ESTRUCTURAS ALGEBRAICAS. Hoja de problemas 6

1. Factoriza los siguientes polinomios en su correspondiente anillo:
   (a) $X^5 + 2X + 2 \in \mathbb{Q}[X]$;
   (b) $X^4 - 1$ en $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{F}_2[X]$ y $\mathbb{F}_3[X]$;
   (c) $X^4 + X^3 - X^2 \in \mathbb{F}_2[X]$.

2. Sea p un número primo.
   a) Demuestra que todos los elementos del grupo multiplicativo $\mathbb{F}_p{}^*$ son raíces del polinomio $X^{p-1} - 1$.
   b) Deduce que el polinomio $X^{p-1} - 1 \in \mathbb{F}_p[X]$ factoriza como producto de $p-1$ polinomios mónicos de grado uno.

3. Sea K un cuerpo de característica p.
   i) Demuestra que $(x + y)^p = x^p + y^p$ para todo $x, y \in K$.
   ii) Deduce que si K es finito la aplicación $x \to x^p$ define un automorfismo de K (el automorfismo de Frobenius).

4. Encuentra un generador del ideal de $\mathbb{Q}[X]$ generado por los polinomios $X^4 + 3X^3 + 2X + 4$ y $X^2 - X - 1$ y en y exprésalo en términos de estos polinomios. ¿Y en $\mathbb{F}_7[X]$?

5. Construye cuerpos con 8, 25 y 125 elementos. (Sugerencia: Procede de forma análoga a la construcción del cuerpo con 4 elementos $\mathbb{F}_2[X]/(X^2 + X + 1)$ que hicimos en clase).

6. Demostrar que **todo cuerpo finito K tiene p^n elementos** para algún $n \in \mathbb{N}$. (Sugerencia: Si $\mathrm{ch}(K) = p$ entonces K contiene al cuerpo $\mathbb{F}_p$ y es, por tanto, un espacio vectorial sobre él). **¡No hay cuerpos con 6 elementos!**

7. 1) Sea G un grupo abeliano $G = G(p_1) \times \cdots \times G(p_d)$ su descomposición como producto directo de sus p-grupos de Sylow. Prueba que G es cíclico $\Leftrightarrow$ cada $G(p_i)$ lo es.
   2) Sea K un cuerpo finito conmutativo (en realidad todos lo son pero eso no es obvio) y consideremos el grupo $G = K^*$. Demuestra que que cada p-grupos de Sylow es cíclico (pues de lo contrario el polinomio $X^{p^r} - 1$, donde p^r es el exponente del grupo, tendría más de p^r raíces).
   3) Concluye que **el grupo multiplicativo de un cuerpo finito es cíclico**.

8. Sea $\phi : A \to B$ un homomorfismo de anillos. Prueba que si A es un cuerpo ϕ es necesariamente inyectivo.

9. Prueba que la conjugación compleja es un automorfismo del cuerpo $\mathbb{C}$.

10. Sea p un número primo. Se considera el conjunto
$$\mathbb{Z}_{(p)} := \left\{ x \in \mathbb{Q} : x = \frac{r}{s} \text{ donde } r, s \in \mathbb{Z} \text{ y } p \text{ no divide a } s \right\}. \quad \text{Se pide}$$
    (a) Demostrar que $\mathbb{Z}_{(p)}$ es un subanillo de $\mathbb{Q}$ (*el localizado de* $\mathbb{Z}$ *en* (p)) y halla el conjunto de las unidades $U(\mathbb{Z}_{(p)}) = \mathbb{Z}^*_{(p)}$.
    (b) Identificar el cuerpo de fracciones de $\mathbb{Z}_{(p)}$.
    (c) Probar que $\mathbb{Z}_{(p)}$ es un anillo principal (y, por tanto, factorial), demostrando que todos sus ideales son de la forma $(p^k) := p^k\mathbb{Z}_{(p)}$. Mostrar la factorización en elementos irreducibles de $75/8$ en $\mathbb{Z}_{(p)}$ para $p = 3, 5$ y 7. (¿Por qué no se pregunta para $p = 2$?).
    (d) Deducir que $(p) := p\mathbb{Z}_{(p)}$ es el único ideal maximal de $\mathbb{Z}_{(p)}$.
    (e) Calcular el núcleo del (único) homomorfismo $\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$.
    (f) Demostrar que el homomorfismo $\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ anterior es suprayectivo. (Sugerencia: Para todo $r/s \in \mathbb{Z}_{(p)}$ y para todo entero m entre 0 y $p-1$ los números $r - ms$ son todos distintos módulo p, luego alguno de ellos es múltiplo de p).

(g) Utiliza el teorema de isomorfía relativo al homomorfismo anterior para identificar qué cuerpo es el anillo cociente de $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$.

11. (a) Prueba que $\mathbb{Z}[\sqrt{-3}] = \left\{a + b\sqrt{3}i; a, b \in \mathbb{Z}\right\}$ es un subanillo de $\mathbb{C}$.

    (b) Prueba que este anillo no es factorial exhibiendo dos factorizaciones distintas de 4.

12. Prueba que el polinomio $Y^5 + X^2Y^4 + X^3Y^3 + X^6Y^2 + X^5Y + X$ es un elemento irreducible de $\mathbb{Q}[X, Y]$.

13. Demostrar que el ieal $I = (3X + 2Y, 3Y) \subset K[X, Y]$ es un ideal maximal si $char(K) \neq 3$ y que es primo no maximal si $char(K) = 3$.

14. Sea K un cuerpo conmutativo y considereremos el homomorfismo

$$\phi := ev_{(T^2,T^3)} : K[X, Y] \to K[T] \quad \text{definido por} \quad \phi(\sum_{ij} a_{ij}X^iY^j) = \sum_{ij} a_{ij}T^{2i}T^{3j}. \quad \text{Se pide}$$

- Comprueba que el ideal $(Y^2 - X^3)$ está contenido en $Ker\phi$.
- Demuestra que, por ser $Y^2 - X^3$ mónico como polinomio en $K[X][Y]$, cualquier polinomio $F(X, Y) \in K[X, Y]$ se puede escribir en la forma

$$F(X, Y) = d(X, Y)(Y^2 - X^3) + a(X) + b(X)Y$$

  donde $d(X, Y) \in K[X, Y]$ y $a(X), b(X) \in K[X]$.
- Deduce de lo anterior que $Ker\phi = (Y^2 - X^3)$.
- Demuestra que la imagen de ϕ es el subanillo $K[T^2, T^3]$ que consiste de todos los polinomios $\sum_i a_iT^i$ con $a_1 = 0$, i.e. todos los polinomios de la forma $a_0 + a_2T^2 + a_3T^3 + \cdots$
- Con todos los datos anteriores explica qué dice el teorema de isomorfía para el homomorfismo ϕ y concluye que $K[X, Y]/(Y^2 - X^3)$ es un dominio de integridad, que el ideal $(Y^2 - X^3) \subset K[X, Y]$ es primo pero no maximal y que $Y^2 - X^3$ es un elemento irreducible de $K[X, Y]$.
- Prueba que $K[X, Y]/(Y^2 - X^3)$ no es principal mostrando que el ideal generado por las clases $\overline{X}$ de X e $\overline{Y}$ de Y no lo es. (Sugerencia: Trabajar con el correspondiente ideal de $K[T^2, T^3]$).
- Usando de nuevo el isomorfismo $K[X, Y]/(Y^2 - X^3) \cong K[T^2, T^3]$ demuestra que $\overline{X}$ e $\overline{Y}$ son elementos irreducibles de $K[X, Y]/(Y^2 - X^3)$.
- De la relación $\overline{Y}^2 = \overline{X}^3$ concluye que el dominio $K[X, Y]/(Y^2 - X^3)$ no sólo no es principal sino que no es ni siquiera factorial.
- Observa que la situación habría sido muy distinta si en la redacción de este ejercicio hubiéramos sustituido el polinomio $Y^2 - X^3$ por el polinomio $Y - X^2$ y, en particular, que entonces el anillo cociente resultante sí habría sido factorial.
  Este hecho tiene que ver con que el últimoo poliniomio representa una parábola, que no tiene puntos singulares, mientras que el anterior representa una cúbica con un punto singular en el origen. Una rama de la matemáticas, la Geometría Algebraica, tiene como objetivo principal el estudio de las propiedades geométricas de ecuaciones polinómicas $F(X_1, \cdots, X_n) = 0$ mediante el estudio de las propiedades algebraícas de los correspondientes anillos cociente $K[X_1, \cdots, X_n]/(F(X_1, \cdots, X_n))$.