Algunos Ejercicios Resueltos para C3.

Profesor: María Leonor Varas
Auxiliares: Sebastian Astroza & Diego Morán

P1 Sea $A \subseteq \mathbb{C}^4$ definido por:

$$A = \{(z_1, z_2, -\overline{z_2}, \overline{z_1}) \ / \ z_1, z_2 \in \mathbb{C}\}$$

Definamos las siguientes operaciones de $A \times A$ en A:

$$(a,b,c,d) \oplus (e,f,g,h) = (a+e\,,\, b+f\,,\, c+g\,,\, d+h)$$
$$(a,b,c,d) \odot (e,f,g,h) = (ae+bg\,,\, af+bh\,,\, ce+dg\,,\, cf+dh)$$

(a) Demuestre que $(A, \oplus, \odot)$ es un anillo no conmutativo con unidad $(1,0,0,1)$
(b) Verifique que $(A\backslash\{0_\oplus\}, \odot)$ es un grupo (donde $0_\oplus$ es el neutro de $\oplus$ en A)

Sol: (a) Para demostrar que $(A, \oplus, \odot)$ es un anillo debemos verificar 4 cosas:

(i) $\oplus$ y $\odot$ son cerradas en A
(ii) $\odot$ distribuye sobre $\oplus$
(iii) $\odot$ asocia
(iv) $(A, \oplus)$ es un grupo abeliano

Demostrémoslas!

Dem(i) Vamos a tomar dos elementos de A y probaremos que la suma circulito ($\oplus$) y la multiplicación circulito ($\odot$)de esos elementos pertenecen a A (de esta manera demostraríamos que las operaciones son cerradas en el conjunto que estamos trabajando).

Sean $a, b \in A$. Por definición del conjunto A sabemos que existen $z_1, z_2, z_3, z_4 \in \mathbb{C}$ tales que:

$$a = (z_1, z_2, -\overline{z_2}, \overline{z_1}) \ \wedge \ b = (z_3, z_4, -\overline{z_4}, \overline{z_3})$$

Veamos que $a \oplus b \in A$:

$$a \oplus b = (z_1, z_2, -\overline{z_2}, \overline{z_1}) \oplus (z_3, z_4, -\overline{z_4}, \overline{z_3}) = (z_1 + z_3, z_2 + z_4, -\overline{z_2} - \overline{z_4}, \overline{z_1} + \overline{z_3})$$

Y usando una de las tantas propiedades del conjugado (el conjugado de la suma es la suma de los conjugados) se tiene que:

$$a \oplus b = (z_1 + z_3, z_2 + z_4, -\overline{z_2 + z_4}, \overline{z_1 + z_3})$$

Y bautizando dos nuevas variables como $z_5 = z_1 + z_3$ y $z_6 = z_2 + z_4$ concluimos que:

$$a \oplus b = (z_5, z_6, -\overline{z_6}, \overline{z_5})$$

con $z_5, z_6 \in \mathbb{C}$.

Por lo tanto $a \oplus b \in A$

Ahora veamos que $a \odot b \in A$:

$$\begin{aligned} a \odot b &= (z_1, z_2, -\overline{z_2}, \overline{z_1}) \odot (z_3, z_4, -\overline{z_4}, \overline{z_3}) \\ &= (z_1 z_3 + z_2(-\overline{z_4}),\ z_1 z_4 + z_2 \overline{z_3},\ -\overline{z_2} z_3 + \overline{z_1}(-\overline{z_4}),\ -\overline{z_2} z_4 + \overline{z_1 z_3}) \\ &= (z_1 z_3 - z_2 \overline{z_4},\ z_1 z_4 + z_2 \overline{z_3},\ -\overline{z_2 \overline{z_3}} - \overline{z_1 z_4},\ -\overline{z_2 \overline{z_4}} + \overline{z_1 z_3}) \\ &= (z_1 z_3 - z_2 \overline{z_4},\ z_1 z_4 + z_2 \overline{z_3},\ -\overline{z_1 z_4 + z_2 \overline{z_3}},\ \overline{z_1 z_3 - z_2 \overline{z_4}}) \end{aligned}$$

Y bautizando dos nuevas variables como $z_7 = z_1 z_3 - z_2 \overline{z_4}$ y $z_8 = z_1 z_4 + z_2 \overline{z_3}$ concluimos que:

$$a \odot b = (z_7, z_8, -\overline{z_8}, \overline{z_7})$$

con $z_7, z_8 \in \mathbb{C}$.

