# Álgebra I: Estructuras algebraicas y la teoría de grupos Examen parcial 2 (diferido / repetido). Soluciones

## Universidad de El Salvador, 8.06.2018

**Problema 1** (1 punto)**.** Encuentre el orden de cada uno de los elementos del grupo diédrico

$$D_n = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, f, fr, fr^2, \ldots, fr^{n-1}\}.$$

*Solución.* El elemento $r$ es una rotación de $360^\circ/n$ y por ende tiene orden $n$, y en general, para las potencias de $r$ se tiene

$$\operatorname{ord} r^i = \frac{n}{\operatorname{mcd}(i,n)}.$$

Cada uno de los elementos $fr^i$ es una reflexión y su orden es 2. También podemos calcular que

$$(fr^i)\,(fr^i) = ffr^{-i}\,r^i = \mathrm{id}.$$

■

---

Para los siguientes dos problemas, consideremos los números complejos

$$\omega := \frac{1+\sqrt{-3}}{2}, \quad \overline{\omega} := \frac{1-\sqrt{-3}}{2}$$

y el conjunto

$$\mathbb{Z}[\omega] := \{a + b\,\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

**Problema 2** (1 punto)**.** Demuestre que $\mathbb{Z}[\omega]$ es un anillo conmutativo respecto a la adición y multiplicación habitual de números complejos.

*Solución.* Tenemos $0 = 0 + 0 \cdot \omega, 1 = 1 + 0 \cdot \omega \in \mathbb{Z}[\omega]$. Está claro que $\mathbb{Z}[\omega]$ está cerrado respecto a la adición y sustracción:

$$(a + b\,\omega) \pm (c + d\,\omega) = (a \pm c) + (b \pm d)\,\omega.$$

Lo más importante es comprobar que $\mathbb{Z}[\omega]$ está cerrado respecto a la multiplicación. Calculamos que

$$\omega^2 = \frac{1 + 2\sqrt{-3} - 3}{4} = \frac{-1+\sqrt{-3}}{2} = \omega - 1.$$

Luego,

$$(a + b\,\omega)\,(c + d\,\omega) = ac + (ad + bc)\,\omega + bd\,\omega^2 = (ac - bd) + (ad + bc + bd)\,\omega.$$

El resto de los axiomas de anillos conmutativos sigue del hecho de que estamos trabajando con números complejos.

■

**Problema 3** (2 puntos)**.**

1) Demuestre que la aplicación
$$N\colon a+b\,\omega \mapsto (a+b\,\omega)\,(a+b\,\overline{\omega})$$
toma sus valores en $\mathbb{Z}$ y es multiplicativa: para cualesquiera $x,y\in\mathbb{Z}[\omega]$ se cumple
$$N(xy)=N(x)\,N(y).$$

2) Demuestre que el grupo de unidades $\mathbb{Z}[\omega]^\times$ es cíclico de orden 6.

*Solución.* Notamos que $\overline{\omega}=1-\omega$. Luego,

$$(a+b\,\omega)\,(a+b\,\overline{\omega})=\left(a+b\,\frac{1+\sqrt{-3}}{2}\right)\,\left(a+b\,\frac{1-\sqrt{-3}}{2}\right)=a^2+ab+b^2.$$

La aplicación $N$ es multiplicativa: tenemos $N(x)=x\,\overline{x}$, y luego

$$N(xy)=xy\,\overline{xy}=x\,\overline{x}\,y\,\overline{y}=N(x)\,N(y).$$

Entonces, $u\in\mathbb{Z}[\omega]^\times$ implica que $N(u)=\pm1$. La ecuación

$$a^2+ab+b^2=-1$$

no tiene soluciones enteras, mientras que la ecuación

$$a^2+ab+b^2=1$$

corresponde a una elipse y por esto tiene un número finito de puntos enteros

$$(a,b)=(\pm1,0),\ (0,\pm1),\ (\pm1,\mp1).$$

Estos puntos corresponden a los elementos
$$\pm1,\ \pm\,\omega,\ \pm\,1\mp\omega.$$
Se puede notar que $\omega=e^{2\pi\sqrt{-1}/6}$ (tenemos $\cos(\pi/3)=1/2$ y $\sin(\pi/3)=\sqrt{3}/2$), así que $\omega$ tiene orden 6. Podemos concluir que todos los elementos de arriba son potencias de $\omega$ y que

$$\mathbb{Z}[\omega]^\times=\{1,\omega,\omega^2,\omega^3,\omega^4,\omega^5\}=\{\pm1,\ \pm\,\omega,\ \pm\,1\mp\omega\}.$$

