WUOLAH

Tema3-AII.pdf

jaliriop

Álgebra II

2º Grado en Matemáticas

Facultad de Ciencias
Universidad de Granada

Reservados todos los derechos.
No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

WUOLAH NEW Print
Todos los apuntes que necesitas están aquí
Al mejor precio del mercado, desde **2 cent.**
Recoge los apuntes en tu copistería más cercana o recíbelos en tu casa
Todas las anteriores son correctas
Imprimir

3 SUBGRUPOS. GENERADORES. RETÍCULOS

Definición: Dados dos grupos G y H, se dice que H es un <u>subgrupo</u> de G, y lo denotamos $H < G$, cuando $H \subseteq G$ es un subconjunto de G, y la aplicación de inclusión $i: H \longrightarrow G$, $x \longmapsto x$ es un homomorfismo de grupos.

Por tanto $xy = i(xy) = i(x)i(y) = xy$
producto en H — producto en G.

Entonces, las operaciones en G y H coinciden y también el neutro y el inverso de cada elemento.

Observación: Todo grupo tiene dos subgrupos (llamados impropios), que son el trivial, $1 < G$, y el total, $G < G$. Cualquier otro subgrupo se dice que es propio.

Ejemplos:

(1). $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$

(2) $\{\text{rotaciones en } D_n\} < D_n$

(3) $n\mathbb{Z} \leq \mathbb{Z}$

(4) $SL_n(\mathbb{K}) < GL_n(\mathbb{K})$

(5) $(\mathbb{Q}^*, \cdot) \not< (\mathbb{R}, +)$

(6) $D_6 \not< D_8$

(7) Si $H < G$ y $G < K \Rightarrow H < K$

Proposición: Sea G un grupo y $H \neq \emptyset$ un subconjunto de G. Entonces equivalen:

i) H es un subgrupo de G.

ii) Se verifican:
a) $\forall x, y \in H \Rightarrow xy \in H$
b) $1 \in H$
c) $\forall x \in H \Rightarrow x^{-1} \in H$

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

DEMOSTRACIÓN:

WUOLAH

Escaneado con CamScanner

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

i) ⇒ ii)] Como las operaciones coinciden, entonces es inmediato

ii) ⇒ iii)] $y \in H \Rightarrow y^{-1} \in H$

$\forall x \in H \Rightarrow xy^{-1} \in H$

iii) ⇒ i)] $\forall x \in H \Rightarrow xx^{-1} = 1 \in H$

$\forall x \in H \Rightarrow 1 \cdot x^{-1} = x^{-1} \in H$

$xy = x(y^{-1})^{-1} \in H.$

Proposición: Sea G un grupo y $H \neq \emptyset$ un subconjunto de G. Supongamos G finito. Entonces H es un subgrupo de G si, y solo si, $\forall x, y \in H \Rightarrow xy \in H$.

⇒] Claro.

⇐] Como G es finito $\Rightarrow$ $\forall x \in G \ \exists n \in \mathbb{N} \mid x^n = 1 \Rightarrow$

$\Rightarrow xx^{n-1} = 1 \Rightarrow x^{-1} = x^{n-1} \Rightarrow x^{-1} \in H$

$x^{n-1} = x \cdot x \cdot \ldots \in H$

Ejemplos:

(1) $\{$permutaciones pares de $S_n\} = A_n < S_n$ por la proposición anterior

(el producto de perm. pares es una permutación par).

(2) Veamos que si $H < \mathbb{Z}$, entonces $\exists n \in \mathbb{N} \mid H = n\mathbb{Z}$.

Como $H \neq \emptyset$, $\exists n \in H$, $\Rightarrow -n \in H \Rightarrow H \cap \mathbb{Z}^+ \neq \emptyset$

Sea n el menor entero positivo de H, y veamos que $H = n\mathbb{Z}$. Como $n\mathbb{Z} \subseteq H$, veamos la otra inclusión.

Sea $m \in H$, y veamos que $m \in n\mathbb{Z}$.

$$\left.\begin{array}{l} m = n \cdot q + r \quad \mid 0 \leq r < n \\ r = \underset{H}{\underset{\cap}{m}} - \underset{H}{\underset{\cap}{nq}} \in H \end{array}\right\} \text{Por ser } n \text{ el menor} \Rightarrow r = 0$$

$m = nq \in n\mathbb{Z}$.

Proposición: Sea $f: G \to G'$ un homomorfismo de grupo.

Entonces:

- Si $H < G \Rightarrow f_*(H) < G'$
- Si $H' < G' \Rightarrow f^*(H') < G$

Escaneado con CamScanner

WUOLAH

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

NEW

WUOLAH Print

Lo que faltaba en Wuolah

Imprimir

- [ ] Todos los apuntes que necesitas están aquí
- [ ] Al mejor precio del mercado, desde **2 cent.**
- [ ] Recoge los apuntes en tu copistería más cercana o recíbelos en tu casa
- [x] Todas las anteriores son correctas

DEMOSTRACIÓN: 8/10/19

- Ejercicio
- Sean $x, y \in f^*(H') \overset{?}{\Rightarrow} xy^{-1} \in f^*(H') \Rightarrow f^*(H')$ subgrupo

$\Downarrow$

$f(x), f(y) \in H'$

$\Downarrow$

$f(x)f(y)^{-1} \in H' \Rightarrow f(x), f(y^{-1}) \in H \Rightarrow f(x)f(y^{-1}) = f(xy^{-1}) \in H'$

Nota: $f^*(1) = \{x \in G \mid f(x) = 1\} = ker(f) < G$

$f_*(G) = \{f(x) \mid x \in G\} = Im(f) < G'$

Proposición: Sea $\{H_\lambda\}_{\lambda \in \Lambda}$ una familia de subgrupos de un grupo G. Entonces $\bigcap_{\lambda \in \Lambda} H_\lambda < G$.

