

Algebra II (Doble grado Informática-Matemáticas)

Mayo- 2020

Tema 8: Grupos finitamente presentados. Clasificación de grupos de orden pequeño.

En las notas que vienen a continuación nos ocupamos de estudiar *Presentaciones de grupos* y daremos la clasificación de todos los grupos de orden ≤ 15 .

Antes de definir lo que es dar un grupo por generadores y relaciones y entonces dar una presentación de un grupo, veamos algunos ejemplos ya estudiados.

Hemos estado utilizando que el grupo cíclico de orden n se puede declarar de la forma:

$$C_n = \langle a | a^n = 1 \rangle.$$

Es decir C_n está generado por el elemento a con relación fundamental $a^n = 1$. Con estos datos podemos determinar cuáles son exactamente los elementos del grupo y la tabla de grupo. Recordemos que

$$C_n = \{1, a, a^2, \dots, a^{n-1}\}$$

y

$$a^r a^s = a^{res(rs;n)}$$

Otro ejemplo que hemos trabajado es el del grupo diédrico

$$D_n = \langle r, s | r^n = 1 = s^2, sr = r^{-1}s \rangle.$$

Decimos que D_n está generado por r y s con relaciones

$$r^n = 1 = s^2; sr = r^{-1}s$$

que nos permite concluir que

$$D_n = \{1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$$

y además conocer completamente la tabla del grupo sin necesidad de recurrir a su descripción original.

Ejemplos análogos a los anteriores son el grupo de Klein o el grupo de los cuaternios. Todos ellos son casos de grupos dados por generadores y relaciones

Definición 0.1. Sea G un grupo generado por s_1, s_2, \dots, s_n . Cualquier ecuación que satisfagan los generadores la llamaremos una relación del grupo G .

Por ejemplo $r^n = 1$, $s^2 = 1$ y $sr = r^{n-1}s$ son relaciones de D_n . Además estas tres relaciones, que hemos llamado hasta ahora fundamentales, tiene la propiedad de que cualquier otra relación entre los elementos del grupo puede deducirse a partir de ellas (Esto no es trivial, se sigue del hecho de que podemos decidir exactamente cuando dos elementos del grupo son iguales utilizando sólo estas tres relaciones).

Definición 0.2. Dar un grupo G por generadores y relaciones es dar un conjunto de generadores $S = \{x_1, \dots, x_n\}$ de G y un conjunto de relaciones R_1, \dots, R_m (aquí cada R_i es una ecuación en los generadores x_1, \dots, x_n y el 1) tales que cualquier otra relación entre los elementos de S puede deducirse a partir de ellas. Llamaremos a estos generadores y relaciones una presentación de G y escribiremos:

$$G = \langle x_1, \dots, x_n | R_1, \dots, R_m \rangle.$$

Ejemplo 0.3. Los grupos cíclicos

$$C_n = \langle a | a^n = 1 \rangle,$$

los grupos diédricos

$$D_n = \langle r, s | r^n = 1 = s^2, sr = r^{-1}s \rangle,$$

o el grupo de Klein que puede presentarse por

$$K = \langle a, b | a^2 = 1 = b^2, ab = ba \rangle.$$

Enunciamos a continuación un teorema muy útil, cuya demostración omitimos pues requiere el estudio de grupos libres que está fuera de los objetivos de este curso.

Teorema 0.4. Sea $\{x_1, \dots, x_n\}$ un conjunto de generadores de un grupo G . Sea H un grupo y a_1, a_2, \dots, a_n elementos de H tales que cualquier relación en G que verifiquen los generadores x_i , también se satisface en H cuando sustituimos cada x_i por a_i . Entonces existe un único homomorfismo

$$f : G \rightarrow H$$

tal que $f(x_i) = a_i$, $i = 1, \dots, n$.

