# Primer Taller Algebra Abstracta

Jonathan Andrés Niño Cortés

3 de septiembre de 2014

Los puntos elegidos por el autor para su calificación son el 1, 3, 8, 11 y 15.

1. $G = \{(a, b) \in \mathbb{R}^2 | a \neq 0\}$ y $(a, b) \cdot (c, d) = (ac, ad+b)$ es un grupo con elemento identidad $(1, 0)$.

   *Demostración.* Primero se debe demostrar la clausura de la operación. Sean (a,b) y (c,d) $\in G$. Como $a$ y $c$ son diferentes a 0, $ac \neq 0$. Por lo tanto $(ac, ad + b) \in G$.

   Asociatividad: Sean $(a, b), (c, d)$ y $(e, f) \in G$. Se debe probar que $[(a, b) \cdot (c, d)] \cdot (e, f) = (a, b) \cdot [(c, d) \cdot (e, f)]$

   $$\begin{aligned} [(a, b) \cdot (c, d)] \cdot (e, f) &= (a, b) \cdot [(c, d) \cdot (e, f)] \\ (ac, ad + b) \cdot (e, f) &= (a, b) \cdot (ce, cf + d) \\ (ace, acf + ad + b) &= (ace, a(cf + d) + b) \\ (ace, acf + ad + b) &= (ace, acf + ad + b) \quad \square \end{aligned}$$

   Identidad: Se debe demostrar que $(1, 0)$ es la identidad. Es decir, que $(1, 0) \cdot (a, b) = (a, b)$ para cualquier $(a, b) \in G$.

   $$\begin{aligned} (1, 0) \cdot (a, b) &= (1a, 1b + 0) \\ &= (a, b) \quad \square \end{aligned}$$

   Inverso: Sea $(a, b) \in G$. Se quiere demostrar que existe un $(c, d) \in G$ tal que $(a, b) \cdot (c, d) = (1, 0)$. Sea $(c, d) = (\frac{1}{a}, \frac{-b}{a})$. $\frac{1}{a}$ y $\frac{-b}{a} \in \mathbb{R}$ porque $a \neq 0$ y $(\frac{1}{a}, \frac{-b}{a}) \in G$ porque $\frac{1}{a} \neq 0$. Veamos que $(a, b) \cdot (\frac{1}{a}, \frac{-b}{a}) = (1, 0)$

   $$\begin{aligned} (a, b) \cdot (\frac{1}{a}, \frac{-b}{a}) &= (a\frac{1}{a}, a\frac{-b}{a} + b) \\ &= (1, -b + b) \\ &= (1, 0) \quad \square \end{aligned}$$

   Por lo tanto $(G, \cdot)$ es un grupo. $\square$

2. El grupo de los cuaterniones

$$Q_8 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \pm \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\}.$$

con la operación de multiplicación de matrices es un grupo.

*Demostración.* Los elementos del grupo se denotan como $\{\pm 1; \pm i; \pm j; \pm k\}$ en el orden de arriba. La multiplicación por 1 ó $-1$ se comporta de la manera esperada $(a * (\pm 1) = \pm a)$. Para construir la tabla de multiplicación demostremos los siguientes produtos.

- $i^2 = -1$.
$$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0*0+i*i & 0*i+i*0 \\ i*0+0*i & i*i+0*0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
- $j^2 = -1$.
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
- $k^2 = -1$.
$$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
- $ij = k$
$$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$
- $jk = i$
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$
- $jk = i$
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$
- $ki = j$
$$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
- Sean $a, b, c \in \{i, j, k\}$ tales que $ab = c$. Entonces $cb = -a$.
  Ya demostramos que para todo $x \in \{i, j, k\}, x^2 = -1$. Por lo tanto:
$$\begin{aligned} ab &= c \\ abb &= cb \\ a(-1) &= cb \\ -a &= cb \end{aligned}$$
  De lo anterior podemos deducir que $ki = j \Rightarrow ji = -k$; $ij = k \Rightarrow kj = -i$; y $jk = i \Rightarrow ik = -j$.

Con las propiedades de los cuaterniones demostradas anteriormente podemos construir la siguiente tabla de multiplicación.

| $Q_8$ | **1** | **-1** | **i** | **-i** | **j** | **-j** | **k** | **-k** |
|---|---|---|---|---|---|---|---|---|
| **1** | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| **-1** | $-1$ | $1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |
| **i** | $i$ | $-i$ | $-1$ | $1$ | $k$ | $-k$ | $-j$ | $j$ |
| **-i** | $-i$ | $i$ | $1$ | $-1$ | $-k$ | $k$ | $j$ | $-j$ |
| **j** | $j$ | $-j$ | $-k$ | $k$ | $-1$ | $1$ | $i$ | $-i$ |
| **-j** | $-j$ | $j$ | $k$ | $-k$ | $1$ | $-1$ | $-i$ | $i$ |
| **k** | $k$ | $-k$ | $j$ | $-j$ | $-i$ | $j$ | $-1$ | $1$ |
| **-k** | $-k$ | $k$ | $-j$ | $j$ | $i$ | $-j$ | $1$ | $-1$ |

Se puede observar que la operación es asociativa porque la operación de multiplicación de matrices es asociativa.

También se puede observer que este grupo posee un elemento identidad que es 1, la matriz identidad.

Finalmente, se puede observar que la tabla de multiplicación es un cuadro latino (es decir, en ninguna fila ni en ninguna columna hay elementos repetidos). Esto implica que cada elemento tiene un inverso. Efectivamente, los inversos de 1 y -1, son si mismos y los inversos de los demás elementos son sus respectivos negativos. □

3. $H = \{\sigma \in \Sigma_n | \sigma(1) = 1\}$ es un subgrupo de $\Sigma_n$.

*Demostración.* En primer lugar se debe demostrar que si $\sigma_1, \sigma_2 \in H$, entonces $\sigma_1 \circ \sigma_2 \in H$. Como $\sigma_1, \sigma_2 \in H$, $\sigma_1(1) = 1$ y $\sigma_2(1) = 1$. Por lo tanto tenemos que

$$\begin{aligned} \sigma_1 \circ \sigma_2(1) &= \sigma_1(\sigma_2(1)) \\ &= \sigma_1(1) \\ &= 1 \end{aligned}$$

Lo que implica que $\sigma_1 \circ \sigma_2 \in H$.

