^{46}\rangle$?

Ejercicio 16. Demostrar que el grupo de unidades $\mathbb{Z}_7^{\times}$ es un grupo cíclico.

Ejercicio 17. Sea G un grupo y sea $C_n = \langle x | x^n = 1\rangle$ 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 $\theta(x^k) = g^k\ \forall k \in \{0, \ldots, n-1\}$.
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 $\theta_g(x) = g$.
3. Si $g \in G$ es tal que $o(g)|n$, entonces el morfismo θ_g es monomorfismo si, y sólo si, $o(g) = n$.
4. Existe un isomorfismo de grupos

   $$U(\mathbb{Z}_n) \cong Aut(C_n),$$

   dado por $r \mapsto f_r$ para cada $r = 1, \ldots, n$ 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 $\varphi(n)$.

Ejercicio 18.

1. Describir explícitamente el grupo de automorfismos $Aut(C_8)$.
2. Demostrar que $Aut(C_8)$ es isomorfo al grupo de Klein.

RELACIÓN 3 SUBGRUPOS. GENERADORES. RETÍCULOS.

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

$A_2 = \{1\}$

$A_3 = \{1, (1\,2\,3), (1\,3\,2)\}$

$A_4 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}$

2.- Sea $D_n = \langle r, s \mid s^2 = r^n = 1,\ sr = r^{n-1}s \rangle$ el grupo diédrico. 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 $0 \leq j < k < n$ y m.c.d.$(k-j, n) = 1$.

3.-

a) Demostrar que el subgrupo de $SL_2(\mathbb{Z}_3)$ generado por los elementos $\tilde{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $\tilde{j} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ es isomorfo al grupo cuaternio Q_2.

$H = \langle \tilde{i}, \tilde{j} \rangle \overset{?}{\cong} Q_2 = \{\pm 1, \pm i, \pm j, \pm k\} \cong Q_2^{abs} = \langle x, y \mid x^4 = 1,\ x^2 = y^2,\ yx = x^{-1}y \rangle$

$$\begin{array}{ccc} Q_2^{abs} & \xrightarrow{\varphi} & H \\ x & \longmapsto & \tilde{i} \\ y & \longmapsto & \tilde{j} \end{array}$$

Solo hay que comprobar que para que φ sea un homomorfismo $\left\{ \tilde{i}^4 = 1 \quad \tilde{i}^2 = \tilde{j}^2 \quad \tilde{j}\tilde{i} = \tilde{i}^{-1}\tilde{j} \right\}$

$\tilde{i}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad \tilde{i}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \tilde{j}^2$ $\quad \tilde{j}\tilde{i} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = \tilde{i}^{-1}\tilde{j}$.

$$\left.\begin{array}{l}\left.\begin{array}{l}\varphi \text{ homomorfismo} \\ H = \langle \tilde{i}, \tilde{j} \rangle\end{array}\right\} \varphi \text{ epimorfismo} \\ \qquad |H| = 8\end{array}\right\} \varphi \text{ isomorfismo.}$$

b) Demostrar que $SL_2(\mathbb{Z}_3)$ 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).

En Q_2 hay 6 elementos de orden 4: $\pm i, \pm j, \pm k$

En S_4 hay 6 elementos de orden 4, los 4-ciclos:

$(1\ 2\ 3\ 4)$ $(1\ 2\ 4\ 3)$

$(1\ 3\ 2\ 4)$ $(1\ 3\ 4\ 2)$

$(1\ 4\ 2\ 3)$ $(1\ 4\ 3\ 2)$

También están los cuadrados. En $SL_2(\mathbb{Z}_3)$ los elementos de orden 4 tienen mismo cuadrado, mientras que en S_4 son distintos, luego nos pasamos de orden 8. Por tanto, no pueden ser isomorfos.

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

$\Leftarrow$] Es claro.

