FACULTAD DE
CIENCIAS
UNIVERSIDAD DE CHILE

Apuntes de Ayudantía

Cuerpos y álgebras

Claudio Bravo Castillo
November 29, 2017

Contents

1. Ejercicios de Cuerpos:

1.1. **Parte básica:**

Problema 1.1. Sea A un dominio de integridad. Pruebe que si A es finito entonces A es cuerpo. Muestre que si A es un k-espacio vectorial de dimensión finita, entonces A es cuerpo.

Problema 1.2. Demuestre que si $\text{car}(F) = 0$, entonces $\mathbb{Q}$ es la intersección de todos los cuerpos contenidos en F. Encuentre un análogo a la proposición anterior para $\text{car}(F) = p$.

Problema 1.3. Sea p primo y $\mathbb{F}_p$ el cuerpo de p elementos. Demuestre que la función $x \mapsto x^p - x$ es nula sobre $\mathbb{F}_p$, pero el polinomio $x^p - x$ no es nulo.

Problema 1.4. Sea F un cuerpo tal que $\text{car}(F) = p$ y $\alpha \in F$. Pruebe que el polinomio $p(x) = x^p - \alpha$ tiene a lo más una raiz en F. Demuestre lo mismo para el polinomio $q(x) = x^{p^k} - \alpha$, donde $k \in \mathbb{N}$.

Problema 1.5. Demuestre que $p(x) = x^3 - 2x - 2$ es un polinomio irreducible sobre $\mathbb{Q}[x]$. Si θ es una raiz de $p(x)$ escriba $(1+\theta+\theta^2)^{-1}(1+\theta)$ y $(1+\theta+\theta^2)(1+\theta)$ como una $\mathbb{Q}$-combinación lineal de $1, \theta, \theta^2$.

Problema 1.6. Sea $F = \mathbb{Q}(\sqrt[n]{2})$ el mínimo cuerpo en $\mathbb{R}$ que contiene a $\mathbb{Q}$ y $\sqrt[n]{2}$. Demuestre que $F = \{a_0 + a_1\sqrt[n]{2} + \cdots + a_{n-1}\sqrt[n]{2^{n-1}} : a_i \in \mathbb{Q}\}$. Determine $[F : \mathbb{Q}]$.

Problema 1.7. Sea $F = \mathbb{F}_2$ el cuerpo de 2 elementos. Muestre que $p(x) = x^2+x+1$ es un polinomio irreducible sobre F. Si θ es una raiz de $p(x)$, demuestre que $[F(\theta) : F] = 2$. Calcule la tabla de multiplicación de $F(\theta)$.

Problema 1.8. Demuestre que si $p \equiv 3 (\text{mod } 4)$, entonces el polinomio $x^2 + 1$ es irreducible sobre $\mathbb{F}_p[x]$.

Problema 1.9. Pruebe que la función $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ es un automorfismo de $\mathbb{Q}(\sqrt{2})$.

1.2. **Extensiones de cuerpos:**

Problema 1.10. Sea F una extensión de k tal que $[F : k] = p$ primo. Pruebe que los únicos cuerpos L tales que $k \subset L \subset F$ son $L = k$ y $L = F$.

Problema 1.11. Calcule $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ y $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$.

Problema 1.12. Demuestre que $F = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ es una extensión de grado 6 de $\mathbb{Q}$. Demostrar que $F = \mathbb{Q}(\sqrt{-3} + \sqrt[3]{5})$ y encontrar el polinomio irreducible de $\sqrt{-3} + \sqrt[3]{5}$ sobre $\mathbb{Q}$.

Problema 1.13. Sea K/F una extensión de cuerpos y sea $\alpha \in K$ tal que $[F(\alpha) : F]$ es finito e impar. Muestre que $\alpha^2 \in K$ cumple con que $[F(\alpha^2) : F]$ es finito e impar y que $F(\alpha) = F(\alpha^2)$.

Problema 1.14. Sea $\rho = e^{\frac{2\pi i}{p}} \in \mathbb{C}$, para $p \neq 2$ primo y sea $F = \mathbb{Q}(\rho)$. Determine $[F : \mathbb{Q}]$ y $[\mathbb{Q}(\rho + \rho^{-1}) : \mathbb{Q}]$.

Problema 1.15. Demuestre que no existe una extensión $L = \mathbb{R}(\theta)$ de $\mathbb{R}$ de grado 3.

Problema 1.16. Sea θ una raiz del polinomio $x^5 + 2x + 1 + i \in \mathbb{Z}[i][x]$. Determine el grado de $\mathbb{Q}(i, \theta)$ sobre $\mathbb{Q}(i)$.

1.3. **Extensiones algebraicas:**

Problema 1.17. Sea $\overline{\mathbb{Q}}$ el cuerpo de todos los números complejos que son algebraicos sobre $\mathbb{Q}$. Demuestre que $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Problema 1.18. Sea $k \subset F \subset K$ cuerpos y sea $\alpha \in K$ un elemento algebraico sobre k. Pruebe que $\alpha \in K$ es algebraicos sobre F y que $\mathrm{irr}_{F,\alpha}(x)$ divide a $\mathrm{irr}_{k,\alpha}(x)$. Concluya que $[F(\alpha) : F] \leq [k(\alpha) : k]$.

Problema 1.19. Sean L, F dos extensiones de k. Considere $L, F \subset K$, para un cierto cuerpo K. Se define el composito LF de L y F como el mínimo subcuerpo de K que contiene a L Y F. Demuestre que si $[F : k], [L : k] < \infty$ entonces $[LF : k] < \infty$ y $[F : k], [L : k]$ dividen a $[LF : k]$.

Problema 1.20. Pruebe que el composito entre $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ es $\mathbb{Q}(\sqrt[6]{2})$.

Problema 1.21. Demustre que $\mathbb{R}(x)$ es una extensión algebraica de $\mathbb{R}(x + x^{-1})$. Determine el grado entre estas extensiones.

Problema 1.22. Sea K una extensión de F y $\alpha \in K$ un elemento transcendente sobre F. Demustre que existe un isomorfismo de cuerpos entre $F(x) = \mathrm{Quot}(F[x])$ y $F(\alpha)$, que es la identidad sobre F.

Problema 1.23. Usando el hecho de que π es trascendente sobre $\mathbb{Q}$, pruebe que π^2 es transcendente sobre $\mathbb{Q}$.

1.4. **Cuerpo de descomposición:**

Problema 1.24. Sea L el cuerpo de descomposición de $p(x) = x^5 - 2$. Determine $[L : \mathbb{Q}]$.

Problema 1.25. Determine el cuerpo de descomposición de $p(x) = x^4 + 3$ sobre $\mathbb{Q}$.

Problema 1.26. Determine el cuerpo de descomposición L de $p(x) = x^4 - 2 - i$ sobre $\mathbb{Q}(i)$. Luego calcule $[L : \mathbb{Q}]$.

Problema 1.27. Determine el cuerpo de descomposición de $p(x) = x^4 - 6x^2 + 2$ sobre $\mathbb{Q}$.

Problema 1.28. Considere el cuerpo de descomposición $E = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ del polinomio $f(x) = (x^2 - 2)(x^2 - 3)$ sobre $\mathbb{Q}$. Pruebe que $\varphi : E \longrightarrow E$ definido por $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$, para todo $a, b \in \mathbb{Q}(\sqrt{3})$, es un automorfismo de E tal que $\varphi(x) = x$ para todo x en $\mathbb{Q}(\sqrt{3})$.

Problema 1.29. Sea α algebraico sobre F. Pruebe que cada homomorfismo φ de $F(\alpha)$ en $\overline{F}$ tal que $\varphi(a) = a \ \ \forall\, a \in F$ lleva α en un conjugado β de α sobre F.

Problema 1.30. Sea $n \in \mathbb{N}$ y $\mathbb{F}_p$ el cuerpo de p elementos. Sea L el cuerpo de descomposicón del polinomio $G(x) = x^{p^n} - x$ sobre $\mathbb{F}_p[x]$. Muestre que $G(x)$ no tiene raices repetidas y que $G(x)$ es reducible sobre $\mathbb{F}_p[x]$. Pruebe que L es el conjunto de raices de $G(x)$. Concluya que $[L : \mathbb{F}_p] = n$.

1.5. **Cuerpos algebraicamente cerrados y finitos:**

Problema 1.31. Sea $\overline{\mathbb{Q}}$ el cuerpo de todos los números complejos que son algebraicos sobre $\mathbb{Q}$. Demuestre que $\overline{\mathbb{Q}}$ es numerable. Pruebe que $\overline{\mathbb{Q}} \cap \mathbb{R}$ es un subcuerpo propio de $\mathbb{R}$. Concluya que $\overline{\mathbb{Q}}$ es un subcuerpo propio de $\mathbb{C}$.

Problema 1.32. Muestre que $p(y) = y^2 + x \in \mathbb{C}(x)[y]$ es irreducible. Concluya que $\mathbb{C}(x)$ no es un cuerpo algebraicamente cerrado.

Problema 1.33. Sea K un cuerpo cualquiera. Pruebe que la clausura algebraica de K tiene cardinal infinito.

Problema 1.34. Demuestre que la clausura algebraica de $\mathbb{Q}$ y $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, entendidas como subconjuntos de $\mathbb{C}$, son iguales.

Problema 1.35. Sea $\mathbb{F}_p$ el cuerpo de p elementos y F la extensión de $\mathbb{F}_p$ de grado n. Pruebe que F tiene p^n elementos y demuestre que para todo $\alpha \in F$ se tiene que $\alpha^{p^n} = \alpha$. Construya un cuerpo de 13^2 elementos.

Problema 1.36. Sea $\mathbb{F}_{p^n}$ la extensión de grado n de $\mathbb{F}_p$. Pruebe que en $\mathbb{F}_{p^n}$ hay $\frac{p^n+1}{2}$ cuadrados.

Problema 1.37. Sea $\mathbb{F}_{p^n} = \{\alpha_1, \cdots, \alpha_{p^n}\}$ la extensión de grado n de $\mathbb{F}_p$. Pruebe que $x^{p^n} - x = (x - \alpha_1) \cdots (x - \alpha_{p^n})$.

Problema 1.38. Sean $\mathbb{F}_{p^n}$ la extensión de grado n de $\mathbb{F}_p$ y $\mathbb{F}_{p^m}$ su análogo de grado m. Muestre que $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ si y solamente si $m|n$. Concluya que $x^{p^m} - x$ divide a $x^{p^n} - x$ sobre $\mathbb{F}_p[x]$ si y solamente si $m|n$.

Problema 1.39. Sea F cuerpo finito. Pruebe que para todo entero positivo n existe un polinomio irreducible en $F[x]$ de grado n.

1.6. **Extensiones separables y polinomios ciclotómicos:**

Problema 1.40. Sean $p(x), q(x) \in F[x]$ dos polinomio separables. Muestre que $p(x)q(x)$ es separable si y solamente si $(p(x), q(x)) = F[x]$.

Problema 1.41. Demustre que $p(x) = x^3 + 5x^2 + 8x + 4$ no es un polinomio separable sobre $\mathbb{Q}$.

Problema 1.42. Pruebe que $x^p - x + a$ es irreducible y separable en $\mathbb{F}_p$ para cualquier primo p y cualquier $a \in \mathbb{F}_p^*$. Sea $\alpha \in \overline{\mathbb{F}_p}$ una raiz de $p(x)$. Pruebe que $\{\alpha + b : b \in \mathbb{F}_p\}$ es el conjunto de todas las raices de $p(x)$.

Problema 1.43. Pruebe que toda extensión finita de un cuerpo finito es separable.

Problema 1.44. Sea K/F una extensión separable con la propiedad que existe $n \in \mathbb{N}$ tal que $[F(\alpha) : F] \leq n$, para todo $\alpha \in K$. Muestre que K/F es finita y que $[K : F] \leq n$.

Problema 1.45. Pruebe que si $n = p^k m$, donde p es primo y m es relativamente primo con p entonces hay exactamente m raíces distintas $n-$ ésimas de la unidad sobre un cuerpo de característica p.

