TEORÍA ALGEBRAICA DE NÚMEROS (8-11-2019) • **Grado en Matemáticas** **Curso 2019–20** | **Hoja 4**

Algo mas de Estructuras Algebraicas.

1. Utilizar las siguientes igualdades para demostrar que los correspondientes anillos no son D.F.U.:

a) $\mathbb{Z}[\sqrt{-5}]$: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$,
b) $\mathbb{Z}[\sqrt{-6}]$: $6 = 2 \cdot 3 = \sqrt{-6}\sqrt{-6}$,

c) $\mathbb{Z}[\sqrt{-10}]$: $14 = 2 \cdot 7 = (2+\sqrt{-10})(2-\sqrt{-10})$,

d) $\mathbb{Z}[\sqrt{-13}]$: $14 = 2 \cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13})$,

e) $\mathbb{Z}[\sqrt{-14}]$: $15 = 3 \cdot 5 = (1+\sqrt{-14})(1-\sqrt{-14})$,

f) $\mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$: $4 = 2 \cdot 2 = \left(\frac{1+\sqrt{-15}}{2}\right)\left(\frac{1-\sqrt{-15}}{2}\right)$,

g) $\mathbb{Z}[\sqrt{-17}]$: $18 = 2 \cdot 3 \cdot 3 = (1+\sqrt{-17})(1-\sqrt{-17})$,

h) $\mathbb{Z}[\sqrt{-21}]$: $22 = 2 \cdot 11 = (1+\sqrt{-21})(1-\sqrt{-21})$,

i) $\mathbb{Z}[\sqrt{-22}]$: $26 = 2 \cdot 13 = (2+\sqrt{-22})(2-\sqrt{-22})$,

j) $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$: $6 = 2 \cdot 3 = \left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right)$,

k) $\mathbb{Z}[\sqrt{-26}]$: $27 = 3 \cdot 3 \cdot 3 = (1+\sqrt{-26})(1-\sqrt{-26})$,

l) $\mathbb{Z}[\sqrt{-29}]$: $30 = 2 \cdot 3 \cdot 5 = (1+\sqrt{-29})(1-\sqrt{-29})$,

m) $\mathbb{Z}[\sqrt{-30}]$: $34 = 2 \cdot 17 = (2+\sqrt{-30})(2-\sqrt{-30})$,

n) $\mathbb{Z}[\sqrt{10}]$: $6 = 2 \cdot 3 = (4+\sqrt{10})(4-\sqrt{10})$,

ñ) $\mathbb{Z}[\sqrt{15}]$: $10 = 2 \cdot 5 = (5+\sqrt{15})(5-\sqrt{15})$,

o) $\mathbb{Z}[\sqrt{26}]$: $10 = 2 \cdot 5 = (6+\sqrt{26})(6-\sqrt{26})$,

p) $\mathbb{Z}[\sqrt{30})$: $6 = 2 \cdot 3 = (6+\sqrt{30})(6-\sqrt{30})$.

2. En $\mathbb{Z}[\sqrt{-5}]$ definimos los ideales

$$\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle, \qquad \mathfrak{q} = \langle 3, 1+\sqrt{-5}\rangle, \qquad \mathfrak{r} = \langle 3, 1-\sqrt{-5}\rangle.$$

a) Demostrar que $\mathfrak{p}, \mathfrak{q}$ y $\mathfrak{r}$ no son principales.

b) Demostrar que $\mathfrak{p}, \mathfrak{q}$ y $\mathfrak{r}$ son ideales maximales, por lo tanto primos.

c) Mostrar que

$$\mathfrak{p}^2 = \langle 2\rangle, \qquad \mathfrak{q}\cdot\mathfrak{r} = \langle 3\rangle, \qquad \mathfrak{p}\cdot\mathfrak{q} = \langle 1+\sqrt{-5}\rangle, \qquad \mathfrak{p}\cdot\mathfrak{r} = \langle 1-\sqrt{-5}\rangle.$$

d) Demostrar que las factorizaciones de 6:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

provienen de diferentes agrupamientos de productos de ideales primos:

$$\langle 6\rangle = \mathfrak{p}^2\mathfrak{q}\cdot\mathfrak{r}.$$

e) Demostrar que los ideales $\langle 2\rangle$ y $\langle 3\rangle$ están generados por elementos irreducibles pero que los ideales no son primos.

3. En $\mathbb{Z}[\sqrt{-6}]$:

a) Comprobar que $\langle 2\rangle = \langle 2, \sqrt{-6}\rangle^2, \langle 3\rangle = \langle 3, \sqrt{-6}\rangle^2$.

b) Encontrar ideales principales $\mathfrak{p}$ y $\mathfrak{q}$ tales que

$$\mathfrak{p}\,\langle 2, \sqrt{-6}\rangle = \mathfrak{q}\,\langle 3, \sqrt{-6}\rangle.$$

4. Sea A un anillo conmutativo con unidad e I, J ideales de A.

a) Demostrar que $I + J$ e $I \cdot J$ son ideales de A.

b) Demostrar que si $I = \langle a_1, \ldots .a_n\rangle$ y $J = \langle b_1, \ldots .b_m\rangle$ entonces

$$I + J = \langle a_1, \ldots .a_n, b_1, \ldots .b_m\rangle \qquad \text{e} \qquad I \cdot J = \langle a_i b_j \;:\; i = 1, \ldots, n; j = 1, \ldots, m\rangle$$

5. Sabemos que el anillo $\mathbb{Z}[\sqrt{-5}]$ no es DIP. ¿Existen infinitos ideales de $\mathbb{Z}[\sqrt{-5}]$ no principales?

6. Demostrar que toda $\mathbb{Z}$-base del grupo abeliano libre $\mathbb{Z}^n$ tiene n elementos.

7. Demostrar que un conjunto $S \subset \mathbb{Z}^n$ es $\mathbb{Z}$-base si sólo si todo elemento de $\mathbb{Z}^n$ se escribe de forma única como combinación de elementos de S.

8. Sea G un grupo abeliano libre de rango n y $\mathcal{B} = \{u_1, \ldots, u_n\}, \mathcal{B}' = \{u'_1, \ldots, u'_n\}$ dos $\mathbb{Z}$-bases de G. Demostrar que la matriz de cambio de $\mathbb{Z}$-base es unimodular (i.e. matriz con coeficientes enteros con determinante ± 1).

9. Para $i = 1, \ldots, n$ definimos $u_i = (a_{i1}, \ldots .a_{in}) \in \mathbb{Z}^n$. Sea $S = \{u_1, \ldots, u_n\}$ y $A = (a_{ij}) \in M_n(\mathbb{Z})$. Demostrar que S es $\mathbb{Z}$-base de $\mathbb{Z}^n$ si y sólo si $|A| = \pm 1$.

10. Sea G un grupo abeliano libre de rango n y H un subgrupo de G. Demostrar que G/H es finito si y sólo si el rango de H es n. En ese caso si $\mathcal{B} = \{u_1, \ldots, u_n\}$ es una $\mathbb{Z}$-base de G y $\mathcal{B}' = \{u'_1, \ldots, u'_n\}$ una base de H tal que $u'_i = (a_{i1}, \ldots, a_{in})_{\mathcal{B}}$ entonces

$$|G/H| = |det(a_{ij})|$$

11. Sea $H = \langle (3, 1, -2), (4, -5, 1), (1, 0, 7)\rangle$ y $G = \mathbb{Z}^3/H$. Determinar el cardinal de G y los invariantes de G.

12. Sea $H = \langle (2, 2, 2), (3, 0, -6)\rangle$ y $G = \mathbb{Z}^3/H$. Determinar el cardinal de G y los invariantes de G.

13. Sea $A = \mathbb{Z}[\sqrt{15}]$ e $I = \langle 7, 1 + \sqrt{15}\rangle$. Determinar el cardinal del anillo cociente A/I.

14. Dado el polinomio irreducible $f(x) = x^3 + x^2 - 2x + 8$ y $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$, sea

$$A = \left\{ a_0 + a_1\alpha + a_2 \frac{(\alpha + \alpha^2)}{2} \mid a_0, a_1, a_2 \in \mathbb{Z} \right\}.$$

a) Demostrar que A es un anillo.

b) Sean $u = 1 + \alpha$ y $v = 3 + \alpha^2$. Demostrar que $u, v \in A$.

c) Sean los ideales de A siguientes:

$$I = \langle 5, u\rangle \qquad \text{y} \qquad J = \langle 5, v\rangle.$$

d) Demostrar

$$I \cdot J = 5A \qquad \text{e} \qquad I + J = A.$$

e) Calcular $|A/I|$ y $|A/J|$.