Algebra II (Doble grado Informática-Matemáticas)

16 de marzo de 2020

Comenzaremos demostrando la última proposición que dejamos enunciada el último día.

Proposición 0.1. *(1) Sean $\alpha, \beta \in S_n$ dos permutaciones disjuntas. Entonces*

$$ord(\alpha\beta) = \text{m. c. m.}(ord(\alpha), ord(\beta)).$$

(2) Sea $\alpha \in S_n$, $\alpha \neq id$, entonces $ord(\alpha) =$ al mínimo común múltiplo de las longitudes de los ciclos dijuntos en que descompone.

Demostración. Veamos (1): En primer lugar observemos que si α, β son disjuntas entonces, $\forall k \geq 1$, α^k, β^k son también disjuntas. En efecto, si $x \in \{1, \ldots, n\}$ es tal que $\alpha^k(x) \neq x$, entonces habrá de ser $\alpha(x) \neq x$, con lo que al ser α y β disjuntas, $\beta(x) = x$ y por tanto $\beta^k(x) = x$.

Sea $r = ord(\alpha), s = ord(\beta)$ y $m = \text{m. c. m.}(r, s)$. Como $\alpha\beta = \beta\alpha$ (por ser disjuntas), $(\alpha\beta)^m = \alpha^m\beta^m = id$ al ser m un múltiplo común de r y s.

Sea $k \geq 1$ tal que $(\alpha\beta)^k = \alpha^k\beta^k = id$. Como α^k, β^k son disjuntas, entonces $\alpha^k = \beta^k = id$, pues si $\alpha^k \neq id$ y $x \in \{1, \ldots, n\}$ es tal que $\alpha^k(x) \neq x$, entonces $\beta^k(x) = x$ con lo que $(\alpha^k\beta^k)(x) = \alpha^k(x) \neq x$ en contradicción con que $\alpha^k\beta^k = id$. Entonces

- $\alpha^k = id \ \wedge \ ord(\alpha) = r \ \Rightarrow r|k$
- $\beta^k = id \ \wedge \ ord(\beta) = s \ \Rightarrow s|k$,

entonces $m = \text{m. c. m.}(r, s)|k$ y se tiene el resultado.

(2) es consecuencia directa de (1) y del hecho de que el orden de un ciclo coincide con su longitud.

□

Ejercicio. (Ejercicio 18 (Relación 2)) Calcular el orden de la permutación

$$\sigma = (1\ 8\ 10\ 4)(2\ 8)(5\ 1\ 4\ 8) \in S_{15}.$$

Resolución. En primer lugar expresamos σ en ciclos disjuntos teniéndose que

$$\sigma = (2\ 10\ 4)(5\ 8),$$

y entonces

$$ord(\sigma) = \text{m. c. m.}(3, 2) = 6.$$

Estamos ya en condiciones de clasificar los grupos de orden 4 y de orden 6. Comenzamos haciendo primero el

Ejercicio. (Ejercicio 20. Relación 2) Demostrar que un grupo generado por dos elementos distintos, de orden 2, que conmutan entre sí, consiste del 1, de esos dos elementos y de su producto. Además es isomorfo al grupo de Klein.

Resolución. Sabemos que si $G = \langle a, b\rangle$ sus elementos son productos de potencias enteras de a, b. Como $ab = ba$ entonces

$$G = \{a^n b^m / n, m \in \mathbb{Z}\}.$$

Por otro lado, como $ord(a) = 2$ entonces $a^n = a^{Res(n;2)}$, análogamente como $ord(b) = 2$ entonces $b^m = a^{Res(m;2)}$. Así

$$G = \{a^r b^s / 0 \leq r \leq 1, 0 \leq s \leq 1\} = \{1, a, b, ab\}$$

y la tabla de G es

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

Finalmente, es fácil ver que la biyección

$1 \mapsto (1, 1)$
$a \mapsto (-1, 1)$
$b \mapsto (1, -11)$
$ab \mapsto (-1, -1)$

establece un isomorfismo entre G y el grupo de Klein $K = \mu_2 \times \mu_2$.

Este ejercicio nos permite dar otra forma de introducir el grupo de Klein. Esto es:

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

Veamos ahora la anunciada clasificación:

Ejercicio. (Ejercicio 23. Relación 2).