Problema 1.46. Sea $K = \mathbb{F}_p(x, t)$ y $F = \mathbb{F}_p(x^p, t^p)$. Pruebe que K es una extensión de F de grado p^2. Demuestre que K/F no es una extensión separable.

Problema 1.47. Sea $\mathbb{F}_{2^2}$ el cuerpo de 4 elementos. Encuentre $\theta \in \mathbb{F}_{2^2}$ tal que $\mathbb{F}(\theta) = \mathbb{F}_{2^2}$. Equivalentemente, encuentre un polonimio $p(x) \in \mathbb{F}_2[x]$ irreducible y de grado 2.

Problema 1.48. Sea $p(x) = x^n - p$, para p primo y sea F su cuerpo de descomposición sobre $\mathbb{Q}$. Calcule $[F : \mathbb{Q}]$.

Problema 1.49. Demuestre que $F = \mathbb{Q}(\text{sen}(2\pi/n))$ es un subcuerpo de $\mathbb{Q}(e^{\frac{2\pi i}{n}})$. Calcule $[F : \mathbb{Q}]$, para $n \geq 3$.

Problema 1.50. Pruebe que si n es impar $n > 1$, entonces $\Phi_{2n}(x) = \Phi_n(x)$.

Problema 1.51. Encuentre el n-ésimo polinomio ciclotómico para $n = 6, 8, 9, 10$ y 12.

1.7. **Teoría de Galois:**

Problema 1.52. Sea F el cuerpo de descomposición de $p(x) = x^3 - 2$. Demuestre que $F/\mathbb{Q}$ es una extensión galoisiana. Calcule $\text{Gal}(F/\mathbb{Q})$.

Problema 1.53. Sean $p, q \in \mathbb{Z}$ primos distintos y $F = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Demustre que $F/\mathbb{Q}$ es una extensión galoisiana. Calcule $\text{Gal}(F/\mathbb{Q})$.

Problema 1.54. Probar que $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ es galoisiana y calcule su grupo de galois.

Problema 1.55. Determine explicitamente los automofismos de la extensión de cuerpos $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.

Problema 1.56. Sea $F = \mathbb{Q}(\sqrt{1 + \sqrt{2}})$. Sabiendo que $[F : \mathbb{Q}] = 4$, demuestre que $F/\mathbb{Q}$ es una extensión galoisiana.

Problema 1.57. Sea $p(x) = (x^{12}-16)(x^3-3) \in \mathbb{Q}[x]$. Pruebe que $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ es el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$. Demustre que $E/\mathbb{Q}$ es una extensión galoisiana.

Problema 1.58. Sea p primo. Pruebe que $\mathbb{F}_{p^n}$ es extensión de Galois sobre $\mathbb{F}_p$ con grupo de Galois cíclico de orden n generado por el automorfismo de Frobenius.

Problema 1.59. Sea K cuerpo cuya característica es relativamente prima con n. Sea ξ_n una raíz primitiva n-ésima de la unidad. Pruebe que $\mathrm{Gal}(K(\xi_n)/K)$ es abeliano.

Problema 1.60. Sea K un cuerpo que contiene a $\{x \in \overline{K} : x^n = 1\}$ y considere $F = K(\beta)$, donde $\mathrm{irr}_{\beta,K}(x) = x^n - a$. Demuestre que F/K es una extensión galoisiana y calcule su grupo de galois.

Problema 1.61. Sea $p(x) = x^p - x - a$, para cierto $a \in \mathbb{F}_p$. Sea $F = \mathbb{F}_p(\alpha)$, para una cierta raiz α de $p(x)$. Muestre que $F/\mathbb{F}_p$ es una extensión galoisiana y calcule $\mathrm{Aut}(F/\mathbb{F}_p)$. Concluya que $F = \mathbb{F}_{p^n}$ y que $p(x)$ es irreducible sobre $\mathbb{F}_p[x]$.

Problema 1.62. Pruebe que todo $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ cumple con $\sigma(\mathbb{R}^2) = \mathbb{R}^2$. Concluya que $a < b$ implica que $\sigma(a) < \sigma(b)$. Pruebe que $|a - b| < \frac{1}{m}$ implica que $|\sigma(a) - \sigma(b)| < \frac{1}{m}$. Concluya que σ es continua. Demustre, usando los hechos anteriores, que $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{id}\}$.

1.8. **Terema fundamental de Galois:**

Problema 1.63. Sea $F = \mathbb{Q}(\sqrt{10}, \sqrt{3})$. Encuentre todos los cuerpos L tales que $\mathbb{Q} \subseteq L \subseteq F$.

Problema 1.64. Sea $F = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. Encuentre todos los cuerpos L tales que $\mathbb{Q} \subseteq L \subseteq F$.

Problema 1.65. Sea $F = \mathbb{Q}(e^{\frac{2\pi i}{7}})$. Encuentre todos los cuerpos L tales que $\mathbb{Q} \subseteq L \subseteq F$.

Problema 1.66. Sea $F = \mathbb{Q}(e^{\frac{2\pi i}{p}})$, para $p \neq 2$ primo. Pruebe que existe una única extensión $L = \mathbb{Q}(\sqrt{D_p})$ de $\mathbb{Q}$ tal que $L \subseteq F$ y $D_p \in \mathbb{Z} - \mathbb{Z}^2$. Determine D_p para $p = 3$ y $p = 5$.

Problema 1.67. Sea K extensión de galois sobre F y sea F' una extensión cualquiera de F. Pruebe que KF' es extensión de galois sobre F' con grupo de galois isomorfo a un subgrupo de $\mathrm{Gal}(K/F)$. Más precisamente, pruebe que $\mathrm{Gal}(KF'/F') \simeq \mathrm{Gal}(K/K \cap F')$. Concluya que $[KF' : F] = \frac{[K:F][F':F]}{[K\cap F':F]}$.

Problema 1.68. Sean K_1, K_2 dos extensiones de galois sobre F. Demuestre que la intersección $K_1 \cap K_2$ es galois sobre F. Pruebe que el composito K_1K_2 es galois sobre F. Pruebe además que el grupo de galois $\mathrm{Gal}(K_1K_2/F)$ es isomorfo al subgrupo H de $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ formado por los elementos cuyas restricciones a la intersección $K_1 \cap K_2$ sean iguales.

Problema 1.69. Sean K_1, K_2 dos extensiones de galois sobre F tales que $K_1 \cap K_2 = F$. Pruebe que $\mathrm{Gal}(K_1K_2/F) = \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$. Recíprocamente, si K es galois sobre F y $G = \mathrm{Gal}(K/F) = G_1 \times G_2$, con G_1, G_2 subgrupos de G, pruebe que K es el composito de dos extensiones de Galois K_1 y K_2 de F tales que $K_1 \cap K_2 = F$.

Problema 1.70. Sea K/F extensión galoisiana, cuyo grupo de galois corresponde a $G = \mathrm{Gal}(K/F)$. Para $\alpha \in K$ definimos $N_{K/F}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha)$. Pruebe que $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$ y que $N_{K/F(\alpha)} \in F^*$, para todo $\alpha \in K^*$. Muestre que si $K = F(\alpha)$ y $\mathrm{irr}_{F,\alpha}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ entonces $N_{K/F}(\alpha) = (-1)^n a_0$.

Problema 1.71. Sea $K = \mathbb{F}_{p^n}$ y $F = \mathbb{F}_p$. Determine $N_{K/F}(\alpha)$, para $\alpha \in K$ elemento arbitrario.

Problema 1.72. Sea K/F extensión galoisiana, cuyo grupo de galois corresponde a $G = \mathrm{Gal}(K/F)$. Para $\alpha \in K$ definimos $tr_{K/F}(\alpha) = \sum_{\sigma\in G} \sigma(\alpha)$. Pruebe que $tr_{K/F}(\alpha+\beta) = tr_{K/F}(\alpha)+tr_{K/F}(\beta)$ y que $tr_{K/F(\alpha)} \in F$, para todo $\alpha \in K$. Muestre que si $K = F(\alpha)$ y $\mathrm{irr}_{F,\alpha}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ entonces $tr_{K/F}(\alpha) = a_{n-1}$.

1.9. **Extensiones por radicales:**

Problema 1.73. Sea $\rho = e^{\frac{2\pi i}{7}}$ y $\alpha = \rho + \rho^{-1}$. Muestre que ρ satisface el polinomio cuadrático $z^2 - \alpha z + 1 \in \mathbb{Q}(\alpha)$. Concluya que ρ satisface un polinomio soluble sobre $\mathbb{Q}(\alpha)$. Pruebe además que ρ satisface un polinomio soluble sobre $\mathbb{Q}$.

Problema 1.74. Sea F cuerpo tal que $\mathrm{car}(F) \neq 2$. Encuentre condiciones necesarias y suficientes para que $F(\sqrt{\alpha}) = F(\sqrt{\beta})$. Use esto para demostrar que $\mathbb{Q}(\sqrt{1-\sqrt{2}}) = \mathbb{Q}(i, \sqrt{2})$. Concluya que $p(x) = x^2 - 2x + 3$ es soluble sobre $\mathbb{Q}$.

Problema 1.75. Probar que si U, V son soluciones del sistema:

$$U^3 + V^3 = -b, \quad 3UV = -a,$$

entonces $U + V$ es solución de la ecuación $x^3 + ax + b = 0$. Utilizar este hecho para encontrar una solución de la ecuacioón.

Problema 1.76. Sean $\alpha_1, \alpha_2, \alpha_3$, las soluciones de la ecuación $x^3 + ax + b = 0$. Sea $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. Probar que $\delta^2 = 27b^2 - 4a^3$.

Problema 1.77. Sea $F(\alpha)/F$ una extension cúbica y $x^3 + ax + b = \mathrm{irr}_{F,\alpha}(x)$. Probar que $F(\alpha)/F$ es galoisiana si y solamente si $27b^2 - 4a^3$ es un cuadrado en F.

2. Ejercicios de Álgebras:

2.1. **Parte básica:**

Problema 2.1. Sea G grupo y sea R anillo conmutativo con unidad. Denote:

$$RG = \{f \in R^G \mid f(x) = 0 \text{ para casi todo } x \in G\}.$$

Defina suma y producto por escalar de los elementos de RG puntualmente y defina una multiplicación en RG por convolución:

$$(fg)(x) = \sum_{(y,z):\, x=yz} f(y)g(z),$$

Demuestre que RG, con la suma y productos anteriores, es una R- álgebra. RG se denomina álgebra de grupo de G sobre R.

Problema 2.2. Sea $A = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}$. Demuestre que:

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z} \right\},$$

es un ideal bilátero de A.

Problema 2.3. Sea R un anillo conmutativo con uno. Pruebe que $Z(\mathbb{M}_n(R)) = R \cdot \mathrm{id}$.

Problema 2.4. Sea R un anillo conmutativo con unidad, X un conjunto cualquiera y $x_0 \in X$ un elemento fijo. Muestre que $I = \{f : X \to R : f(x_0) = 0\}$ es un ideal bilátero de R^X.

Problema 2.5. Sea F cuerpo tal que $\mathrm{car}(F) \neq 2$. Sea $A = \left(\frac{a,b}{F}\right)$ un álgebra de cuaterniones sobre F y considere $x = c + z \in A = F \oplus A_+$. Se definen el conjugado de x por $\bar{x} = c - z$ y su norma $N(x) = x\bar{x}$. Pruebe que:

i.- $\forall x \in A$ se tiene que $N(x) \in F$ y que $x\bar{x} = \bar{x}x$, $\bar{\bar{x}} = x$.
ii.- $\forall x \in F$ se tiene que $\bar{x} = x$.
iii.- $\forall x, y \in A$ se tiene que $\overline{x+y} = \bar{x} + \bar{y}$, $\overline{xy} = \bar{y}\bar{x}$.
iv.- $\forall x, y \in A$, se tiene que $N(x) = N(\bar{x})$, $N(xy) = N(x)N(y)$.
v.- $\forall k \in F$, $\forall x \in A$ se tiene que $N(k) = k^2$, $N(kx) = k^2 N(x)$.