Corolario 0.5. Teorema de Dyck Sea G un grupo y

$$G = \langle x_1, \dots, x_n | R_1, \dots, R_m \rangle$$

una presentación de G . Sea H un grupo y a_1, a_2, \dots, a_n elementos de H tales que las ecuaciones R_1, \dots, R_m son validas en H al sustituir x_i por a_i . Entonces existe un único homomorfismo

$$f : G \rightarrow H$$

tal que $f(x_i) = a_i$, $i = 1, \dots, n$.

En las hipótesis del corolario si

- (1) $H = \langle a_1, \dots, a_n \rangle$ entonces f es un epimorfismo,
- (2) si además de (1) se tiene que $|G| = |H|$ entonces f es un isomorfismo.

Ejemplo 0.6. Haciendo uso del Teorema de Dyck veamos que el grupo de los cuaternios $Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$ puede presentarse de la forma

$$Q_2 = \langle a, b | a^4 = 1, b^2 = a^2, ba = a^3b \rangle.$$

En efecto, llamemos $G = \langle a, b | a^4 = 1, b^2 = a^2, ba = a^3b \rangle$. Sabemos que $i^4 = 1$, $i^2 = j^2$ y $ji = -k = (-i)j = i^3j$. Entonces por el teorema de Dyck, existe un único

$$f : G \rightarrow Q_2, \text{ tal que } f(a) = i, f(b) = j.$$

Además puesto que $Q_2 = \langle i, j \rangle$, entonces f es un epimorfismo. Para ver que es un isomorfismo veamos que $|G| = 8$. En primer lugar, por el primer teorema de isomorfismo, $G/Ker(f) \cong Q_2$, en particular $|G| = |Q_2| \cdot |Ker(f)| \geq 8$.

Por otro lado, puesto que $a^4 = 1$ entonces $H = \langle a \rangle$ tiene orden ≤ 4 . Como $bab^{-1} = a^3bb^{-1} = a^3 \in H$ entonces $H \trianglelefteq G$ y $G/H = \langle bH \rangle$. Ahora como $(bH)^2 = b^2H = a^2H = H$, entonces $|G/H| \leq 2$. Consecuentemente $|G| = |G/H| \cdot |H| \leq 8$, y $G \cong Q_2$.

Definición 0.7. Para cada $k \geq 1$ se define el k -ésimo grupo díclico, como el grupo presentado por

$$Q_k = \langle a, b | a^{2k} = 1, b^2 = a^k, ba = a^{-1}b \rangle.$$

Como hemos visto, para el caso $k = 2$ tenemos el grupo de los cuaternios. El caso $k = 1$ es fácil ver que se trata del grupo cíclico de orden 4, esto es

$$C_4 \cong \langle a, b | a^2 = 1, b^2 = a, ba = a^{-1}b \rangle.$$

Observación 0.8. En general, para $k \geq 3$, Q_k tiene un cociente isomorfo a D_k y entonces no es abeliano y $2k \leq |Q_k| \leq 4k$. Además si $k = 2r + 1$ entonces $|Q_k| = 4k$.

En efecto, sabemos que $D_k = \langle r, s | r^k = 1 = s^2, sr = r^{-1}s \rangle$ y entonces $r^{2k} = (r^k)^2 = 1$, $s^2 = 1 = r^k$ y $sr = r^{-1}s$. El teorema de Dyck nos asegura

la existencia de un homomorfismo $f : Q_k \rightarrow D_k$ tal que $f(a) = r$ y $f(b) = s$. Como r y s generan D_k , entonces f es un epimorfismo con lo que

$$Q_k / \text{Ker}(f) \cong D_k.$$

Además $|D_k| = 2k$ es un divisor de $|Q_k|$ y en particular

$$2k \leq |Q_k|.$$

Para la otra desigualdad, puesto que $a^{2k} = 1$ entonces $H = \langle a \rangle$ tiene orden $\leq 2k$. Como $bab^{-1} = a^{-1}bb^{-1} = a^{-1} \in H$ entonces $H \trianglelefteq Q_k$ y $Q_k/H = \langle bH \rangle$. Ahora como $(bH)^2 = b^2H = a^kH = H$, entonces $|Q_k/H| \leq 2$. Consecuentemente $|Q_k| = |Q_k/H| \cdot |H| \leq 4k$.

