Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y Teoría de Galois
Primer Semestre 2020

Soluciones - Práctico 1

1. - G grupo con la suma:
     - Neutro: $a = 0, b = 0$
     - Asociativa: $(a + b\sqrt{2}) + ((c + d\sqrt{2}) + (e + f\sqrt{2})) = (a + c + e) + (b + d + f)\sqrt{2}$ y por tanto no importa el orden en que se sume.
     - Opuesto: $a + b\sqrt{2} + (-a - b\sqrt{2}) = 0$.
   - $G^\times$ grupo con la multiplicación:
     - Neutro: $a = 1, b = 0$
     - Asociativa: $(a + b\sqrt{2}) \times ((c + d\sqrt{2}) \times (e + f\sqrt{2}))$ análogo a lo anterior, usamos la asociativa de los reales.
     - Opuesto: $(a + b\sqrt{2}) \times \frac{a-b\sqrt{2}}{a^2-2b^2} = 1$.

2. - Operación $*$ bien definida: Para esto, veamos que $x * y$ pertenece al grupo. Si $x + y < 1$, entonces $[x + y] = 0$ y por tanto $x * y = x + y - [x + y] < 1$. Si $2 > x + y \geq 1$, entonces $[x + y] = 1$ y por tanto $x * y = x + y - [x + y] < 1$. Observar que $x + y < 2$.
   - G grupo:
     - Neutro: 0
     - Asociativa: usaremos la propiedad de la parte entera $[x + n] = [x] + n, \quad \forall n \in \mathbb{Z}$:

$$\begin{aligned} x * (y * z) &= x * (y + z - [y + z]) \\ &= x + (y + z - [y + z]) - [x + (y + z - [y + z])] \\ &= x + y + z - [y + z] - [x + y + z - [y + z]] \\ &= x + y + z - [x + y + z] \end{aligned}$$

       de esta forma el resultado no depende del orden en que se realicen las operaciones.
     - Opuesto: $x * (1 - x) = 0$

3. - $\rho^l\sigma = \sigma\rho^{n-l}$: Por inducción en l. Para $l = 0$ no hay nada que demostrar, para $l = 1$ es la definición.

$$\begin{aligned} \rho^l\sigma &= \rho^{l-1}\rho\sigma \\ \text{(usando } l = 1) &= \rho^{l-1}\sigma\rho^{n-1} \\ \text{(usando hipótesis inductiva)} &= \sigma\rho^{n-l+1}\rho^{n-1} \\ &= \sigma\rho^{n-l}\rho^n \\ \text{(usando } \rho^n = id) &= \sigma\rho^{n-l} \end{aligned}$$

   - Alcanza con demostrarlo para los generadores del grupo (si un elemento conmuta con los generadores, entonces conmuta con todos los elementos). Es claro que $\rho^{n/2}\rho = \rho\rho^{n/2}$ y de lo demostrado anteriormente es inmediato que $\rho^{n/2}\sigma = \sigma\rho^{n/2}$.

4. $g^2 = 1$ entonces $g^{-1} = g$. Por tanto,

$$gf = g^{-1}f^{-1} = (fg)^{-1} = fg$$

   y todos los elementos conmutan.

5. $|g| = 2m+1$, para algún $m \in \mathbb{N}$. Por tanto, $g^{2m+1} = 1$, así que $g^{2(m+1)} = g$. Tomamos $k = m+1$.

6. Ejercicio de Entrega

7. (a)

$$\begin{aligned} a^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad a^3 = -a, \quad a^4 = -a^2 = id \\ b^2 &= \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}. \quad b^3 = id \\ ab &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \quad (ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \end{aligned}$$

De las cuentas previas se deducen las afirmaciones a demostrar.

(b) En $\mathbb{Z}_2 \oplus \mathbb{Z}$, considerar $a = (1,1)$ y $b = (0,-1)$. Cada uno de ellos tiene orden infinito, y $a+b = (1,0)$, que tiene orden 2.

8.
- Sean $n = |f|, m = |g|$, entonces $(fg)^{mn} = fgfg...fg = f^{nm}g^{nm} = 1$. Por tanto, $|fg| < \infty$ y además $|fg| \mid nm$.
- De la parte anterior tenemos que $|fg| \mid nm$. Ahora veremos que $m \mid |fg|$. Como conmutan, $1 = (fg)^{|fg|} = f^{|fg|}g^{|fg|}$, lo cual implica que $f^{-|fg|} = g^{|fg|}$. Entoces,

$$g^{|fg|n} = (g^{|fg|})^n = (f^{-|fg|})^n = 1$$

Entonces $m \mid |fg|n$. Como $(n,m) = 1$, se tiene $m \mid |fg|$. Analogamente para n. Por tanto, $nm \mid |fg|$

9. (a) Verificación inmediata

(b) Observar que tenemos

$$\begin{aligned} Q &= \{a^{n_1}b^{m_1}...a^{n_l}b^{m_l} : l \in \mathbb{N}, n_i, m_i \in Z\} \\ &= \{a^n b^m : 0 \leq n, m \leq 3\} \end{aligned}$$

donde usamos la identidad de la parte anterior para cambiar de lugar a con b, y que ambos tienen orden 4. Ahora, tenemos 16 posibles elementos en Q. Los elementos de la forma b^2a^l son iguales a a^{l+2}. Los elementos de la forma b^3a^l son iguales a ba^{l+2}.

(c)

$$\begin{aligned} \langle a \rangle &= \{1, a, a^2, a^3\} \\ \langle b \rangle &= \{1, b, a^2, ba^2\} \\ \langle ab \rangle &= \{1, ab, a^2, a^3b\} \end{aligned}$$

10. Ejercicio de Entrega

11. (a) Dado un grupo , el mapa $g \mapsto hg$ es un automorfismo. Por tanto,

$$\tau(c) = \tau\left(\frac{1}{|G|}\sum_{\phi}\phi(p)\right) = \frac{1}{|G|}\sum_{\phi\in G}\tau(\phi(p)) = \frac{1}{|G|}\sum_{\phi'\in G}\phi'(p) \tag{1}$$

(b) Como las traslaciones y antitraslaciones no tienen puntos fijos, deducimos que G está formado por rotaciones y simetrías axiales.

(c)
- $H < \mathbb{R}$: La rotación de ángulo 0 está en G, por tanto $\theta = 0 \in H$. Si $\rho_{c,\theta}, \rho_{c,\psi} \in G$, entonces la composición es $\rho_{c,\theta+\psi} \in G$, por ser grupo y por tanto cerrado por la operación de composición. Por tanto, $\theta + \psi \in H$.

- Como $H < \mathbb{R}$, entonces H es denso o es de la forma $\alpha\mathbb{Z}$, $\alpha \in \mathbb{R}^+$. Si fuera denso, entonces G sería infinito, pero por hipótesis G finito. Por tanto, $H = \alpha\mathbb{Z}$. Al ser $\rho_{c,2\pi} = id \in G$, deducimos que $\alpha = 2\pi/m$, para algún $m \in \mathbb{N}$.
- Si G contiene alguna simetría axial, σ, entonces basta con tomar el subgrupo generado por $\sigma, \rho_{c,2\pi/m}$ y observar que debe dar todo G. Entonces $G = D_m$.

12. Mismo razonamiento que en las partes c y d del ejercicio anterior: si sólo tiene rotaciones, entonces es cíclico, y si tiene alguna simetría, entoces es un diedral.