DEMOSTRACIÓN:

Como $1 \in H_\lambda \ \forall \lambda \in \Lambda \Rightarrow 1 \in \bigcap_{\lambda \in \Lambda} H_\lambda \neq \emptyset$

Tomemos $x, y \in \bigcap_{\lambda \in \Lambda} H_\lambda \Rightarrow x, y \in H_\lambda \ \forall \lambda \in \Lambda \overset{H_\lambda \text{ subgrupo}}{\Rightarrow}$

$\Rightarrow x, y^{-1} \in H_\lambda \ \forall \lambda \in \Lambda \Rightarrow xy^{-1} \in H_\lambda \ \forall \lambda \in \Lambda \Rightarrow xy^{-1} \in \bigcap_{\lambda \in \Lambda} H_\lambda$

$\Rightarrow \bigcap_{\lambda \in \Lambda} H_\lambda$ es un subgrupo.

Observación: La unión de subgrupos no es, en general, un subgrupo

$$\left.\begin{array}{l} 2\mathbb{Z} < \mathbb{Z} \\ 3\mathbb{Z} < \mathbb{Z} \end{array}\right\} \quad 2\mathbb{Z} \cup 3\mathbb{Z} \overset{?}{<} \mathbb{Z}$$

$$\underset{\substack{\notin \\ 2\mathbb{Z} \cup 3\mathbb{Z}}}{1} = 3 - 2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$$

Definición: Sea G un grupo, y sea $S \subseteq G$ un subconjunto. El <u>subgrupo de G generado por S</u>, denotado $\langle S \rangle$, es la intersección de todos los subgrupos de G que contienen a S (por tanto, $\langle S \rangle$ es el menor subgrupo de G que contiene a S).

Proposición: Sea G un grupo, $S \subseteq G$ subconjunto, y consideremos $\langle S \rangle$. Entonces:

1) Si $S = \emptyset \Rightarrow \langle S \rangle = 1$

2) Si $S \neq \emptyset$, $\langle S \rangle = \{x_1^{\delta_1} x_2^{\delta_2} \ldots x_n^{\delta_n} \mid n \geq 1, x_i \in S, \delta_i = \pm 1\}$ (productos finitos de elementos de S y sus inversos).

3) Si $S \neq \emptyset$ y G finito, $\langle S \rangle = \{x_1 x_2 \ldots x_n \mid n \geq 1, x_i \in S\}$

Escaneado con CamScanner
WUOLAH
Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.
Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

DEMOSTRACIÓN:

2) Observar que $\{x_1^{\delta_1} \dots x_n^{\delta_n} \mid n \geq 1,\ x_i \in S,\ \delta_i = \pm 1\}$ satisface la propiedad de la intersección, es decir, que es un subgrupo de G que contienea a S y es el menor.

3) Igual.

Ejemplos:

(1) D_n, $S = \{r\} \Rightarrow \langle S \rangle = \{1, r, r^2, \dots, r^{n-1}\} < D_n$

(2)

$$i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{C})$$

$\underset{Q_2}{\langle i, j \rangle} = \{\pm I, \pm i, \pm j, \pm K\}$ donde $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ $\ulcorner GL_2(\mathbb{C})$

(3) S_4

$\langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} < S_4$

$= V$ (grupo de klein)

(4) S_n

$\langle (x_1\, x_2\, x_3) \rangle < S_n$

$= A_n$

Definición: Si H_λ con $\lambda \in \Lambda$ es una familia de subgrupos de un grupo G, se define el compuesto de la familia, denotado por $\bigvee_{\lambda \in \Lambda} H_\lambda$, como el subgrupo de G generado por la unión $\bigcup_{\lambda \in \Lambda} H_\lambda \subseteq G$.

Si H_λ es una familia finita, lo notaremos $H_1 \vee H_2 \vee \dots \vee H_n$.

Notación: Si $H, K < G$, notaremos $HK = \{hk \mid h \in H, k \in K\} \subseteq G$

Proposición: Si $H, K < G$, se tiene que

$HK = H \vee K$ (y por tanto un subgrupo) $\Longleftrightarrow HK = KH$.