En segundo lugar se debe demostrar que si $\sigma \in H$, $\sigma^{-1} \in H$. Como $\sigma \in \Sigma_n$, existe $\sigma^{-1}$ tal que $\sigma^{-1} \circ \sigma = \mathbf{1}$. Esto implica que

$$\sigma^{-1} \circ \sigma(1) = \mathbf{1}(1) = 1$$

Pero por otra parte $\sigma(1) = 1$. Luego

$$\sigma^{-1} \circ \sigma(1) = \sigma^{-1}(\sigma(1)) = \sigma^{-1}(1)$$

Uniendo las dos equivalencias anteriores obtenemos que $\sigma^{-1}(1) = 1$. Por lo tanto $\sigma^{-1} \in H$. □

4.

- $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 4 & 8 & 6 & 3 & 7 \end{pmatrix}$

  La permutación $\alpha$ se puede expresar en ciclos separados de la siguiente manera:

  $$\alpha = (1\ 5\ 8\ 7\ 3\ 2)$$

  Se puede factorizar en transposiciones de la siguiente manera:

  $$\alpha = (1\ 2)(1\ 3)(1\ 7)(1\ 8)(1\ 5)$$

  Por lo cual $\alpha$ es impar.

- $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 6 & 3 & 5 & 8 & 4 & 7 \end{pmatrix}$

  La permutación $\beta$ se puede expresar en ciclos separados de la siguiente manera:

  $$\beta = (3\ 6\ 8\ 7\ 4)$$

  Se puede factorizar en transposiciones de la siguiente manera:

  $$\beta = (3\ 4)(3\ 7)(3\ 8)(3\ 6)$$

  Por lo cual $\beta$ es par.

- $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

  La permutación $\gamma$ se puede expresar en ciclos separados de la siguiente manera:

  $$\gamma = (1\ 8\ 3\ 6)(2\ 7)(4\ 5)$$

  Se puede factorizar en transposiciones de la siguiente manera:

  $$\gamma = (1\ 6)(1\ 3)(1\ 8)(2\ 7)(4\ 5)$$

  Por lo cual $\gamma$ es impar.

- $\alpha\beta\gamma$

  $\alpha\beta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 8 & 2 & 5 & 1 & 6 \end{pmatrix}$

  Para calcular el orden debemos hallar el $k$ tal que $(\alpha\beta\gamma)^k = \mathbf{1}$. Con la ayuda de una rutina creada utilizando el lenguaje Java y el ambiente de programación eclipse, se determino que dicho $k$ es 15.

- $\beta\alpha\gamma$

  $\beta\alpha\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 7 & 3 & 5 & 1 & 2 \end{pmatrix}$

  Utilizando la rutina mencionada anteriormente se determino que el orden de esta permutación también era de 15.

5. I.) Sea $G$ un grupo, $a \in G$ y $m, n \in \mathbb{Z}$ relativamente primos. Si $a^m = 1$, entonces existe $b \in G$ tal que $a = b^n$.

*Demostración.* $m, n \in \mathbb{Z}$ son primos relativos es equivalente a que $(m, n) = 1$. Por la identidad de Bezout, existen $s, t \in \mathbb{Z}$ tales que $ms + nt = 1$. Por lo tanto podemos escribir $a$ de la siguiente manera.

$$a = a^1 = a^{ms+nt} = a^{ms}a^{nt} = (a^m)^s(a^t)^n$$

Pero $a^m = 1$. Por lo tanto

$$(a^m)^s(a^t)^n = 1^s(a^t)^n = 1(a^t)^n = (a^t)^n$$

Por lo tanto uniendo las anteriores equivalencias tenemos que existe un $b = a^k$, tal que $a = b^n$. □

II.) Sea $G$ un grupo finito y $m \in \mathbb{Z}$ tal que $(|G|, m) = 1$. Demostrar que la ecuación $x^m = a$ tiene una única solución en $G$.

*Demostración.* Como $a \in G$, $a^{|G|} = 1$. Por lo demostrado anteriormente podemos concluir que existe un $x \in G$ tal que $x^m = a$. □

Antes de demostrar la unicidad del x. Vamos a demostrar que $(|<a>|, m) = 1$. Por el teorema de Lagrange, $|<a>|$ divide a $|G|$, pues $<a>$ es un subgrupo de $G$. Ahora por lo anterior $(|<a>|, m)$ divide a $|G|$ y divide a $m$. Por lo tanto, $(|<a>|, m) \leq (|G|, m)$. Pero como $(|G|, m) = 1$, esto implica que $(|<a>|, m) = 1$ también.

Ahora podemos demostrar la unicidad de la siguiente manera. Sean $x, x' \in G$ tales que $x^m = a = (x')^m$. Por lo demostrado en el numeral I), tenemos que $x = a^t$ y $x' = a^{t'}$ para $t, t' \in \mathbb{Z}$. Por lo tanto podemos escribir la expresión $x^m = a = (x')^m$ de la siguiente manera.

$$\begin{aligned} x^m &= (x')^m \\ (a^t)^m &= (a^{t'})^m \\ a^{tm} &= a^{t'm} \\ a^{tm}a^{-t'm} &= a^{t'm}a^{-t'm} \\ a^{tm-t'm} &= a^{t'm-t'm} \\ a^{m(t-t')} &= a^0 \\ a^{m(t-t')} &= 1 \end{aligned}$$

Lo anterior implica que existe $k \in \mathbb{Z}$ tal que $|<a>|k = m(t - t')$.

Ahora utilizando la identidad de Bezout de nuevo, esta vez para $(|<a>|, m)$, obtenemos que $1 = |<a>|b + mc$ para $b, c \in \mathbb{Z}$. Partiendo de esta expresión tenemos

$$\begin{aligned} 1 &= |<a>|b + mc \\ 1(t-t') &= (t-t')(|<a>|b + mc) \\ (t-t') &= |<a>|b(t-t') + m(t-t')c \\ (t-t') &= |<a>|b(t-t') + |<a>|kc \\ (t-t') &= |<a>|[b(t-t') + kc] \end{aligned}$$

Lo anterior implica que $(t-t')$ es divisible por $|<a>|$. Luego $a^{t-t'} = 1$. Transformado de nuevo esta expresión

$$\begin{aligned} a^{t-t'} &= 1 \\ a^t a^{-t'} &= 1 \\ a^t a^{-t'} a^{t'} &= 1a^{t'} \\ a^t 1 &= a^{t'} \\ a^t &= a^{t'} \\ x &= x' \end{aligned}$$

Por lo tanto, $x$ es único en $G$.

6. $M = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} | x \in \mathbb{R} \right\}$ con la operación de multiplicación de matrices es un grupo isomorfo con la operación de suma.