Supongamos ahora que $k = 2r + 1$. Consideramos el grupo cíclico $C_4 = \langle x | x^4 = 1 \rangle$, puesto que $(x^2)^{2k} = (x^4)^k = 1$, $(x^2)^k = x^{2k} = x^{4r+2} = x^2$ y $x \cdot x^2 = x^3 = x^2 \cdot x = (x^2)^{-1}x$, de nuevo por el teorema de Dyck, existe un epimorfismo $g : Q_k \rightarrow C_4$ tal que $g(a) = x^2$ y $g(b) = x$. En particular $Q_k / \text{Ker}(g) \cong C_4$, con lo que $4 \mid |Q_k|$. Como $2k$ también divide a $|Q_k|$ entonces $\text{mcm}(4, 2k)$ es un divisor de $|Q_k|$.

Como k es impar entonces $\text{mcm}(4, 2k) = 4k$ con lo que $4k \leq |Q_k|$; como la otra desigualdad se tiene para todo k , concluimos que $|Q_k| = 4k$, como queríamos demostrar.

0.1. Clasificación de los grupos abelianos de orden ≤ 15 .

- (1) Sabemos que todo grupo de orden un número primo es isomorfo al cíclico y entonces los grupos

de orden 2	son isomorfos a	C_2
de orden 3	son isomorfos a	C_3
de orden 5	son isomorfos a	C_5
de orden 7	son isomorfos a	C_7
de orden 11	son isomorfos a	C_{11}
de orden 13	son isomorfos a	C_{13}

- (2) Sabemos que todo grupo de orden p^2 , p un número primo, es abeliano. Por otro lado, si $|A| = p^2$, sus divisores elementales son $\{p^2\}$ o $\{p, p\}$, es decir

$$A \cong C_{p^2} \text{ ó } A \cong C_p \times C_p.$$

Entonces los grupos

de orden 4	son isomorfos a	C_4 ó $C_2 \times C_2$
de orden 9	son isomorfos a	C_9 ó $C_3 \times C_3$

- (3) Nos ocupamos ahora de los grupos de orden 6, 10 y 14. Para ello veamos primero el siguiente resultado

Proposición 0.9. Si p es un primo impar, todo grupo de orden $2p$ es isomorfo a C_{2p} o a D_p .

Demostración. Sea G con $|G| = 2p$. Sabemos que el número de p -subgrupos de Sylow, n_p verifica

$$n_p | 2 \text{ y } n_p \equiv 1 \pmod{p} \Rightarrow n_p = 1.$$

Sea \mathcal{P} el único p -subgrupo de Sylow. Sabemos que $\mathcal{P} \triangleleft G$ y $|\mathcal{P}| = p$ y entonces $\mathcal{P} = \langle a | a^p = 1 \rangle \cong C_p$.

Respecto a los 2-subgrupos de Sylow, como anteriormente sabemos que

$$n_2 | p \text{ y } n_2 \equiv 1 \pmod{2} \Rightarrow \begin{cases} n_2 = 1 \\ \text{ó} \\ n_2 = p \end{cases}$$

Caso $n_2 = 1$: Sea \mathcal{Q} el único 2-subgrupo de Sylow, entonces $\mathcal{Q} \cong C_2$, y como $n_p = 1$ entonces

$$G \cong \mathcal{P} \times \mathcal{Q} \cong C_p \times C_2 \cong C_{2p}.$$

Caso $n_2 = p$: Notemos que en este caso el grupo G no es abeliano. Puesto que $[G : \mathcal{P}] = \frac{|G|}{|\mathcal{P}|} = 2$, sólo hay dos clases laterales a derecha y G es la unión de ellas. Esto es

$$G = \mathcal{P} \cup \mathcal{P}b = \{1, a, \dots, a^{p-1}, b, ab, \dots, a^{p-1}b\},$$

siendo $b \notin \mathcal{P}$.