$\Rightarrow$] Siempre se tiene la inclusión $\langle X \rangle \subseteq X$. Veamos que también tenemos la contraria. Como $\langle X \rangle$ es el menor subgrupo de G que contiene a X, si X es un subgrupo, entonces, es claro que $\langle X \rangle = X$.

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 entre sí, esto es, $m.c.d(o(a), o(b)) = 1$.

a) Razonar que $\langle a \rangle \cap \langle b \rangle = \{1\}$

b) Demostrar que $o(ab) = o(a)o(b)$

$$\begin{tikzcd}[column sep=small] & G \arrow[dl, dash] \arrow[dr, dash] & \\ \langle a\rangle \arrow[dr, dash] & & \langle b\rangle \arrow[dl, dash] \\ & \langle a\rangle\cap\langle b\rangle \arrow[d, dash] & \\ & 1 & \end{tikzcd}$$

$$\rightsquigarrow \left.\begin{array}{l} |\langle a\rangle\cap\langle b\rangle| \,\big|\, |\langle a\rangle| \\ |\langle a\rangle\cap\langle b\rangle| \,\big|\, |\langle b\rangle| \end{array}\right\} \Rightarrow |\langle a\rangle\cap\langle b\rangle| \,\big|\, m.c.d.(o(a), o(b)) = 1$$

$$\Downarrow$$

$$|\langle a\rangle\cap\langle b\rangle| = 1$$

$$\Downarrow$$

$$\langle a\rangle\cap\langle b\rangle = \{1\}$$

$$\left.\begin{array}{l} o(a) = n \\ o(b) = m \end{array}\right. \overset{?}{\Rightarrow} o(ab) = nm$$

- $(ab)^{nm} \overset{ab=ba}{=} a^n b^m = 1$
- $(ab)^t = 1 \overset{?}{\Rightarrow} nm \mid t$

$$\Downarrow$$

$$a^t b^t = 1 \Rightarrow a^t = b^{-t} \in \langle a\rangle\cap\langle b\rangle = \{1\} \Rightarrow a^t = 1,\ b^t = 1$$

$$a^t = 1 \Rightarrow n \mid t, \quad b^t = 1 \Rightarrow m \mid t \quad\Rightarrow\quad nm = m.c.d.(n,m) \mid t$$

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.

Tomemos $G = D_3$ y $a = s$, $b = r$ $\quad o(a) = 2 \quad o(b) = 3$

$$abab = srsr = srr^{-1}s = 1 \Rightarrow o(ab) = 2 \neq 2\cdot 3 = o(a)o(b).$$

7. Sea G un grupo y $a, b \in G$ dos elementos de orden finito. ¿Es ab necesariamente de orden finito? (PISTA: Considerar el grupo $GL_2(\mathbb{Q})$ y los elementos $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$).

$$aa = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow a^4 = 1 \Rightarrow o(a) = 4 < \infty$$

$$bb = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

$$bbb = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow b^6 = 1 \Rightarrow o(b) = 6 < \infty$$

$$ab = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$(ab)(ab) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$$

$$(ab)(ab)(ab) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$$

Supongamos que $(ab)^{n-1} = \begin{pmatrix} 1 & 1-n \\ 0 & 1 \end{pmatrix}$ y veamos que $(ab)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ $\forall n \in \mathbb{N}$.

$$(ab)^n = (ab)(ab)^{n-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1-n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

Por tanto, $(ab)^n \neq 1 \quad \forall n \in \mathbb{N} \Rightarrow o(ab) = \infty$.

8.- En el grupo S_3, se considera el conjunto
$H = \{1, (1\,2\,3), (1\,3\,2)\}$

a) Demostrar que H es un subgrupo de S_3.

$H = A_3$ el grupo alternado de S_3, luego es claramente un subgrupo de S_3.

b) Describir las diferentes clases de S_3 módulo H.

$S_3/\sim_H$

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

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

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

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

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

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

$S_3/\sim_H = \{H, \{(1\,2), (1\,3), (2\,3)\}\}$.