*Demostración.* En primer lugar demostremos que para cualquier $A, B \in M$, $A \times B \in M$. Si $A, B \in M$, entonces existen $a, b \in \mathbb{R}$ tales que $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Luego

$$A \times B = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix}$$

Por lo tanto $A \times B \in M$.

Además si $A \in M$, entonces $A^{-1} \in M$. Para observese que si $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, entonces $A^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$. En efecto tenemos que

$$A \times A^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -a+a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

y podemos notar que $A^{-1} \in M$.

Lo anterior implica que $M$ es un subgrupo del grupo $GL(2,\mathbb{R})$. Por lo tanto es un grupo en si mismo.

Ahora queremos encontrar un isomorfismo entre $M$ y $\mathbb{R}$. Definamos la función $f : \mathbb{R} \longmapsto M$ de la siguiente manera.

$$f(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Claramente esta función es bijectiva pues cada matriz tiene una preimagen correspondiente y si dos elementos en $\mathbb{R}$ son diferentes sus imagenes también lo serán.

Ahora queremos probar que para $a, b \in \mathbb{R}$, $f(a+b) = f(a)f(b)$.

Efectivamente

$$f(a)f(b) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} = f(b+a).$$

Y como el grupo $(\mathbb{Z}, +)$ es abeliano $f(b+a) = f(a+b)$. Por lo tanto $f$ es un isomorfismo de $\mathbb{Z}$ a $M$. □

7. I.) *Demostración.* Sean $G, G'$ dos grupos finitos y sea $\phi : G \longmapsto G'$ un isomorfismo entre grupos. Queremos ver que para cualquier $g \in G$ el orden de $g$ es igual al orden de $\phi(g)$. Sea $g \in G$, sea $n$ el orden de $g$ y sea $m$ el orden de $\phi(g)$. Por el teorema de Lagrange tenemos que $g^n = 1$. Por lo tanto, $\phi(1) = \phi(a^n) = \phi(a)^n$ ($\phi(a^n) = \phi(a)^n$ porque $\phi$ es un isomorfismo). Esto implica también por el teorema de Lagrange que $m$ divide a $n$.

Ahora como $\phi$ es una biyección podemos tomar su inversa $\phi^{-1}$ como un isomorfismo entre $G'$ y $G$. Sea m el orden de $\phi(g)$. Se cumple que $\phi(g)^m = 1$. Por lo tanto,

$$\begin{aligned} \phi^{-1}(\phi(1)) &= \phi^{-1}(\phi(g)^m) \\ 1 &= \phi^{-1}(\phi(g^m)) \\ 1 &= g^m. \end{aligned}$$

Por lo que también tenemos que el orden d $g$ divide a $m$. Finalmente como $n|m$ y $m|n$ y ambos son positivos entonces $m = n$. □

II.) El número de isomorfismos entre dos grupos de orden cíclico es igual a $\varphi(n)$.

*Demostración.* Para responder esta pregunta consideremos el grupo $\mathbb{Z}/n$. Recordemos que si $x$ es un elemento en un grupo con orden $n$, entonces $<x>$ es isomorfo a $\mathbb{Z}/n$ y el isomorfismo es tal que mapea $x^k$ a $\bar{k}$ (por $\bar{k}$ denotamos la clase de equivalencia de $k$ módulo $n$). Por lo tanto, si tomamos los elementos dentro de $\mathbb{Z}/n$ tales que su orden es igual a $n$ entonces podemos crear un isomorfismo

entre $\mathbb{Z}/n$ y el grupo generado por dichos elementos. Notese que para generadores diferentes el isomorfismo sera diferente. Entonces el número de isomorfismos es igual al número de generadores de $\mathbb{Z}/n$.

Ahora demostramos que si $\bar{x} \in \mathbb{Z}/n$, $(\bar{x}, n) = 1$, entonces el orden de $\bar{x}$ es $n$. $\bar{x}^k$ lo denotamos como $k\bar{x}$, pues en este caso la operación es aditiva.

$k\bar{x} = \bar{0}$ es equivalente a que $kx \equiv 0 \pmod{n}$. Lo anterior implica que $n$ divide a $kx$. Como $(\bar{x}, n) = 1$ entonces $n$ debe dividir a $k$. De hay que el mínimo $k > 0$ tal que $k\bar{x} = \bar{0}$ es $k = n$. Por lo tanto el orden de $\bar{x}$ es $n$. Finalmente el conjunto de los elementos que cumplen $(\bar{x}, n) = 1$ es el grupo $\mathrm{U}(n)$. Y la cardinalidad de este grupo es $\varphi(n)$. □

8. I).
   - $\gamma_a$ es inyectiva.
     Sea $\gamma_a(x) = \gamma_a(y)$, entonces

$$\begin{aligned} \gamma_a(x) &= \gamma_a(y) \\ axa^{-1} &= aya^{-1} \\ a^{-1}axa^{-1}a &= a^{-1}aya^{-1}a \\ 1x1 &= 1y1 \\ x &= y \end{aligned}$$

   - $\gamma_a$ es sobreyectiva.
     Sea $x \in G$, entonces $\exists y \in G : \gamma_a(y) = x$. Tomemos $y = a^{-1}xa$, entonces $\gamma_a(y) = \gamma_a(a^{-1}xa) = aa^{-1}xaa^{-1} = 1x1 = x$.
   - $\gamma_a$ es un isomorfismo.

$$\gamma_a(x)\gamma_a(y) = axa^{-1}aya^{-1} = ax(a^{-1}a)ya^{-1} = axya^{-1} = \gamma_a(xy).$$

   II). Si $a, b \in G$, entonces $\gamma_a \circ \gamma_b = \gamma_{ab}$. Sea $x \in G$, entonces

$$\begin{aligned} \gamma_a \circ \gamma_b(x) &= \gamma_a(\gamma_b(x)) \\ &= \gamma_a(bxb^{-1}) \\ &= abxb^{-1}a^{-1} \\ &= \gamma_{ab}(x) \end{aligned}$$

9. I). Para demostrar que $\sim$ es una relación de equivalencia, demostramos que $\sim$ es reflexiva, simétrica y transitiva.
   - $\sim$ es reflexiva.
     Tomese $g = \mathbf{1}$. Entonces $x = \mathbf{1}x\mathbf{1}^{-1}$.
   - $\sim$ es simétrica.