1. Demostrar que si G es un grupo de orden 4 entonces es isomorfo al grupo cíclico o es isomorfo al grupo de Klein.

2. Demostrar que si G es un grupo de orden 6 entonces es isomorfo al grupo cíclico o es isomorfo al grupo diédrico D_3.

Resolución. 1.- Sea G con $|G| = 4$. Por el teorema de Lagrange, sabemos que el orden de cualquier elemento es un divisor del orden del grupo. Así si $a \in G$, $a \neq 1$ entonces $1 \neq ord(a)|4$, y entonces $ord(a) = 2$ ó $ord(a) = 4$. Distinguimos entonces los dos siguientes casos:

Caso 1 $\exists a \in G$ tal que $ord(a) = 4$. Entonces $G = \langle a\rangle$ y $G \cong C_4$.

Caso 2 $\forall a \in G$, $a \neq 1$, es $ord(a) = 2$. Entonces $G = \{1, a, b, c\}$ con $ord(a) = ord(b) = ord(c) = 2$. Haciendo uso del Ejercicio 6 de la Relación 1, G es abeliano.

Por otro lado $ab = c$ (pues si $ab = 1 \Rightarrow a = b^{-1} = b$, si $ab = a \Rightarrow b = 1$ y si $ab = b \Rightarrow a = 1$), con lo que

$$G = \langle a, b / a^2 = 1 = b^2, ab = ba\rangle$$

y por el ejercicio anterior G es isomorfo al grupo de Klein.

2.- Sea G con $|G| = 6$. Como anteriormente si $a \in G$, $a \neq 1$ entonces $1 \neq ord(a)|6$, y entonces $ord(a) = 2$, $ord(a) = 3$ ó $ord(a) = 6$. Distinguimos entonces los dos siguientes casos:

Caso 1: El grupo G es abeliano.

Observamos primero que no puede ocurrir que todos los elementos de G tengan orden 2. Pues, si así fuera, considerando $a, b \in G$ con $a \neq b$, tendríamos $a^2 = 1 = b^2$ y $ab = ba$ (pues G es abeliano), con lo que $\langle a, b\rangle = \{1, a, b, ab\} \leq G$ y, por el teorema de Lagrange, $|\langle a, b\rangle| = 4$ tendría que ser un divisor de $|G| = 6$ lo cual es una contradicción.

Consecuentemente $\exists a \in G$ tal que $ord(a) = 6$ ó $ord(a) = 3$.

Si $ord(a) = 6$. Entonces $G = \langle a\rangle$ y $G \cong C_6$.

Si $ord(a) = 3$, sea $H = \langle a\rangle = \{1, a, a^2\} \leq G$. Entonces $[G : H] = \frac{|G|}{|H|} = \frac{6}{3} = 2$ y hay únicamente dos clases laterales a derecha módulo H. Esto es $H/G = \{H, Hb\}$ con $b \in G$ y $b \notin H$. Veamos que $ord(b) = 2$:

Consideramos el elemento $b^2 \in G = H \cup Hb$ entonces $b^2 \in H$ ó $b^2 \in Hb$. Como $Hb = \{b, ab, a^2b\}$ entonces $b^2 \notin Hb$ (pues si $b^2 = a^jb$, $0 \leq j \leq 2$, entonces $b = a^j \in H$ en contradicción con que b no es un elemento de H) y así $b^2 \in H$. Ahora $b^2 \neq a$ y $b^2 \neq a^2$, pues si, por ejemplo, $b^2 = a$ entonces $ord(b^2) = 3$ y tendríamos que $ord(b) = 3$, pero entonces $b = (b^2)^2 = a^2$ y llegaríamos a que $b \in H$ (de igual forma razonaríamos si $b^2 = a^2$). Concluimos pues que $b^2 = 1$ y b tiene orden 2.

Hacemos ahora uso del Ejercicio 17 de la Relación 2 y como $ab = ba$ (G es abeliano) y $\mathrm{m.c.d.}(ord(a), ord(b)) = \mathrm{m.c.d.}(3, 2) = 1$, entonces $ord(ab) = ord(a)ord(b) = 6$, y entonces $G \cong C_6$.

Caso 2: El grupo G no es abeliano.

En este caso no existen elementos de orden 6 (pues si así fuera G sería isomorfo a C_6 y entonces abeliano) y, de nuevo por el Ejercicio 6 de la Relación 2, no todos los elementos tienen orden 2. Consecuentemente $\exists a \in G$ con $ord(a) = 3$.