$S_3/_H\sim$

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

13 22 31

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

11

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

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

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

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

$S_3/_H\sim = \{H, \{(1\,2), (1\,3), (2\,3)\}\}$

9.-

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

En el caso $|G|$ finito es claro: Por el Teorema de Lagrange

$|G| = [G:H]\,|H| \rightarrow |G| = |G|\,|H| \Leftrightarrow |H| = 1 \Leftrightarrow H = \{1\}$

$\searrow |G| = 1\,|H| \Leftrightarrow |G| = |H| \underset{H<G}{\Leftrightarrow} H = G$

b) Demostrar que si se tienen subgrupos $G_2 < G_1 < G$, entonces $[G : G_2] = [G : G_1][G_1 : G_2]$

c) Demostrar que si se tiene una cadena descendente de subgrupos de la forma $G = G_0 > G_1 > \dots > G_{r-1} > G_r$ entonces

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

d) Demostrar que si se tiene una cadena descendente de subgrupos de la forma $G = G_0 > G_1 > \dots > G_{r-1} > G_r = 1$, entonces

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

10.-

a) 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.

Si $\exists a \in G \mid o(a) = 4 \Rightarrow \left.\begin{array}{l}|\langle a\rangle| = 4 \\ \langle a\rangle \leq G\end{array}\right\} G = \langle a\rangle \cong \mathbb{Z}_4$ cíclico.

Si $\nexists a \in G \mid o(a) = 4 \Rightarrow \forall x \in G\setminus\{1\}$ $o(x) = 2 \Rightarrow G \cong V$

$a^2 = 1$

$b^2 = 1$

$(ab)^2 = 1 \Rightarrow ab = ba$

$$V^{abs} = \langle x, y \mid x^2 = 1 = y^2,\ xy = yx \rangle \cong V$$

$V^{abs} \xrightarrow{\text{isomorfismo}} G$, $x \mapsto a$, $y \mapsto b$.

Todo grupo de orden menor o igual que 5 es abeliano.

- 1 → trivial
- 2 → primo ⇒ $\mathbb{Z}_2$ cíclico → abel.
- 3 → primo ⇒ $\mathbb{Z}_3$ cíclico → abel
- 4 → $\mathbb{Z}_4$ ⇒ cíclico → abel
  ↘ V ⇒ abeliano
- 5 → primo ⇒ $\mathbb{Z}_5$ cíclico → abel.

b) 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 diédrico D_3.

Si $\exists a \in G \mid o(a) = 6 \Rightarrow \left.\begin{array}{l}|\langle a\rangle| = 6 \\ \langle a\rangle \leq G\end{array}\right\} G = \langle a\rangle \cong \mathbb{Z}_6$ cíclico

Si $\nexists a \in G \mid o(a) = 6 \Rightarrow \forall x \in G\setminus\{1\}$ $o(x) = \begin{cases} 2 \\ 3 \end{cases}$

Si $o(a) = 3 \Rightarrow a^3 = 1 \Rightarrow a^{-1} = a^2 \neq a$

luego no es posible (basta contar) que $\forall x \in G\setminus\{1\}$ sean de orden 3 ni de orden 2.

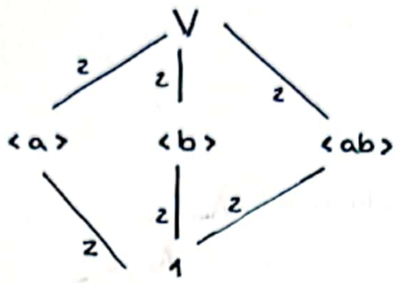
11.- Describir los retículos de subgrupos de los siguientes grupos:

i) el grupo V de klein.

