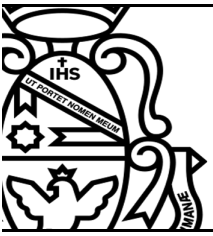

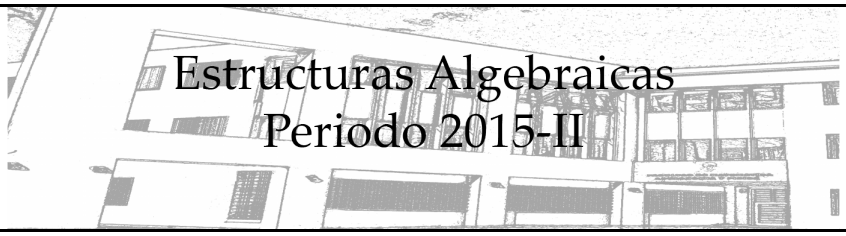

Estructuras Algebraicas
Periodo 2015-II

FAMAF

Práctico 6

1. Sean R un Dominio de Ideales Principales e I un ideal en R distinto de cero. Probar que I es maximal si y sólo si I es primo.

2. Sea $R := \{a + b\sqrt{10} \,|\, a, b \in \mathbb{Z}\}$. Probar las siguientes afirmaciones.

   (a) R es subanillo de $\mathbb{R}$.

   (b) La función $N : R \to \mathbb{Z}$ dada por $N(a + b\sqrt{10}) := a^2 - 10b^2$ satisface $N(uv) = N(u)N(v)$, para todo u, $v \in R$.

   (c) $N(u) = 0$ si y sólo si $u = 0$.

   (d) u es una unidad en R si y sólo si $N(u) = \pm 1$.

   (e) 2, 3, $4 + \sqrt{10}$ y $4 - \sqrt{10}$ son elementos irreducibles de R.

   (f) 2, 3, $4 + \sqrt{10}$ y $4 - \sqrt{10}$ no son elementos primos de R.

3. (a) Si a, $n \in \mathbb{Z}$, con $n > 0$, entonces existen q, $r \in \mathbb{Z}$ tales que $a = qn + r$, donde $|r| \leq n/2$.

   (b) Los enteros Gaussianos $\mathbb{Z}[i]$ forman un dominio Euclidiano con $\varphi(a + bi) = a^2 + b^2$.

4. Sea R el anillo $\mathbb{Z}[\sqrt{2}]$ Pruebe que R es un domino Euclidiano considerando *la norma*

$$\varphi(a + b\sqrt{2}) = |a^2 - 2b^2|$$

   donde $|\cdot|$ es valor absoluto. ¿Qué puede decir de las unidades de R? Pruebe que $\sqrt{2}$ y los primos de $\mathbb{Z}$ de la forma $8k + 3$ ó $8k + 5$ son primos en R ¿Puede caracterizar los primos de $\mathbb{Z}[\sqrt{2}]$?

5. Determine todas las unidades en el anillo de enteros Gaussianos $\mathbb{Z}[i]$.

6. Calcular el máximo común divisor de $11 + 7i$ y $18 - i$ en $\mathbb{Z}[i]$.

7. Sea R un dominio de factorización única (DFU), $d \in R$, $d \neq 0$. Probar que existe sólo un número finito de ideales principales distintos que contienen al ideal (d).

8. Si R es un dominio de factorización única, a, $b \in R$ *coprimos* (i. e. el máximo común divisor de a y b es una unidad) y $a|bc$, entonces $a|c$.