DEMOSTRACIÓN:

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Escaneado con CamScanner

WUOLAH

Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

WUOLAH NEW
Print
Todos los apuntes que necesitas están aquí
Al mejor precio del mercado, desde **2 cent.**
Recoge los apuntes en tu copistería más cercana o recíbelos en tu casa
Todas las anteriores son correctas
Imprimir

$\Rightarrow$] $\forall kh \in KH$, $\quad kh = (h^{-1}k^{-1})^{-1} \in HK \Rightarrow KH \subseteq HK$

$\forall hk \in HK$, $\quad hk = (k^{-1}h^{-1})^{-1} \Rightarrow k^{-1}h^{-1} = h_1 k_1 \quad h_1 \in H, \ k_1 \in K$

$hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH \Rightarrow HK \subseteq KH$

Por tanto $KH = HK$

$\Leftarrow$] Tomemos $hk, \ h_1 k_1 \in HK$

$$(hk)(h_1k_1)^{-1} = h\underbrace{kk_1^{-1}}_{k_2}\cdot\underbrace{h_1^{-1}}_{h_2} = hh_3k_3 \in HK \Rightarrow HK < G \overset{?}{\Rightarrow} HK = H \vee K$$

$HK = KH$

Definición: (clases laterales de un subgrupo en un grupo):

Si $H < G$, en G definimos dos relaciones binarias:

$$\begin{cases} y \underset{H}{\sim} x \iff x^{-1}y \in H \\ y \sim_H x \iff yx^{-1} \in H \end{cases}$$

Ambas relaciones, $\underset{H}{\sim}$ y $\sim_H$, son de equivalencia.

$y \underset{H}{\sim} x \Rightarrow x^{-1}y \in H \Rightarrow x^{-1}y = h \in H \Rightarrow y = xh \qquad xH = \{xh \mid h \in H\}$ clase de equivalencia de x, $\underset{H}{\sim}$

clase lateral por la izquierda de H en G definida por x

$y \sim_H x \Rightarrow yx^{-1} \in H \Rightarrow yx^{-1} = h \in H \Rightarrow y = hx \qquad Hx = \{hx \mid h \in H\}$ clase de equivalencia de x, $\sim_H$

clase lateral por la derecha de H en G definida por x

Consideramos los respectivos conjuntos cocientes.

$G/\underset{H}{\sim} = \{xH\}$

$G/\sim_H = \{Hx\}$

11/10/19

Nota: $G/\underset{H}{\sim}$ y $G/\sim_H$ son en general distintos.

Ejemplo: $G = S_3 \quad H = \langle (1\ 2) \rangle = \{1, (1, 2)\}$

$G/\underset{H}{\sim}$

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

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

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

$G/\underset{H}{\sim} = \{H, \ (1\ 3)H, \ (2\ 3)H\}$

WUOLAH

Escaneado con CamScanner
Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

$G/\sim_H$

$H1 = H$

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

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

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

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

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

ii) Existen biyecciones $xH \longleftrightarrow H \longleftarrow Hx \quad \forall x \in G$

$xh \longmapsto h \longmapsto hx$

iii) Existe una biyección entre $G/_H\sim \cong G/\sim_H$ dada por

$xH \longmapsto Hx^{-1}$

DEMOSTRACIÓN

i) Evidente porque $\underset{xH}{x = x1} = \underset{Hx}{1x}$ porque $1 \in H \; \forall H < G$

ii) Las aplicaciones dadas son biyectivas inmediatamente.

iii) Veamos que la aplicación dada está bien definida:

$xH = yH \overset{?}{\Rightarrow} Hx^{-1} = Hy^{-1}$

$\Downarrow$

$yx^{-1} \in H \Rightarrow (y^{-1}x)^{-1} = x^{-1}y \in H \Rightarrow x^{-1} \sim_H y^{-1}$

Veamos que es inyectiva:

Dados $xH, yH \in G/_H\sim \mid Hx^{-1} = Hy^{-1} \overset{?}{\Rightarrow} xH = yH$

$\Downarrow$

$x^{-1} \sim_H y^{-1} \Rightarrow x^{-1}y \in H \Rightarrow x\,{}_H\!\sim y$

Claramente es sobreyectiva. $\forall Hy \;\; \exists y^{-1}H \mid y^{-1}H \longmapsto Hy$

Luego biyectiva.

Definición: Dado $H < G$, el cardinal de $G/\sim_H$ (que es el de $G/_H\sim$) se llama el <u>índice de H en G</u>, y se denota $[G:H]$.

Teorema de Lagrange: Sea G un grupo finito y $H < G$. Entonces $|H| \mid |G|$ y se tiene que

$|G| = [G:H] \cdot |H|$.

Escaneado con CamScanner
WUOLAH
Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa
Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

DEMOSTRACIÓN:

Sean $x_1 = 1, x_2, \dots, x_n$ representantes de las clases laterales de $G/\underset{H}{\sim}$.

Entonces $|G| = |H| + |x_2H| + \dots + |x_nH| \underset{|x_iH| = |H| \ \forall x_i}{=} n|H|$ con $n = [G:H]$

Por tanto $|H| \,\big|\, |G|$.

Observación: El recíproco, en general, NO es cierto.

Ejemplo: A_4 $\qquad |A_4| = 12$

Aunque $6 | 12$, A_4 no tiene subgrupos de orden 6.

$A_4 = \{1, (12)(34), (13)(24), (14)(23), \text{3-ciclos}\}$

Supongamos que $H < A_4$ tal que $|H| = 6$.

- Si en H solo hubiera un 3-ciclo (habría 2, él y su inverso). $\Rightarrow H = \{\underbrace{1, (12)(34), (13)(24), (14)(23)}_{V \text{ grupo de klein}}, \text{3-ciclo, inverso}\}$

Pero entonces $4 | 6 \rightarrow$ contradicción.