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

$o(1) = 1$

$o(a) = o(b) = o(ab) = 2$

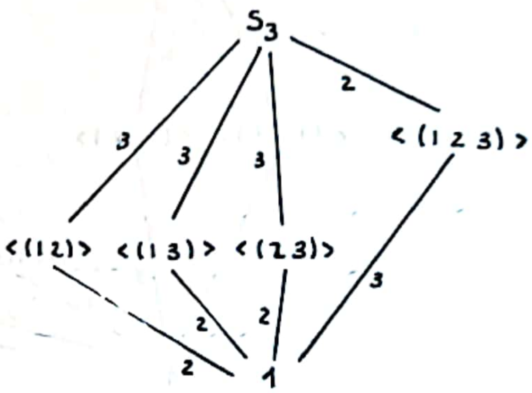


ii) el grupo simétrico S_3.

$o(1) = 1$

$o((12)) = o((13)) = o((23)) = 2$

$o((123)) = o((132)) = 3$

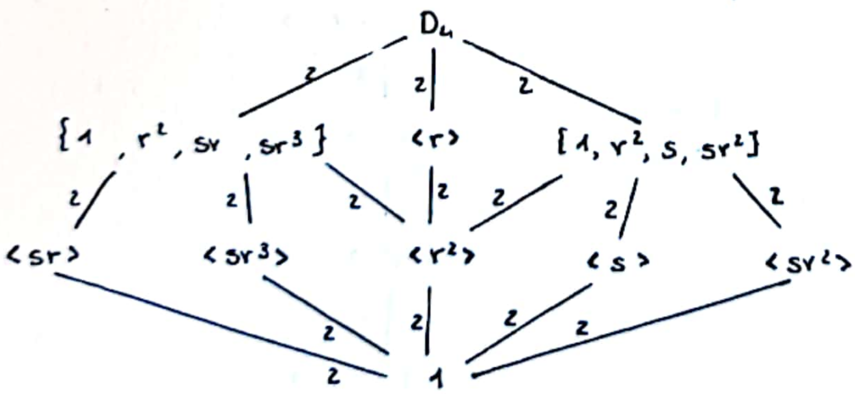


iii) el grupo diédrico D_4

$o(1) = 1$

$o(r^2) = o(s) = o(sr) = o(sr^2) = o(sr^3) = 2$

$o(r) = o(r^3) = 4$

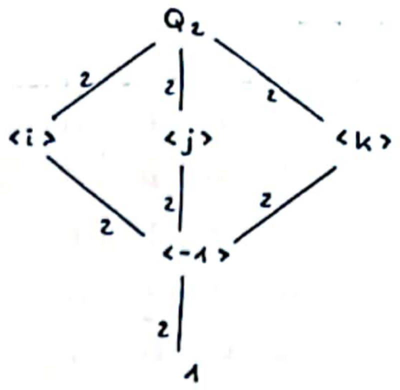


d) el grupo cuaternio Q_2.

