ESTRUCTURAS ALGEBRAICAS. GRUPO M3. CURSO 2019-2020.
CARLOS ANDRADAS Y ANDONI DE ARRIBA.

Generalidades en anillos. Divisores de cero. Unidades. Subanillos.

1. Consideramos las matrices
$$I = \mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ y } C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$
de $\mathcal{M}_2(\mathbb{C})$. Definimos el *anillo de los cuaternios reales*
$$\mathbb{H} = \{aA + bB + cC + dI : a, b, c, d \in \mathbb{R}\} \subseteq \mathcal{M}_2(\mathbb{C}).$$
   (a) Demostrar que $x = aA + bB + cC + dI \in \mathbb{H}$ es nulo si, y sólo si, lo son a, b, c y d.
   (b) Demostrar las igualdades
$$A^2 = B^2 = C^2 = -I,\ BC = -CB = A,$$
$$CA = -AC = B \text{ y } AB = -BA = C.$$
   (c) Deducir que $\mathbb{H}$ es un subanillo unitario de $\mathcal{M}_2(\mathbb{C})$.
   (d) Se define el *conjugado* de un cuaternio $x = aA + bB + cC + dI \in \mathbb{H}$ como $\bar{x} = -aA - bB - cC + dI \in \mathbb{H}$. Calcular $x\bar{x}$ y $\bar{x}x$. Deducir que $\mathbb{H}$ es un anillo de división. Si definimos la *aplicación norma* $N\colon \mathbb{H} \longrightarrow \mathbb{R}$ por
$$N\left(aA + bB + cC + dI\right) := a^2 + b^2 + c^2 + d^2,$$
   demostrar que esta es multiplicativa[1].
   (e) Sea $\mathbb{I}$ el *anillo de los cuaternios enteros*. A saber,
$$\mathbb{I} = \{aA + bB + cC + dI : a, b, c, d \in \mathbb{Z}\}.$$
   Probar que este es subanillo de $\mathbb{H}$ (luego, la restricción de N a $\mathbb{I}$ está bien definida), y deducir que $x \in \mathbb{I}$ es unidad si, y sólo si, $N(x) = 1$.
2. Demostrar que
$$\mathbb{Z}\left[\sqrt{3}\right] = \left\{a + b\sqrt{3} : a, b \in \mathbb{Z}\right\}$$
es subanillo unitario de $\mathbb{C}$ con infinitas unidades. ¿Pasa lo mismo con $\mathbb{Z}\left[\sqrt{-3}\right]$?
3. El anillo de los *enteros de Gauss* es
$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\},$$
donde $i = \sqrt{-1}$. Demostrar que $\mathbb{Z}[i]$ es un subanillo unitario de $\mathbb{C}$ sin divisores de cero. Encontrar sus unidades.
4. Un anillo unitario A se dice *de Boole* si para cada $a \in A$ se tiene que $a^2 = a$.
   (a) Probar que A es conmutativo y que $2a = 0$ para cada $a \in A$.
   (b) Probar que todo elemento de A distinto de 0 y de 1 es un divisor de cero.
5. El *centro de un anillo* A se define por
$$Z(A) := \{a \in A : ab = ba,\ \forall\ b \in A\}.$$
Demostrar que este es un subanillo conmutativo. Si A es unitario, entonces su centro contiene al elemento unidad. Deducir de todo esto que el centro de un anillo de división es un cuerpo.

[1]Una aplicación $f\colon A \longrightarrow B$ entre anillos se dice *multiplicativa* si $f(ab) = f(a)f(b)$ para todo $a, b \in A$.