- Tiene que haber más de un 3-ciclo y su inverso.

$$\begin{matrix} (x_1\ x_2\ x_3) & (x_1\ x_3\ x_2) \\ (x_1\ x_2\ x_4) & (x_1\ x_4\ x_2) \end{matrix} \Rightarrow \begin{matrix} (x_1\ x_2\ x_3)(x_1\ x_4\ x_2) \in H \\ \begin{matrix} x_1 \to x_4 \\ x_2 \to x_2 \\ x_3 \to x_1 \\ x_4 \to x_3 \end{matrix} \quad \begin{matrix} \| \\ (x_1\ x_4\ x_3) \\ (x_1\ x_3\ x_4) \end{matrix} \end{matrix}$$

Tenemos ya 6 elementos más la identidad, luego $|H| > 6 \Rightarrow$ contradicción.

Por tanto, A_4 no tiene subgrupos de orden 6.

Observación: Si G finito $\Rightarrow [G:H] = \frac{|G|}{|H|}$. En otro caso, no tiene sentido.

Observación: $\mathbb{Z}$ $\begin{cases} \{0\} \rightsquigarrow [\mathbb{Z}:0] = \infty & \text{subgrupo de índice infinito} \\ \underset{n \neq 0}{n\mathbb{Z}} \rightsquigarrow [\mathbb{Z}:n\mathbb{Z}] = n. & \text{subgrupo de índice finito.} \end{cases}$

Corolario: El orden de un elemento de un grupo finito divide siempre al orden del grupo.

DEMOSTRACIÓN:

Sea G finito y $x \in G \rightsquigarrow \langle x \rangle < G \Rightarrow \underset{\substack{\| \\ o(x)}}{|\langle x \rangle|} \,\big|\, G$

Escaneado con CamScanner
WUOLAH
Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.
Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

Corolario: Si G es finito y tenemos una torre $K < H < G \Rightarrow [G:K] = [G:H]\cdot[H:K]$.

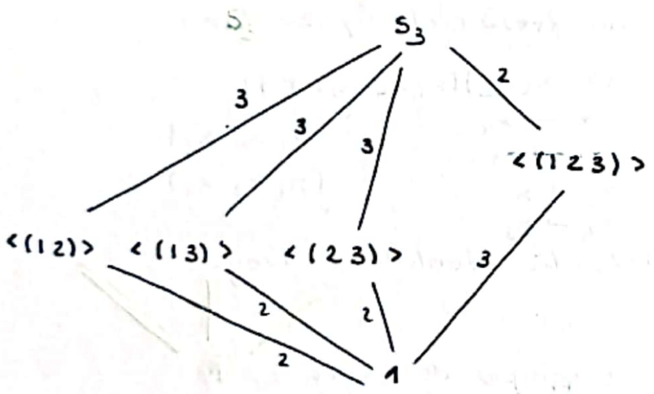
DEMOSTRACIÓN:

$$\left.\begin{array}{l} |G| = [G:K]\cdot|K| \\ |G| = [G:H]\cdot|H| = [G:H]\cdot[H:K]\cdot|K| \end{array}\right\} [G:K] = [G:H]\cdot[H:K]$$

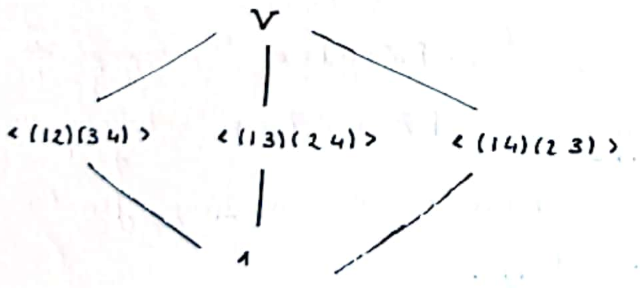
RETÍCULO DE SUBGRUPOS DE UN GRUPO

Definición: Sea G un grupo finito. El <u>retículo de subgrupos de G</u> es un grafo orientado cuyos vértices son los subgrupos de G y en el que hay una arista orientada entre dos vértices H y K si $H \subseteq K$ y no hay subgrupos intermedios entre H y K.

Ejemplo: S_3 $\quad |S_3| = 6$



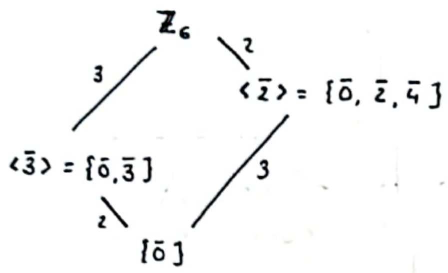
Ejemplo: $V = \{1, (12)(34), (13)(24), (14)(23)\}$