9. Sea (R, φ) dominio Euclidiano (DE), $a \in R$. Probar que a es unidad en R si y sólo si $\varphi(a) = \varphi(1_R)$.

10. (Algoritmo Euclidiano). Sea (R, φ) un dominio Euclidiano (DE). Sean a, $b \in R$, con $b \neq 0$. Usando sucesivamente la propiedad (ii) de la definición de anillo Euclidiano[1] se tiene:

$$\begin{array}{rlll}
a = q_0 b + r_1 & \text{con} & r_1 = 0 & \text{ó} \quad \varphi(r_1) < \varphi(b); \\
b = q_1 r_1 + r_2 & \text{con} & r_2 = 0 & \text{ó} \quad \varphi(r_2) < \varphi(r_1); \\
r_1 = q_2 r_2 + r_3 & \text{con} & r_3 = 0 & \text{ó} \quad \varphi(r_3) < \varphi(r_2); \\
\vdots & & & \\
r_k = q_{k+1} r_{k+1} + r_{k+2} & \text{con} & r_{k+2} = 0 & \text{ó} \quad \varphi(r_{k+2}) < \varphi(r_{k+1}); \\
\vdots & & &
\end{array}$$

    Sea $r_0 = b$ y sea n el mínimo entero tal que $r_{n+1} = 0$ (un tal n existe pues $(\varphi(r_k))_k$ forma una sucesión estrictamente decreciente de enteros no negativos). Probar que r_n es el máximo común divisor de a y b.

11. Sea $\mathbb{K}$ cuerpo. Probar que (x) es un ideal maximal en $\mathbb{K}[x]$.

[1] Hungerford, Def. III.3.8, pag. 139.

12. (a) Si D es un dominio íntegro y c es un elemento irreducible en D, entonces $D[x]$ no es un dominio de ideales principales (DIP).
    (b) Mostrar que $\mathbb{Z}[x]$ no es un dominio de ideales principales.
    (c) Sea $\mathbb{K}$ cuerpo y $n \in \mathbb{Z}$, con $n \geq 2$. Probar que $\mathbb{K}[x_1, \ldots, x_n]$ no es un dominio de ideales principales. [Ayuda: mostrar que x_1 es irreducible en $\mathbb{K}[x_1, \ldots, x_n]$].

13. Encuentre todas las soluciones de $x^2 - 3x - 4 = 0$ en $\mathbb{Z}_6$.

14. Sea R el anillo de polinomios $\mathbb{Z}[x]$ y sea $I = \{f(x) \in R : f(-1) = f(1) = 0\}$. Pruebe que I es un ideal principal de R.

15. Sean D un dominio íntegro y c_j, $d_j \in D$, $0 \leq j \leq n$, con $c_0, \ldots, c_n$ distintos entre sí. Probar que existe a lo sumo un polinomio $f \in D[x]$ de grado n tal que $f(c_j) = d_j$, $0 \leq j \leq n$.

16. Sea $\mathbb{K}$ un cuerpo y sea R el anillo de polinomios $\mathbb{K}[x, y]$. Fije dos elementos a y b de $\mathbb{K}$. Pruebe que el ideal $I = (x - a, y - b)$ es un ideal maximal de R ¿Qué puede decir si consideramos más variables?

17. Pruebe que $\mathbb{Q}[x]/(x^2 - 2)$ es un anillo isomorfo a $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

18. Pruebe que $f(x) = x^2 + 1$ es un polinomio reducible en $\mathbb{Z}_2[x]$ y que $f(x) = x^2 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$. ¿Cuántos polinomios irreducibles de grado 2 tiene $\mathbb{Z}_2[x]$?

19. Sea R el anillo $\mathbb{Z}[z_0] := \{a + bz_0 : a, b \in \mathbb{Z}\}$ donde z_0 es el número complejo $z_0 := \frac{1}{2}(1 + \sqrt{19}i)$ y considere *la norma* en R, $|\cdot|$, inducida por la norma usual de $\mathbb{C}$. Pruebe los siguientes enunciados:
    (a) $a + bz_0$ es unidad en $\mathbb{Z}[z_0]$ si y solo si $|a + bz_0| = 1$ si y solo si $\mathbb{Z}[z_0]$ es 1 o -1.
    [Hint: $|a + bz_0| = a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2$.]
    (b) Muestre que 3 y 2 son elementos irreducibles de $\mathbb{Z}[z_0]$.
    [Hint: Muestre que no existe un $a + bz_0$ tal que $|a + bz_0| = (a + \frac{b}{2})^2 + \frac{19}{4}b^2 = 2$]
    (c) Pruebe que R no puede ser un dominio Euclídeo.
    [Hint: Razone por el absurdo y suponga que existe φ tal que (R, φ) es dominio Euclídeo. Fije un $w \in R$ que no sea cero ni unidad tal que $\varphi(w)$ es mínimo y aplique *algoritmo de la división* a 2 y w; e.d. $2 = wq + r$.]

