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.)

2. Sabemos que $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ dispone de:

i) 6 elementos de orden 4 cumpliendo $i^2 = j^2 = k^2$

De la misma forma, S_4 contiene también 6 elementos de orden 4 pero $(1234)^2 \neq (1324)^2 \neq (1243)^2$.

pero no coinciden todos; luego no pueden ser isomorfo

Otra forma es tratar con el menor subgrupo que contiene pero eso es el total y no tienen el mismo número de elementos

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

$\Leftarrow$) Es claro por ser un grupo contenido en G.

$\Rightarrow$) Si $X < G$ entonces $\langle X \rangle$ es el menor subgrupo que contiene a X entonces, como X es un subgrupo entonces $X = \langle X \rangle$

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

1. Sabemos que $\langle a \rangle \cap \langle b \rangle < \langle a \rangle$ y $\langle a \rangle \cap \langle b \rangle < \langle b \rangle$ entonces:

$$\left.\begin{array}{l} |\langle a \rangle \cap \langle b \rangle| \mid |\langle a \rangle| \\ |\langle a \rangle \cap \langle b \rangle| \mid |\langle b \rangle| \end{array}\right\} \Rightarrow |\langle a \rangle \cap \langle b \rangle| \mid mcd(o(a), o(b)) = 1 \Rightarrow |\langle a \rangle \cap \langle b \rangle| = 1 \Rightarrow \langle a \rangle \cap \langle b \rangle = 1$$

2. Sea $o(a) = r$ y $o(b) = s$, $(ab)^{rs} \underset{\text{conmutación}}{=} a^{rs} b^{rs} = 1$. Si $\exists t \mid (ab)^t = a^t b^t = 1 \Rightarrow a^t = b^{-t} \in \langle a \rangle \cap \langle b \rangle = 1$

$\Rightarrow r \mid t \wedge s \mid t \Rightarrow rs \mid t$

↳ realmente $mcm(r,s) \mid t$ — rs pues r y s coprimos

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.

En S_3 tomando $a=(12)$ y $b=(123)$ obtenemos que $o(ab)=2$ y $o(a)o(b)=6$

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

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

$o(a)=4 \wedge o(b)=6$ pero $ab = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ cuyo orden es infinito pues $(ab)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ $\forall n \in \mathbb{N}$

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.

1. Si $|G|=4$ entonces $o(a) \mid 4$ $\forall a$, es decir, es 2 o 4. Distinguimos casos:

•) Si no hay elementos de orden 4 entonces hay 3 elementos de orden 2 es el grupo de Klein

•) Si hay un elemento de orden 4 $\Rightarrow G = \langle a \rangle \cong \mathbb{Z}_4 \cong C_4$

2. Distinguimos casos:

-) Si $\exists a \in G \mid o(a)=6 \Rightarrow G = \langle a \rangle$

-) Si no hay elementos de orden 6 entonces $\exists b \mid o(b)=3$ o $o(b)=2$

i) Si no hay elementos de orden 2 $\Rightarrow$ habría un número par de elementos de orden 3 más el trivial $\Rightarrow |G| \neq 6$

ii) Si no hay elementos de orden 3 $\Rightarrow \forall x,y \in G$ $xy \in G$ luego luego el grupo de Klein; $V \leq G \Rightarrow 4 \nmid 6$

iii) Luego hay elementos de ambos órdenes $\Rightarrow \exists a,b \mid o(a)=2, o(b)=3$

luego $G = \{1, a, b, b^2, ab, ab^2\} = D_3$

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.

$\Leftarrow$) Es fácil, piensa

$\Rightarrow$) Sea $a \in G, a \neq 1$ entonces $\langle a \rangle \leq G$, como G no tiene subgrupos propios $\langle a \rangle = G$.

Si $|G| = n \cdot m$ entonces $\underset{\neq 1}{\langle a^m \rangle}$ debe ser un subgrupo cíclico de G $\{$ porque es subgrupo propio

luego $|G| = p$ primo

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

Usaremos que si $o(x)=n \Rightarrow \langle x^k \rangle = \langle x^d \rangle$ con $d = mcd(k,d)$ $\wedge$ $o(x^k) = \frac{n}{d}$

- $mcd(48,136)=8$ · $mcd(72,136)=8$

Luego $\langle t^{48} \rangle = \langle t^8 \rangle$ $\wedge$ $\langle t^{72} \rangle = \langle t^8 \rangle$, entonces $\langle t^{48}, t^{72} \rangle = \langle t^8 \rangle$ pues $\langle t^{48}, t^{72} \rangle = \langle t^{48} \rangle \vee \langle t^{72} \rangle$

Ahora, como $\langle t^{46} \rangle = \langle t^2 \rangle$, pues $mcd(136,46)=2$. Es decir $H_1 < H_2$ ya que $t^8 = (t^2)^4$

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 $\theta(x^k) = g^k$ $\forall k \in \{0, \dots, n-1\}$.
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 $r = 1, \dots, n$ 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 $\varphi(n)$.

1. Sabemos que $g = \varphi(x) \Rightarrow g^n = \varphi(x)^n = \varphi(x^n) = 1$ luego $o(g)|n$. Supongamos $\exists m \in \mathbb{Z} \mid g^m = 1 \Rightarrow g^m = \varphi(x)^m = \varphi(x^m) = 1$, es decir, $x^m = 1 \Rightarrow n|m$.