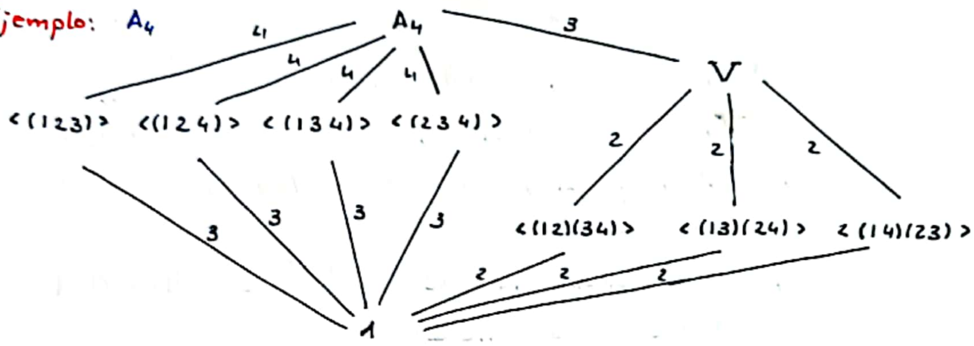
Reservados todos los derechos.
No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.
Escaneado con CamScanner
WUOLAH
Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

WUOLAH NEW
Print
Todos los apuntes que necesitas están aquí
Al mejor precio del mercado, desde **2 cent.**
Recoge los apuntes en tu copistería más cercana o recíbelos en tu casa
Todas las anteriores son correctas
Imprimir
Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Ejemplo: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$



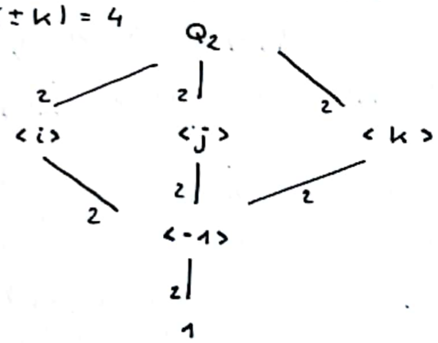
Ejemplo: A_4



Ejemplo: $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ 14/10/19

$o(-1) = 2$

$o(\pm i) = o(\pm j) = o(\pm k) = 4$



Ejemplo: $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} = \langle r, s \mid r^4 = 1 = s^2, sr = r^{-1}s \rangle$

$|D_4| = 8$

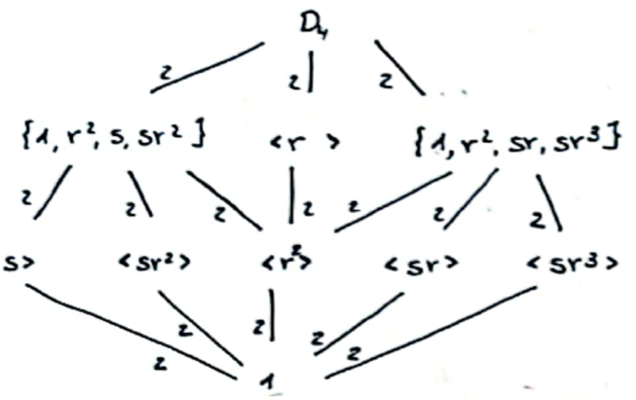
$o(1) = 1$

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

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

r^2 conmuta con el resto de elementos.

WUOLAH
Escaneado con CamScanner



Observación: Grupos isomorfos tienen retículos isomorfos.

Observación: Grupos no isomorfos pueden tener retículos isomorfos (por ejemplo, grupos de orden 16).

GRUPOS CÍCLICOS.

Recordemos que un grupo G es cíclico si $\exists a \in G \mid$
$G = \langle a \rangle$ $(\forall x \in G \;\; x = a^n \;\; n \in \mathbb{Z})$.

Nuestros objetivos son:

- Clasificar todos los grupos cíclicos
- Estudiar el retículo de subgrupos de un grupo cíclico
- Estudiar los posibles generadores de un grupo cíclico.

Proposición:

i) Si G es cíclico $\Rightarrow$ G es abeliano.

ii) Si $|G| = p$ primo $\Rightarrow$ G es cíclico.

iii) Si G es un grupo y $x \in G$ con $o(x) = n$, entonces $x^k = 1 \Leftrightarrow n \mid k$

iv) Si G es un grupo y $x \in G$ $\rightarrow$ a) Si $o(x) = \infty \Rightarrow$ todas las potencias de x son elementos distintos de G

b) Si $o(x) = n \Rightarrow 1, x, \dots, x^{n-1}$ son distintos, $\langle x \rangle = \{1, x, \dots, x^{n-1}\}$ y $x^i = x^j \Leftrightarrow n \mid i - j$

DEMOSTRACIÓN:

i) G cíclico $\rightsquigarrow$ $G = \langle a \rangle$ y $x, y \in G \Rightarrow x = a^n$, $y = a^m \Rightarrow$
$\Rightarrow xy = a^n a^m = a^{n+m} = a^m \cdot a^n = yx$

ii) $|G| = p$ primo y sea $x \in G \setminus \{1\}$ y consideremos
$1 \neq \langle x \rangle < G$. Por el Teorema de Lagrange, $|\langle x \rangle| \mid |G| = p \Rightarrow$
$\Rightarrow$ $|\langle x \rangle| = 1 \rightarrow$ No porque $\langle x \rangle \neq 1$.
$|\langle x \rangle| = p \Rightarrow \langle x \rangle = G \Rightarrow G$ cíclico

Escaneado con CamScanner
WUOLAH
Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa
Reservados todos los derechos.
No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

iii) $\Leftarrow]$ Si $n|k \Rightarrow k = n\cdot s \Rightarrow x^k = x^{ns} = (x^n)^s = 1^s = 1$