Como $\text{ord}(b) | 2p = |G|$ entonces $\text{ord}(b) = 2, p$, ó $2p$, notemos que no puede ser 1 pues $b \neq 1$. Si $\text{ord}(b) = p$ entonces $\langle p \rangle$ es un p -subgrupo de Sylow de G con lo que $\langle p \rangle = \mathcal{P}$ y en particular $b \in \mathcal{P}$ y llegamos a una contradicción. Si $\text{ord}(b) = 2p$ entonces $\langle b \rangle = G$ con lo que el grupo G sería abeliano, de nuevo llegamos a una contradicción. Consecuentemente $\text{ord}(b) = 2$.

Si consideramos ahora el elemento $ba \in G$ tendremos que $\text{ord}(ba) = 1, 2, p$, ó $2p$. Si $\text{ord}(ba) = 1$ entonces $ba = 1 \Rightarrow b = a^{-1} \in \mathcal{P}$, contradicción. Si $\text{ord}(ba) = p \Rightarrow \langle ba \rangle = \mathcal{P} \Rightarrow ba \in \mathcal{P} \Rightarrow b \in \mathcal{P}$, también contradicción. Finalmente si $\text{ord}(ba) = 2p$ entonces G sería abeliano y descartamos por tanto esta posibilidad. Consecuentemente $\text{ord}(ba) = 2$ y tendremos: $(ba)^2 = baba = 1 \Rightarrow bab = a^{-1} \Rightarrow ba = a^{-1}b$ y nuestro grupo tiene la siguiente presentación:

$$G = \langle a, b | a^p = 1 = b^2, ba = a^{-1}b \rangle \cong D_p.$$

□

Entonces como consecuencia de la proposición anterior los grupos

de orden 6	son isomorfos a	C_6 ó D_3
de orden 10	son isomorfos a	C_{10} ó D_5
de orden 14	son isomorfos a	C_{14} ó D_7

(4) Veamos que **sólo hay un grupo de orden 15 que es C_{15}** :

En efecto si $|G| = 15 = 3 \cdot 5$, entonces si n_3, n_5 denotan el número de 3-subgrupos de Sylow y de 5-subgrupos de Sylow, respectivamente, tenemos

$$n_3 | 5 \text{ y } n_3 \equiv 1 \pmod{3} \Rightarrow n_3 = 1,$$

sea \mathcal{P} el único 3-subgrupo de Sylow que puesto que $|\mathcal{P}| = 3$, entonces $\mathcal{P} \cong C_3$

$$n_5 | 3 \text{ y } n_5 \equiv 1 \pmod{5} \Rightarrow n_5 = 1,$$

sea \mathcal{Q} el único 5-subgrupo de Sylow que puesto que $|\mathcal{Q}| = 5$, entonces $\mathcal{Q} \cong C_5$

Consecuentemente G es producto directo interno de \mathcal{P} y \mathcal{Q} y tenemos

$$G \cong \mathcal{P} \times \mathcal{Q} \cong C_3 \times C_5 \cong C_{15}.$$

(5) Grupos de orden 8:

Caso abeliano: Si G es un grupo de orden 8 y abeliano entonces las posibles listas de divisores elementales son

1. $\{2^3\}$ y entonces $G \cong C_8$,
2. $\{2^4, 2\}$ y entonces $G \cong C_4 \times C_2$ y
3. $\{2, 2, 2\}$ y entonces $G \cong C_2 \times C_2 \times C_2$.

Caso no abeliano: Sea G un grupo de orden 8 y no abeliano (notemos que aquí no a lugar a la discusión sobre subgrupos de Sylow pues solo hay uno que es el propio G). En primer lugar, puesto que G no es abeliano entonces no tiene elementos de orden 8 pues sino sería cíclico. Por tanto sus elementos son de orden 4 o 2. Pero no todos los elementos son de orden 2 pues en ese caso sabemos que también sería abeliano, consecuentemente $\exists a \in G$ tal que $\text{ord}(a) = 4$.