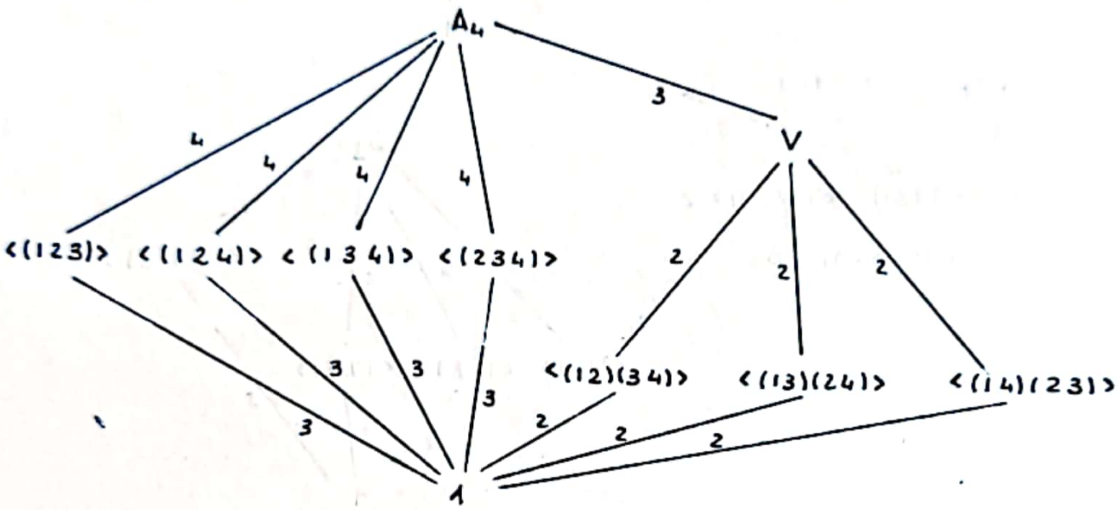
$o(1) = 1$

$o(-1) = 2$

$o(i) = o(-i) = o(j) = o(-j) = o(k) = o(-k) = 4$



e) el grupo alternado A_4.



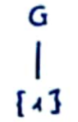
12.- Describe el retículo de subgrupos del grupo cíclico

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

Siendo p un número primo. En particular, describe el retículo de subgrupos del grupo cíclico $C_8 = \langle x \mid x^8 = 1 \rangle$.

$$\begin{tikzcd}[arrows=-]
C_{p^n} = \langle x \rangle \arrow[d, "p"] \\
\langle x^{p^1} \rangle \arrow[d, "p"] \\
\langle x^{p^2} \rangle \arrow[d, "p"] \\
\cdots \arrow[d, "p"] \\
\langle x^{p^{n-1}} \rangle \arrow[d, "p"] \\
\langle x^{p^n} \rangle = 1
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[arrows=-]
C_8 = \langle x \rangle \arrow[d, "2"] \\
\langle x^{2^1} \rangle \arrow[d, "2"] \\
\langle x^{2^2} \rangle \arrow[d, "2"] \\
1 = \langle x^{2^3} \rangle
\end{tikzcd}$$

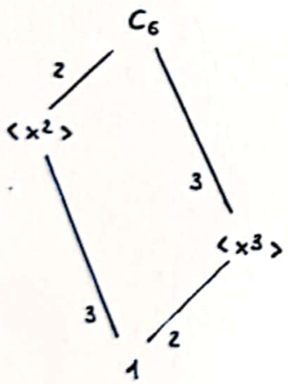
13.- Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es

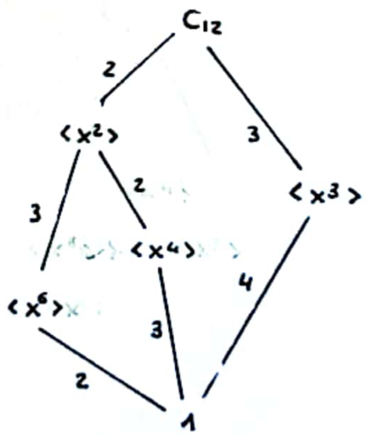


si, y solo si, $G = C_p$ es un grupo cíclico de orden primo.

14.- Describir los retículos de subgrupos de los grupos cíclicos $C_6 = \langle x \mid x^6 = 1 \rangle$ y $C_{12} = \langle x \mid x^{12} = 1 \rangle$

$12 = 2^2 \cdot 3$





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

$48 \cdot 3 = 144 \equiv 8$

$\langle t^2 \rangle$

46
46
46

$138 \equiv 2 \mod 36$

Escaneado con CamScanner

(10)

2) Si G grupo de orden 6 $\begin{cases} G \text{ cíclico} \Rightarrow G \cong \mathbb{Z}_6 \\ G \cong D_3 \end{cases}$

Si $\exists a \in G \mid o(a) = 6 \Rightarrow |\langle a \rangle| = 6 \Rightarrow G = \langle a \rangle \cong \mathbb{Z}_6$.

Si $\nexists \underset{\neq 1}{a} \in G \mid o(a) = 6 \Rightarrow o(a) = \{ 2, 3$

Si $\forall a \in G \setminus \{1\}$ tuviera $o(a) = 3$ contando elementos llegamos a una contradicción $\begin{matrix} a \neq a^{-1} \\ b \neq b^{-1} \\ c \neq c^{-1} \end{matrix} \Rightarrow$ habría 7 elementos $\Rightarrow$ NO PUEDE SER.