Por lo tanto $a \odot b \in A$

Dem(ii) Para demostrar que $\odot$ distribuye sobre $\oplus$ debemos ver que:

$$\forall u, v, w \in A \quad u \odot (v \oplus w) = (u \odot v) \oplus (u \odot w)$$

y además, como no sabemos si $\odot$ conmuta debemos probar también que:

$$(v \oplus w) \odot u = (v \odot u) \oplus (w \odot u)$$

Por efectos de ahorro de tinta y papel (ya saben... pobres arbolitos) vamos a probar solo la primera igualdad. La segunda queda de tarea para ustedes.

Sean $u, v, w \in A$. Sabemos que los podemos escribir de la siguiente forma: $u = (a, b, c, d)$, $v = (e, f, g, h)$ y $w = (j, k, m, n)$.

Notemos que:

$u \odot (v \oplus w) = (a, b, c, d) \odot [(e, f, g, h)) \oplus (j, k, m, n)]$

$= (a, b, c, d) \odot (e + j, f + k, g + m, h + n)$

$= (a(e+j)+b(g+m), a(f+k)+b(h+n), c(e+j)+d(g+m), c(f+k)+d(h+n))$

$= (ae+aj+bg+bm\,,\, af+ak+bh+bn\,,\, ce+cj+dg+dm\,,\, cf+ck+dh+dn)$

$= (ae+bg\,,\, af+bh\,,\, ce+dg\,,\, cf+dh) \oplus (aj+bm\,,\, ak+bn\,,\, cj+dm\,,\, ck+dn)$

$= [(a, b, c, d) \odot (e, f, g, h)] \oplus [(a, b, c, d) \odot (j, k, m, n)]$

$= (u \odot v) \oplus (u \odot w)$

Por lo tanto:

$$u \odot (v \oplus w) = (u \odot v) \oplus (u \odot w)$$

Notemos que esta demostración de distributividad es aplicable no sólo para A, sino que para todo $\mathbb{C}^4$ (recuerde que $A \subseteq \mathbb{C}^4$)

Dem(iii) Debemos demostrar que $\odot$ asocia. En otras palabras, debemos demostrar que:

$$\forall u, v, w \in A \;\; u \odot (v \odot w) = (u \odot v) \odot w$$

Nuevamente haremos una demostración más general que la pedida (similar a la parte anterior)

Sean $u, v, w \in A$. Sabemos que los podemos escribir de la siguiente forma: $u = (a, b, c, d)$, $v = (e, f, g, h)$ y $w = (j, k, m, n)$.

Notemos que:

$(u \odot v) \odot w = [(a, b, c, d) \odot (e, f, g, h))] \odot (j, k, m, n)$

$= (ae + bg, af + bh, ce + dg, cf + dh) \odot (j, k, m, n)$

$= ((ae + bg)j + (af + bh)m\ ,\ (ae + bg)k + (af + bh)n\ ,\ (ce + dg)j + (cf + dh)m\ ,\ (ce + dg)k + (cf + dh)n)$

$= (a(ej+fm)+b(gj+hm)\ ,\ a(ek+fn)+b(gk+hn)\ ,\ c(ej+fm)+d(gj+hm)\ ,\ c(ek+fn)+d(gk+hn))$

$= (a,b,c,d) \odot (ej+fm\ ,\ ek+fn\ ,\ gj+hm\ ,\ gk+hn)$

$= (a,b,c,d) \odot [(e,f,g,h) \odot (j,k,m,n)]$

$= u \odot (v \odot w)$

Por lo tanto:

$$u \odot (v \odot w) = (u \odot v) \odot w$$

Que es lo que queríamos demostrar.

Dem(iv) Ahora debemos ver que $(A, \oplus)$ es un grupo abeliano. Para ello tenemos que verificar lo siguiente:

(*) $\oplus$ es cerrada en A
(**) $\oplus$ asocia
(***) $\oplus$ conmuta
(****) Existe neutro en A para $\oplus$
(*****) Todo elemento en A tiene un inverso (para $\oplus$) que también está en A.