De hecho, todo esto es *exactamente lo mismo* que el ejercicio 4.1 de las tareas, solo formulado en diferentes palabras. ∎

**Problema 4** (2 puntos)**.** Calcule la serie inversa para $1-2X+X^2\in\mathbb{Z}[\![X]\!]$.

*Solución.* Tenemos
$$f=\sum_{i\ge0}a_i\,X^i,\quad \text{donde } a_0=1,\ a_1=-2,\ a_3=1,\ a_i=0 \text{ para } i>3.$$
Ahora si la serie inversa es
$$g=\sum_{k\ge0}b_k\,X^k,$$
entonces

$$\begin{aligned}
b_0&=a_0^{-1}=1,\\
b_1&=-a_0^{-1}\,(a_1\,b_0)=2,\\
b_k&=-a_0^{-1}\sum_{1\le i\le k}a_i\,b_{k-i}=2\,b_{k-1}-b_{k-2} \text{ para } k\ge2.
\end{aligned}$$

De estas relaciones se ve que $b_k = k+1$. En efecto, es cierto para $k = 0, 1$, y luego, si es cierto para $b_k$, entonces

$$b_{k+1} = 2\,b_k - b_{k-1} = 2\,(k+1) - k = k+2.$$

Así que

$$g = 1 + 2\,X + 3\,X^2 + 4\,X^3 + 5\,X^4 + 6\,X^5 + \cdots$$

■

**Problema 5** (2 puntos)**.** Demuestre que las matrices

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

generan un subgrupo de $\mathrm{GL}_3(\mathbb{Z})$ que es isomorfo a $S_3$.

*Solución.* La primera matriz es la matriz de la permutación $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 3$, mientras que la segunda matriz es la matriz de permutación $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$. Tenemos entonces el 3-ciclo $(1\ 2\ 3)$ y la transposición $(1\ 2)$. Son generadores de $S_3$. ■

**Problema 6** (2 puntos)**.** Encuentre todos los homomorfismos entre el grupo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo $n$ respecto a la adición y el grupo $\mathbb{C}^\times$ de los números complejos no nulos respecto a la multiplicación.

*Solución.* Sea $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times$ un homomorfismo. El grupo $\mathbb{Z}/n\mathbb{Z}$ es cíclico, generado por $[1]_n$, y por lo tanto $f$ está definido por la imagen de $[1]_n$. Además, todo homomorfismo preserva la operación de grupo (adición en $\mathbb{Z}/n\mathbb{Z}$ corresponde a la multiplicación en $\mathbb{C}^\times$) y el elemento neutro ($[0]_n \in \mathbb{Z}/n\mathbb{Z}$ corresponde a $1 \in \mathbb{C}^\times$), así que

$$f([1]_n)^n = f(n \cdot [1]_n) = f([n]_n) = f([0]_n) = 1.$$

Esto significa que $f([1]_n)$ es una raíz $n$-ésima de la unidad y por ende $\operatorname{im} f \subseteq \mu_n(\mathbb{C})$. Las raíces $n$-ésimas también forman un grupo cíclico de orden $n$, así que hay $n$ diferentes homomorfismos $f\colon \mathbb{Z}/n\mathbb{Z} \to \mu_n(\mathbb{C})$ definidos por

$$f_k\colon [1]_n \mapsto e^{\frac{2\pi k\sqrt{-1}}{n}} \quad \text{para } k = 0, 1, 2, \ldots, n-1.$$

(Recuerde el ejercicio 6.9 de las tareas donde hemos estudiado los homomorfismos $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.) ■