Sea $H = \langle a \rangle = \{1, a, a^2, a^3\}$. Como $[G : H] = 2$ entonces $H \trianglelefteq G$ y si $b \in G$ es un elemento tal que $b \notin H$ entonces H, Hb son las dos únicas clases laterales a derecha, consecuentemente

$$G = H \cup Hb = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Consideremos el elemento b^2 entonces $b^2 \in H$ ó $b^2 \in Hb$. Si

$$b^2 \in Hb \Rightarrow \begin{cases} b^2 = b & \Rightarrow b = 1 & \text{contradicción} \\ b^2 = ab & \Rightarrow b = a & \text{contradicción} \\ b^2 = a^2b & \Rightarrow b = a^2 & \text{contradicción} \\ b^2 = a^3b & \Rightarrow b = a^3 & \text{contradicción} \end{cases}$$

Así pues $b^2 \in H$. Ahora si $b^2 = a \Rightarrow \text{ord}(b^2) = \text{ord}(a) = 4 \Rightarrow \text{ord}(b) = 8$ en contradicción con que G no es abeliano. Análogamente si $b^2 = a^3$ implicaría que $\text{ord}(b) = 8$ y tendríamos una contradicción. Consecuentemente $b^2 = 1$ ó $b^2 = a^2$.

Caso $b^2 = 1$. Veamos que $ba = a^3b$.

En efecto, como $H \trianglelefteq G$, entonces $bab^{-1} \in H$ y como $b^2 = 1 \Rightarrow b = b^{-1}$, así $bab \in H$. Ahora

$bab \neq 1$ pues si $bab = 1 \Rightarrow ba = b \Rightarrow a = 1$ que es una contradicción,

$bab \neq a$ pues si $bab = a \Rightarrow ba = ab \Rightarrow G$ sería abeliano, que es una contradicción,

$bab \neq a^2$ pues si $bab = a^2 \Rightarrow baba = a^3 \Rightarrow \text{ord}(ba) = 8 \Rightarrow$ que G es abeliano, que es una contradicción.

Consecuentemente $bab = a^3 \Rightarrow ba = a^3b$ y nuestro grupo es

$$G\langle a, b | a^4 = 1 = b^2, ba = a^3b \rangle \cong D_4.$$

Caso $b^2 = a^2$. Veamos que también en este caso $ba = a^3b$.

En efecto, como $H \trianglelefteq G$, entonces $bab^{-1} \in H$. Ahora

$bab^{-1} \neq 1$ pues si $bab^{-1} = 1 \Rightarrow ba = b \Rightarrow a = 1$ que es una contradicción,

$bab^{-1} \neq a$ pues si $bab^{-1} = a \Rightarrow ba = ab \Rightarrow G$ sería abeliano, que es una contradicción,

$bab^{-1} \neq a^2$ pues si $bab^{-1} = a^2 \Rightarrow bab^{-1} = b^2 \Rightarrow ab^{-1} = b \Rightarrow a = b^2 \Rightarrow a = a^2 \Rightarrow a = 1$, que es una contradicción.

Consecuentemente $bab^{-1} = a^3 \Rightarrow ba = a^3b$ y nuestro grupo es

$$G\langle a, b | a^4 = 1, a^2 = b^2, ba = a^3b \rangle \cong Q_2.$$

(6) Grupos de orden 12:

Caso abeliano: Si G es un grupo de orden 12 y abeliano entonces las posibles listas de divisores elementales son

1. $\{2^2, 3\}$ y entonces $G \cong C_4 \times C_2 \cong C_{12}$ y
2. $\{2, 2, 3\}$ y entonces $G \cong C_2 \times C_2 \times C_3 \cong C_6 \times C_2$.

Caso no abeliano: Sea G un grupo de orden 12 y no abeliano. Si n_3 denota el número de 3-subgrupos de Sylow, sabemos que $n_3 \mid 4$ y $n_3 \equiv 1 \pmod{3}$ con lo que $n_3 = 1$ ó $n_3 = 4$.