Sea $x, y \in G$ tales que $x \sim y$, entonces existe $g \in G$ tal que $x = gyg^{-1}$. Manipulando esta expresión obtenemos.

$$\begin{aligned} x &= gyg^{-1} \\ g^{-1}xg &= g^{-1}gyg^{-1}g \\ g^{-1}xg &= (g^{-1}g)y(g^{-1}g) \\ g^{-1}xg &= y \end{aligned}$$

Por lo tanto existe $g' = g^{-1}$ tal que $y = g'x(g')^{-1}$. Es decir, $y \sim x$.

- $\sim$ es transitiva.
  Sean $x, y, z \in G$ tales que $x \sim y$ y $y \sim z$. Por lo tanto existen $g_1, g_2 \in G$ tales que $x = g_1 y g_1^{-1}$ y $y = g_2 z g_2^{-1}$. Sustituyendo $y$ en la primera ecuación tenemos que
  $$x = g_1(g_2 z g_2^{-1})g_1^{-1} = (g_1 g_2)z(g_2^{-1}g_1^{-1})$$
  Por lo tanto, existe $g = g_1 g_2$ tal que $x = gzg^{-1}$, es decir $x \sim z$.

II). Para obtener las clases podemos utilizar la tabla de multiplicación de la operación de conjugación. Si enumeramos los elementos del grupo $G$ como $g_i$ para $0 \leq i \leq |G|$. Entonces el elemento $c_{ij}$ (fila $i$, columna $j$) es igual a $g_i g_j g_i^{-1}$. Los elementos en la columna $j$ serian entonces los elementos de la clase $[g_j]$.

- $Q_8$

| $Q_8$ | **1** | **-1** | **i** | **-i** | **j** | **-j** | **k** | **-k** |
|---|---|---|---|---|---|---|---|---|
| **1** | 1 | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| **-1** | 1 | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| **i** | 1 | $-1$ | $i$ | $-i$ | $-j$ | $j$ | $-k$ | $k$ |
| **-i** | 1 | $-1$ | $i$ | $-i$ | $-j$ | $j$ | $-k$ | $k$ |
| **j** | 1 | $-1$ | $-i$ | $i$ | $j$ | $-j$ | $-k$ | $k$ |
| **-j** | 1 | $-1$ | $-i$ | $i$ | $j$ | $-j$ | $-k$ | $k$ |
| **k** | 1 | $-1$ | $-i$ | $i$ | $-j$ | $j$ | $k$ | $-k$ |
| **-k** | 1 | $-1$ | $-i$ | $i$ | $-j$ | $j$ | $k$ | $-k$ |

Por lo tanto las clases de $Q_8$ son $\bar{1} = \{1\}, \bar{-1} = \{-1\}, \bar{i} = \{i, -i\}, \bar{j} = \{j, -j\}, \bar{k} = \{k, -k\}$.

- $S_3$

| $S_3$ | **1** | **(2 3)** | **(1 2)** | **(1 3)(1 2)** | **(1 2)(1 3)** | **(1 3)** |
|---|---|---|---|---|---|---|
| **1** | 1 | (2 3) | (1 2) | (1 3)(1 2) | (1 2)(1 3) | (1 3) |
| **(2 3)** | 1 | (2 3) | (1 3) | (1 2)(1 3) | (1 3)(1 2) | (1 2) |
| **(1 2)** | 1 | (1 3) | (1 2) | (1 2)(1 3) | (1 3)(1 2) | (2 3) |
| **(1 3)(1 2)** | 1 | (1 3) | (2 3) | (1 3)(1 2) | (1 2)(1 3) | (1 2) |
| **(1 2)(1 3)** | 1 | (1 2) | (1 3) | (1 3)(1 2) | (1 2)(1 3) | (2 3) |
| **(1 3)** | 1 | (1 2) | (2 3) | (1 2)(1 3) | (1 3)(1 2) | (1 3) |

De la anterior tabla se concluye que las clases de equivalencia son $\bar{1} = \{1\}, \bar{(12)} = \{(12), (13), (23)\}, \bar{(12)(13)} = \{(12)(13), (13)(12)\}$.

10. I). *Demostración.* Sean $a, b \in G$ tales que $ab = ba$ y $a^m = \mathbf{1} = b^n$. Ahora tomemos el producto $(ab)^k$. Si $a, b$ conmutan, se puede demostrar facilmente por inducción que $(ab)^k = a^k b^k$.

**Lema 1.** *Si $ab = ba$ entonces $(ab)^k = a^k b^k$.*

*Demostración.* En primer lugar el caso en que $k \geq 0$. El caso base $k = 0$ es obvio pues $(ab)^0 = a^0 b^0 = \mathbf{1}$.
Ahora supongamos que $(ab)^k = a^k b^k$. Y tomemos $(ab)^{k+1}$. Podemos reescribirlo como $a(ba)^k b$. Y como $ab = ba$, $(ba)^k = (ab)^k$. Por lo tanto,

$$(ab)^{k+1} = a(ba)^k b = a(ab)^k b = aa^k b^k b = a^{k+1} b^{k+1}.$$

Ahora si $k < 0$ se tiene que $a^k = (a^{-1})^{k'}$ con $k' = -k > 0$. Ahora el enunciado del lema queda como $((ab)^{-1})^{k'} = (a^{-1})^{k'} (b^{-1})^{k'}$. Y tenemos que si $a, b$ conmutan entonces $b^{-1}a^{-1} = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$. Por lo tanto $a^{-1}$ y $b^{-1}$ conmutan. Entonces podemos utilizar la prueba de inducción anterior y concluir que para todo $k < 0$, $(ab)^k = a^k b^k$. □

Por lo tanto, si $k$ es el mínimo común multiplo de $m$ y $n$ entonces

$$(ab)^k = a^k b^k = a^{sm} b^{tn} = (a^m)^s (b^n)^t = \mathbf{1}^s \mathbf{1}^t = \mathbf{11} = \mathbf{1}.$$

Ahora una de las consecuencias del teorema de Lagrange es que el orden de $ab$ debe dividir a $k$. Por lo tanto, el orden debe ser un número entero y por lo tanto finito. □

II).
- $A^4 = 1$
  $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
  $A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
  $A^4 = A^2 A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- $1 = B^3$
  $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
  $B^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$
  $B^3 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Sin embargo, tomemos $AB$
$AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ Se puede demostrar facilmente por inducción que $(AB)^k = \begin{pmatrix} 1 & k \\ 1 & 0 \end{pmatrix}$. Por lo tanto para que $(AB)^k$ sea cero, $k$ debe ser

cero. Pero la definición de orden, utiliza los $k > 0$. Por lo tanto no existe ningun $k > 0$ tal que $(AB)^k = I$, es decir, el orden de $AB$ es infinito.