Si $\forall a \in G \setminus \{1\}$ tuviera $o(a) = 2$ también llegamos a contradicción

$$a, b \in G \begin{cases} a^2 = 1 \\ b^2 = 1 \end{cases}$$
$$\Downarrow$$
$$ab \in G \Rightarrow (ab)^2 = 1 \Rightarrow ab = ba$$
$$H = \{1, a, b, ab\} \cong V \text{ con } H < G \Rightarrow 4 \mid 6$$
$$\Downarrow$$
CONTRADICCIÓN

Por tanto, tienen que existir $a \in G \mid o(a) = 3$
$b \in G \mid o(b) = 2$

$\Rightarrow G = \{1, a, a^2, b, ab, a^2 b\}$ $\quad ba \neq 1 \leftarrow$ NO $\quad ba = a \leftarrow$ NO

$ba = \begin{cases} ab \Rightarrow o(ab) \overset{*}{=} o(a)o(b) = 6 \\ a^2 b \end{cases}$ $\quad ba = a^2 \leftarrow$ NO $\quad ba = b \leftarrow$ NO

CONTRADICCIÓN

$\Downarrow$

$ba = a^2 b$

* Si dos elementos conmutan y sus órdenes son primos relativos, el orden del producto es el producto de los órdenes.

$$\begin{matrix} D_3 & \longrightarrow & G \\ r & \longmapsto & a \\ s & \longmapsto & b \end{matrix} \qquad \begin{cases} a^3 = 1 \\ b^2 = 1 \\ ba = a^2 b \end{cases} \overset{\text{Dyck}}{\Longrightarrow} \text{ISOMORFISMO.}$$

Escaneado con CamScanner

Hay tantos homomorfismos de C_n en G como elementos x de G tal que $o(x) \mid n$.

(17) G y $C_n = \langle x \mid x^n = 1 \rangle$

1) $\theta: C_n \longrightarrow G$ homomorfismo $\theta(x) = g \overset{?}{\Rightarrow}$

$\overset{?}{\Rightarrow} o(g) \mid n$ y $\theta(x^k) = g^k \quad \forall k \in \{0, \dots, n-1\}$

$1 = \theta(1) = \theta(x^n) = \theta(x)^n = g^n \Rightarrow o(g) \mid n$

$\theta(x^k) = \theta(x)^k = g^k$

2) $\forall g \in G \mid o(g) \mid n \quad \exists!\ \theta_g: C_n \longrightarrow G$ homomorfismo con $\theta_g(x) = g$

Consideramos $C_n \xrightarrow{\theta_g} G$
$x \longmapsto g$ si $o(g) \mid n$ (En tal caso $g^n = 1$
$\Downarrow$ Teorema de Dyck
$\exists!\ \theta_g \mid \theta_g(x) = g$
homomorfismo.)

3) Si $g \in G$ con $o(g) \mid n \Rightarrow [\theta_g$ es monomorfismo $\Leftrightarrow o(g) = 1]$

Hay tantos monomorfismos de C_n en G como elementos x de G tal que $o(x) = n$

θ_g monomorfismo $\Longleftrightarrow \ker(\theta_g) = 1 \Leftrightarrow \theta_g(x^k) = g^k \neq 1$
$\forall k = 1, \dots, n-1$
$\Updownarrow g^n = 1$
$o(g) = n$.

para usar notación aditiva en ambos casos.

4) $U(\mathbb{Z}_n) \cong Aut(C_n) \cong Aut(C_n)$..