Dem(*) Ya lo demostramos en la parte **(a).i**

Dem(**) Propuesto para el estudiante. De todas maneras es algo directo de la asociatividad de la suma en los complejos (de hecho debiera salirles mental).

Dem(***) Propuesto. Casi directo de la conmutatividad de la suma en los complejos.

Dem(****) Debemos demostrar lo siguiente:

$$(\exists e \in A)\ \ (\forall u \in A)\ \ e \oplus u = u \oplus e = u$$

Nuestro candidato a neutro es $e = (0,0,0,0)$ (por razones obvias no?). Como es nuestro único candidato estamos obligados a hacerlo ganar. Así que verifiquemos que es el neutro!

Sea $u \in A$. Sabemos que existen $z_1, z_2 \in \mathbb{C}$ tal que $u = (z_1, z_2, -\overline{z_2}, \overline{z_1})$. Por lo tanto:

$$\begin{aligned} e \oplus u &= (0,0,0,0) \oplus (z_1, z_2, -\overline{z_2}, \overline{z_1}) \\ &= (0 + z_1, 0 + z_2, 0 - \overline{z_2}, 0 + \overline{z_1} + 0) \\ &= (z_1, z_2, -\overline{z_2}, \overline{z_1}) \\ &= u \end{aligned}$$

Y por otro lado, como $\oplus$ conmuta :

$$\begin{aligned} u \oplus e &= e \oplus u \\ &= u \end{aligned}$$

Y por último... como un chequeo de sanidad mental... debemos verificar que $(0,0,0,0) \in A$. Pero eso es bastante fácil de ver, ya que tomando $z_3 = z_4 = 0$ se tiene que:

$$(0,0,0,0) = \underbrace{(0,0,-\overline{0},\overline{0})}_{\forall r \in \mathbb{R} \;\; \overline{r} = r} = (z_3, z_4, -\overline{z_4}, \overline{z_3})$$

Como $z_3 = z_4 = 0 \in \mathbb{C}$, podemos deducir que $(0,0,0,0) \in A$.

Dem(*****) Lo que hay que demostrar es:

$$(\forall u \in A) \;\; (\exists v \in A) \;\; u \oplus v = v \oplus u = e = (0,0,0,0)$$

Sea $u \in A$. Sabemos que existen $z_1, z_2 \in \mathbb{C}$ tal que $u = (z_1, z_2, -\overline{z_2}, \overline{z_1})$.

Nuestro candidato a inverso será $v = (-z_1, -z_2, \overline{z_2}, -\overline{z_1})$. Claramente es el inverso, ya que cada componente de v es el inverso aditivo de cada componente de u. Pruebe usted mismo las igualdades de más arriba (si es que todavía desconfía).

Hasta ahora hemos demostrado que $(A, \oplus, \odot)$ es un anillo. Nos falta ver que NO es conmutatitivo y que tiene unidad $= (1,0,0,1)$.

Claramente no es conmutativo ya que considerando z_1, z_2, z_3 y z_4 complejos distintos, podemos construir dos elementos a y b de A de la forma siguiente:

$$a = (z_1, z_2, -\overline{z_2}, \overline{z_1}) \;\wedge\; b = (z_3, z_4, -\overline{z_4}, \overline{z_3})$$

Notemos que:

$$\begin{aligned} a \odot b &= (z_1, z_2, -\overline{z_2}, \overline{z_1}) \odot (z_3, z_4, -\overline{z_4}, \overline{z_3}) \\ &= (z_1 z_3 + z_2(-\overline{z_4})\,,\; z_1 z_4 + z_2 \overline{z_3}\,,\; -\overline{z_2} z_3 + \overline{z_1}(-\overline{z_4})\,,\; -\overline{z_2} z_4 + \overline{z_1 z_3}) \end{aligned}$$

Y además:

$$\begin{aligned} b \odot a &= (z_3, z_4, -\overline{z_4}, \overline{z_3}) \odot (z_1, z_2, -\overline{z_2}, \overline{z_1}) \\ &= (z_3 z_1 + z_4(-\overline{z_2})\,,\; z_3 z_2 + z_4 \overline{z_1}\,,\; -\overline{z_4} z_1 + \overline{z_3}(-\overline{z_2})\,,\; -\overline{z_4} z_2 + \overline{z_3 z_1}) \end{aligned}$$

De esta manera podemos ver que $b \odot a$ no tiene porque ser igual a $a \odot b$.