11. I). $H < G \Leftrightarrow HH^{-1} \subseteq H$.

$\Rightarrow$ Suponga que $H < G$, entonces tomemos un $h \in HH^{-1}$. Por definición, existe $h_1 \in H$ y $h_2 \in H^-1$ tal que $h = h_1h_2$. Por otra parte que $h_2 \in H^-1$ implica que existe $h_3 \in H$ tal que $h_2 = h_3^{-1}$. Como $H$ es subgrupo, si $h_3 \in H$, entonces su inverso $h_3^{-1} = h_2$ también esta en $H$. Y como $h_1, h_2 \in H$, $h = h_1h_2 \in H$.

$\Leftarrow$ Suponga que $HH^{-1} \subseteq H$. Queremos ver que $H$ es un subgrupo de $G$.

En primer lugar, ya que el conjunto es no vacio, tomemos cualquier $a \in H$. Por lo tanto $a^{-1} \in H^{-1}$ y $\mathbf{1}= aa^{-1} \in HH^{-1}$. Y por nuestro supuesto inicial, $\mathbf{1} \in H$.

Tomemos de nuevo cualquier $a \in H$. Como $a \in G$ y $G$ es un grupo podemos escribir $\mathbf{1} = a^{-1}a$ que esta contenido en $H$ por lo demostrado anteriormente. Además $a^{-1} \in H^{-1}$, luego $a^{-1}aa^{-1} = a^{-1} \in HH^{-1}$ y por lo tanto $a^{-1} \in H$.

Por ultimo tomemos $a, b \in H$. Por lo demostrado anteriormente $b^{-1} \in H$. Luego $(b^{-1})^{-1} = b \in H^-1$. Entonces $ab \in HH^{-1}$ y por lo tanto $ab \in H$.

II). $H < G \Leftrightarrow \forall a \in H : Ha = H$.

$\Rightarrow$ Suponga que $H < G$ y tome cualquier $a \in H$. Se quiere ver que $Ha = H$, para ello utilice el método de doble contenencia.

$\subseteq$ Sea $x \in Ha$, por lo tanto $x = ha$ para algun $h \in H$, pero como $a \in H$ y $H$ es un grupo, $ha = x \in H$.

$\supseteq$ Sea $x \in H$, como $a \in H$ y $H$ es subgrupo se cumple que $a^{-1} \in H$. De nuevo como $H$ es subgrupo, $xa^{-1} \in H$. Por lo anterior $xa^{-1}a = x \in Ha$.

$\Leftarrow$ Suponga que $\forall a \in H : Ha = H$.

Como $H$ es no vacio, tomemos un $a \in H$. Como $Ha = H$, $a \in Ha$. Es decir existe $h \in H$ tal que $ha = a$. El único elemento que tiene esta propiedad es el elemento identidad de $G$, $\mathbf{1}$. Por lo tanto $h = \mathbf{1} \in H$.

Tomese de nuevo un elemento $a \in H$. Como ya demostramos $\mathbf{1} \in H$. pero como $Ha = H$, debe cumplirse que $\mathbf{1} \in Ha$. Es decir debe existir un elemento $h \in H$ tal que $ha = 1$. Esta es la propiedad del inverso de $a$ que se ha demostrado es único para cada $a$. Por lo tanto $h = a^{-1} \in H$.

Finalmente tomese dos elementos $a, b \in H$, tenemos que $Hb = H$ y como $a \in H$ tenemos que $ab \in Hb$, luego $ab \in H$.

12. Sea $G$ un grupo y $H, K$ dos subgrupos de $G$.

I). $H \cup K$ es un subgrupo de $G$ si y y solo si $H < K$ o $K < H$.

$\Leftarrow$ Si tenemos que $H < K$ o $K < H$ entonces $H \cup K$ es $H$ o $K$. En ambos casos $H \cup K$ es un subgrupo.

$\Rightarrow$ Supongamos que $H \cup K$ es un subgrupo. Tomemos cualquier elemento $h \in H$ y cualquier $k \in H$. Ambos pertenecen a $H \cup K$, luego $hk \in H \cup K$. Por lo tanto

hay dos casos, $hk \in H$ o $hk \in K$. Si $hk \in H$ entonces como $H$ es subgrupo de $G$ y $h \in H$, $h^{-1} \in H$ y$h^{-1}hk = k \in H$. Esto implica que $K < H$.

Si $hk \in K$ entonces como $K$ es subgrupo de $G$ y $k \in K$, $k^{-1} \in H$ y$hkk^{-1} = h \in K$. Esto implica que $H < K$.

Por lo tanto, o bien $H < K$ o $K < H$.

II). Como lo demostrado anteriormente es una doble implicación tenemos que si una proposición no se cumple la otra tampoco se cumplira. En particular, si $H$ no es subgrupo de $K$ ni $K$ es subgrupo de $H$ entonces $H \cup K$ no es un subgrupo. A modo de ilustración tomese G el grupo cíclico de orden 12. Sea $H$ el subgrupo generado por $\bar{3}$ y $K$ el subgrupo generado por $\bar{4}$. Claramente, ni $H$ esta contenido en $K$, ni $K$ esta contenido en $H$. Ahora tomemos la unión de $H$ y $K$. Tenemos que $\bar{3} \in H$ y $\bar{4} \in K$ pero $\bar{3} + \bar{4} = \bar{7}$ (notación aditiva pues la operación del grupo es la suma) no se encuentra ni en $H$ ni en $K$. Luego $H \cup K$ no puede ser un subgrupo.

13. Los únicos subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, donde $n$ es un entero.

Es claro que los conjuntos de la forma $n\mathbb{Z}$ son subgrupos de $\mathbb{Z}$. En primer lugar, $0 \in n\mathbb{Z}$ porque $0 = n * 0$. En segundo lugar si $na \in n\mathbb{Z}$ su inverso aditivo $-na$ también se encuentra en $n\mathbb{Z}$. Finalmente si tomamos dos elementos $na$ y $nb$ en $n\mathbb{Z}$ su suma $na + nb = n(a + b)$ también estará en $n\mathbb{Z}$.

Ahora para demostrar que todos los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, tomemos cualquier $H < \mathbb{Z}$.

Como $H$ es subgrupo $H$ debe contener el elemento 0. En el caso en que $H$ solo contenga este elemento entonces podemos escribir a $H$ como $0\mathbb{Z}$, ya que $0 * n = 0, \forall n \in \mathbb{Z}$.