Problema 2.6. Sea $A = \left(\frac{a,b}{F}\right)$ un álgebra de cuaterniones sobre F, tal que $\mathrm{car}(F) \neq 2$. Pruebe que son equivalentes:

i.- A es un álgebra de división.
ii.- Existe $x \in A, x \neq 0$ tal que $N(x) \neq 0$.
iii.- Si c_0, c_1, c_2 satisfacen la ecuación $x_0^2 = ax_1^2 + bx_2^2$ entonces $c_0 = c_1 = c_2 = 0$.

Problema 2.7. Sean $a, b \in \mathbb{R}$ dos números positivos. Pruebe que $A = \left(\frac{a,b}{\mathbb{R}}\right)$ es isomorfa a un álgebra de matrices.

Problema 2.8. Sea $A = \left(\frac{a,b}{F}\right)$ un álgebra de cuaterniones sobre F, tal que $\text{car}(F) \neq 2$. Pruebe que $Z(A) = F \cdot 1_A$.

Problema 2.9. Sea $A = \left(\frac{a,b}{\mathbb{C}}\right)$ un álgebra de cuaterniones sobre $\mathbb{C}$. Muestre que A no es un álgebra de división. Usando el hecho de que toda álgebra de cuaterniones sobre $\mathbb{C}$ es isomorfa a $\mathbb{M}_2(\mathbb{C})$, concluya que A es central (e.d: su centro es $\mathbb{C}$) y simple.

2.2. **Homomorfismos de álgebras:**

Problema 2.10. Sea A una R-álgebra e $J \subset I$ ideales de A. Pruebe que J es un ideal de I y que $(A/J)/(I/J) \cong A/I$.

Problema 2.11. Sean $\phi : A \to B$, $i : C \to B$ homomorfismos de R-álgebras, donde i es inyectivo. Pruebe que existe un único homomorfismo de álgebras $f : A \to C$ tal que $i \circ f = \phi$ si y solamente si $\text{Im}(\phi) \subset \text{Im}(i)$.

Problema 2.12. Probar que si J es un ideal bilátero de R, entonces $\mathbb{M}_n(J)$ es un ideal bilátero de $\mathbb{M}_n(R)$ y $\mathbb{M}_n(R)/\mathbb{M}_n(J) \cong \mathbb{M}_n(R/J)$.

Problema 2.13. Probar que $\mathbb{M}_n(R_1 \times R_2) \cong \mathbb{M}_n(R_1) \times \mathbb{M}_n(R_2)$.

Problema 2.14. Pruebe que toda álgebra de cuaterniones sobre $\mathbb{C}$ es isomorfa a $\left(\frac{1,1}{\mathbb{C}}\right)$.

Problema 2.15. Encuentre dos álgebras de cuaterniones sobre $\mathbb{Q}$ no isomorfas.

2.3. **Productos tensoriales de módulos y álgebras:**

Problema 2.16. Sean M, N, T tres R-módulos. Pruebe que se tiene el siguiente isomorfismo de R-módulos:

$$\text{Bil}(M \times N; T) \simeq \text{Hom}_R(M, \text{Hom}_R(N, T)).$$

Problema 2.17. Sean M, M', N, N' cuatro R-módulos. Pruebe que se tienen los siguientes isomorfismos de R-módulos:

i.- $(M \oplus M') \otimes_R N \simeq (M \otimes_R N) \oplus (M' \otimes_R N)$.

ii.- $(M \otimes_R N) \otimes_R M' \simeq M \otimes_R (N \otimes_R M')$.

Problema 2.18. Sean M un R-módulos y $N = R^n$. Pruebe que $M \otimes_R N \simeq M^n$, como R-módulos.

Problema 2.19. Sea G grupo abeliano finito de orden n. Pruebe que el $\mathbb{Q}$-módulo $\mathbb{Q} \otimes_{\mathbb{Z}} G$ es cero.

Problema 2.20. Sean I, J ideales de R, entonces $R/I, R/J$ son $R-$ módulos. Pruebe que $R/I \otimes_R R/J \simeq R/(I + J)$, como R-módulos.

Problema 2.21. Sean I ideal de R, entonces R/I es un $R-$ módulo. Sea M un R-módulo. Pruebe que $R/I \otimes_R M \simeq M/IM$.

Problema 2.22. Sea $A = \mathbb{M}_n(K)$ y L/K una extensión de cuerpos. Pruebe que $A \otimes_K L \cong \mathbb{M}_n(L)$, como K-álgebras.

Problema 2.23. Sea A una K-álgebra y L/K una extensión de cuerpos. Pruebe que $A_L = L \otimes_K A$ es una L-álgebra. A_L se denomina extensión escalar de A. Pruebe que si $\{a_1, a_2, \cdots, a_n\}$ es una base de A entonces $\{1 \otimes a_1, 1 \otimes a_2, \cdots, 1 \otimes a_n\}$ es una base de A_L, vista como L-álgebra.

Problema 2.24. Sean G, G' grupos. Pruebe que $R[G \times G'] \simeq R[G] \otimes_R R[G']$, como R-álgebras.

Problema 2.25. Sea $A = \mathbb{M}_n(K)$ y $B = \mathbb{M}_m(K)$. Pruebe que $A \otimes_K B \cong \mathbb{M}_{mn}(K)$, como K-álgebras.

2.4. **Álgebra tensorial $T(M)$:**

Problema 2.26. Sean M, M', N, N' R-módulos y $f : M \to M'$, $g : N \to N'$ aplicaciones lineales. Pruebe que:

i.- Existe una única aplicación R-lineal $h : M \otimes_R N \to M' \otimes_R N'$ tal que:

$$h(m \otimes n) = f(m) \otimes g(n) \ \ \forall\, m \in M, n \in N.$$

En lo que sigue h se anota por $f \otimes g$.

ii.- $id_M \otimes id_N = id_{M \otimes_R N}$.

iii.- Si f y g son epiyectivas, entonces $f \otimes g$ epiyectiva

Problema 2.27. El producto tensorial $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ es libre de rango 4 como módulo sobre $\mathbb{R}$, con base $\{e_1 = 1 \otimes 1, \ e_2 = 1 \otimes i, \ e_3 = i \otimes 1, \ e_4 = i \otimes i\}$.

i.- Escriba la mutiplicación de dos elementos cualesquiera en el álgebra $A = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

ii.- Sea $\varepsilon_1 = \frac{1}{2}(e_1 + e_4)$ y $\varepsilon_2 = \frac{1}{2}(e_1 - e_4)$. Pruebe que $\varepsilon_1 \varepsilon_2 = 0$, $\varepsilon_1 + \varepsilon_2 = 1$, $\varepsilon_j^2 = \varepsilon_j$, para $j = 1, 2$. Deduzca que A es isomorfa como anillo al producto directo de dos ideales principales, a saber, $A \simeq A\varepsilon_1 \times A\varepsilon_2$.

iii.- Pruebe que la aplicación $\varphi : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ definida por $\varphi(z_1, z_2) = (z_1 z_2, z_1 \overline{z_2})$ es un aplicación $\mathbb{R}-$ bilineal.

iv.- Sea $\phi : A \to \mathbb{C} \times \mathbb{C}$ el homomorfismo de $\mathbb{R}-$módulos obtenido a partir del homomorfismo φ de la parte [iii]. Pruebe que $\phi(\varepsilon_1) = (0, 1)$ y $\phi(\varepsilon_2) = (1, 0)$. Pruebe que ϕ es isomorfismo de $\mathbb{C}$-álgebras, es decir $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$.

Problema 2.28. Pruebe que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = \{0\}$. Concluya que $T(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

Problema 2.29. Demuestre que $T(\mathbb{M}_n(K)) = \bigoplus_{k=0}^{\infty} \mathbb{M}_{n^k}(K)$.

Problema 2.30. Sea K un cuerpo y S un K-álgebra graduado. Muestre que S tiene un único ideal graduado maximal.

Problema 2.31. Sea S un R-álgebra graduado. Muestre que I es un ideal homogeneo de S si y solamente si I admite un sistema homogeneo de generadores.

Problema 2.32. Sea S un R-álgebra graduado y $\mathfrak{p}$ un ideal homogeneo en S. Muestre que $\mathfrak{p}$ es un ideal primo si y solamente si la relación $ab \in \mathfrak{p}$, con a, b homogeneos, implica $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

2.5. **Álgebra simétrica** $S(M)$**:**

Problema 2.33. En el anillo $R = \mathbb{Z}[x]$, sea $I = (2, x)$ el ideal generado por 2 y por x. Entonces el anillo $\mathbb{Z}/2\mathbb{Z} = R/I$ es un $R-$ módulo aniquilado por x y por 2.

i.- Pruebe que $\varphi : I \times I \to \mathbb{Z}/2\mathbb{Z}$, definida por:

$$\varphi(a_0 + \cdots + a_n x^n, b_0 + \cdots + b_m x^m) = \frac{a_0}{2} b_1 \pmod 2,$$

es R-bilineal.

ii.- Pruebe que hay un homomorfismo de $R-$ módulos de $I \otimes_R I \to \mathbb{Z}/2\mathbb{Z}$, que lleva $p(x) \otimes q(x)$ en $\frac{p(0)}{2} q'(0)$, donde $q'(x)$ es el polinomio derivado de $q(x)$.

iii.- Pruebe que $2 \otimes x \neq x \otimes 2$.

Problema 2.34. Muestre que $S(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z} \oplus \bigoplus_{i=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$.

Problema 2.35. Sea K un cuerpo de caracteristica 2 y A una $K-$álgebra tal que $a^2 = 0$, para todo $a \in A$. Sea $\varphi : M \to A$ un homomorfismo de K-álgebras. Pruebe que existe un único homomorfismo $\phi : S(M) \to A$ tal que $\phi|_M = \varphi$.

Problema 2.36. Pruebe que si M es un R-módulo cíclico entonces $T(M) = S(M)$.

Problema 2.37. Sea V un F espacio vectorial de dimensión n. Pruebe que $S(V)$ es isomorfa a la F-álgebra graduada de anillos de polinomios en n variables.

2.6. **Álgebra exterior** $\Lambda(M)$**:**

Problema 2.38. Sea V un K-espacio vectorial con base $B = \{v_1, \cdots, v_n\}$. Pruebe que todo $z \in \Lambda^n(V)$ se escribe como $z = \det(A) v_1 \wedge v_2 \wedge \cdots \wedge v_n$, donde $A \in \mathbb{M}_n(K)$.

Problema 2.39. Sea V espacio vectorial de dimensión finita sobre un cuerpo F con base $B = \{v_1, \cdots, v_n\}$. Pruebe que los vectores:

$$v_{i1} \wedge v_{i2} \wedge \cdots \wedge v_{ik}, \quad \text{para } 1 \leq i_1 < i_2 \cdots < i_k \leq n,$$

son una base de $\Lambda^k(V)$, y $\Lambda^k(V) = \{0\}$ si $k > n$. Cuando $k = 0$, el vector base es el elemento 1 de F.

Problema 2.40. Sea K un cuerpo de caracteristica impar y V un K-espacio vectorial de dimensión finita. Pruebe que $V \otimes_K V = S^2(V) \oplus \Lambda^2(V)$.

Problema 2.41. Sea $x \in \Lambda^k(M), y \in \Lambda^t(M)$. Pruebe que $x \wedge y = (-1)^{kt} y \wedge x$.

Problema 2.42. Sea $R = \mathbb{Z}[x, y]$ e $I =< x, y >$.

i.- Pruebe que si $ax + by = a'x + b'y$ en R entonces existe un polinomio $f(x, y) \in R$ tal que $a' = a + yf$ y $b' = b - xf$

ii.- Pruebe que la función $\varphi : I \times I \longrightarrow \mathbb{Z} = R/I$ definida por $\varphi(ax + by, cx + dy) = (ad - bc) + I$ es bilineal alternada.

Problema 2.43. Sea $R = \mathbb{Z}[x, y]$. Pruebe que:

i.- Si $M = R$, entonces $\Lambda^2(M) = \{0\}$.

ii.- Si $M = I =< x, y >$, entonces $\Lambda^2(I) \neq \{0\}$. Use la función φ construída en el ejercicio anterior.