Sea $H = \langle a\rangle = \{1, a, a^2\}$. Como en el caso anterior, $[G : H] = 2$, $H/G = \{H, Hb\}$ con $b \in G$ y $b \notin H$. Entonces

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

Razonando igual que en el caso anterior, $ord(b) = 2$.

Consideremos ahora el elemento $ba \in G$. Tenemos $ba \in H \cup Hb \Rightarrow ba \in H \vee ba \in Hb$. Ahora, $ba \notin h$ (pues is $ba = a^j$, $0 \leq j \leq 2$ entonces $b = a^{j-1} \in H$), así $ba \in Hb = \{b, ab, a^2b\}$.

Como $ba \neq ab$ (pues a, b son generadores de G y este no es abelianos) y $ba \neq b$(pues $a \neq 1$) entonces $ba = a^2b$. Concluímos pues que

$$G = \langle a, b/a^3 = 1, b^2 = 1, ba = a^2b\rangle$$

y entonces $G \cong D_3$. Lo que concluye el ejercicio.

Nos ocupamos a continuación de la descripción del retículo de subgrupos de algunos grupos finitos.

Empezaremos por los grupos cíclicos finitos. Para estos tenemos el siguiente resultado que describe completamente quién es el retículo de subgrupos del grupo cíclico de orden n.

Teorema 0.2. *Sea $C_n = \langle a/a^n = 1\rangle$ el grupo cíclico de orden n ($n \geq 2$). Se verifica:*

(1) Para cada divisor positivo d de n el subgrupo cíclico $\langle a^{\frac{n}{d}}\rangle \leq C_n$ tiene orden d y así $\langle a^{\frac{n}{d}}\rangle = C_d$.

(2) Si $H \leq C_n$, $H \neq \{1\}$, y $s = min\{r \geq 1/a^r \in H\}$, entonces s es un divisor de n, $H = \langle a^s\rangle$. De manera que $H = C_k$ siendo $k = \frac{n}{s}$.

(3) Sea $Div(n) := \{d \geq 1/d|n\}$. La aplicación

$$Div(n) \longrightarrow Sub(C_n), \;\; d \mapsto \langle a^{\frac{n}{d}}\rangle$$

es biyectiva

(4) Dados $d_1, d_2 \in Div(n)$, se verifica:

$$d_1|d_2 \;\Leftrightarrow\; \langle a^{\frac{n}{d_1}}\rangle \leq \langle a^{\frac{n}{d_2}}\rangle.$$

Demostración. (1) Supongamos que $n = dn'$. Sabemos que $ord(a^{n'}) = \frac{n}{\text{m.c.d.}(n',n)} = \frac{n}{n'} = d$, de manera que $\langle a^{\frac{n}{d}}\rangle$ es efectivamente el subgrupo cíclico de orden d.
(2) Notemos, en primer lugar que puesto que H no es el grupo trivial entonces el conjunto $\{r \geq 1/a^r \in H\}$ es no vacío y entonces tiene mínimo. Sea pues $s = min\{r \geq 1/a^r \in H\}$. Puesto que $a^s \in H$, entonces $\langle a^s\rangle \leq H$.

Veamos la otra inclusión: Sea m, con $1 \leq m \leq n$ tal que $a^m \in H$. Dividiendo m entre s, será $m = qs + r$ con $0 \leq r < s$. Pero entonces $a^r = a^m(a^s)^{-q} \in H$ se reconoce como un elemento de H, y por la minimalidad de s ha de ser $r = 0$, esto es $s|m$ y $a^m = (a^s)^q \in \langle a^s\rangle$. Deducimos entonces que $H \leq \langle a^s\rangle$ y de la doble inclusión tenemos la igualdad, es decir $H = \langle a^s\rangle$. Además, puesto que $a^n = 1 \in H$ entonces $s|n$.

Finalmente, puesto que $ord(a^s) = \frac{n}{\text{m.c.d.}(s,n)} = \frac{n}{s}$, entonces $H = C_{\frac{n}{s}}$.
(3) Es consecuencia directa de (1) y (2)
(4) $\Rightarrow$) Si $d_1|d_2$ entonces $\frac{n}{d_2}|\frac{n}{d_1}$ y entonces $a^{\frac{n}{d_1}} \in \langle a^{\frac{n}{d_2}}\rangle$, por tanto $\langle a^{\frac{n}{d_1}}\rangle \leq \langle a^{\frac{n}{d_2}}\rangle$.