Y ya casi para terminar notemos que $(1, 0, 0, 1)$ es la unidad del anillo $(A, \oplus, \odot)$ ya que $\forall z_1, z_2 \in \mathbb{C}$ se tiene:

$$\begin{aligned} (1, 0, 0, 1) \odot (z_1, z_2, -\overline{z_2}, \overline{z_1}) &= (1z_1 + 0(-\overline{z_2}), 1z_2 + 0\overline{z_1}, 0z_1 + 1(-\overline{z_2}), 0z_2 + 1\overline{z_1}) \\ &= (z_1, z_2, -\overline{z_2}, \overline{z_1}) \end{aligned}$$

Osea, $(1, 0, 0, 1)$ es el neutro para $\odot$ en A. Además es distinto del neutro de la adición ($\oplus$), condiciones suficientes para que hablemos de *unidad* en el anillo.

(b) Debemos ver que $(A \backslash \{0_\oplus\}, \odot)$ es un grupo. Para ello tenemos que verificar lo siguiente:

(*) $\odot$ es cerrada en $A \backslash \{0_\oplus\}$
(**) $\odot$ asocia
(***) Existe neutro en $A \backslash \{0_\oplus\}$ para $\odot$
(****) Todo elemento en $A \backslash \{0_\oplus\}$ tiene un inverso (para $\odot$) que también está en A.

(*), (**) y (***) puede demostrarlas facilmente si se inspira en la parte **(a)**.

Para demostrar (****) debemos verificar que:

$$(\forall a \in A \backslash \{0_\oplus\}) \;\; (\exists b \in A \backslash \{0_\oplus\}) \;\; a \odot b = e_\odot$$

Donde $0_\oplus = (0, 0, 0, 0)$ y $e_\odot = (1, 0, 0, 1)$.

Demostrémoslo!

Sea $a \in A\backslash\{0_\oplus\}$. Debemos encontrar $b \in A\backslash\{0_\oplus\}$ tal que $a \odot b = (1,0,0,1)$. Como $a \in A\backslash\{0_\oplus\}$ podemos decir que es de la forma: $(z_1, z_2, -\overline{z_2}, \overline{z_1})$ con z_1, z_2 complejos no nulos. Si consideramos $b = (e, f, g, h)$ podemos ver que:

$$\begin{aligned} & a \odot b = (1,0,0,1) \\ \Leftrightarrow\ & (z_1, z_2, -\overline{z_2}, \overline{z_1}) \odot (e, f, g, h) = (1,0,0,1) \\ \Leftrightarrow\ & (z_1 e + z_2 g, z_1 f + z_2 h, -\overline{z_2} e + \overline{z_1} g, -\overline{z_2} f + \overline{z_1} h) = (1,0,0,1) \end{aligned}$$

Lo que equivale a resolver el siguiente sistema de ecuaciones:

$$z_1 e + z_2 g = 1 \tag{1}$$

$$z_1 f + z_2 h = 0 \tag{2}$$

$$-\overline{z_2} e + \overline{z_1} g = 0 \tag{3}$$

$$-\overline{z_2} f + \overline{z_1} h = 1 \tag{4}$$

Despejemos g de la ecuación (3).

$$\begin{aligned} & -\overline{z_2} e + \overline{z_1} g = 0 \\ \Leftrightarrow\ & \overline{z_1} g = \overline{z_2} e \\ \Leftrightarrow\ & g = \frac{\overline{z_2} e}{\overline{z_1}} \end{aligned}$$

Pero recordando que $\forall z \in \mathbb{C}\ \ z^{-1} = \frac{1}{z} = \frac{\overline{z}}{|z|^2}$

$$\Leftrightarrow g = \frac{\overline{z_2} e z_1}{|z_1|^2}$$

Reemplazando este valor en (1) se tiene:

$$\begin{aligned} & z_1 e + z_2 \frac{\overline{z_2} e z_1}{|z_1|^2} = 1 \\ \Leftrightarrow\ & z_1 e + \frac{|z_2|^2}{|z_1|^2} z_1 e = 1 \end{aligned}$$