Problema 2.44. Sea R un dominio de integridad y sea F su cuerpo de cuocientes.

i.- Considerando F como un R-módulo, pruebe que $\Lambda^2(F) = \{0\}$.
ii.- Sea I un R-submódulo de F, por ejemplo, un ideal de R. Pruebe que $\Lambda^i(I)$ es un módulo de torsión cada $i \geq 2$.
iii.- De un ejemplo de un dominio de integridad R y un R-módulo I en F tal que $\Lambda^i(I) \neq \{0\}$ para $i \geq 0$.

AYUDANTÍAS

CUERPOS Y ÁLGEBRAS (PRIMAVERA 2017)

3. Cuerpos:

Ayudantía 1: En esta ayudantía estudiaremos la parte básica de la teoría de cuerpos.

1.- **Problema 1:** Sea A un dominio de integridad.
i.- Pruebe que si A es finito entonces A es un cuerpo.
ii.- Muestre que para todo $z \in \mathbb{Z}[i]$ se cumle que $\mathbb{Z}[i]/(z)$ es un cuerpo o no es un dominio de integridad.

Desarrollo:
i.- Debemos probar que todo elemento no nulo en A tiene un inverso multiplicativo. Sea $x \in A - \{0\}$ y considere $\phi : A \to A$ el homomorfismo de grupos definido por $\phi(a) = ax$. Note que $\ker(\phi) = \{a \in A : ax = 0\} = \{0\}$, ya que A es un DI. Como $(A, +)$ es un grupo finito concluimos que ϕ es un isomorfismo. En particular, ϕ es sobreyectivo. Por lo tanto existe $y \in A$ tal que $xy = yx = 1$.
ii.- Recordemos que para todo $z \in \mathbb{Z}[i]$ el cociente $\mathbb{Z}[i]/(z)$ es finito. De hecho, se puede demostrar que $|\mathbb{Z}[i]/(z)| = N(z)$. Aplicando [i] se obtiene lo pedido. Otra forma de demostrar este hecho, es recordar que $\mathbb{Z}[i]$ es un DIP. Luego si $\mathbb{Z}[i]/(z)$ es un dominio de integridad, se tiene que (z) es un ideal primo, luego un ideal maximal. De esto se sigue que $\mathbb{Z}[i]/(z)$ es un cuerpo.

2.- **Problema 2:** Sea $\mathbb{F}_p$ el cuerpo de p elementos.
i.- Demustre que la función $x \mapsto x^p - x$ es nula en $\mathbb{F}_p$
ii.- Concluya que el polinomio $p(x) = x^p - p$ es no nulo y se factoriza en producto de polinomios lineales en $\mathbb{F}_p$.

Desarrollo:
i.- Basta probar que para todo $x \in \mathbb{F}_p$ se tiene que $x^p = x$. Para probar esto, observe que $(\mathbb{F}_p^*, \cdot)$ es un grupo finito de cardinal $p-1$. Luego, por teorema de Lagrange, tenemos que para todo $x \in \mathbb{F}_p^*$ se tiene que $x^{p-1} = 1$. Esto implica que $x^p = x$, para todo $x \in \mathbb{F}_p$.
ii.- Dado que $p(x)$ tiene coeficientes no nulos, se tiene que $p(x)$ es un polinomio no nulo. Por otro lado, como $p(x)$ es un polinomio de grado p que tiene p raices distintas en $\mathbb{F}_p$, se tiene que $p(x) = \prod_{a \in \mathbb{F}_p}(x - a)$.

3.- **Problema 3:** Sea $F = \mathbb{Q}(\sqrt[n]{2})$ el mínimo cuerpo contenido en $\mathbb{R}$ que contiene a $\mathbb{Q}$ y $\sqrt[n]{2}$. Demuestre que $F = \{a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1} \sqrt[n]{2^{n-1}} : a_i \in \mathbb{Q}\}$. Determine $[F : \mathbb{Q}] = \dim_{\mathbb{Q}} F$.

Desarrollo: Sea $X = \{a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1} \sqrt[n]{2^{n-1}} : a_i \in \mathbb{Q}\}$. Como $\sqrt[n]{2} \in L$, es facil demostra que $X \subset L$. Luego, para demostrar que $L = X$, basta demostra que X es un cuerpo. Esto ya que, como $\sqrt[n]{2} \in X$ y $\mathbb{Q} \subset X$ se tiene que $X \supset L$. En lo que sigue demostraremos que X es un cuerpo. Sea $\phi : \mathbb{Q}[x] \to X$ el homomorfismo de anillos definido por $\phi(x) = \sqrt[n]{2}$. Claramente ϕ es sobreyectivo y $p(x) = x^2 - 2 \in \ker(\phi)$. Note que por criterio de Einsentein, se tiene que $p(x)$ es irreducible. Dado que $\mathbb{Q}[x]$ es un DIP, podemos suponer que $\ker(\phi) = s(x)$. Entonces $p(x) = s(x)t(x)$, para cierto $t(x) \in \mathbb{Q}[x]$. Como $p(x)$ es irreducible, tenemos que $t(x) \in \mathbb{Q}$ y en particular $(p(x)) = \ker(\phi)$. Concluimos que $X \cong \mathbb{Q}[x]/(p(x))$ es un cuerpo. Para calcular $[F : \mathbb{Q}]$ note que $\{1, \sqrt[n]{2}, \cdots, \sqrt[n]{2^{n-1}}\}$ es una base de X como $\mathbb{Q}$ espacio vectorial. Esto pues claramente genera el espacio y sus elementos son linealmente independientes, debido a que si no, existiría un polinomio de grado menor a $p(x)$ que se anula en $\sqrt[n]{2}$, lo que contradice el hecho de que $\ker(\phi) = (p(x))$. Se sigue que $[F : \mathbb{Q}] = \dim_{\mathbb{Q}} F = n$.

4.- **Problema 4:** Sea $p(x) = x^3 + 12x + 3 \in \mathbb{Q}[x]$ y θ una raiz de $p(x)$. Sea $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(p(x))$ el mínimo cuerpo contenido en $\mathbb{C}$ que contiene a $\mathbb{Q}$ y θ.

i.- Exprese $(\theta^2 + \theta + 5)(\theta + 3)$ en términos de $\{1, \theta, \theta^2\}$.

ii.- Exprese $(\theta^2 + 3)^{-1}$ en términos de $\{1, \theta, \theta^2\}$.

Desarrollo:

i.- Note que $a = (\theta^2+\theta+5)(\theta+3) = \theta^3+4\theta^2+8\theta+15$. Luego una preimagen de a por el homomorfismo ϕ, definido en [3], es $r(x) = x^3 + 4x^2 + 8x + 15$. Note que $r(x) = p(x)+4x^2-4x+12$. Por lo tanto, si evaluamos la igualdad anterior en $x = \theta$ obtenemos que $a = 4\theta^2 - 4\theta + 12$.

ii.- Por un argumento análogo al mostrado en [3], debemos encontrar un polinomio $f(x)$ tal que $f(\theta)(\theta^2 + 3) = 1$. Tomando preigamenes vía ϕ, deducimos que debemos encontrar $f(x), g(x) \in \mathbb{Q}[x]$ tales que $(x^2 + 3)f(x) + p(x)g(x) = 1$. Para encontrar dichos polinomios, debemos aplicar algoritmo de división. En efecto tenemos que:

$$p(x) = x(x^2 + 3) + (9x + 3),$$
$$x^2 + 3 = \frac{x}{9}(9x + 3) + \left(3 - \frac{1}{3}x\right),$$
$$9x + 3 = -27\left(-\frac{1}{3}x + 3\right) + 84.$$

Luego $84 = (x^2 + 3)\left(27 - x + \frac{1}{9}x^2\right) + \left(1 - \frac{1}{9}x\right)p(x)$. Evaluando en θ, concluimos que $(\theta^2 + 3)^{-1} = \frac{1}{84}\left(27 - \theta + \frac{1}{9}\theta^2\right)$.

Ayudantía 2: En esta ayudantía trabajaremos con indice de cuerpos y estudiaremos la extensión de homomorfismos.

Observación 3.1. Sea $K(\alpha) \cong K[x]/(p(x))$, una extensión simple, donde $p(x)$ es un polinomio irreducible. El argumento mostrado en el problema [3] de la ayudantía 1, muestra que $\{s(x) \in K[x] : s(\alpha) = 0\} = (p(x))$.

1.- **Problema 1:** Sea $L = \mathbb{F}_5(\sqrt{2})$ el mínimo cuerpo que contiene a $\mathbb{F}_5$ y una raiz de $2 \in \mathbb{F}_5$.

i.- Muestre que L es una extensión cuadrática de $\mathbb{F}_5$.

ii.- Pruebe que $x^2 + 2$ se descompone en $L[x]$.

Desarrollo:

i.- Sabemos que $L \cong \mathbb{F}_5[x]/(p(x))$, para cierto polinomio irreducible $p(x) \in \mathbb{F}_2[x]$ tal que $p(\sqrt{2}) = 0$. Por definición, $x^2 - 2$ se anula en $\sqrt{2}$. Por lo tanto, si demostramos que $x^2 - 2$ es irreducible en $\mathbb{F}_5[x]$, tenemos que $[L : \mathbb{F}_5] = \deg(x^2 - 2) = 2$. Observe que $\mathbb{F}_5^2 = \{0, 1, -1\}$. Por lo tanto $x^2 - 2$ no tiene raices en $\mathbb{F}_5$. Esto implica que $x^2 - 2$ es irreducible sobre $\mathbb{F}_5[x]$.

ii.- Note que $(2\sqrt{2})^2 = 8 = -2$ en L. Por lo tanto $x^2 + 2 = (x - 2\sqrt{2})(x + 2\sqrt{2})$ en $L[x]$.

2.- **Problema 2:** Sea $w = e^{\frac{2\pi i}{3}}$ y considere el cuerpo $L = \mathbb{Q}(\sqrt[3]{2}, w)$.

i.- Pruebe que $[L : \mathbb{Q}] = 6$.

ii.- Muestre que $\sqrt[3]{2} \notin L$, para todo $L = \mathbb{Q}(\theta_1, \cdots, \theta_n)$, donde $\theta_i^2 \in \mathbb{Q}$.

Desarrollo:

i.- Sabemos que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3$. Por la multiplicatividad del grado, para probar lo pedido, basta demostrar que $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$. En efecto, sabemos que $q(x) = x^2 + x + 1$ es un polinomio que se anula en w. Por otro lado, sabemos que $L \cong \mathbb{Q}(\sqrt[3]{2})[x]/(p(x))$, donde $p(x)$ es un polinomio irreducible. La observación 3.1 implica que $p(x)$ divide a $x^2 + x + 1$. Por lo tanto $[L : \mathbb{Q}(\sqrt[3]{2})] \leq 2$. Si $[L : \mathbb{Q}(\sqrt[3]{2})] = 1$, entonces el cuerpo $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ conincide con L, el cual contiene el elemento no real, a saber $w \in L$. Esto implica que $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$ y se concluye lo pedido.

ii.- Definimos $L_i = \mathbb{Q}(\theta_1, \cdots, \theta_i)$, para $i \in \{1, \cdots n\}$. Note que $L_{i+1} = L_i(\theta_{i+1})$, donde $\theta_{i+1}^2 \in L_i$. Por lo tanto $[L_{i+1} : L_i] \in \{1, 2\}$. Esto implica que $[L : \mathbb{Q}] = 2^t$, para cierto $t \leq n$. Luego, si $\sqrt[3]{2} \in L$, se tiene que $\mathbb{Q}(\sqrt[3]{2}) \subset L$, por lo que 3 divide a 2^t. Esto nos lleva a una contradicción.

3.- **Problema 3:** Sea $a = \sqrt{2} + \sqrt{3}$ y sean $L = \mathbb{Q}(a)$ y $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

i.- Pruebe que $\sqrt{6} \in L$.

ii.- Pruebe que $[K : \mathbb{Q}] = 4$.

iii.- Demuestre que $L \neq \mathbb{Q}(\sqrt{6})$.

iv.- Concluir que $L = K$.

v.- Encontrar un polinomio irreducible sobre $\mathbb{Q}[x]$ que se anule en a.