$\Leftarrow$) Recíprocamente, si $\langle a^{\frac{n}{d_1}}\rangle \leq \langle a^{\frac{n}{d_2}}\rangle$, por (1) y el teorema de Lagrange, será $d_1|d_2$.

□

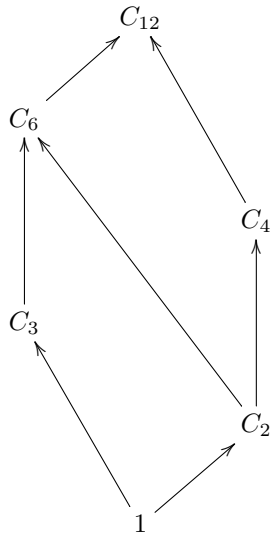
Ejercicio. Ejercicio 28. Relación 2. Describir el retículo de subgrupos de $C_{p^n} = \langle x/x^{p^n} = 1\rangle$.

Resolución. Puesto que $Div(p^n) = \{p^k/0 \leq k \leq n\}$, el grupo cíclico C_{p^n} tiene un único subgrupo cíclico $C_{p^k} = \langle x^{p^{n-k}}\rangle$ de orden p^k para cada k con $0 \leq k \leq n$.

Así que el retículo de subgrupos tiene la forma:

Ejercicio. Ejercicio 30. Relación 2. Describir el retículo del grupos $C_{12} = \langle x / x^{12} = 1 \rangle$.

Resolución. Puesto que $Div(12) = \{1, 2, 3, 4, 6, 12\}$ para cada uno de ellos tendrá un subgrupo cíclico del correspondiente orden, Así obtenemos el subgrupo trivial $1 = \langle a^{12} = 1 \rangle$, los grupos cíclicos de orden $2, 3, 4, 6$ que son, respectivamente $C_2 = \langle x^6 \rangle$, $C_3 = \langle x^4 \rangle$, $C_4 = \langle x^3 \rangle$ y $C_6 = \langle x^6 \rangle$, y el total, correspondiente al divisor 12, C_{12}. Por otro lado, por el apartado (4) del teorema anterior, C_i está contenido en C_j si y sólo si i divide a j. Por tanto el retículo de subgrupos es el siguiente:



La siguiente proposición nos ayuda a identificar subgrupos de un grupo cíclico dados por diferentes generadores:

Proposición 0.3. *Sea $C_n = \langle a / a^n = 1\rangle$ el grupo cíclico de orden n. Entonces*

(1) $\langle a^m\rangle = \langle a^{\text{m.c.d.}(m,n)}\rangle$.

(2) $\langle a^{m_1}, a^{m_2}, \ldots, a^{m_k}\rangle = \langle a^{\text{m.c.d.}(m_1,m_2,\ldots,m_k,n)}\rangle$.

Demostración. (1) Sea $d = \text{m. c. d.}(m, n)$. Sabemos que C_n tiene un único subgrupo de orden $\frac{n}{d}$: $\langle a^d\rangle$. Puesto que $|\langle a^m\rangle| = ord(a^m) = \frac{n}{d}$, necesariamente $\langle a^m\rangle = \langle a^{\text{m.c.d.}(m,n)}\rangle$.
(2) Sea $d = \text{m. c. d.}(m_1, m_2, \ldots, m_k, n)$. Como $d|m_i$, concluimos que $a^{mi} \in \langle a^d\rangle$, para todo $i = 1, \ldots, k$. Así que $\langle a^{m_1}, a^{m_2}, \ldots, a^{m_k}\rangle \leq \langle a^d\rangle$. Para la otra inclusión, utilizamos el teorema de Bezout, y elegimos enteros $t_1, t_2, \ldots, t_k, t$ tal que $d = t_1m_1 + t_2m_2 + \cdots + t_km_k + tn$. Pero entonces $a^d = (a^{m_1})^{t_1}(a^{m_2})^{t_2}\ldots(a^{m_k})^{t_k}$ es un elemento del subgrupo $\langle a^{m_1}, a^{m_2}, \ldots, a^{m_k}\rangle$ y consecuentemente tenemos la otra inclusión $\langle a^d\rangle \leq \langle a^{m_1}, a^{m_2}, \ldots, a^{m_k}\rangle$ y entonces la igualdad. □

Ejercicio. Ejercicio 31. Relación 2 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 $H_2 = \langle t^{46}\rangle$?