Además, es claro que, $g^k = \varphi(x^k)$ por definición de homomorfismo

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 $n = 4$.

$A_2 = \{1\}$

$A_3 = \{1, (123), (132)\}$

$A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

Ejercicio 2. Sea $D_n = \langle r, s \,|\, s^2 = r^n = 1,\ sr = r^{n-1}s \rangle$ 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 $m.c.d.(k - j, n) = 1$.

Sea $n \in \mathbb{N}$ fijo pero arbitrario y $A = \langle r^j s, r^k s$ vamos a ver que $D_n \cong A$; para ello, definimos

$$\begin{aligned} \varphi : D_n &\longrightarrow A \\ r &\longmapsto r^j s \\ s &\longmapsto r^k s \end{aligned}$$

y vamos a ver que es isomorfismo. Para ello, debemos ver que sea homomorfismo, es decir, para $x, y \in D_n$, $\varphi(xy) = \varphi(x)\varphi(y)$, pero esto se cumple pues lleva sistemas de generadores en sistemas de generadores. Para ver que son isomorfos basta con probar que $(r^j s)^n = 1$, $(r^k s)^2 = 1$ y que $r^j s = s r^{n-j}$.

Nota: $\langle r^j s, r^k s \rangle$ es subgrupo pues para $x, y \in A$, $xy \in A$.

Isomorfo no es igual

Doble inclusión

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.

1. Para ello, como S_3 es finito, bastará con ver que, si $x, y \in H \Rightarrow xy \in H$

- $Id\,x = x = x\,Id$ - $(123)(132) = Id$
- $(123)(123) = (132)$ - $(132)(123) = Id$
- $(132)(132) = (123)$

Luego es un subgrupo

2. Esto es sencillo, pues si $x \in S_3$, bastará calcular $xH = \{k \mid k = xh$ para algún $h \in H\}$ y análogamente Hx.

Ejercicio 9. Sea G un grupo finito.

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

1. Si $H < G$:

i) $[G:H] = |G| \Leftrightarrow H = \{1\}$

$\Rightarrow$) Sabemos, por el Teorema visto en clase,

$[G:H] = \frac{|G|}{|H|}$, como $[G:H] = |G| \Rightarrow |H| = 1$

luego $H = \{1\}$

$\Leftarrow$) Si $H = \{1\}$, $|H| = 1 \Rightarrow [G:H] = |G|$

ii) $[G:H] = 1 \Leftrightarrow H = G$, es análogo y sencillo

2. $|G| = [G:G_2] \cdot |G_2|$

$|G| = [G:G_1] \cdot |G_1| = [G:G_1][G_1:G_2]|G_2|$ $\Big\} \Rightarrow [G:G_1][G_1:G_2] = [G:G_2]$

3. Basta con aplicar una sencilla inducción con el apartado 2 de caso base.

4. Basta aplicar el apartado anterior al caso en el que $G_r = 1$.

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.

Se calcularon durante el desarrollo del Tema 3; están en los apuntes.

Ejercicio 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

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

Usaremos el corolario que nos dice que $\exists! S < G \mid |S| = m$ con $m \in Div(p^n)$ y como p es primo es fácil ver que $Div(p^n) = \{1, p, p^2, \dots, p^n\}$ luego los subgrupos propios son

Orden $p \rightarrow \langle x^{p^{n-1}} \rangle$

$$\begin{array}{l} \text{Orden } p^2 \longrightarrow \langle x^{p^{n-2}} \rangle \\ \quad | \\ \text{Orden } p^n \longrightarrow \{1\} \end{array}$$

Luego el retículo general es:

$$\begin{array}{c} C_{p^n} \\ | \\ \langle x^p \rangle \\ | \\ \langle x^{p^2} \rangle \\ | \\ \vdots \\ | \\ \langle x^{p^n} \rangle \\ | \\ \{1\} \end{array}$$

En el caso de C_8, el retículo es:

$$\begin{array}{c} C_8 \\ | \\ \langle x^2 \rangle \\ | \\ \langle x^4 \rangle \\ | \\ \{1\} \end{array}$$

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

Se hace de forma idéntica a la segunda parte del ejercicio anterior

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

$\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$, $\mathbb{Z}_7 = \langle 2 \rangle$ luego es cíclico

Ejercicio 18.

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

1. Sabemos por el ejercicio anterior que $Aut(C_8) \cong \mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ y además, $f_r(x) = x^r$ $\forall r \in \{1, 3, 5, 7\}$
luego, para 1, $f_1(x) = x^1$, $f_3(x) = x^3$, $f_5(x) = x^5$ y $f_7(x) = x^7$

2. Para ver que $Aut(C_8) \cong V$ bastará ver que $\mathcal{U}(\mathbb{Z}_8) \cong V$, pero $o(\mathcal{U}(\mathbb{Z}_8)) = 4$ y $o(x) = 2$ $\forall x \in \mathcal{U}(\mathbb{Z}_8)$
luego como todo grupo de orden 4 es isomorfo a $\mathbb{Z}_4$ o a V y en $\mathbb{Z}_4$ no hay elementos de orden 2 vemos que $\mathcal{U}(\mathbb{Z}_8) \cong V$. Ahora bien; como $Aut(C_8) \cong \mathbb{Z}_8^\times$ por el ejercicio 17 obtenemos la isomorfía que buscamos.