Desarrollo:

i.- Note que $a^2 = 5 + 2\sqrt{6}$. Luego, tenemos que $\sqrt{6} = \frac{a^2 - 5}{2} \in L$.

ii.- Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Luego, para probar que $[K : \mathbb{Q}] = 4$, basta demostrar que $[K : \mathbb{Q}(\sqrt{2})] = 2$. Note que $K = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \cong$

$\mathbb{Q}(\sqrt{2})[x]/(p(x))$, donde $p(x)$ divide a x^2-3, puesto que x^2-3 se anula en $\sqrt{3}$. Luego $[K:\mathbb{Q}(\sqrt{2})] \in \{1,2\}$. Observe que si $[K:\mathbb{Q}(\sqrt{2})]=1$, entonces $\sqrt{3}=a+b\sqrt{2}$, para ciertos $a,b\in\mathbb{Q}$. Luego, tenemos que $3=a^2+2b^2+2ab\sqrt{2}$. Por lo tanto $b=0$, lo que implica que $\sqrt{3}\in\mathbb{Q}$. Esto es contradictorio. Concluimos que $[K:\mathbb{Q}(\sqrt{2})]=2$.

iii.- Supogamos que $L=\mathbb{Q}(\sqrt{6})$. Entonces $[L:\mathbb{Q}]=2$ y entonces existe $a,b\in\mathbb{Q}$ tales que $(\sqrt{2}+\sqrt{3})^2+a(\sqrt{2}+\sqrt{3})+b=0$. Por lo tanto, se tiene que $2\sqrt{6}+a\sqrt{2}+a\sqrt{3}+5+b=0$. Por otro lado, lo demostrado en [ii] implica que $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ es un conjunto linealmente independiente (ver teorema 1.2.3 del apunte). Este hecho, nos lleva a una contradicción. Por lo tanto $L\neq\mathbb{Q}(\sqrt{6})$.

iv.- Claramente se tiene que $L\subset K$. Por [i] e [iii] tenemos que $\mathbb{Q}(\sqrt{6})\subsetneq L$. Por lo tanto $[L:\mathbb{Q}]=4$. Esto nos permite concluir que $[K:L]=1$. Luego $L=K$.

v.- En efecto $a^2=5+2\sqrt{6}$, luego tenemos que $(a^2-5)^2=24$. Por lo tanto, se tiene que $q(x)(x)=x^4-10x^2+1$ es un polinomio que se anula en a. Lo mostrado en [iv] implica que $L=\mathbb{Q}[x]/(p(x))$, donde $p(x)$ es irreducible de grado 4. Por otro lado, de la observación 3.1, se sigue que $p(x)$ divide a $q(x)$. Por igualdad en el grado, tenemos que $p(x)=uq(x)$, donde $u\in\mathbb{Q}$. Esto implica que $q(x)$ es irreducible.

4.- **Problema 4:** Sea $L=K(\alpha)\cong K[x]/(p(x))$ una extensión de grado n de K y $\sigma: L\to L$ un automorfismo tal que $\sigma|_K=\mathrm{id}$.

i.- Pruebe que $\sigma(\alpha)$ es una raiz de $p(x)$. Concluya que, si $p(x)$ tiene todas sus raices distintas, entonces:

$$\mathrm{Aut}(L/K)=\{\sigma: L\to L \text{ automorfismo } : \sigma|_K=\mathrm{id}\},$$

cumple con $|\mathrm{Aut}(L/K)|\leq n$.

ii.- Sea $L=\mathbb{Q}(\sqrt{d})$, con $d\in\mathbb{Z}$ libre de cuadrados. Pruebe $|\mathrm{Aut}(L/\mathbb{Q})|=2$.

Desarrollo:

i.- Basta probar que $\beta=\sigma(\alpha)$ cumple con $p(\beta)=0$. En efecto, se tiene que si $p(x)=a_0+a_1x+\cdots+a_nx^n$ entonces $p(\beta)=a_0+a_1\sigma(\alpha)+a_n\sigma(\alpha^n)=\sigma(p(\alpha))=0$, debido a que $\sigma(a_i)=a_i$. Note que si dos automorfismos $\phi_1,\phi_2: L\to L$ cumplen con $\phi_1(\alpha)=\phi_1(\alpha)$, entonces $\phi_1=\phi_2$. Por lo tanto, tenemos que existen tantos o menos automorfismos que el número de raices distintas de $p(x)$. De esto se sigue que $|\mathrm{Aut}(L/K)|\leq n$.

ii.- Por [i] tenemos que los posibles automorfismos están definidos por $\sqrt{d}\mapsto\sqrt{d}$ y $\sqrt{d}\mapsto-\sqrt{d}$. Es más, como $L=\{a+b\sqrt{d}: a,b\in\mathbb{Q}\}$, se tiene que los posibles automorfismos son id y g, donde $g(a+b\sqrt{d})=a-b\sqrt{d}$. Es inmediato que id es un isomorfismo. El argumento que sigue muestra que c también lo es. Note que $g\neq 0$, por lo tanto g es un homomorfismo inyectivo. Como $g|_{\mathbb{Q}}=\mathrm{id}$, tenemos que g es un homomorfismo lineal inyectivo. Por ende es sobreyectivo. Concluimos que c es un isomorfismo.

Ayudantía 3: En esta ayudantía estudiaremos extensiones algebraicas.

1.- **Problema 1:** Sean L, F dos extensiones de k. Considere $L, F \subset K$, para un cierto cuerpo K. Se define el composito LF de L y F como el mínimo subcuerpo de K que contiene a L Y F. Demuestre que si $[F:k], [L:k] < \infty$ entonces $[LF:k] < \infty$ y $[F:k], [L:k]$ dividen a $[LF:k]$.

Demostración: Primero demostremos que $[LF : k] < \infty$. En efecto, si $[F : k], [L : k] < \infty$ entonces $F = k(\alpha_1, \cdots, \alpha_n)$, donde cada α_i es algebraico sobre k y análogamente $F = k(\beta_1, \cdots, \beta_m)$, donde cada β_i es algebraico sobre k. Luego tenemos que el cuerpo $k(\alpha_i, \beta_j)$ contiene a F y L. Por ende $k(\alpha_i, \beta_j) \supset FL$. Por otro lado, como $\alpha_i, \beta_j \in FL$, tenemos que $k(\alpha_i, \beta_j) \subset FL$. Como FL es una extensión algebraica y finitamente generada de k, concluimos que FL es una extensión finita de k. Ahora bien, el hecho que $[F:k], [L:k]$ dividen a $[LF:k]$ se sigue de que $k \subset L, F \subset FL$. Esto debido a que $[LF:F][F:k] = [LF:k]$ y $[LF:L][L_k] = [LF:k]$.

2.- **Problema 2:** Sea K una extensión de F y $\alpha \in K$ un elemento transcendente sobre F. Demustre que existe un isomorfismo de cuerpos entre $F(x) = \text{Quot}(F[x])$ y $F(\alpha)$, que es la identidad sobre F.

Demostración: Sea $\psi : F[x] \to F(\alpha) \subset K$ el homomorfismo definido por $\psi(p(x)) = p(\alpha)$. Note que $\ker(\psi) = \{0\}$, pues en caso contrario existe $p(x) \in F[x] - \{0\}$ tal que $p(\alpha) = 0$, lo que contradice la trascendencia de α. Luego ψ es un homomorfismo inyectivo. Dado que $F(\alpha)$ es un cuerpo, tenemos que ψ se factoriza a $F(x)$ vía el homomorfismo de cuerpos $\phi : F(x) \to F(\alpha)$ definido por $\phi\left(\frac{p(x)}{q(x)}\right) = \frac{p(\alpha)}{q(\alpha)}$. Note que ϕ es un inyectivo, pues no es nulo. Además, por definición de ϕ, tenemos que $\phi|_F = \text{id}$. Solo debemos probar que $\text{Im}(\phi) = F(\alpha)$. En efecto, el cuerpo $L = \text{Im}(\phi)$ contiene a α y a F, pues $\phi|_F = \text{id}$ y $\phi(x) = \alpha$. Por lo tanto $L \supset F(\alpha)$. Por otro lado, por definición de conjunto imagen, tenemos que $L \subset F(\alpha)$. Concluimos que $L = F(\alpha)$ y que por ende ϕ es un isomorfismo.

Ayudantía 4: En esta ayudantía trabajaremos con cuerpos de descomposición y clausura algebraica.

1.- **Problema 1:** El siguiente problema tiene por objetivo calcular cuerpos de descomposición.

i.- Sea F un cuerpo, $\overline{F}$ su clausura algebraica y $p(x) \in F[x]$ un polinomio cualquiera. Muestre que el cuerpo de descomposición $K \subset \overline{F}$ de $p(x)$ sobre F es $K = F(\alpha_1, \cdots, \alpha_n)$, donde $\{\alpha_i\}_{i=1}^n \subset \overline{F}$ es el conjunto de raices de $p(x)$.

ii.- Demuestre que el cuerpo de descomposición de $p(x) = x^4 + ax^2 + b^2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(z)$, donde $z = \sqrt{\frac{-a+\sqrt{a^2-4b^2}}{2}}$.

iii.- Demuestre que el cuerpo de descomposicón de $x^6 - 3$ sobre $\mathbb{F}_5$ tiene grado dos.

Desarrollo:

i.- Es sencillo ver que $p(x) = \prod_{i=1}^n (x - \alpha_i)$ en $F(\alpha_1, \cdots, \alpha_n)[x]$. Supongamos que $F \subset M \subset \overline{F}$ es otro cuerpo en el que $p(x)$ se factoriza linealmente. Como los factores lineales de $p(x)$ son de la forma $x - \alpha_i$ se tiene que $\alpha_i \in M$, para todo $i \in \{1, \cdots, n\}$. Por lo tanto $F(\alpha_1, \cdots, \alpha_n) \subset M$ y en particular la inclusión $F(\alpha_1, \cdots, \alpha_n) \to M$ es un homomorfismo no trivial que extiende la inclusión $F \to M$.

Para efecto de todos los cálculos que siguen entendemos los cuerpos de descomposición como subconjuntos de la clausura algebraica respectiva.

ii.- Note que las raices de $p(x)$ son de la forma $\pm\sqrt{\frac{-a\pm\sqrt{a^2-4b^2}}{2}}$. Luego el cuerpo de descomposición de $p(x)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(z, z')$, donde $z' = \sqrt{\frac{-a-\sqrt{a^2-4b^2}}{2}}$ y z es como antes. Por otro lado tenemos que $zz' = b$. Por lo tanto $z' = \frac{b}{z}$ y se tiene que $\mathbb{Q}(z)$ es el cuerpo de descomposición de $p(x)$.

iii.- Observe que $3 = 2^3$ en $\mathbb{F}_5$, por ende $x^6 - 3 = (x^2 - 2)(x^4 + 2x^2 + 4)$. Escribiendo $x^4+2x^2+4 = (x^2+ax+b)(x^2+cx+d)$ se obtiene que $a = -c = 2$ y $b = d = -2$. Por lo tanto $x^6 - 3 = (x^2 - 2)(x^2 + 2x - 2)(x^2 - 2x - 2)$. Sea $\theta \in \overline{\mathbb{F}_5}$ un elemento tal que $\theta^2 = 2$. Escribimos $z = a\theta + b$. Luego si $z^2 \pm 2z - 2 = 0$, se tiene que $z = 2\theta \mp 1$ o $z = -2\theta \mp 1$. Esto implica que el cuerpo de descomposión de $p(x)$ es $L = \mathbb{F}_5(\theta)$, el cual sabemos tiene grado 2 sobre $\mathbb{F}_5$.

2.- **Problema 2:** Sea K una extensión finita de F. Pruebe que K es el cuerpo de descomposición de un polinomio en $F[x]$ si y solamente si todo polinomio irreducible en $F[x]$ que tiene una raiz en K se factoriza completamente en $K[x]$.