(Recuerde que $z\overline{z} = |z|^2$)

$$\Leftrightarrow z_1 e (1 + \frac{|z_2|^2}{|z_1|^2}) = 1$$

$$\Leftrightarrow z_1 e = \frac{|z_1|^2}{|z_1|^2 + |z_2|^2}$$

$$\Leftrightarrow e = \frac{|z_1|^2}{|z_1|^2 + |z_2|^2} \frac{\overline{z_1}}{|z_1|^2} = \frac{\overline{z_1}}{|z_1|^2 + |z_2|^2}$$

Y con este resultado podemos encontrar g.

$$g = \frac{\overline{z_2} e z_1}{|z_1|^2} = \frac{\overline{z_2} \frac{\overline{z_1}}{|z_1|^2 + |z_2|^2} z_1}{|z_1|^2} = \frac{\overline{z_2}}{|z_1|^2 + |z_2|^2}$$

Casi de manera análoga (pero usando las ecuaciones (2) y (4)) podemos ver que:

$$f = \frac{-z_2}{|z_1|^2 + |z_2|^2} = -\overline{g}$$

y además:

$$h = \frac{z_1}{|z_1|^2 + |z_2|^2} = \overline{e}$$

Por lo tanto encontramos el inverso de a. Ese inverso sería:

$$b = (\frac{\overline{z_1}}{|z_1|^2 + |z_2|^2}, \frac{-z_2}{|z_1|^2 + |z_2|^2}, \frac{\overline{z_2}}{|z_1|^2 + |z_2|^2}, \frac{z_1}{|z_1|^2 + |z_2|^2})$$

Puede usted verificar (muy sencillamente) que $b \in A \backslash \{0_\oplus\}$

P2 (a) Pruebe que $\forall z \in \mathbb{C}$ con $|z| = 2$ se cumple que:

$$2 \leq |z - 4| \leq 6$$

(b) Pruebe que:

$$\frac{1 + sen(\theta) + icos(\theta)}{1 + sen(\theta) - icos(\theta)} = sen(\theta) + icos(\theta)$$

y deduzca que:

$$\left(1 + sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})\right)^7 - i\left(1 + sen(\frac{\pi}{7}) - icos(\frac{\pi}{7})\right)^7 = 0$$

Sol: (a) Sea $\forall z \in \mathbb{C}$ con $|z| = 2$. Si escribimos $z = a + ib$ podemos ver que:

$$\begin{aligned} & |z| = 2 \\ \Leftrightarrow & \sqrt{a^2 + b^2} = 2 \\ \Leftrightarrow & a^2 + b^2 = 4 \\ \Leftrightarrow & a^2 = 4 - \underbrace{b^2}_{\geq 0} \\ \Rightarrow & a^2 \leq 4 \\ \Rightarrow & |a| \leq 2 \\ \Leftrightarrow & -2 \leq a \leq 2 \end{aligned}$$

Estas desigualdades las ocuparemos en un rato más (así que guárdelas en su memoria).

Ahora veamos que:

$$\begin{aligned} |z - 4| &= |a + ib - 4| = |(a - 4) + ib| = \sqrt{(a - 4)^2 + b^2} \\ &= \sqrt{a^2 - 8a + 16 + b^2} = \sqrt{a^2 + b^2 - 8a + 16} = \sqrt{4 - 8a + 16} \\ &= 2\sqrt{5 - 2a} \end{aligned}$$

Y utilizando las desigualdades que usted tiene en su memoria deducimos que:

$$2 \leq |z - 4| \leq 6$$

(b) Note que si llamamos $z = 1 + sen(\theta) + icos(\theta)$ tenemos que:

$$\frac{1 + sen(\theta) + icos(\theta)}{1 + sen(\theta) - icos(\theta)} = \frac{z}{\overline{z}}$$