Entonces supongamos que A tiene mas elementos. Ahora como $\mathbb{Z}$ es un conjunto ordenado tenemos que $\forall a, b \in \mathbb{Z} : a \leq b \vee b \leq a$. Por lo tanto podemos definir el conjunto $S = \{h \in H : h > 0\}$. Este conjunto es no vacío porque si se toma cualquier $h \in H$ tal que $h \neq 0$ tenemos dos casos. Si $h > 0$ entonces $h \in S$. Si $h < 0$ entonces su inverso $-h$ esta en $S$. El conjunto $S$ por lo tanto es un subconjunto de los números naturales y por la propiedad de buen orden de los números naturales tiene mínino. Sea este mínimo $n$. Queremos ver que $H = n\mathbb{Z}$. Para ello utilizamos el método de la doble contenencia.

- $n\mathbb{Z} \subseteq H$ Esto es cierto porque $n \in H$ luego cualquier multiplo de $n$ también esta en $H$ porque los multiplos son las potencias en el grupo $\mathbb{Z}$.
- $H \subseteq n\mathbb{Z}$ Supongamos por contradicción que no es asi. Entonces existe $h \in H$ tal que $n$ no divide a h. Entonces tomese $d = (n, h)$. Por la identidad de Bezout tenemos que existen $s, t \in \mathbb{Z}$ tales que $(n, h) = ns + ht$. Como $H$ es un subgrupo $ns \in H$ (notación aditiva para $a^s$), $ht \in H$ y $ns + ht \in H$. Por lo tanto $d \in H$.

  Ahora notese que $d < n$. Primero como $d$ divide a $n$ y ambos son positivos entonces $d \leq n$. Pero si $d = n$ entonces $n = (n, h)$ dividiria a $h$ lo cual es una contradicción con nuestra suposición de que $h \notin n\mathbb{Z}$, luego $d < n$. Pero por definición de máximo

común divisor este siempre es mayor a 0. Luego encontramos un elemento más pequeño que $n$ que pertenece a $S$. Esto contradice la minimalidad de $n$. Por lo tanto todos los elementos $h \in H$ deben ser múltiplos de $n$.

14. Si $n > 2$ entonces el grupo alterno $A_n$ esta generado por todos los 3-cíclos.

    En clase se ha demostrado que toda permutación se puede expresar como productos de transposiciones. El grupo alterno $A_n$ es el subgrupo de las permutaciones que se pueden expresar como un producto de un número par de transposiciones. Por lo tanto uno puede descomponer cualquier permutación en $A_n$ como el producto de parejas de transpocisiones $(a\ b)(c\ d)$. Por lo tanto las parejas de transposiciones son generadores de $A$. Ahora si demostramos que cualquier par de transposiciones se puede expresar como producto de 3-cíclos, entonces demostrariamos que los 3-ciclos también son generadores de $A_n$. Debe tenerse en cuenta que ninguno de los elementos que conforme el cíclo pueden ser iguales entre si porque de lo contrario el ciclo quedaria mal definido.

    Entonces tomemos cualquier par de transposiciones $(a\ b)(c\ d)$, como $(a\ b) = (b\ a)$ para cualquier transposición, vamos a suponer sin pérdida de generalidad que $a < b$ y $c < d$. Entonces tenemos los siguiente casos: (Notese que si $a = b$ entonces $(a\ b)$ no seria una transposición).

    - $a, b, c$ y $d$ son diferentes entre sí: Por lo tanto (a b)(c d)=(a b c)(b c d). Y los dos ciclos estan bien definidos.
    - $b = c$: Observece que en este caso $a, b$ y $d$ no son iguales entre sí porque $a < b = c < d$. Entonces sustituyendo $c$ por $b$, $(a\ b)(c\ d) = (a\ b)(b\ d) = (a\ b\ d)$ y este ciclo esta bien definido.
    - $a = c \wedge b = d$: Entonces $(a\ b) = (c\ d)$ y por lo tanto $(a\ b)(c\ d) = (a\ b)(a\ b) = \mathbf{1}$. Pero $\mathbf{1}$ puede escribirse como el producto de cualquier ciclo $(ijk)$ y su inverso $(kji)$.
    - $a = c \wedge b \neq d$: Entonces $(a\ b)(c\ d) = (b\ a)(c\ d) = (b\ a\ d)$ y este ciclo esta bien definido.
    - $a \neq c \wedge b = d$: Entonces $(a\ b)(c\ d) = (a\ b)(d\ c) = (a\ b\ c)$ y este ciclo esta bien definido.
    - $a = d$: En este caso $c \neq b$ porque $c < d = a < b$ Entonces $(a\ b)(c\ d) = (b\ a)(d\ c) = (b\ a\ c)$ y este ciclo esta bien definido.

      Los casos presentados anteriormente son exhaustivos. Por lo tanto los 3-ciclos generan a $A_n$.

15. Para demostrar lo anterior primero demostramos la siguiente proposición.

    **Lema 2.** *En $S_n$, si $k \leq n-2$ entonces los ciclos de tamaño $k$ se pueden escribir como producto de ciclos de tamaño $k+2$.*

*Demostración.* Tomemos cualquier ciclo de orden $k$, $(i_1 \ \cdots \ i_k)$. Ahora tomemos dos elementos $a, b$ tales que $a \neq b$ y $a, b$ diferentes a los elementos en $(i_1 \ \cdots \ i_k)$. Tomemos ahora el siguiente producto de ciclos de orden $k+2$.

$$(i_1 \ \cdots \ i_k \ a \ b)(a \ b \ i_k \ \cdots \ i_1)(i_1 \ \cdots \ i_k \ a \ b)$$

Recordemos que un ciclo se puede expresar como producto de transposiciones de la siguiente manera

$$(r_1 \ \cdots \ r_k) = (r_1 \ r_2)(r_2 \ r_3) \cdots (r_{k-1} \ r_k)$$

Luego podemos reescrbir nuestro producto de la siguiente manera:

$$[(i_1 \ i_2) \cdots (i_{k-1} \ i_k)(i_k \ a)\underline{(a \ b)}][\underline{(a \ b)}(b \ i_k)\underline{(i_k \ i_{k-1}) \cdots (i_2 \ i_1)}][(i_1 \ i_2) \cdots (i_{k-1} \ i_k)\underline{(i_k \ a)}(a \ b)]$$

Podemos ver que las partes de la expresión subrayadas son iguales a $\mathbf{1}$. Luego las podemos borrar y obtenemos

$$(i_1 \ i_2) \cdots (i_{k-1} \ i_k)\underline{(i_k \ a)(b \ i_k)(i_k \ a)}(a \ b)$$