Demostración: Supongamos que todo polinomio irreducible que tiene una raiz en K se factoriza completamente. Escribimos $K = F(\theta_1, \cdots, \theta_r)$ y sea $p_i(x) = m_{\theta_i, F}(x)$. Note que $p_i(x)$ es irreducible y tienen una raiz en K. Por lo tanto $p_i(x)$ se descompone completamente en K. Esto implica que K es el cuerpo de descomposición de $p(x) = \prod_{i=1}^r p_i(x)$. Supongamos ahora que K es el cuerpo de descomposición de un polinomio $q(x) \in F[x]$ y sea $\overline{F}$ una clausura algebraica de F que contiene a K. Para concluir lo pedido basta probar que si $\alpha, \beta \in \overline{F}$ son raices de un polinomio irreducible

$p(x) \in F[x]$ y $\alpha \in K$, entonces $\beta \in K$. Por la proposición 1.2.11 vista en clase, se tiene que existe un isomorfismo $i : F(\alpha) \to F(\beta)$ tal que $i|_F = \text{id}$. Note que, por el ejericicio 1i, K es un cuerpo de descomposición de $q(x) \in F(\alpha)[x]$. Por el mismo argumento $K(\beta)$ es un cuerpo de descomposición de $q(x) \in F(\beta)[x]$. Luego, por el Teorema 1.2.9 existe un isomorfismo $\psi : K(\alpha) \to K(\beta)$ tal que $\psi|_{F(\alpha)} = \text{id}$. Por lo tanto, si $\alpha \in K$, tenemos que $1 = [K(\alpha) : K] = \frac{[K(\alpha):F(\alpha)][F(\alpha):F]}{[K:F]} = \frac{[K(\beta):F(\beta)][F(\beta):F]}{[K:F]} = [K(\beta) : K]$. Concluimos que $\beta \in K$.

3.- **Problema 3:** Sea $F \subset K \subset \overline{F}$, donde K/F es una extensión finita. Pruebe que K es el cuerpo de descomposición de un polinomio en $F[x]$ si y solamente si para todo homomorfismo $\phi : K \to \overline{F}$ tal que $\phi|_F = \text{id}$ se cumple que $\phi(K) = K$.

Demostración: Primero supongamos que $K = F(\theta_1, \cdots, \theta_r)$ es el cuerpo de descompocisión de un polinomio en $F[x]$ y consideremos $\phi : K \to \overline{F}$ como una incrustación cualquiera. Recordemos que en el problema 4 de la ayudantía II, probamos que $\phi(\theta_i)$ es una raiz de $m_{F,\theta_i}(x)$, puesto que $\phi|_F = \text{id}$. Luego, por el problema 2, tenemos que $\phi(\theta_i) \in K$. Esto implica que $\phi(K) \subset K$. Por otro lado $\phi : K \to K$ es una aplicación F-lineal inyectiva, entre espacios de dimensión finita. Concluimos que $\phi(K) = K$. Supongamos ahora que, para toda incrustación $\phi : K \to \overline{F}$ se cumple que $\phi(K) = K$. Sea $p(x) \in F[x]$ un polinomio irreducible, $\alpha \in K$ una raiz de $p(x)$ y $\beta \in \overline{F}$ una otra raiz de $p(x)$. Definimos el isomorfismo $\psi : K(\alpha) \to K(\beta) \subset \overline{F}$ por $\psi(\alpha) = \beta$ (ver proposición 1.2.11). Recordemos que, por ser K/F una extensión finita, tenemos que existen $\theta_i \in K$ tales que $\{\alpha, \theta_2, \cdots, \theta_r\}$ es una base de L como K-espacio vectorial. Por ende $K = F(\alpha)(\theta_2, \cdots, \theta_r)$. Sea L_1 el mínimo cuerpo, contenido en $\overline{F}$, que contiene a F y a todos los conjugados de los elementos θ_i y α. Sea L_2 el mínimo cuerpo que contiene a los conjugados θ_i y β. Note que L_1 y L_2 son los cuerpos de descomposición de $r(x) = p(x) \prod m_{\theta_i,F}(x)$ en $F(\alpha)$ y $F(\beta)$ respectivamente. Por el Teorema 1.4.9, concluimos que existe un homomorfismo no trivial $\psi : L_1 \to L_2 \subset \overline{F}$ tal que $\phi|_{K(\alpha)} = \psi$. En particular tenemos un homomorfismo no trivial $\phi : K \to \overline{F}$ tal que $\phi|_{K(\alpha)} = \psi$. Por hipótesis, esto implica que $\psi(K) = K$. Concluimos que $\beta = \phi(\alpha) \in K$. Por el problema 2, concluimos lo pedido.

Ayudantía 5: En esta ayudantía trabajaremos con extensiones separables.

1.- **Problema 1:** Considere el polinomio $P(x) \in \mathbb{F}_p[x]$ dado por $P(x) = x^p - x + a$ con $a \in \mathbb{F}_p^*$. Sea $\alpha \in \bar{\mathbb{F}}_p$ una raíz de $P(x)$.

i.- Pruebe que $\alpha + b$ es una raíz de $P(x)$ para todo $b \in \mathbb{F}_p$. Concluya que $P(x)$ es separable.

ii.- Sea $F \subset F(\alpha) \subset \overline{F}$, donde $\alpha \in \overline{F}$ es un elemento algebraico y sea $X = \{\phi : F(\alpha) \to \overline{F} : \phi|_F = \mathrm{id}\}$. Demuestre que $|X| \leq n$ y que $|X| = n$ si y solamente si $m_{\alpha,F}(x)$ es separable.

iii.- Concluya que $P(x)$ es irreducible.

Desarrollo:

i.- Sabemos que para todo $b \in \mathbb{F}_p$ se tiene que $b^p = b$. Por lo tanto $(\alpha + b)^p - (\alpha + b) + a = \alpha^p - \alpha + a + b^p - b = 0$. Luego, dado que $\{\alpha + b : b \in \mathbb{F}_p\}$ tiene p elementos, tenemos que $P(x)$ es separable.

ii.- La misma demotración del problema 4 de la ayudantía 2 prueba que $\phi(\alpha)$ es una raiz de $m_{\alpha,F}(x)$. Observe que si dos homomorfismos $\phi_1, \phi_2 : F(\alpha) \to \overline{F}$ cumplen con $\phi_1(\alpha) = \phi_1(\alpha)$, entonces $\phi_1 = \phi_2$. Por otro lado, dada una raiz $\beta \in \overline{F}$ de $m_{\alpha,F}(x)$, existe isomorfismo $\phi : F(\alpha) \to F(\beta) \subset \overline{F}$ definido por $\phi(\alpha) = \beta$ (Ver proposición 1.2.11). Esto nos permite concluir que G está en biyección con el número de raices de $m_{\alpha,F}(x)$. De esto se sigue lo pedido.

iii.- Note que para todo $b \in \mathbb{F}_p$ existe un homomorfismo $\phi_b : \mathbb{F}(\alpha) \to \overline{\mathbb{F}_p}$ definido por $\phi_b(\alpha) = \alpha + b$. Luego tenemos que $|G| = p$. De [i] e [ii] se tiene que $m_{\alpha,\mathbb{F}_p}(x)$ tiene grado p. Por lo tanto $m_{\alpha,\mathbb{F}_p}(x) = P(x)$.

2.- **Problema 2:** Sea $\mathbb{F}_p$ el cuerpo finito de p elementos. Sea $L = \mathbb{F}_p(u, v)$ el cuerpo de cocientes del anillo de polinomios $\mathbb{F}_p[u, v]$ y sea $K = \mathbb{F}_p(u^p, v^p)$ el cuerpo de cocientes del anillo de polinomios $\mathbb{F}_p[u^p, v^p]$. Demuestre que L/K es una extensión de grado p^2, en donde todo elemento de L es inseparable sobre K o bien pertenece a K.

Demostración: Considere $F = \mathbb{F}_p(u, v^p) = \mathrm{Quot}(\mathbb{F}_p[u, v^p])$. Note que $F = K(u)$ y que $L = F(v)$. El elemento $u \in F$ se anula en el polinomio $p(x) = x^p - u^p \in K[x]$, donde u^p es un elemento primo en el anillo $\mathbb{F}_p(v^p)[u^p]$. Por lema de Einsenstein tenemos que $p(x)$ es irreducible en $\mathbb{F}_p(v^p)[u^p]$. Luego, por lema de Gauss, tenemos que $p(x)$ es irreducible en $K[x]$. Esto implica que $[F : K] = p$. Por otro lado $v \in L$ se anula en el polinomio $q(x) = x^p - v^p \in F[x]$, donde v^p es un elemento primo en el anillo $\mathbb{F}_p(u)[v^p]$. Por lema de Einsenstein tenemos que $p(x)$ es irreducible en $\mathbb{F}_p(u)[v^p]$. Luego, por lema de Gauss, tenemos que $p(x)$ es irreducible en $F[x]$. Esto nos lleva a que $[L : F] = p$. Concluimos que $[L : K] = p^2$. Considere ahora un elemento $y \in L$ cualquiera. Por definición de cuerpo de cocientes $y = \frac{r(u,v)}{s(u,v)}$, donde $s(u, v) \neq 0$. Note que todo polinomio $r(u, v) = p_0(u) + p_1(u)v + \cdots + p_n(u)v^n \in \mathbb{F}_p[u, v]$ satisface que $r(u, v)^p = p_0(u)^p + p_1(u)^p v^p + \cdots + p_n(u)^p v^{np}$. Ahora bien, todo polinomio $q(u) = a_0 + a_1 u + \cdots + a_n u^n \in \mathbb{F}_p[u]$ cumple con $q(u)^p = a_0 + a_1 u^p + \cdots + a_n u^{np}$, puesto que $a_i^p = a_i$, para todo $a_i \in \mathbb{F}_p$. De esto se

sigue que $r(u,v)^p = r(u^p, v^p)$. Por lo tanto $y^p = \frac{r(u^p,v^p)}{s(u^p,v^p)} \in K$. Esto implica que el elemento $y \in L$ satisface el polinomio $p(x) = x^p - \alpha$, con $\alpha \in K$. Por lo tanto $m_{y,K}(x)$ divide a $x^p - \alpha$. Note que $p(x) = (x-y)^p$ en F. Por ende $m_{y,K}(x)$ es inseparable o bien tiene grado 1. Esto nos permite concluir que $y \in L$ es inseparable sobre K o bien $y \in K$.

3.- **Problema 3:** Sea K un cuerpo de característica p y $\alpha \in \overline{K}$ un elemento separable. Pruebe que $K(\alpha) = K(\alpha^{p^i})$, para todo $i \in \mathbb{N}$.

Demostración: Es facil probar que $K(\alpha^{p^i}) \subset K(\alpha)$, por ende solo debemos demostrar que $K(\alpha^{p^i}) \supset K(\alpha)$. Note que α satisface el polinomio $r(x) \in K(\alpha^{p^i})$ definido por $r(x) = x^{p^i} - \alpha^{p^i}$. Por otro lado tenemos que $m_{\alpha,K(\alpha^{p^i})}(x)$ divide a $m_{\alpha,K}(x)$, puesto que $m_{\alpha,K}(x) \in K(\alpha^{p^i})[x]$ es un polinomio que se anula en α. Por el mismo argumento $m_{\alpha,K(\alpha^{p^i})}(x)$ divide a $r(x)$. Por hipótesis sabemos que $m_{\alpha,K}$ es separable. Luego, el hecho de que $m_{\alpha,K(\alpha^{p^i})}(x)$ divide a $m_{\alpha,K}(x)$, implica que $m_{\alpha,K(\alpha^{p^i})}(x)$ es separable. Ahora bien, en $K(\alpha)$ se tiene que $r(x) = (x-\alpha)^{p^i}$. Por ende la condición de que $m_{\alpha,K(\alpha^{p^i})}(x)$ divida a $r(x)$, implica que $m_{\alpha,K(\alpha^{p^i})}(x) = x - \alpha$. Esto nos permite concluir que $\alpha \in K(\alpha^{p^i})$.

Ayudantía 6: En esta ayudantía trabajaremos con cuerpos finitos, construicciones con regla y comás y polinomios ciclotómicos.

1.- **Problema 1:** Determine el número de polinomios distintos de cada grado que tiene la factorización en irreducibles en $\mathbb{F}_2[x]$ de $P(x) = x^{256} + x$.