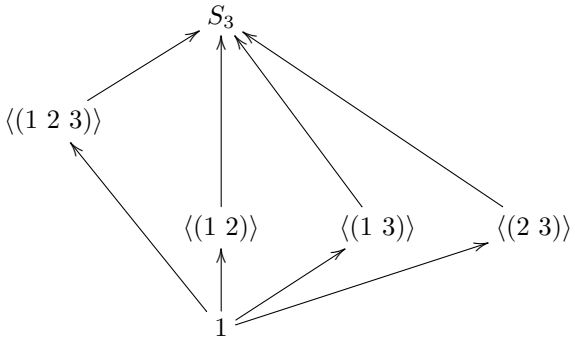
Resolución. Puesto que $\text{m. c. d.}(48, 72, 136) = 8$ entonces $H_1 = \langle t^{48}, t^{72}\rangle = \langle t^8\rangle$. Puesto que $\text{m. c. d.}(46, 136) = 2$ entonces $H_2 = \langle t^{46}\rangle = \langle t^2\rangle$. Finalmente, puesto que $2|8$,, $t^8 \in \langle t^2\rangle$. Así que $H_1 \leq H_2$.

Para el caso de grupos no cíclicos, la descripción del retículo dependerá de cada grupo particular.

Veamos un par de ejemplos

Ejercicio. 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.

Resolución. Veamos ii) y iii)
ii) El retículo de subgrupos de S_3 tiene el siguiente grafo

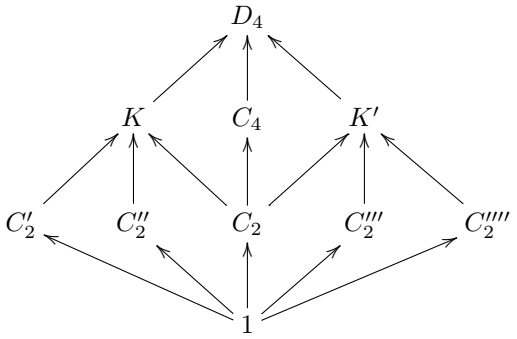


En efecto, puesto que $|S_3| = 6$, sus subgrupos propios serán necesariamente, por el teorema de Langrange, de orden 2 ó 3. Puesto que son de orden primo habrán de ser cíclicos. Buscamos entonces los diferentes elementos de orden 2, esto es $(1\ 2), (1\ 3)$ y $(2\ 3)$, y los de orden 3, esto es $(1\ 2\ 3)$ y $(1\ 3\ 2) = (1\ 2\ 3)^{-1}$. Estos dos últimos generan el mismo subgrupo, de donde se sigue que el retículo es el descrito.

iii) El retículo de subgrupos de

$$D_4 = \langle r, s / r^4 = 1 = s^2, sr = r^3 s \rangle = \{1, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$$

tiene el siguiente grafo:



donde

$$C_4 = \langle r \rangle = \{1, r, r^2, r^4\}$$

es cíclico de orden 4,

$$K = \{1, r^2, s, r^2 s\}, \;\; K' = \{1, r^2, rs, r^3 s\}$$

son grupos tipo Klein, y

$$C_2 = \{1, r^2\}, \; C_2' = \{1, s\}, \; C_2'' = \{1, r^2 s\}, \; C_2''' = \{1, rs\}, \; C_2'''' = \{1, r^3 s\}$$

son subgrupos cíclicos de orden 2.
En efecto Puesto que $|D_4| = 8$, los subgrupos propios habrán de ser de orden 2 ó 4. Los de orden 2 serán los generados por los diferentes elementos de orden 2 en D_4: $r^2, s, rs, r^2 s, r^3 s$.

Los de orden 4, por el Ejercicio 23 Relación 2, son cíclicos de orden 4 o tipo Klein. Los elementos de orden 4 de D_4 son r y $r^3 = r^{-1}$ que generan el mismo subgrupo cíclico de orden 4. Los posibles subgrupos tipo Klein, por el Ejercicio 20 Relación 2, estarán generados por dos elementos distintos de orden 2 que conmutan entre sí. Las combinaciones posibles con los cinco elementos de orden 2, antes mencionados, nos conducen exactamente a dos diferentes tales subgrupos K y K'.