Recordando que $\forall v \in \mathbb{C} \;\; v^{-1} = \frac{1}{v} = \frac{\overline{v}}{|v|^2}$ podemos ver que:

$$\frac{z}{\overline{z}} = \frac{z^2}{|z|^2}$$

Luego:

$$\begin{aligned}
\frac{1 + sen(\theta) + icos(\theta)}{1 + sen(\theta) - icos(\theta)} &= \frac{(1 + sen(\theta) + icos(\theta))^2}{|1 + sen(\theta) + icos(\theta)|^2} \\
&= \frac{(1 + sen(\theta))^2 + 2i(1 + sen(\theta))cos(\theta) - cos(\theta)^2}{(1 + sen(\theta))^2 + cos(\theta)^2} \\
&= \frac{1 + 2sen(\theta) + sen(\theta)^2 + 2i(1 + sen(\theta))cos(\theta) - cos(\theta)^2}{1 + 2sen(\theta) + sen(\theta)^2 + cos(\theta)^2}
\end{aligned}$$

Recordando que $sen(\theta)^2 + cos(\theta)^2 = 1$ y $1 - cos(\theta)^2 = sen(\theta)^2$ se tiene que:

$$\begin{aligned}
\frac{1 + sen(\theta) + icos(\theta)}{1 + sen(\theta) - icos(\theta)} &= \frac{2sen(\theta)^2 + 2sen(\theta) + 2i(1 + sen(\theta))cos(\theta)}{2(1 + sen(\theta))} \\
&= \frac{2sen(\theta)(1 + sen(\theta)) + 2i(1 + sen(\theta))cos(\theta)}{2(1 + sen(\theta))} \\
&= sen(\theta) + icos(\theta)
\end{aligned}$$

Demostrar la otra igualdad se hace utilizando lo que acabamos de demostrar con $\theta = \frac{\pi}{7}$. Osea:

$$\frac{1 + sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})}{1 + sen(\frac{\pi}{7}) - icos(\frac{\pi}{7})} = sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})$$

Elevando a la septima esa ecuación se tiene:

$$\frac{\left(1 + sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})\right)^7}{\left(1 + sen(\frac{\pi}{7}) - icos(\frac{\pi}{7})\right)^7} = \left(sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})\right)^7$$

Pero:

$$\begin{aligned}
\left(sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})\right)^7 &= \left(cos(\frac{\pi}{2} - \frac{\pi}{7}) + isen(\frac{\pi}{2} - \frac{\pi}{7})\right)^7 \\
&= \left(cos(\frac{5\pi}{14}) + isen(\frac{5\pi}{14})\right)^7
\end{aligned}$$

Ya estamos casi listos[1] , ahora falta recordar la bendita fórmula de De Moivre: $(cos(\theta) + isen(\theta))^n = cos(n\theta) + isen(n\theta)$

$$\begin{aligned}\left(sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})\right)^7 &= \left(cos(\frac{5\pi}{2}) + isen(\frac{5\pi}{2})\right) \\ &= 0 + 1i \\ &= i\end{aligned}$$

Luego es realmente fácil concluir que:

$$\left(1 + sen(\frac{\pi}{7}) + icos(\frac{\pi}{7})\right)^7 - i\left(1 + sen(\frac{\pi}{7}) - icos(\frac{\pi}{7})\right)^7 = 0$$

[1]Si le resulta demasiado mágico esto de escribir $sen(\frac{\pi}{7})$ como $sen(\frac{\pi}{2} - \frac{\pi}{7})$ puede intentar factorizar y ocupar la paridad del coseno y la imparidad del seno.

P3 Sea $(G, *)$ un grupo, de neutro e. Dado $A \subseteq G$ se define:

$$\langle A \rangle = \bigcap_{H \text{ subgrupo de } G,\ A \subseteq H} H = \{g \in G \ / \ \forall\ H \text{ subgrupo de } G,\ A \subseteq H\ ,\ g \in H\}$$

$\langle A \rangle$ se llama el subgrupo de G generado por A.

a) Demuestre que $\langle A \rangle$ es el subgrupo más pequeño que contienen a A, es decir, pruebe que:

a.1) $A \subseteq \langle A \rangle$.

a.2) $\langle A \rangle$ es subgrupo.

a.3) Si $W \subseteq G$, subgrupo y $A \subseteq W$ entonces $\langle A \rangle \subseteq W$.

b) Pruebe que:

$$\langle A \rangle = \{a_1^{m_1} * \cdots * a_n^{m_n} \ / \ n \in I\!N,\ a_i \in A,\ m_i \in \mathbb{Z},\ \forall i = 1, \ldots, n\}$$

c) Muestre que:

$$\langle A \rangle = A \Leftrightarrow A \textit{ es subgrupo.}$$

Concluya que $\langle \langle A \rangle \rangle = \langle A \rangle$.

Sol: a) a.1) Si $a \in A$ entonces claramente $a \in H,\ \forall\ H$ *subgrupo de* $G,\ A \subseteq H$, lo que prueba que

$$A \subseteq \langle A \rangle$$

a.2) Lo primero que hay que verificar siempre es que, efectivamente, $\langle A \rangle \subseteq G$. En nuestro caso, esto es claro de la definición, pues $\langle A \rangle$ es una intersección de subconjuntos de G, por lo tanto $\langle A \rangle$ es subconjunto de G.

Para ver que es subgrupo, usemos la forma compacta, debemos entonces probar 2 cosas:

1. $\langle A \rangle \neq \emptyset$:

Recordemos que si H es subgrupo, entonces $e \in H$, luego es trivial ver que $e \in H,\ \forall\ H \subseteq G,\ H$ *subgrupo*, $A \subseteq H$, por lo que:

$$e \in \bigcap_{H \text{ subgrupo de } G,\ A \subseteq H} H$$

Así, hemos probado que $\langle A \rangle$ tiene al menos un elemento.

2. $\forall\ a_1,\ a_2 \in \langle A\rangle\ ,\ a_1 * a_2^{-1} \in \langle A\rangle$:

Sean $a_1,\ a_2 \in \langle A\rangle$, luego, por definición de este conjunto, obtenemos:

$$a_1,\ a_2 \in H\ \forall\ H\ subgrupo\ de\ G,\ A \subseteq H$$

Lo que implica, dado que si H subgrupo existen los inversos, que:

$$a_1,\ a_2^{-1} \in H\ \forall\ H\ subgrupo\ de\ G,\ A \subseteq H$$

Usando ahora que si H es subgrupo, entonces es cerrado para la operación se tiene:

$$a_1 * a_2^{-1} \in H\ \forall\ H\ subgrupo\ de\ G,\ A \subseteq H$$

Lo que es equivalente, por definición, a:

$$a_1 * a_2^{-1} \in \langle A\rangle$$

En conclusión, $\langle A\rangle$ es subgrupo de G.

a.3) Sea $W \subseteq G$ subgrupo, tal que $A \subseteq W$. Debemos ver que $\langle A\rangle \subseteq W$.

Recordemos que:

$$\langle A\rangle = \bigcap_{H\ subgrupo\ de\ G,\ A\subseteq H} H$$

Claramente, como W forma parte de los conjuntos que se están intersectando en el lado izquierdo de la igualdad, se tiene:

$$\bigcap_{H\ subgrupo\ de\ G,\ A\subseteq H} H \subseteq W$$

Esto prueba que $\langle A\rangle \subseteq W$.

b) Denotemos $C = \{a_1^{m_1} * \cdots * a_n^{m_n}\ /\ n \in I\!N,\ a_i \in A,\ m_i \in \mathbb{Z}, \forall\ i = 1, \ldots, n\}$

Veremos primero que C es subgrupo de G.
Claramente, $C \subseteq G$, pues C contiene a elementos de A (luego elementos de G) operados entre sí o con sus inversos, y por ser grupo, todos los resultados de estas operaciones quedan dentro del conjunto G.

1. $C \neq \emptyset$:
Dado $a \in A$, tomando $n = 2,\ m_1 = 1,\ m_2 = -1,\ y\ a_1 = a_2 = a$, vemos que $e = a * a^{-1} \in C$.

Por lo tanto, $C \neq \emptyset$.