Ahora la parte subrayada es de la forma $(x \ y)(x \ z)(x \ y)$. En clase demostramos que esto es igual a $(y \ z)$ luego se puede cambiar la parte subrayada por $(a \ b)$.

$$(i_1 \ i_2) \cdots (i_{k-1} \ i_k)\underline{(a \ b)(a \ b)}$$

Finalmente vemos que la parte subrayada es de nuevo $\mathbf{1}$. Por lo tanto obtenemos

$$(i_1 \ i_2) \cdots (i_{k-1} \ i_k)$$

que reescribiendolo de nuevo es nuestro ciclo original $(i_1 \ \cdots \ i_k)$. □

Ahora podemos probar facilmente que los ciclos de longitud $n$ impar generan $A_n$ utilizando inducción sobre $k = n - 1/2$. El caso base cuando $k = 1$, es decir $n = 3$ ya lo demostramos en el ejercicio anterior. El paso inductivo es que si los ciclos de longitud $n$ genera a $A_n$ entonces los ciclos de longitud $n+2$ tambien generan a $A_n$ y esto es cierto por lo demostrado en el Lema anterior. Como los ciclos de longitud $n+2$ generan a los ciclos de longitud $n$ y estos a su vez generan a $A_n$ entonces los ciclos de longitud $n+2$ generan a $A_n$.

Igualmente podemos probar que los ciclos de longitud $n$ par generan a $S_n$. Inducción de $k = n/2$. El caso base cuando $k = 1$, es decir $n = 2$ son las transposiciones las cuales ya se demostro en clase que generan a $S_n$. El paso inductivo es que si los ciclos de longitud $n$ genera a $S_n$ entonces los ciclos de longitud $n+2$ tambien generan a $S_n$. De nuevo, como los ciclos de longitud $n+2$ generan a los ciclos de longitud $n$ y estos a su vez generan a $S_n$ entonces los ciclos de longitud $n+2$ generan a $A_n$.

16. Sea $Q_8$ el grupo definido en el punto 2 y sea $H$ el subgrupo $\{\pm 1\}$. Encontrar las clases laterales derechas e izquierdas de $H$ y comparar las dos particiones de $Q_8$ obtenidas

    Partiendo de la tabla de multiplicación de $Q_8$ hallada en el punto 2, podemos ver que las clases izquierdas de $H$ son $H = \{\pm 1\}$, $iH = \{\pm i\}$, $jH = \{\pm j\}$ y , $kH = \{\pm k\}$. Si tomamos ahora las clases laterales izquierdas de nuevo partiendo de la tabla de multiplicación obtendremos $H = \{\pm 1\}$, $Hi = \{\pm i\}$, $Hj = \{\pm j\}$ y , $Hk = \{\pm k\}$. Entonces vemos que las particiones generadas por las clases laterales derechas e izquierdas son identicas. Esto es consecuencia de que $H$ es un subgrupo normal de $Q_8$.

17. Demostrar que un subgrupo $H$ de $G$ de indice 2 es normal.

    *Demostración.* Partiendo de la definición de indice, el subgrupo $H$ genera dos clases laterales izquierdas y dos clases laterales derechas. Una de las clases debe ser $\mathbf{1}H = H = H\mathbf{1}$ que como vemos es una clase lateral tanto izquierda como derecha. Por lo tanto la otra clase lateral (tanto la izquierda como la derecha) debe contener el resto de los elementos de $G$. Asi que probamos que las clases laterales izquierdas son iguales a las clases laterales derechas. Luego $H$ es un subgrupo normal.

    Como corolario podemos afirmar que $A_n$ es subgrupo normal de $S_n$. □

18. *Demostración.* Tomemos cualquier elemento $g \in G$. Queremos probar que $g$ puede expresarse como multiplicación de elementos de $H \cup X$. Entonces tomemos la imagen de $g$, $\pi(g) = gH$. Ahora sabemos que $G/H$ esta generado por $\pi(X)$. En particular $gH$ puede expresarse como producto de elementos en $\pi(X)$. Sea $W$ una expresión de $gH$ como palabra de los elementos de $\pi(X)$. Por nuestra definición de la operación para $G/H$,si tomo cualquier representante dentro de las clases incluidas en $W$ puedo obtener una palabra de $w$ sustituyendo la clases lateral por su respectivo representante y esta palabra representara un elemento en $gH$.

    Sin importar el representante que tome de la clase siempre voy a llegar a una palabra en $gH$, entonces tomemos como representante los elementos que pertenezcan a $X$. Tenemos por lo tanto que $w$ esta formado por elemento de $X$. Pero recordemos que $w \in gH$. Por lo tanto, $w = gh$ para algun $h \in H$. Esto implica que $wh^{-1} = ghh^{-1} = g$ con $h^{-1} \in H$ porque $H$ es subgrupo. Por lo tanto logramos escribir $g$ como producto de elementos de $X$ y $H$. Como $g$ fue cualquier $g \in G, G = <H \cup X>$. □

19. Sea el 4-grupo $V = \{\mathbf{1}; (1\ 2)(3\ 4); (1\ 3)(2\ 4); (1\ 4)(2\ 3)\}$

    I.) Para demostrar que el anterior grupo es un grupo normal vamos a utilizar el siguiente criterio. $H \trianglelefteq G \Leftrightarrow gHg^{-1} = H, \forall g \in G$. Veamos que esto es cierto para un $g$ en particular. Por ejemplo, tomemos $g = (1\ 2) = g^{-1}$ y calculemos todos los productos $gh^{-1}$.

$$(1\ 2)\mathbf{1}(1\ 2) = \mathbf{1}; (1\ 2)(1\ 2)(3\ 4)(1\ 2) = (1\ 2)(3\ 4)$$
$$(1\ 2)(1\ 3)(2\ 4)(1\ 2) = (1\ 4)(2\ 3); (1\ 2)(1\ 4)(2\ 3)(1\ 2) = (1\ 3)(2\ 4)$$

Vemos que para este elemento efectivamente $gHg^{-1} = H$. Ahora veamos que para cualquier transposición en $S_4$ $gHg^{-1} = H$. Para esto calculamos la tabla de conjugación que utilizamos en el punto 8 II), colocando los elementos del subgrupo $V$ en las columnas y las transposiciones en las filas.

| $V_4$ | **1** | **(1 2)(3 4)** | **(1 3)(2 4)** | **(1 4)(2 3)** |
|---|---|---|---|---|
| **(1 2)** | 1 | (1 2)(3 4) | (1 4)(2 3) | (1 3)(2 4) |
| **(1 3)** | 1 | (1 4)(2 3) | (1 3)(2 4) | (1 2)(3 4) |
| **(1 4)** | 1 | (1 3)(2 4) | (1 2)(3 4) | (1 4)(2 3) |
| **(2 3)** | 1 | (1 3)(2 4) | (1 2)(3 4) | (1 4)(2 3) |
| **(2 4)** | 1 | (1 4)(2 3) | (1 3)(2 4) | (1 2)(3 4) |
| **(3 4)** | 1 | (1 2)(3 4) | (1 4)(2 3) | (1 3)(2 4) |

Entonces vemos que en todas las filas de la tabla aparecen los elementos de $V$ en diferente orden. Por lo tanto para cualquier transposición $gHg^{-1} = H$.