$\Rightarrow]$ Si $x^k = 1$ dividimos $k = nq + r$ con $0 \leq r < n \Rightarrow$

$\Rightarrow x^r = x^k \cdot x^{-nq} = 1 \cdot 1 = 1 \underset{o(x)=n}{\Rightarrow} r = 0 \Rightarrow k = nq \Rightarrow n|k$.

iv) a) Si $o(x) = \infty \Rightarrow \nexists n \in \mathbb{N} \mid x^n = 1 \Rightarrow$ todas las potencias de x son distintas

Si $x^i = x^j \Rightarrow x^{i-j} = 1$ · Contradicción.

b) Si $o(x) = n \Rightarrow 1, x, \dots, x^{n-1}$ distintos y $x^n = 1$

$\langle x \rangle = \{1, x, \dots, x^{n-1}\}$ y

$x^i = x^j \Leftrightarrow n | i-j$ (por iii))

Proposición: Sea G un grupo y $a \in G$. Entonces existe un único homomorfismo de grupos $\varphi_a : \mathbb{Z} \to G \mid \varphi_a(1) = a$.

DEMOSTRACIÓN:

Supuesto que tal φ_a existe $\Rightarrow \begin{cases} \varphi_a(n) = \varphi_a(1 \overset{n)}{+ \dots +} 1) = \varphi_a(1)^n = a^n & n > 0 \\ \varphi_a(n) = \varphi_a(-(-n)) = \varphi_a(-n)^{-1} = (a^{-n})^{-1} = a^n & n < 0 \end{cases}$

Entonces $\varphi_a(n) = a^n \ \forall n \in \mathbb{Z}$.

Definamos $\varphi_a : \mathbb{Z} \to G \mid \varphi_a(n) = a^n$ y veamos que es un homomorfismo: $\varphi_a(n+m) = a^{n+m} = a^n \cdot a^m = \varphi_a(n) \cdot \varphi_a(m)$ y además, $\varphi_a(1) = a^1 = a$

En ese caso $Im(\varphi_a) = \{\varphi_a(n) \mid n \in \mathbb{Z}\} = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$

Teorema: Si G es cíclico, entonces $G \cong \mathbb{Z}$ o bien $G \cong \mathbb{Z}_n$ para algún n.

DEMOSTRACIÓN:

Supongamos $G = \langle a \rangle$ y consideremos el homomorfismo $\varphi_a : \mathbb{Z} \longrightarrow G$, $\varphi_a(n) = a^n$. Como $G = \langle a \rangle = Im(\varphi_a)$, entonces φ_a es sobreyectivo (epimorfismo).

Por otro lado, $ker(\varphi_a) = \{n \in \mathbb{Z} \mid \varphi_a(n) = a^n = 1\}$

- Si $\underset{o(a)=\infty}{\nexists n \neq 0 \mid a^n = 1} \Rightarrow ker(\varphi_a) = \{0\} \Rightarrow \varphi_a$ inyectivo $\Rightarrow$
  $\Rightarrow \varphi_a$ isomorfismo $\Rightarrow G \cong \mathbb{Z}$.
- Si $\exists n \neq 0 \mid a^n = 1$ tomamos $n > 0$ y consideramos el grupo $\mathbb{Z}_n$ y la aplicación $\bar{\varphi}_a : \mathbb{Z}_n \longrightarrow G$, $\bar{\varphi}_a(\bar{r}) = a^r$

$\bar{\varphi}_a$ está bien definida: $\bar{r} = \bar{s} \overset{?}{\Rightarrow} a^r = a^s$

$$\begin{array}{ccc} \bar{r} = \bar{s} & & a^r = a^s \\ \Downarrow & & \Uparrow \\ r - s \in n\mathbb{Z} & & \\ \Downarrow & & \\ n | r-s & \Rightarrow & a^{r-s} = 1 \end{array}$$

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Escaneado con CamScanner

WUOLAH

Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

$\bar{\varphi}_a$ es además un homomorfismo (comprobar)

Veamos que $\bar{\varphi}_a$ es inyectivo:

$$\bar{r}, \bar{s} \in \mathbb{Z}_n \mid \bar{\varphi}_a(\bar{r}) = \bar{\varphi}_a(\bar{s}) \overset{?}{\Longrightarrow} \bar{r} = \bar{s}$$

$$\Downarrow$$

$$a^r = a^s$$

$$\Downarrow$$

$$a^{r-s} = 1 \Rightarrow n \mid r-s$$

$\bar{\varphi}_a$ es también sobreyectivo por ser G cíclico generado por a

$\forall x \in G \quad x = a^r \ \exists r \ $ y $\ \bar{\varphi}_a(\bar{r}) = x = a^r$

Luego $\bar{\varphi}_a$ isomorfismo y $G \cong \mathbb{Z}_n$.

Si $H < \mathbb{Z} \Rightarrow H = n\mathbb{Z} \ \exists n \Rightarrow H$ es cíclico infinito

$$\left(H \cong \mathbb{Z} \quad \begin{array}{c} \mathbb{Z} \longrightarrow H \\ 1 \longmapsto n \end{array} \right)$$

Luego todo subgrupo de un grupo cíclico infinito vuelve a ser cíclico infinito.

15/10/19

Proposición: Sea $G = \langle a \rangle$ un grupo cíclico con $o(a) = n$. Entonces para cada divisor positivo m de n existe un único subgrupo de G de orden m que es cíclico generado por $a^{\frac{n}{m}}$ y estos son los únicos subgrupos de G (por tanto, todos cíclicos).

DEMOSTRACIÓN:

$$m \mid n \quad o(a^{n/m}) = m \begin{cases} (a^{n/m})^m = a^n = 1 \\ \text{si } (a^{n/m})^t = 1 \Rightarrow a^{\frac{nt}{m}} = 1 \Rightarrow n \mid \frac{nt}{m} \Rightarrow \end{cases}$$

$$\Rightarrow ns = \frac{nt}{m} \Rightarrow ms = t \Rightarrow m \mid t.$$

Consideramos ahora cualquier subgrupo H de G. Por el Teorema de Lagrange, $|H| \mid |G| = n$, así que si $|H| = m$, entonces $m \mid n$, y vamos a ver que $H = \langle a^{n/m} \rangle$.

Sea $k = \min\{t > 0 \mid a^t \in H\}$ (tal t existe porque a^t recorre todo G), y veamos que $H = \langle a^k \rangle$.

Como $a^k \in H \Rightarrow \langle a^k \rangle \subseteq H$

Además, $\forall b \in H < G = \langle a \rangle \Rightarrow b = a^s$ y dividiendo $s = kq + r$ con $0 \leq r < k$. Entonces $a^r = a^{s-kq} = \underset{H}{\overset{\cap}{a^s}} \cdot \underset{H}{\overset{\cap}{a^{-kq}}} \in H \underset{k\,min}{\Rightarrow} r = 0 \Rightarrow$

$\Rightarrow s = kq \Rightarrow b = a^s = (a^k)^q \in \langle a^k \rangle \Rightarrow H \subseteq \langle a^k \rangle$.

Escaneado con CamScanner

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

WUOLAH NEW Print

- Todos los apuntes que necesitas están aquí
- Al mejor precio del mercado, desde **2 cent.**
- Recoge los apuntes en tu copistería más cercana o recíbelos en tu casa
- ✓ Todas las anteriores son correctas

Imprimir

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Por tanto $H = \langle a^k \rangle$.

Ahora, puesto que $a^n = 1 \in H \Rightarrow k | n$ y veamos que $o(a^k) = \frac{n}{k}$

$(a^k)^{\frac{n}{k}} = a^n = 1$

Si $(a^k)^s = 1 \Rightarrow a^{ks} = 1 \Rightarrow n | ks \Rightarrow nt = ks \Rightarrow \frac{n}{k} t = s \Rightarrow \frac{n}{k} | s$

y por tanto, $|H| = m = |\langle a^k \rangle| = \frac{n}{k} \Rightarrow k = \frac{n}{m} \Rightarrow H = \langle a^k \rangle = \langle a^{\frac{n}{m}} \rangle$.

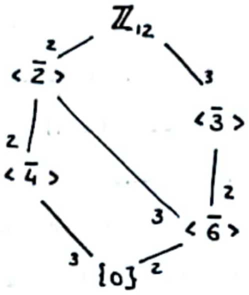
Ejemplo: $\mathbb{Z}_{12}$

$2 \rightsquigarrow \langle \overline{\tfrac{12}{2}} \rangle = \langle \bar{6} \rangle = \{\bar{0}, \bar{6}\} \cong \mathbb{Z}_2$

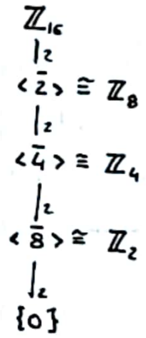
$3 \rightsquigarrow \langle \overline{\tfrac{12}{3}} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\} \cong \mathbb{Z}_3$

$4 \rightsquigarrow \langle \overline{\tfrac{12}{4}} \rangle = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \cong \mathbb{Z}_4$

$6 \rightsquigarrow \langle \overline{\tfrac{12}{6}} \rangle = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\} \cong \mathbb{Z}_6$



Ejemplo: Si G es cíclico de orden p^n con p primo, sus únicos subgrupos son cíclicos de órdenes p^r, $0 \le r \le n$



¿G cíclico o cualquiera?

↓

Proposición: Sea $x \in G$ con $o(x) = n$. Entonces $\forall k > 0$, $\langle x^k \rangle = \langle x^d \rangle$ con $d = m.c.d(n,k)$, y $o(x^k) = \frac{n}{d}$.

DEMOSTRACIÓN:

$d = m.c.d.(n,k) \Rightarrow d | k \Rightarrow \langle x^k \rangle \subseteq \langle x^d \rangle$.