$\mathbb{Z}_n \xrightarrow{\theta_{\bar{r}}} \mathbb{Z}_n$ homomorfismos biyectivos
$\bar{1} \longrightarrow \bar{r}$ $\Downarrow |\mathbb{Z}_n| = |\mathbb{Z}_n|$
con ~~o(...)~~ homomorfismos inyectivos
$o(\bar{r}) \mid n$
(ejercicio anterior).
$\bar{k} \longmapsto k\bar{r} = \overline{kr}$

$Aut(\mathbb{Z}_n) = \{\theta_{\bar{r}} \mid o(\bar{r}) = n\} =$

$= \{\theta_{\bar{r}} \mid m.c.d(r, n) = 1\} \Rightarrow |Aut(\mathbb{Z}_n)| = \varphi(n)$

Definimos entonces

$U(\mathbb{Z}_n) \xrightarrow{\phi} Aut(\mathbb{Z}_n)$

$m.c.d(n, r) = 1 \Rightarrow \bar{r} \longmapsto \phi(\bar{r}) = \theta_{\bar{r}} \quad \leftarrow \phi$ biyectiva evidentemente

$\phi(\bar{r}\bar{s}) \overset{?}{=} \phi(\bar{r})\phi(\bar{s})$

$\forall \bar{k} \in \mathbb{Z}_n \Rightarrow \phi(\bar{r}\bar{s})(\bar{k}) = \theta_{\bar{r}\bar{s}}(\bar{k}) = \theta_{\overline{rs}}(\bar{k}) = \overline{rsk}$

$(\phi(\bar{r})\phi(\bar{s}))(\bar{k}) = \phi(\bar{r})(\theta_{\bar{s}}(\bar{k})) = \phi(\bar{r})(\overline{sk}) = \theta_{\bar{r}}(\overline{sk}) = \overline{rsk}$

homomorfismo.

(18) 1) Describir explícitamente $Aut(C_8)$

$|Aut(\mathbb{Z}_8)| = \varphi(8) = 8 \cdot \left(1 - \frac{1}{2}\right) = 4.$

$$\begin{array}{ccc} C_8 & \xrightarrow{\theta_{x^k}} & C_8 \\ x & \longmapsto & x^k \end{array} \qquad \left[\begin{array}{lcl|l} x \xmapsto{\theta_x} x & \Rightarrow & Id_{C_8} \\ x \longmapsto x^3 & \Rightarrow & \theta_{x^3} \\ x \longmapsto x^5 & \Rightarrow & \theta_{x^5} \\ x \longmapsto x^7 & \Rightarrow & \theta_{x^7} \end{array}\right]$$

$Aut(C_8) = \{ Id_{C_8}, \theta_{x^3}, \theta_{x^5}, \theta_{x^7} \}$

$o(Id_{C_8}) = 1$

$o(\theta_{x^3}) = 2 \qquad x \xmapsto{\theta_{x^3}} x^3 \xmapsto{\theta_{x^3}} x^9 = x$

$o(\theta_{x^5}) = 2 \qquad x \xmapsto{\theta_{x^5}} x^5 \xmapsto{\theta_{x^5}} x^{25} = x$

$o(\theta_{x^7}) = 2 \qquad x \xmapsto{\theta_{x^7}} x^7 \xmapsto{\theta_{x^7}} x^{49} = x$

$\Downarrow$

No es cíclico $\Rightarrow$ Como es de orden 4, es klein $\Rightarrow$

$\Rightarrow \quad Aut(C_8) \cong V$

(15) $C_{136} = \langle t \mid t^{136} = 1 \rangle$

$H_1 = \langle t^{48}, t^{72} \rangle \qquad H_2 = \langle t^{46} \rangle$

$o(x) = n \Rightarrow \langle x^k \rangle = \langle x^{m.c.d(n,k)} \rangle \quad , \quad o(x^k) = \frac{n}{m.c.d(n,k)}$

$$\left.\begin{array}{l} H_2 = \langle t^{46} \rangle = \langle t^2 \rangle \\ \left.\begin{array}{l} \langle t^{48} \rangle = \langle t^8 \rangle \\ \langle t^{72} \rangle = \langle t^8 \rangle \end{array}\right\} H_1 = \langle t^8 \rangle \end{array}\right\} \Rightarrow H_1 < H_2$$