2. $\forall\ c_1,\ c_2 \in C,\ c_1 * c_2^{-1} \in C$:

Si $c_1,\ c_2 \in C$, existen $n, l \in \mathbb{N};\ m_1, \ldots, m_n,\ p_1, \ldots p_l \in \mathbb{Z},\ a_1, \ldots a_n, \in A$, $b_1, \ldots, b_l \in A$ tales que:

$$c_1 = a_1^{m_1} * \cdots * a_n^{m_n}$$

$$c_2 = b_1^{p_1} * \cdots * b_l^{p_l}$$

Con esto, y recordando que, en general, $(a * b)^{-1} = b^{-1} * a^{-1}$, podemos escribir:

$$c_2^{-1} = b_l^{-p_l} * \cdots * b_1^{-p_1}$$

Calculemos,

$$\begin{array}{rcl} c & = & c_1 * c_2^{-1} \\ & = & (a_1^{m_1} * \cdots * a_n^{m_n}) * (b_l^{-p_l} * \cdots * b_1^{-p_1}) \\ & = & a_1^{m_1} * \cdots * a_n^{m_n} * b_l^{-p_l} * \cdots * b_1^{-p_1} \end{array}$$

Inspirándonos en la última igualdad, si tomamos $k = n + l,\ r_1 = m_1, \ldots, r_n = m_n,\ r_{n+1} = p_1, \ldots, r_{n+l} = p_l;\ d_1 = a_1, \ldots, d_n = a_n,\ d_{n+1} = b_1, \ldots, d_{n+l} = b_l$, se obtiene:

$$c = d_1^{r_1}, \ldots, d_k^{r_k}$$

Lo que nos dice que $c \in C$, que es lo que queríamos probar.

Se concluye así que C es subgrupo de G.

Por otro lado, $A \subseteq C$, en efecto:
Si $a \in A$, entonces tomando $n = 1,\ m_1 = 1\ y\ a_1 = a$ deducimos que $a \in C$.

Probemos ahora la igualdad de conjuntos que nos piden:

- $\subseteq$ De lo hecho anteriormente tenemos que C *subgrupo de* $G,\ A \subseteq C$, entonces, por lo visto en la parte A):

$$\langle A \rangle \subseteq C$$

- $\supseteq$ Sea H talque H *subgrupo de* $G,\ A \subseteq H$.
  Usando que H es un subgrupo que contiene a los elementos de A, deducimos que $\forall n \in \mathbb{N},\ a_1, \ldots, a_n \in A,\ m_1 \ldots, m_n \in \mathbb{Z}$:

$$a_1^{m_1} * \cdots * a_n^{m_n} \in H$$

Lo que implica, por definición de intersección de conjuntos y ya que lo anterior fue para H cualquiera, que $\forall\ n \in \mathbb{N},\ a_1, \ldots, a_n \in A,\ m_1 \ldots, m_n \in \mathbb{Z}$:

$$a_1^{m_1} * \cdots * a_n^{m_n} \in \bigcap_{H\ subgrupo\ de\ G,\ A \subseteq H} H$$

Así, usando un poco de imaginación, concluimos que $C \subseteq \langle A \rangle$.

c) Probemos la equivalencia que nos piden:

$\Rightarrow$ Este es el implica fácil, pues tenemos como hipótesis, que $\langle A \rangle = A$, y nosotros ya sabemos que $\langle A \rangle$ es un grupo (lo probamos en la parte a)), entonces necesariamente A es un grupo.

$\Leftarrow$ Debemos probar una igualdad de conjuntos.
Observemos primero que, como A es un grupo que contiene a A y rescatando del olvido una propiedad de la intersección ($C \cap D \subseteq C$), se tiene lo siguiente:

$$\langle A \rangle = \bigcap_{H \subseteq G,\ H\ subgrupo\ A \subseteq H} H \subseteq A$$

Lo que nos da una de las inclusiones que necesitamos.

Para la otra inclusión, no necesitamos que A sea subgrupo, pero si necesitamos una propiedade de la intersección (si $E \subseteq C,\ E \subseteq C$ entonces $E \subseteq D \cap D$). En efecto:

$$A \subseteq \bigcap_{H \subseteq G,\ H\ subgrupo\ A \subseteq H} H \subseteq \langle A \rangle$$

Hemos terminado de probar la igualdad de conjuntos, y por ende, este implica también está listo.

Ahora, ocupando el $\Leftarrow$ para el grupo $\langle A \rangle$, obtenemos:

$$\langle \langle A \rangle \rangle = \langle A \rangle$$

The End