Práctica 3

1. Decidir cuáles de los siguientes elementos de $\mathbb{Z}[i]$ son irreducibles: $1+i$, $3-7i$, 5, 7,$-4+5i$. ¿Es $10 = (3-i)(3+i) = 2 \cdot 5$ un ejemplo de factorización no única en $\mathbb{Z}[i]$? ¿Por qué?

2. Mostrar que 6 y $2(1+\sqrt{-5})$ son divisibles por 2 y $(1+\sqrt{-5})$, pero no tienen un máximo común divisor en $\mathbb{Z}[\sqrt{-5}]$. ¿Tienen un mínimo común múltiplo?

3. Sea $\mathcal{D} = \mathbb{Z}[\sqrt{-5}]$. Mostrar que $\sqrt{-5} \mid (a+b\sqrt{-5})$ en $\mathcal{D}$ si y sólo si $5 \mid a$ en $\mathbb{Z}$. Probar que $\sqrt{-5}$ es primo en $\mathcal{D}$ y que 5 se factoriza de manera única como producto de irreducibles aunque el anillo no sea un dominio de factorización única.

4. (a) Probar que si la ecuación $x^3 + y^3 = z^3$ tiene solución no trivial en $\mathbb{Z}$, entonces $3 \mid xyz$.

   (b) Sea ξ una raíz cúbica primitiva de la unidad. Probar que $\mathbb{Z}[\xi]$ es un dominio euclideano y que $\mathcal{U}(\mathbb{Z}[\xi]) = G_6$, el grupo de raíces sextas de la unidad.

   (c) Verificar que $1-\xi$ es irreducible en $\mathbb{Z}[\xi]$ y que $3 = (1-\xi)^2(1+\xi)$.

   (d) Probar que si una ecuación del tipo

   $$X^3 + Y^3 + u(1-\xi)^{3n} Z^3 = 0$$

   con $u \in G_6$ y $n \in \mathbb{N}$ tiene una solución (x, y, z) con $x, y, z \in \mathbb{Z}[\xi]$ coprimos dos a dos y tales que $1-\xi \nmid xyz$, entonces:

      i. Debe ser $n \geq 2$. (Sugerencia: Mirar módulo el ideal (9) de $\mathbb{Z}[\xi]$.)

      ii. Existe $u' \in G_6$ tal que la ecuación

      $$X^3 + Y^3 + u'(1-\xi)^{3(n-1)} Z^3 = 0$$

      tiene una solución (x', y', z') con $x', y', z' \in \mathbb{Z}[\xi]$ coprimos dos a dos y tales que $1-\xi \nmid x'y'z'$.
      (Sugerencia: Observar que $(x+y)(x+\xi y)(x+\xi^2 y) = -u(1-\xi)^{3n} z^3$.)

   (e) Deducir que la ecuación de Fermat de exponente 3,

   $$x^3 + y^3 = z^3,$$

   no tiene solución (no trivial) en $\mathbb{Z}$.

5. Sea $\mathcal{I}$ el ideal de $\mathbb{Z}[\sqrt{-3}]$ generado por 2 y $1+\sqrt{-3}$. Probar que $\mathcal{I} \neq (2)$ pero que $\mathcal{I}^2 = 2\mathcal{I}$. Deducir que no hay factorización única en ideales primos en el anillo $\mathbb{Z}[\sqrt{-3}]$. Probar que $\mathcal{I}$ es el único ideal primo que contiene a (2) y que (2) no es un producto de ideales primos.

6. Sea $\mathcal{D} = \mathbb{Z}[\sqrt{-5}]$

   (a) Verificar la siguiente factorización en $\mathbb{Z}[\sqrt{-5}]$:

   $$6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

   Probar que 2, 3, $(1+\sqrt{-5})$ y $(1-\sqrt{-5})$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$, pero no son primos.

   (b) Considere los siguientes ideales en $\mathcal{D}$:

   $$\mathcal{P} = (2, 1+\sqrt{-5}), \quad \mathcal{Q} = (3, 1+\sqrt{-5}), \quad \mathcal{R} = (3, 1-\sqrt{-5}).$$

   Probar que son maximales, y por lo tanto primos.
   Hallar $\mathcal{P}^2, \mathcal{PQ}, \mathcal{PR}, \mathcal{QR}$. Observar que las dos factorizaciónes del item anterior provienen de agrupar de dos maneras diferentes la factorización en ideales primos

   $$(6) = \mathcal{P}^2\mathcal{QR}.$$

   (c) Probar que los ideales $\mathcal{P}, \mathcal{Q}$ y $\mathcal{R}$ no pueden ser principales.

7. Sea $\mathcal{D}$ el anillo de enteros de un cuerpo de números K. Sean $\mathcal{P}$ y $\mathcal{Q}$ dos ideales primos distintos en $\mathcal{D}$. Probar que $\mathcal{P} + \mathcal{Q} = \mathcal{D}$ y que $\mathcal{P} \cap \mathcal{Q} = \mathcal{PQ}$.

8. Sean K un cuerpo de números, $\mathcal{D}$ su anillo de enteros y $\mathcal{A} \neq 0$ un ideal de $\mathcal{D}$. Sea $\alpha \neq 0$ en $\mathcal{A}$. Usando la descomposición en ideales primos y el teorema chino del resto, probar que existe $\beta \in \mathcal{A}$ tal que $\mathcal{A} = (\alpha, \beta)$.

9. Sean K un cuerpo de números, $\mathcal{D}$ su anillo de enteros y $\mathcal{A} \neq 0$ un ideal de $\mathcal{D}$.

   (a) Probar que $\mathcal{A}$ tiene una $\mathbb{Z}$-base $\{\alpha_1, ..., \alpha_n\}$, con $n = [K : \mathbb{Q}]$.

   (b) Se define la *norma* de $\mathcal{A}$ como el cardinal de $\mathcal{D}/\mathcal{A}$.
   Probar que

   $$N(\mathcal{A}) = \left| \frac{\Delta(\alpha_1, ..., \alpha_n)}{\Delta} \right|^{\frac{1}{2}}$$

   donde Δ es el discriminante de K.

   (c) Si $\mathcal{A} = (\alpha)$ es principal, entonces $N(\mathcal{A}) = |N(\alpha)|$.

   Sugerencia: Usar el Teorema de Estructura de grupo abelianos finitamente generados.

10. En $\mathbb{Z}[\sqrt{-5}]$ encontrar una $\mathbb{Z}$-base $\{\alpha_1, \alpha_2\}$ para el ideal $(2, 1+\sqrt{-5})$ y chequear la fórmula
$$N(2, 1+\sqrt{-5}) = \left|\frac{\Delta(\alpha_1, \alpha_2)}{\Delta}\right|^{\frac{1}{2}}.$$

11. (a) Sea $\mathcal{D}$ el anillo de enteros de un cuerpo de números. Sean $\mathcal{A}, \mathcal{B} \neq 0$ ideales de $\mathcal{D}$ y $\mathcal{P}$ un ideal primo de $\mathcal{D}$.
    i. Probar que $\mathcal{D}/\mathcal{A} \simeq (\mathcal{D}/\mathcal{AP})/(\mathcal{A}/\mathcal{AP})$ y $\mathcal{A}/\mathcal{AP} \simeq \mathcal{D}/\mathcal{P}$.
    ii. Deducir que $N(\mathcal{AP}) = N(\mathcal{A})N(\mathcal{P})$.
    iii. Probar que $N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$.
    (Sugerencia: factorizar $\mathcal{B}$ como producto de ideales primos de $\mathcal{D}$.)

    (b) Sean K un cuerpo de números, $n = [K : \mathbb{Q}]$, $\mathcal{D}$ el anillo de enteros de K y $\mathcal{A} \neq 0$ un ideal de $\mathcal{D}$. Probar que:
    i. Si $N(\mathcal{A})$ es primo en $\mathbb{Z}$, entonces $\mathcal{A}$ es un ideal primo de $\mathcal{D}$.
    ii. Si $\mathcal{A}$ es un ideal primo de $\mathcal{D}$, entonces $N(\mathcal{A}) = p^m$ con $p \in \mathbb{N}$ primo y $m \in \mathbb{N}$ tal que $m \leq n$.

12. Encontrar todos los ideales en $\mathbb{Z}[\sqrt{-2}]$ de norma 18.