Ahora podemos probar que $gHg^{-1} = H$ para cualquier $g$. Esto es posible porque $g$ puede expresarse como producto de transposiciones. Además si $g = t_1 t_2 \cdots t_n$, donde $t_i$ son transposiciones en $S_4$; $\forall i : 1 \leq i \leq n$, entonces $g^{-1} = t_n t_{n-1} \cdots t_1$. Entonces, $gHg^{-1}$ lo podemos escribir de la siguiente manera.

$$t_1 t_2 \cdots t_{n-1} \underline{t_n H t_n} t_{n-1} \cdots t_2 t_1$$

Pero ya demostramos que la parte subrayada es igual a $H$. Luego la podemos sustituir por $H$.

$$t_1 t_2 \cdots \underline{t_{n-1} H t_{n-1}} \cdots t_2 t_1$$

Si repetimos este proceso $n$ veces obtendremos al final que $gHg^{-1} = H$.

II.) Demostrar que $<(1\ 2)(3\ 4)>$ es subgrupo normal de $V$ pero no de $S_4$.

$(1\ 2)(3\ 4)^2 = \mathbf{1}$. Por lo tanto $<(1\ 2)(3\ 4)> = \{\mathbf{1}, (1\ 2)\}$. Ahora si construimos una tabla de conjugación que tenga los elementos de $V$ en las filas y los elementos de $<(1\ 2)(3\ 4)>$ obtenemos:

| $<(1\ 2)(3\ 4)>$ | **1** | **(1 2)(3 4)** |
|---|---|---|
| **1** | 1 | (1 2)(3 4) |
| **(1 2)(3 4)** | 1 | (1 2)(3 4) |
| **(1 3)(2 4)** | 1 | (1 2)(3 4) |
| **(1 4)(2 3)** | 1 | (1 2)(3 4) |

Como vemos las filas son iguales a $<(1\ 2)(3\ 4)>$ por lo tanto $<(1\ 2)(3\ 4)>$ es subgrupo de $V$. Ahora para demostrar que $<(1\ 2)(3\ 4)>$ no es subgrupo normal de $S_4$ busquemos un contraejemplo. Tomemos por ejemplo $g = (1\ 3)$. En este caso vemos que $(1\ 3)\mathbf{1}(1\ 3) = \mathbf{1}$ y $(1\ 3)(1\ 2)(3\ 4)(1\ 3) = (1\ 4)(2\ 3)$. Por lo tanto, $(1\ 3)H(1\ 3)$ es diferente a $H$ y $H$ no es un subgrupo normal de $S_4$.

20. I). *Demostración.* Partamos del hecho que si $H$ y $K$ son subgrupos de $G$, entonces $H \cap K$ es un subgrupo de $G$. Además es subgrupo tanto de $H$ como de $K$. Ahora por el teorema de Lagrange tenemos que el orden de $H \cap K$ debe dividir tanto a $|H|$ como a $|K|$, entonces $|H \cap K|$ dede ser menor o igual a $(|H|, |K|)$. Pero $(|H|, |K|) = 1$ por nuestra suposición. Luego $|H \cap K| = 1$, es decir $H \cap K$ es el subgrupo trivial $\{\mathbf{1}\}$. □

II). Tomemos un subgrupo $K < G$ de cardinalidad $|H|$. Ahora tomemos la imagen de $K$ sobre $G/H$ por la aplicación natural $\pi$. Sea este conjunto $\pi(K)$.

$\pi(K)$ es un subgrupo de $G/H$. En primer lugar la clase $H$ esta incluida en $\pi(K)$ porque $\mathbf{1} \in K$ y $\pi(1) = H$. Tomemos un elemento $\bar{k} \in \pi(K)$. Por lo tanto existe un elemento $k \in K$ tal que $\pi(k) = \bar{k}$ .

Ahora tomemos el elemento $k^{-1} \in K$ porque $K$ es subgrupo y tomemos $\pi(k^{-1})$.

Como $\pi$ es un homomorfismo tenemos que $\pi(k)\pi(k^{-1}) = \pi(kk^{-1}) = \pi(1) = H$. Por lo tanto $\bar{k}$ tiene inverso.Ahora si tomamos dos elementos cualquiera en $\pi(K)$, por ejemplo, $\bar{a}, \bar{b}$. Tenemos que existen $a, b \in K$ tales que $\bar{a} = \pi(a)$ y $\bar{b} = \pi(b)$. Por lo tanto, $\bar{a}\bar{b} = \pi(a)\pi(b) = \pi(ab)$ y $\pi(ab) \in \pi(K)$ porque $ab \in K$.

Ahora como $\pi(K)$ es subgrupo de $G/H$ tenemos que $|\pi(K)|$ debe dividir a $|G/H| = [G : H]$ por el teorema de Lagrange.

Por otra parte, utilizando el primer teorema de isomorfismo tenemos que $|K/\ker(\pi)| = |\pi(K)|$. El núcleo de $\pi$ en el dominio $K$ es $K \cap H$ que también es un grupo normal por lo demostrado en clase. Por lo tanto $K/\ker(\pi) = K/K \cap H$. De nuevo por el teorema de Lagrange tenemos que $|K/K \cap H| = |K|/|K \cap H|$. Por lo tanto $|K|/|K \cap H| = |\pi(K)|$. Es decir, $|K| = |\pi(K)||K \cap H|$, es decir $|\pi(K)|$ divide a $|K| = |H|$.

Recapitulando, tenemos que $|\pi(K)|$ divide a $[H : G]$ y a $|H|$. Pero $([G : H], |H|) = 1$, luego $|\pi(K)| = 1$. Esto implica que el grupo $\pi(K)$ debe ser igual a $H$. Lo anterior implica además que $K \subseteq H$. Pero como $|K| = |H|$ y son finitos, $K$ debe ser igual a $H$.