20. Pruebe que:
    (a) DE $\Rightarrow$ DIP con identidad.
    (b) DIP $\Rightarrow$ DFU.

    Dar contraejemplos que muestren que las recíprocas no son ciertas.

21. Describir los siguientes anillos.
    (a) $\mathbb{Z}[x]/(2, x)$.
    (b) $\mathbb{Z}[x]/(2x)$.
    (c) $\mathbb{Z}[i]/(i)$.
    (d) $\mathbb{Z}[i]/(1 + i)$.

22. (a) Sea R el anillo de todas las matrices 2×2 sobre $\mathbb{Z}$. Probar que, para todo $A \in R$, $(x + A)(x - A) = x^2 - A^2$ en $R[x]$.
    (b) Sea R un anillo cualquiera y sean f, g, $h \in R[x]$ tales que $f = gh$. ¿Puede asegurar que $f(r) = g(r)h(r)$, para todo $r \in R$?

23. Estudiar el criterio de Eisenstein [Hungerford, Chap III, Th. 6.15].

24. Pruebe que $x^n - 2$ es un polinomio irreducible de $\mathbb{Z}[x]$ para todo $n \geq 1$; en consecuencia hay polinomios irreducibles en $\mathbb{Z}[x]$ de cualquier grado.

25. Encuentre un máximo común divisor de $x^m - 1$ y $x^n - 1$ en $\mathbb{Z}[x]$.

26. Sean p un número primo en $\mathbb{Z}$ y $f \in \mathbb{Z}[x]$ con $\text{grad}(f) \geq 1$. Sea $\overline{f}$ el polinomio en $\mathbb{Z}_p[x]$ obtenido de f reduciendo todos los coeficientes módulo p. Si $\overline{f}$ es irreducible sobre $\mathbb{Z}_p[x]$ y $\text{grad}(f) = \text{grad}(\overline{f})$, entonces f es irreducible en $\mathbb{Q}[x]$.

27. Considere el polinomio $f(x) = x^4 - 10x^2 + 1$ en $\mathbb{Q}[x]$. Pruebe que $\overline{f(x)} := f(x) \bmod(p)$ es reducible para cualquier primo p mientras que $f(x)$ es irreducible en $\mathbb{Q}[x]$.

28. Encuentre la descomposición de $f(x) = x^5 - 3x^3 + 3x^2 + 4x + 2$ como producto de polinomios irreducibles en $\mathbb{Z}_5[x]$.

29. Sea D un dominio entero y $c \in D$. Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$ y $g(x) = f(x - c)$. Entonces f(x) es irreducible en $D[x]$ si y solo si $g(x)$ es irreducible.

30. Sea p un número primo y sea $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$. Probar que $f(x)$ es irreducible en $\mathbb{Z}[x]$. ¿Es irreducible en $\mathbb{Q}[x]$? ¿en $\mathbb{R}[x]$?

31. Sea $f(x, y) = xy^2 - x^4$, polinomio en $\mathbb{Z}[x, y]$. Factorizar f como producto de polinomios irreducibles en $\mathbb{Z}[x, y]$. Hacer lo mismo para el polinomio $f(x) = x^3 + (3m - 1)x + (3n + 1)$, polinomio en $\mathbb{Q}[x]$, donde $m, n \in \mathbb{Z}$ y $f(x, y, z) = x^3 + y^3 + z^3 - 3xyz$, visto como polinomio de $\mathbb{Z}[x, y, z]$ y visto como polinomio de $\mathbb{C}[x, y, z]$.

Ejercicios Adicionales

1. [Cohen] Sea R un anillo conmutativo con identidad. Si todo ideal primo de R es principal entonces TODOS los ideales de R son principales.

2. ¿Se puede saber los primos de $\mathbb{Z}[\sqrt{-1}]$?

   (a) [Fermat's Christmas Theorem] Sea p un número primo en $\mathbb{Z}$. Las siguientes condiciones son equivalentes:

      i. $p = 2$ ó p es de la forma $4k + 1$.
      ii. La ecuación $x^2 \equiv -1 \pmod{p}$ tiene solución.
      iii. p es compuesto en $\mathbb{Z}[\sqrt{-1}]$.
      iv. p es la suma de dos cuadrados en $\mathbb{Z}$.

      [Hint: Pequeño teorema de Fermat para estudiar la cantidad de raíces de $x^{p-1} - 1$ en $\mathbb{Z}_p$]

   (b) Pruebe que todo primo en $\mathbb{Z}[\sqrt{-1}]$ es asociado a uno de los siguientes primos:

      i. $1 + \sqrt{-1}$
      ii. $z = a + b\sqrt{-1}$ o $\overline{z} = a - b\sqrt{-1}$ donde $\varphi(z) = a^2 + b^2 = p$ siendo p un número primo impar en $\mathbb{Z}$ de la forma $4k + 1$.
      iii. p un número primo impar en $\mathbb{Z}$ de la forma $4k + 3$.

3. [McCoy 1942] Sea R anillo conmutativo con identidad. Si $f(x) = \sum_{j=0}^{n} a_j x^j$ es un divisor de cero en $R[x]$, entonces existe $b \in R$, $b \neq 0$, tal que $ba_n = ba_{n-1} = \cdots = ba_0 = 0$.

4. Sea $\mathbb{K}$ un cuerpo y f un polinomio en $\mathbb{K}[x]$ de grado 2 ó de grado 3, entonces f es reducible en $\mathbb{K}[x]$ si y solo si f tiene una raíz en $\mathbb{K}$.

5. Sean R anillo conmutativo con identidad y $f(x) = \sum_{j=0}^{n} a_j x^j \in R[x]$. Probar que f es unidad en $R[x]$ si y sólo si a_0 es unidad en R y $a_1, \ldots, a_n$ son elementos nilpotentes de R.

6. Sea $\mathbb{K}$ un cuerpo y $f(x)$ irreducible sobre $\mathbb{K}[x]$. Pruebe que existe un cuerpo $\overline{\mathbb{K}}$ *extendiendo a* $\mathbb{K}$ tal que f tiene un raíz en $\overline{\mathbb{K}}$.

7. Sea p un número primo en $\mathbb{Z}$, y sean $\mathbb{K}$ un cuerpo y $c \in \mathbb{K}$. Pruebe que:

   (a) $x^p - c$ es irreducible en $\mathbb{K}[x]$ si y solo si $x^p - c$ no tiene raíces en $\mathbb{K}$.

   (b) Si $\text{char}(\mathbb{K}) = p$, entonces $x^p - x - c$ es irreducible en $\mathbb{K}[x]$ si y solo si $x^p - x - c$ no tiene raíces en $\mathbb{K}$. Si $\text{char}(\mathbb{K}) = 0$, el resultado es falso.

8. ¿Se pueden saber los ideales primos de $\mathbb{Z}[x]$?
   Pruebe que los ideales de la forma

   (a) $(f(x))$ con $f(x)$ irreducible
   (b) (p) con p un número primo de $\mathbb{Z}$.
   (c) $(p, f(x))$ con p primo y $f(x)$ irreducible en $\mathbb{Z}_p[x]$.
   (d) (0)

   son ideales primos de $\mathbb{Z}[x]$ (y de hecho, se puede probar que son los únicos ideales primos).