Demostración: En todo lo que sigue fijamos una clausura algebraica K de $\mathbb{F}_2$. Note que si $p(x)$ es un polinomio irreducible que divide a $P(x)$ entonces toda raiz $\alpha \in K$ de $p(x)$ satisface $\alpha^{2^8} = \alpha^{256} = \alpha$. Por lo tanto $\alpha \in \mathbb{F}_{2^8}$, donde $\mathbb{F}_{2^8}$ es la única extensión de grado 8 de $\mathbb{F}_2$ contenida en K. Por otro lado si $\alpha \in \mathbb{F}_{2^8}$, entonces $p(x) = m_{\alpha,\mathbb{F}_2}(x)$ divide a $P(x)$, puesto que $P(\alpha) = 0$. Note que, como $P'(x) = -1$, se tiene que $P(x)$ no tiene raices repetidas en K. En particular cada uno de los factores irreducibles de $P(x)$ tienen potencia uno en su factorización y todos son separables. Concluimos que $P(x)$ es el producto de los polinomios minimales de elementos en $\mathbb{F}_{2^8}$. En particular, solo existen polinomios de grado $1, 2, 4$ y 8 que dividen a $P(x)$. Es sencillo ver (Ejericicio), a partir de la caractetización de las extensiones finitas de cuerpos finitos como cuerpos de descomposición, que:

$$\mathbb{F}_{2^{2^i}} \supset \mathbb{F}_{2^{2^{i-1}}} \supset \cdots \supset \mathbb{F}_2,$$

y que, como para todo $k \in \mathbb{N}$ se tiene que $[\mathbb{F}_{2^{2^k}} : \mathbb{F}_{2^{2^{k-1}}}] = 2$, no existen cuerpos L_k distintos de $\mathbb{F}_{2^{2^k}}, \mathbb{F}_{2^{2^{k-1}}}$ tales que $\mathbb{F}_{2^{2^k}} \supset L_k \supset \mathbb{F}_{2^{2^{k-1}}}$. Por lo tanto, todo elemento $\alpha \in \mathbb{F}_{2^{2^i}} - \mathbb{F}_{2^{2^{i-1}}}$ es un elemento primitivo de la extensión $\mathbb{F}_{2^{2^i}}/\mathbb{F}_2$. Por ende $m_{\alpha,\mathbb{F}_2}(x)$ tiene grado 2^i. Vía esta caracterización determinamos la factorización de $P(x)$ como sigue.

i.- Note que los polinomios de grado 1 que dividen a $P(x)$ son tantos como elementos en $\mathbb{F}_2$. En efecto, estos son $x, x-1$.

ii.- Por otro lado el número de polinomios irrecibles de grado 2 que divide a $P(x)$ es $\frac{1}{2}(|\mathbb{F}_{2^2}| - |\mathbb{F}_2|) = 1$. En efecto, dicho polonimio es $x^2 + x + 1$.

iii.- El número de polinomios irreducible de grado 4 que divide a $P(x)$ es $\frac{1}{4}(|\mathbb{F}_{2^4}| - |\mathbb{F}_{2^2}|) = 3$.

iv.- Por último, el número de polinomios irreducible de grado 8 que divide a $P(x)$ es $\frac{1}{8}(|\mathbb{F}_{2^8}| - |\mathbb{F}_{2^4}|) = 30$.

2.- **Problema 2:** El siguiente problema trata acerca de construcciones con regla y compás.

i.- Muestre que el n-ágono regular es constructible si y solamente si $\cos\left(\frac{2\pi}{n}\right)$ es constructible.

ii.- Pruebe que es imposible construir con regla y compás el nonágono regular.

iii.- Demuestre que es posible construir con regla y compás el pentágono regular.

Desarrollo:

i.- Entonces $\beta = \operatorname{sen}\left(\frac{2\pi}{n}\right) = \sqrt{1-\alpha^2}$ es constructible, ya que $1 - \alpha^2$ lo es. Luego, trazamos una linea vertical sobre $(\alpha, 0)$ de largo β y unimos el punto (α, β) con $(0, 0)$ y $(1, 0)$. Note que para construir dica linea vertical hay que intersectar la recta $x = \alpha$ con la circunferencia centrada en α y de radio β. El método anterior nos permite construir un lado del n-ágono regular. Se concluye por inducción que podemos construir dicho n-ágono. Por otro lado, si el n-ágono regular es constructible entonces todos sus vértices son constrictibles. Asumiento que el centro de dicho n-ágono es

$(0,0)$ obtenemos que el punto (α,β) es constructible. En particular α es constructible.

ii.- Por el item [i] basta probar que $\alpha = \cos(40)$ no es constructible. Por la identidad $\cos(3a) = 4\cos(a)^3 - 3\cos(a)$, obtenemos que α satisface el polinomio $p(x) = 4x^3 - 3x + \frac{1}{2}$, el cual no tiene raices en $\mathbb{Q}$. Por lo tanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Por teorema de Wantzel, concluimos que α no es constructible.

iii.- Nuevamente por [i] basta probar que $\alpha = \cos(72)$ es constructible. Sea $\zeta_5 = e^{\frac{2\pi}{5}} \in \mathbb{C}$. Note que $2\cos(72) = \zeta_5 + \zeta_5^{-1}$. Luego, por el problema 3i de la Prueba 1, tenemos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Concluimos, por teorema de Wantzel, que α es constructible.

3.- **Problema 3:** Sea $p \in \mathbb{Z}$ un primo, $e \in \mathbb{Z}_{>1}$ y $\Phi_n(x)$ el n-ésimo polinomio ciclotómico. Muestre que $\Phi_{p^e}(x) = \Phi_p\left(x^{p^{e-1}}\right)$.

Demostración: Sabemos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$, para todo $n \in \mathbb{N}$. Si aplicamos este resultado al caso particular de $n = p^e$, obetenemos que:

$$\Phi_{p^e}(x) = \frac{x^{p^e} - 1}{\prod_{d|p^e, d\neq p^e} \Phi_d(x)}.$$

Por otro lado, como los enteros positivos que dividen a p^e y no son p^e son p^i, con $i \in \{0, \cdots, e-1\}$, tenemos que $\prod_{d|p^e, d\neq p^e} \Phi_d(x) = \prod_{d|p^{e-1}} \Phi_d(x)$. Por lo tanto:

$$\Phi_{p^e}(x) = \frac{x^{p^e} - 1}{\prod_{d|p^{e-1}} \Phi_d(x)} = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1}.$$

Si hacemos la sustitución $u = x^{p^{e-1}}$, obtenemos que $\Phi_{p^e}(x) = \frac{u^p - 1}{u - 1} = \Phi_p(u) = \Phi_p\left(x^{p^{e-1}}\right)$.

4. Teoría de Galois:

Ayudantía 7: En esta ayudantía estudiaremos grupos de automorfismo de cuerpos y extensiones galoisianas. Denotamos por $\mathrm{Aut}(L/K)$ al grupo de automorfismos de L que fijan K.

1.- **Problema 1:**

i.- Calcule $\mathrm{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p(x^p))$.

ii.- Calcule $\mathrm{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p(x^p - x))$. Demuestre que $\mathbb{F}_p(x)$ es una extensión galoisiana de $\mathbb{F}_p(x^p - x)$

Desarrollo:

i.- Para la extensión $K = \mathbb{F}_p(x)$ de $F = \mathbb{F}_p(x^p)$ se cumple que $K = F(x)$, donde $x \in K$ cumple con $m_{x,F}(y) = p(y) = y^p - x^p \in F[y]$ (ver problema 2 de la ayudantía 5). Note que $p(y)$ tiene una sola raiz en $\overline{F}$, puesto que $p(y) = (y - x)^p$, en cualquier anillo de polinomios que contenga a x (por ejemplo en $K[y]$). Ahora bien, como los automorfismos de K que son la identidad en F llevan x a una raiz de $p(x)$ que esté en K, tenemos que el único automorfismo posible es $\phi : x \mapsto x$, es decir $\phi = \mathrm{id}$.

ii.- Al igual que en [i], es sencillo notar que la extensión $K = \mathbb{F}_p(x)$ de $F = \mathbb{F}_p(x^p - x)$ se cumple que $K = F(x)$, donde $x \in K$ es anulado por el polinomio $p(y) = y^p - y - x^p + x \in F[y]$. Note que $p(y)$ tiene por raices a los elementos $\{x+i : i \in \mathbb{F}_p\}$. Por lo tanto $p(y)$ es un polinomio separable y en particular $m_{x,F}(y)$ lo es. Como $p(y)$ tiene todas sus raices en K, tenemos que $m_{x,F}(y)$ tiene todas sus raices en K. Esto prueba que K es el cuerpo de descomposición sobre F del polinomio separable $m_{x,F}(y)$. El corolario 1.5.2 implica que K/F es una extensión galoisiana y por ende $|\mathrm{Aut}(K/F)| = [K : F]$. De hecho las funciones $\phi_i : K \to K$ definidas por $\phi_i(x) = x + i$, donde $i \in \mathbb{F}_p$, son automorfismos (Esto se puede demostrar probando, a partir de la defínción, que dichas funciones son homomorfismos de anillos, luego como no son nulas, estas deben ser homomorfismos inyectivos entre F-espacios de igual dimensión y finita). Por lo tanto existen p automorfismos $\phi : K \to K$ que son la identidad sobre F. En particular, como $p = [K_F]$, tenemos que $m_{x,F}(y) = p(y)$. Es inmediato, de la defínción de ϕ_1, que este automorfismo tiene orden p. Concluimos que $\mathrm{Aut}(K/F) \cong C_p$.

2.- **Problema 2:** Sea p un primo y $\zeta_p = e^{\frac{2\pi i}{p}}$. Considere $K = \mathbb{Q}(\sqrt[p]{2})$ y $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$.

i.- Muestre que $|\mathrm{Aut}(K)| = 1$.

ii.- Pruebe que L es una extensión galoisiana de $\mathbb{Q}$ y determine su grupo de galois.

Desarrollo:

i.- Es directo del hecho de que los homomorfismos envian la unidad de un cuerpo a si misma, que $\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q})$. Por otro lado, sabemos que una $\mathbb{Q}$-incrustación de K (en particular un $\mathbb{Q}$-automorfismo) lleva $\sqrt[p]{2}$ a otra raiz de $m_{\sqrt[p]{2},\mathbb{Q}}(x) = x^p - 2$. Pero la única raiz de $m_{\sqrt[p]{2},\mathbb{Q}}(x)$ en K es $\sqrt[p]{2}$, dado que todas las demás raices complejas tienen parte imaginaria no nula y $K \subset \mathbb{R}$. Por lo tanto, si $\phi \in \mathrm{Aut}(K/\mathbb{Q})$ se tiene que $\phi(\sqrt[p]{2}) = \sqrt[p]{2}$. Concluimos que $\mathrm{Aut}(K) = \{\mathrm{id}\}$.

ii.- Por definición L es el cuerpo de descomposición del un polinomio separable $x^p - 2$. Por el corolario 1.5.2 tenemos que L es una extensión galoisiana de $\mathbb{Q}$. En la prueba 1 demostramos que $[L : \mathbb{Q}] = p(p-1)$. Por lo tanto $|\mathrm{Gal}(L/\mathbb{Q})| = p(p-1)$, en particular $[L : \mathbb{Q}(\zeta_p)] = p$ y por ende $m_{\sqrt[p]{2},\mathbb{Q}(\zeta_p)}(x) = x^p - 2$. Por otro lado, como los automorfismos de K llevan los generadores ζ_p, $\sqrt[p]{2}$ a sus conjugados tenemos que estos son de la forma:

$$\phi_{ij} : \sqrt[p]{2} \to \sqrt[p]{2}\zeta_p^i, \quad \zeta_p \to \zeta_p^j,$$

donde $i = 0, \cdots, p-1$ y $j = 1, \cdots, p-1$. La función ϕ_{ij} es un automorfismo ya que es la extensión a K del homomorfismo $\psi_j : \mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p)$ definida por $\psi_j(\zeta_p) = \zeta_p^j$. Esto se demuestra aplicando la proposición 1.2.11 al homomorfismo ψ_j y al polinomio irreducible $m_{\sqrt[p]{2},\mathbb{Q}(\zeta_p)}(x) = x^p - 2$. Sea $l \in \{1, \cdots, p-1\}$ tal que $\langle \bar{l} \rangle = (\mathbb{Z}/p\mathbb{Z})^*$ y considere:

$$\sigma : \sqrt[p]{2} \to \sqrt[p]{2}\zeta_p, \quad \zeta_p \to \zeta_p,$$
$$\tau : \sqrt[p]{2} \to \sqrt[p]{2}, \quad \zeta_p \to \zeta_p^l.$$

Note que, como $\tau^i(\zeta_p) = \zeta_p^{l^i}$, tenemos que las $p-1$ potencias de τ recorren el conjunto $\{\phi_{0j} : j = 1, \cdots, p\}$. Ahora bien, como $\sigma^i(\sqrt[p]{2}) = \sqrt[p]{2}\zeta_p^i$, tenemos que $\{\phi_{ij}\} = \{\sigma^i\tau^j : i = 1, \cdots, p \text{ y } j = 1, \cdots, p-1\}$. Esto prueba que $\mathrm{Aut}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$. Por último note que $\sigma^l\tau = \tau\sigma$. Esto nos permite concluir que $\mathrm{Aut}(L/\mathbb{Q}) = \langle \sigma, \tau : \sigma^p = \mathrm{id}, \tau^{p-1} = \mathrm{id}, \sigma^l\tau = \tau\sigma \rangle = C_p \rtimes C_{p-1}$.