Además, $\exists\, u, v \mid d = un + vk \Rightarrow x^d = \underbrace{x^{un}}_{=1} x^{vk} = (x^k)^v \Rightarrow \langle x^d \rangle \subseteq \langle x^k \rangle$ $\Bigg\} \Rightarrow$

$\Rightarrow \langle x^k \rangle = \langle x^d \rangle$

Para ver que $o(x^k) = \frac{n}{d}$, como $o(x^k) = (x^d)$, veamos que $o(x^d) = \frac{n}{d}$

$$\begin{cases} (x^d)^{n/d} = x^n = 1 \\ (x^d)^s = 1 \Rightarrow x^{ds} = 1 \Rightarrow n | ds \Rightarrow nt = ds \Rightarrow \frac{n}{d} t = s \Rightarrow \frac{n}{d} | s \end{cases}$$

Ejemplo: G, $o(x) = 15$

$\langle x^6 \rangle = \langle x^3 \rangle \qquad o(x^6) = \frac{15}{3} = 5.$

↑

$m.c.d.(15, 6) = 3$

WUOLAH

Escaneado con CamScanner

Ejemplo: $\mathbb{Z}_{12}$, $o(\bar{2}) = 6$

$\langle \bar{8} \rangle = \langle \bar{4} \rangle$ $\quad o(\bar{8}) = \frac{6}{2} = 3.$

$\bar{8} = 4 \cdot \bar{2}$

$m.c.d(6,4) = 2$

Corolario: Sea $x \in G$, $o(x) = n$. Entonces $\langle x^i \rangle = \langle x^j \rangle$ si, y solo si, $m.c.d(n,i) = m.c.d(n,j)$.

Corolario: Sea $G = \langle x \rangle$, con $o(x) = n$. Entonces $\langle x^k \rangle = \langle x \rangle$ si, y solo si, $m.c.d.(n,k) = 1$. (Por tanto, el número de generadores de G es $\varphi(n)$).

Ejemplo: $\mathbb{Z}_{12}$

$\mathbb{Z}_{12} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$

$\varphi(12) = \varphi(3)\varphi(4) = 2 \cdot 2 = 4.$

PRODUCTO DIRECTO DE GRUPOS CÍCLICOS.

Dados $G, H \rightsquigarrow G \times H = \{(x,y) \mid x \in G, y \in H\}$

- En general, el producto de grupos cíclicos no es cíclico.

Por ejemplo, $\mathbb{Z} \times \mathbb{Z}$ no es cíclico. Si lo fuera, $\mathbb{Z} \times \mathbb{Z} = \langle (r,s) \rangle$

$$\Rightarrow (1,0) = n(r,s) \Rightarrow \begin{cases} 1 = nr \Rightarrow n = \pm 1 = r \\ y \\ 0 = s \end{cases}$$

$(0,1) = n(1,0) \Rightarrow 1 = 0$ contradicción.

- Si $|G| = n$ y $|H| = m$, entonces $|G \times H| = nm$.
- Si $a \in G$, $b \in H$, entonces $o((a,b)) = m.c.m(o(a), o(b))$

Ejemplo: Veamos que $\mathbb{Z}_2 \times \mathbb{Z}_2$ no es cíclico.

Si lo fuera, salvo isomorfismos, sería $\mathbb{Z}_4$, puesto que tiene 4 elementos. Sin embargo

$$\left.\begin{aligned} o((0,0)) &= 1 \\ o((1,0)) &= 2 \\ o((0,1)) &= 2 \\ o((1,1)) &= 2 \end{aligned}\right\}$$

Como no hay elementos de orden 4, no puede ser $\mathbb{Z}_4$, luego $\mathbb{Z}_2 \times \mathbb{Z}_2$ no es cíclico.

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Escaneado con CamScanner

WUOLAH

Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa

Ejemplo: Veamos si $\mathbb{Z}_2 \times \mathbb{Z}_3$ es cíclico.

$\left.\begin{array}{l} \text{En tal caso, sería isomorfo a } \mathbb{Z}_6. \\ \text{Como } o((\bar{1},\bar{1})) = \text{m.c.m.}(2,3) = 6 \end{array}\right\} \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ cíclico

Proposición: Sean G, H grupos cíclicos finitos. Entonces $G \times H$ es cíclico si, y solo si, $\text{m.c.d.}(|G|, |H|) = 1$.

DEMOSTRACIÓN:

Supongamos que $G = \langle x \rangle$, $o(x) = n$ y $H = \langle y \rangle$, $o(y) = m$.

$\Leftarrow]$ Consideremos $\langle (x,y) \rangle < G \times H$

$o((x,y)) = \text{m.c.m.}(o(x), o(y)) = \text{m.c.m}(n,m) \underset{\text{m.c.d.}(n,m)=1}{=} nm \Rightarrow$

$\Rightarrow |\langle (x,y) \rangle| = nm = |G \times H| \Rightarrow G \times H = \langle (x,y) \rangle$ cíclico

$\Rightarrow]$ Si $G \times H$ es cíclico $\Rightarrow G \times H = \langle (a,b) \rangle \Rightarrow$

$\Rightarrow |G \times H| = nm = o((a,b)) = \text{m.c.m}(o(a), o(b))$ con $o(a) \mid n$ y $o(b) \mid m \Rightarrow$

$\Rightarrow o(a) = n$ y $o(b) = m \Rightarrow \text{m.c.m.}(n,m) = nm \Rightarrow \text{m.c.d.}(n,m) = 1$

Escaneado con CamScanner
WUOLAH
Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.
Tenemos lo que nos faltaba: Imprime tus apuntes al mejor precio y recíbelos en casa