Si $n_3 = 4$ entonces como ya hemos visto en los ejercicios,

$$G \cong A_4$$

.

Supongamos $n_3 = 1$ y sea \mathcal{P} el único 3-subgrupo de Sylow de G . Sabemos que $\mathcal{P} \trianglelefteq G$ y como $|\mathcal{P}| = 3$ entonces $\mathcal{P} = \langle x \mid x^3 = 1 \rangle = \{1, x, x^2\}$. Veamos que en este caso existe en G un elemento de orden 6.

Para ello consideramos la clase de conjugación de x , $cl(x) = \{gxg^{-1} \mid g \in G\}$. Como $\mathcal{P} \trianglelefteq G$ entonces $cl(x) \subseteq \mathcal{P}$ y así $cl(x) = \{x\}$ ó $cl(x) = \{x, x^2\}$ (notemos que $cl(x)$ no puede contener al 1 pues $gxg^{-1} = 1 \Rightarrow x = 1$, que es una contradicción). Como $[G : c_G(x)] = |cl(x)|$, siendo $c_G(x) = \{g \in G \mid gx = xg\}$ el centralizador de x en G , entonces $|c_G(x)| = 6$ ó $|c_G(x)| = 12$. En ambos casos, por el Teorema de Cauchy, existe $z \in c_G(x)$ con $ord(z) = 2$.

Sea $a = xz$. Como $xz = zx$ y $mcd(ord(x), ord(z)) = 1$, entonces $ord(a) = ord(x) \cdot ord(z) = 6$, consideremos $K = \langle a \rangle = \{1, a, a^2, a^3, a^4, a^5\}$. Como $[G : K] = 2$ entonces $K \trianglelefteq G$ y si $b \in G$ es un elemento tal que $b \notin K$ entonces K, Kb son las dos únicas clases laterales a derecha, consecuentemente

$$G = K \cup Kb = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}.$$

Puesto que $bab^{-1} \in K$ y $ord(bab^{-1}) = ord(a) = 6 \Rightarrow bab^{-1} = a$ ó a^5 . Pero $bab^{-1} = a \Rightarrow ba = ab$ y G sería abeliano, consecuentemente

$$bab^{-1} = a^5 \Rightarrow ba = a^5b.$$

Consideremos el elemento b^2 entonces $b^2 \in K$ ó $b^2 \in Kb$. Si $b^2 \in Kb \Rightarrow b^2 = a^i b \Rightarrow b = a^i \in K$, lo cual es una contradicción. Así pues, necesariamente $b^2 \in K$. Ahora Si $b^2 = a \Rightarrow ord(b^2) = ord(a) = 5 \Rightarrow ord(b) = 12$ en contradicción con que G no es abeliano. Análogamente si $b^2 = a^5$ implicaría que $ord(b) = 12$ y tendríamos una contradicción.

Si $b^2 = a^2$ entonces

$$(a^{-1})^2 = (bab^{-1})^2 = ba^2b^{-1} = bb^2b^{-1} = b^2 \Rightarrow (a^{-1})^2 = a^2 \Rightarrow a^4 = 1$$

con lo que el orden de a sería 4, en contradicción con que tiene orden 6.

Si $b^2 = a^4$ entonces

$$(a^{-1})^4 = (bab^{-1})^4 = ba^4b^{-1} = b^2 = a^4 \Rightarrow a^8 = a^2 = 1,$$

con lo que el orden de a sería 2, de nuevo una contradicción.

Consecuentemente $b^2 = 1$ ó $b^2 = a^3$.

Caso $b^2 = 1$. , puesto que $ba = a^5b$, nuestro grupo es

$$G = \langle a, b | a^6 = 1 = b^2, ba = a^5b \rangle \cong D_6.$$

Caso $b^2 = a^3$. puesto que $ba = a^5b$, nuestro grupo es

$$G = \langle a, b | a^6 = 1, a^3 = b^2, ba = a^5b \rangle \cong Q_3.$$

Resumimos todo el estudio anterior en la siguiente tabla

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