3.- **Problema 3:** Sea K el cuerpo de descomposición de $p(x) = x^3 + 2x + 2$ sobre $\mathbb{F}_3$.

i.- Muestre que K es una extensión galoisiana de grado 3 de $\mathbb{F}_3$.

ii.- Demuestre que $\mathrm{Gal}(K/\mathbb{F}_3)$ está generado por el automorfismo de Frobenius.

Desarrollo:

i.- Sea $\overline{\mathbb{F}_3}$ una clausura algebraica de $\mathbb{F}_3$ fija. Note que $p(x) = x^3 - x + 2$ y dicho polinomio es separable. De hecho, si $\alpha \in \overline{F}_3$ es una raiz de $p(x)$, entonces $\{\alpha, \alpha+1, \alpha+2\}$ son las raices de $p(x)$. Luego, como K es el cuerpo de descomposición de un polinomio separable, se tiene que K es una extensión galoisiana de $\mathbb{F}_3$. Por otro lado, como $K = \mathbb{Q}(\alpha)$ con $m_{\alpha,\mathbb{F}_3}(x) = p(x)$, se tiene que $[K : \mathbb{F}_3] = 3$.

ii.- En clases se demostró que $K = \mathbb{F}_{3^3} = \{\alpha \in \overline{\mathbb{F}_3} : \alpha^{3^3} = \alpha\}$. Por otro lado, por [i], tenemos que K tiene 3 automorfismos que son la identidad sobre $\mathbb{F}_3$. Sea $\phi : K \to K$ el automorfismo de Frobenius definido por $\phi(a) = a^3$. Note que ϕ^2 es un homomorfismo distinto de la identidad, ya que si $\phi^2(a) = a^9 = a$ para todo $a \in K$, se tiene que $r(x) = x^9 - x$ tiene 27 raices distintas. No obstante $\phi^3(a) = a^{3^3} = a$ para todo $a \in K$. Esto nos lleva a que $\phi^3 = \mathrm{id}$. Por lo tanto $\phi \in \mathrm{Aut}(K/\mathbb{F}_3)$ es un elemento de orden 3. Concluimos que $\mathrm{Gal}(K/\mathbb{F}_3) \cong C_3$ y que dicho grupo está generado por el automorfismo de Frobenius.

Ayudantía 8: En esta ayudantía estudiaremos grupos de Galois, subgrupos de este y subcuerpos de extensiones galoisianas.

1.- **Problema 1:** Sea $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

i.- Demuestre que K es una extensión galoisiana de $\mathbb{Q}$.

ii.- Calcule $G = \text{Gal}(K/\mathbb{Q})$.

iii.- Determine los cuerpos fijos por cada uno de los subgrupos de G.

Desarrollo:

i.- Note que K es el cuerpo de descomposición, contenido en $\mathbb{C}$, del polinomio $p(x) = (x^2 - 2)(x^3 - 3)$. Por otro lado las raices de $p(x)$ son $\{\pm\sqrt{2}, \pm\sqrt{3}\}$. Esto implica que $p(x)$ es un polinomio separable. Se sigue del corolario 2.1.5 que K es una extensión galoisiana de $\mathbb{Q}$.

ii.- El problema 7 del control 1 implica que $[K : \mathbb{Q}] = 4$. Por ende $\text{Gal}(K/\mathbb{Q})$ tiene 4 elementos. Considere las funciones $\sigma, \tau : K \to K$ definidas por $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ y $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$. Note que $\sigma \circ \tau = \tau \circ \sigma$ es la función definida por $\sigma \circ \tau(\sqrt{2}) = -\sqrt{2}$ y $\sigma \circ \tau(\sqrt{3}) = -\sqrt{3}$. Por otro lado, como todo $\mathbb{Q}-$automorfismo lleva $\sqrt{3}$ a $\pm\sqrt{3}$ y $\sqrt{2}$ a $\pm\sqrt{2}$, se tiene que id, σ, τ y $\sigma\tau$ son las únicas funciones que pueden ser $\mathbb{Q}-$automorfismo de K. Concluimos que $\text{Gal}(K/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \sigma\tau\}$. Es inmediato de la defínción de σ y τ que $\sigma^2 = \text{id}$, $\tau^2 = \text{id}$. Concluimos que:

$$G = \langle \sigma, \tau : \sigma^2 = \tau^2 = \text{id}, \sigma\tau = \tau\sigma \rangle \cong C_2 \times C_2.$$

iii.- Los subgurpos no triviales de G son $\langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle$. Dado que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es una $\mathbb{Q}$-base de K tenemos que:

$$K^{\langle\sigma\rangle} = \{z = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : z = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}\}.$$

Por lo tanto $K^{\langle\sigma\rangle} = \{a + c\sqrt{3} : a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})$. Por un argumento análogo se tiene que $K^{\langle\tau\rangle} = \mathbb{Q}(\sqrt{2})$ (ejercicio). Ahora bien, como $z = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in K^{\langle\sigma\tau\rangle}$ si y solamente si $z = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$, se tiene que $K^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt{6})$. Por otro lado, es sencillo ver que $K^{\{\text{id}\}} = K$ y que si $z = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ cumple con $z = \sigma(z)$, $z = \tau(z)$, entonces se tiene que $b = c = d = 0$. Por lo tanto $K^G = \mathbb{Q}$. Concluimos que $\{\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}), K\}$ son cuerpos fijos por los subgrupos de G.

2.- **Problema 2:** Sea $K = \mathbb{Q}(\sqrt[3]{2}, w)$, donde $w = e^{\frac{2\pi i}{3}}$.

i.- Demuestre que K es una extensión galoisiana de $\mathbb{Q}$ y determine $G = \text{Gal}(K/\mathbb{Q})$.

ii.- Determine los cuerpos fijos por cada uno de los subgrupos de G.

Desarrollo:

i.- Observe que K es el cuerpo de descomposición, contenido en $\mathbb{C}$, del polinomio separable $p(x) = x^3 - 2$. Esto implica que $K/\mathbb{Q}$ es una extensión galoisiana. Por otro lado, en la ayudantía 7 se probó que para $w = e^{\frac{2\pi i}{p}}$ y $l \in \{1, \cdots, p-1\}$ un generador de $(\mathbb{Z}/p\mathbb{Z})^*$ se tiene que:

$$\text{Gal}(\mathbb{Q}(\sqrt[p]{2}, w)/\mathbb{Q}) = \langle \sigma, \tau : \sigma^p = \text{id}, \tau^{p-1} = \text{id}, \sigma^l\tau = \tau\sigma \rangle,$$

donde:

$$\sigma : \sqrt[p]{2} \to \sqrt[p]{2}\zeta_p, \quad \zeta_p \to \zeta_p,$$
$$\tau : \sqrt[p]{2} \to \sqrt[p]{2}, \quad \zeta_p \to \zeta_p^l.$$

En particular, tomando $p = 3$ en la identidad anterior, tenemos que $G = \langle \sigma, \tau : \sigma^3 = \mathrm{id}, \tau^2 = \mathrm{id}, \sigma^{-1}\tau = \tau\sigma \rangle \cong D_6$.

ii.- Los subgrupos no triviales de G son $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\tau\sigma\rangle$ y $\langle\tau\sigma^2\rangle$. Por otro lado, se sigue del problema 2 de la prueba 1, tenemos que:

$$\beta = \{1, \sqrt[3]{2}, \sqrt[2]{4}, w, w\sqrt[3]{2}, w\sqrt[3]{4}\},$$

es una $\mathbb{Q}$-base de K. Por lo tanto, $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + a_4 w + a_5 w\sqrt[3]{2} + a_6 w\sqrt[3]{4} \in K^{\langle\tau\rangle}$ si y solamente si $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + a_4 w^{-1} + a_5 w^{-1}\sqrt[3]{2} + a_6 w^{-1}\sqrt[3]{4}$. Pero $w^{-1} = -1 - w$ y por ende $z = a_1 - a_4 + (a_2 - a_5)\sqrt[3]{2} + (a_3 - a_6)\sqrt[3]{4} - a_4 w - a_5 w\sqrt[3]{2} - a_6 w\sqrt[3]{4}$. Por la independencia lineal de β tenemos que $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4}$. Esto implica que $K^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$. Por un argumento análogo se tiene que $K^{\langle\tau\sigma\rangle} = \mathbb{Q}(w\sqrt[3]{2})$ y $K^{\langle\tau\sigma^2\rangle} = \mathbb{Q}(w^2\sqrt[3]{2})$ (ejercicio). Por otro lado $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + a_4 w + a_5 w\sqrt[3]{2} + a_6 w\sqrt[3]{4} \in K^{\langle\sigma\rangle}$ si y solamente si $z = a_1 + a_2 w\sqrt[3]{2} + a_3 w^2\sqrt[3]{4} + a_4 w + a_5 w^2\sqrt[3]{2} + a_6\sqrt[3]{4} = a_1 + a_2 w\sqrt[3]{2} + a_3(-w-1)\sqrt[3]{4} + a_4 w + a_5(-w-1)\sqrt[3]{2} + a_6\sqrt[3]{4}$. Nuevamente por la independencia lineal de β tenemos que $a_2 = a_3 = a_5 = a_6$. Esto nos lleva a que $K^{\langle\sigma\rangle} = \mathbb{Q}(w)$. Es sencillo ver que $K^{\{\mathrm{id}\}} = K$ y que $K^G = \mathbb{Q}(w)^G = \mathbb{Q}$. Concluimos que $\{\mathbb{Q}, \mathbb{Q}(w), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}w), \mathbb{Q}(\sqrt[3]{2}w^2)\}$ son los cuerpos fijos por los subgrupos de G.

3.- **Problema 3:** Sea $\overline{\mathbb{F}_p}$ una clausura algebraica de $\mathbb{F}_p$ y $K = \mathbb{F}_{p^n}$ la extensión de grado n de $\mathbb{F}_p$ contenida en $\overline{\mathbb{F}_p}$.

i.- Demuestre que K es una extensión galoisiana de $\mathbb{F}_p$.

ii.- Determine el grupo $G = \mathrm{Gal}(K/\mathbb{Q})$.

iii.- Determine los cuerpos fijos por cada uno de los subgrupos de G.

Desarrollo:

i.- Recordemos que en clases se demostró que K es el cuerpo de descomposición de polinomio $p(x) = x^{p^n} - x$, donde $p'(x) = -1$. Esto implica que $p(x)$ es un polinomio separable y por ende K es una extensión galoisiana de $\mathbb{F}_p$.

ii.- Lo probado en [i] implica que $|G| = [K : \mathbb{F}_p] = n$. