3.1. Anillos y subanillos

- Un **anillo** $(R, +, \cdot)$ es un conjunto no vacío R con dos operaciones internas, denominadas suma y producto: $+ : R \times R \to R$ y $\cdot : R \times R \to R$, verificando las propiedades siguientes:

  r_1) $(R, +)$ es un grupo abeliano cuyo elemento neutro se denomina **elemento nulo** o **cero del anillo** y se nota por $0_R \in R$. Para cada $a \in R$ el inverso de a con la operación suma se denomina **opuesto de** a y se nota por a' o $-a \in R$: $(-a) + a = a + (-a) = 0_R$.

  r_2) Propiedad **asociativa del producto**: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todos $a, b, c \in R$.

  r_3) Propiedades **distributivas**: $\forall\ a, b, c \in R$ se verifica:
  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ y $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

- Un anillo $(R, +, \cdot)$ que verifica r_4), se dice que es un **anillo conmutativo**:

  r_4) Propiedad **conmutativa del producto**: Para todos $a, b \in R$ se verifica que $a \cdot b = b \cdot a$.

- Un anillo $(R, +, \cdot)$ que verifica r_5), se dice que es un **anillo con identidad**:

  r_5) Existe elemento neutro para la operación producto, dicho elemento se denomina **identidad del anillo** y se nota por 1_R: $\exists\ 1_R \in R$ tal que $1_R \neq 0_R$ y $1_R \cdot a = a \cdot 1_R = a \quad \forall a \in R$

- Un anillo con identidad $(R, +, \cdot)$ que verifica r_6), se denomina **anillo de división**:

  r_6) Existe el **inverso**, para la operación producto, de todo elemento no nulo del anillo:
  $\forall\ a \in R$ con $a \neq 0_R$, existe $a^{-1} \in R$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$.

- Un anillo, conmutativo y de división, que verifica las propiedades r_4), r_5) y r_6), se denomina **cuerpo**

Propiedades de anillos

Sea $(R, +, \cdot)$ un anillo. Para todos $a, b \in R$ se verifican las siguientes propiedades:

1. $0_R \cdot a = a \cdot 0_R = 0_R$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$

Definición de subanillo

Sea $(R, +, \cdot)$ un anillo. Un **subanillo** de R es un subconjunto $S \subseteq R$ tal que $(S, +, \cdot)$ es anillo.

Caracterización de subanillo

Sea $(R, +, \cdot)$ un anillo. Un subconjunto no vacío $\emptyset \neq S \subseteq R$ es subanillo de $(R, +, \cdot)$ si y sólo si

1. Para todos $a, b \in S$ se cumple que $a - b \in S$
2. Para todos $a, b \in S$ se cumple que $a \cdot b \in S$

Producto directo de anillos

Se llama **producto directo** de los anillos $(R_1, +_1, \cdot_1)$ y $(R_2, +_2, \cdot_2)$ al anillo $(R_1 \times R_2, +, \cdot)$, donde las operaciones suma y producto se definen coordenada a coordenada: $\forall\ (a_1, a_2), (b_1, b_2) \in R_1 \times R_2$
$(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1,\ a_2 +_2 b_2) \in R_1 \times R_2, \qquad (a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot_1 b_1,\ a_2 \cdot_2 b_2) \in R_1 \times R_2$

3.1. Problemas

1. Estudiar si los siguientes conjuntos, con las operaciones usuales de suma y producto, tienen estructura de anillo. En caso afirmativo indicar si es conmutativo, con identidad, de división y si es cuerpo.

   a) $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ siendo $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
   b) $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ siendo $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.
   c) $(S, +, \cdot)$ siendo $S = \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Z}\}$.
   d) $(\mathbb{Z}[i], +, \cdot)$ siendo $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}] = \{a + bi : a, b \in \mathbb{Z}\}$.
   e) $(\mathbb{Z}_p[i], +_p, \cdot_p)$ siendo $\mathbb{Z}_p[i] = \mathbb{Z}_p[\sqrt{-1}] = \{a + bi : a, b \in \mathbb{Z}_p\}$.
   f) $(T, +, \cdot)$ siendo $T = \{a + bi : a \in \mathbb{Z}, b \in 2\mathbb{Z}\}$.

2. Encontrar todos los valores $k, m \in \mathbb{Z}$ para los cuales $(\mathbb{Z}, \oplus, \odot)$ es un anillo, siendo para todo $x, y \in \mathbb{Z}$, $x \oplus y = x + y - k$ y $x \odot y = x + y - mxy$. Para tales valores estudiar si el anillo correspondiente es conmutativo, tiene identidad, es de división y si es cuerpo.

3. Se considera el conjunto $\mathbb{Q}$ con las operaciones de suma y producto definidas del siguiente modo: Para todo $x, y \in \mathbb{Q}$, $x \oplus y = x + y + 7$, $x \odot y = x + y + \frac{xy}{7}$. Estudiar si $(\mathbb{Q}, \oplus, \odot)$ es un anillo y en caso afirmativo indicar si es un anillo conmutativo, si tiene identidad, si es de división y si es cuerpo.

4. *a*) Encontrar todos los subanillos de $\mathbb{Z}_{12}$, $\mathbb{Z}_{18}$, $\mathbb{Z}_{24}$
   b) Construir un diagrama de Hasse del conjunto de subanillos de cada uno de los anillos indicados en el apartado anterior, donde el orden parcial está determinado por la inclusión de conjuntos.

5. Sea $S = \{(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} : a = b + c\}$. Demostrar que S no es subanillo de $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

6. Estudiar si los siguientes conjuntos son subanillos de $\mathbb{Z}^{2\times 2}$

   a) $S = \{\begin{pmatrix} x & x \\ 2y & y \end{pmatrix} : x, y \in \mathbb{Z}\}$, *b*) $S = \{\begin{pmatrix} x & x-y \\ x-y & y \end{pmatrix} : x, y \in \mathbb{Z}\}$,
   c) $S = \{\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{Z}\}$, *d*) $S = \{\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} : x, y, z \in \mathbb{Z}\}$,
   e) $S = \{\begin{pmatrix} 2x & 2y \\ 2z & 2t \end{pmatrix} : x, y, z, t \in \mathbb{Z}\}$, *f*) $S = \{\begin{pmatrix} x & x-y \\ y & x-y \end{pmatrix} : x, y \in \mathbb{Z}\}$.

7. Encontrar un $n \in \mathbb{N}$ tal que

   a) En $\mathbb{Z}_n$ no es cierta la siguiente propiedad: $\forall a \in \mathbb{Z}_n$ tal que $a^2 = a \Rightarrow a = 0$ ó $a = 1$
   b) En $\mathbb{Z}_n$ no es cierta la siguiente propiedad: $\forall a, b \in \mathbb{Z}_n$ tales que $ab = 0 \Rightarrow a = 0$ ó $b = 0$
   c) En $\mathbb{Z}_n$ no es cierta la siguiente propiedad: $\forall a, b, c \in \mathbb{Z}_n$ tales que $ab = ac \Rightarrow a = 0$ ó $b = c$

8. Sean $(S, +_1, \cdot_1)$ y $(T, +_2, \cdot_2)$ anillos y sea $R = S \times T$ el anillo producto. Demostrar que:

   a) Si S y T son conmutativos entonces R es conmutativo
   b) Si S y T tienen identidades respectivas $1_S \in S$ y $1_T \in T$ entonces R tiene identidad.
   c) Si S y T son cuerpos ¿Es R un cuerpo?