6. Si A es dominio de integridad y existe $x \in A$ tal que $x^2 = 1$, probar que $x = \pm 1$.
7. Sea A un anillo unitario y $x \in A$ un elemento nilpotente[2]. Demostrar que $1-x \in \mathcal{U}(A)$ es una unidad. Pista: Factorizar $1 - x^n$.
8. Sea A un anillo conmutativo y unitario, $x \in \mathcal{U}(A)$ una unidad y $\mathcal{N}(A) = A \backslash \mathcal{U}(A)$.
   (a) Probar que $\rho_x : \mathcal{N}(A) \to A;\ y \mapsto xy$ es inyectiva y que $\operatorname{Im}(\rho_x) \subseteq \mathcal{N}(A)$.
   (b) Demostrar que ρ_x es biyectiva si $\mathcal{N}(A)$ es un conjunto finito.
   (c) Probar que si A es un dominio infinito, entonces $\mathcal{N}(A) = \{0\}$ o $\mathcal{N}(A)$ es infinito.

Homomorfismos de anillos. Ideales. Anillos cociente. Teoremas de Isomorfía.

9. Probar que todo ideal primo $\mathfrak{p} \subseteq A$ de un anillo de Boole es maximal. Demostrar que $A/\mathfrak{p}$ tiene dos elementos. Deducir que si A es un dominio de integridad entonces es isomorfo a $\mathbb{Z}_2$.
10. (a) Sean $n, m > 0$ dos enteros positivos cualesquiera. Clasificar los homomorfismos de anillos unitarios en los siguientes casos:
      (i) $f : \mathbb{Z}_n \to \mathbb{Z}$,
      (ii) $f : \mathbb{Z} \to \mathbb{Z}_n$ y
      (iii) $f : \mathbb{Z}_m \to \mathbb{Z}_n$.
   (b) Clasificar los ideales de $\mathbb{Z}_n$ para $n > 1$ entero. Pista: Ver primero para valores concretos.
11. (a) Probar que todo homomorfismo de anillos **unitario** $f : \mathbb{K} \longrightarrow A$ con dominio un cuerpo es inyectivo. ¿Pueden existir homomorfismos de anillos unitarios que vayan de $\mathbb{Q}$ en $\mathbb{Z}$?
   (b) ¿Podemos sustituir que el homomorfismo sea unitario por **no nulo**? Hallar (y demostrar) bajo que condiciones son nociones equivalentes el ser no nulo y el ser unitario.
   (c) Dar un ejemplo de homomorfismo entre anillos unitarios con dominio un cuerpo que no sea ni nulo, ni unitario. Pista: ¿En qué parte falla la prueba de (b)?
12. Sean $\mathbb{K}$ un cuerpo que contiene a los números racionales y $f : \mathbb{Q} \to \mathbb{K}$ un homomorfismo de cuerpos. Demostrar que $f(x) = x$ para cada $x \in \mathbb{Q}$. Deducir que el único endomorfismo del cuerpo $\mathbb{R}$ es la identidad.
13. Sea A un anillo unitario, conmutativo y finito. Demostrar que todo elemento no nulo de A es divisor de cero o unidad. Deducir que si A es un dominio de integridad entonces es un cuerpo.
14. Demostrar que el homomorfismo $\pi_4 : \mathbb{Z} \to \mathbb{Z}_4; n \mapsto n + 4\mathbb{Z}$ transforma todos los cuadrados de enteros impares en el mismo elemento. Deducir que ningún elemento de la sucesión $11, 111, 1111, \ldots$ es un cuadrado.
15. (a) Demostrar que
$$\mathbb{Q}[i] = \{a + ib : a, b \in \mathbb{Q}\}$$
   es un subcuerpo de $\mathbb{C}$ isomorfo al cuerpo de fracciones de $\mathbb{Z}[i]$.
   (b) Probar que $S = \{(a - b) + i(a + b) : a, b \in \mathbb{Z}\}$ es un ideal en $\mathbb{Z}[i]$.
16. Sea $C^\infty(\mathbb{R})$ el anillo de funciones $f : \mathbb{R} \to \mathbb{R}$ infinito diferenciables. Demostrar que el homomorfismo evaluación $\mathrm{ev}_0 : C^\infty(\mathbb{R}) \to \mathbb{R}; f \mapsto f(0)$ es sobreyectivo y su núcleo es un ideal maximal y principal.

[2] Un *elemento* $x \in A$ de un anillo se dice *nilpotente* si existe $m > 0$ entero tal que $x^m = 0$.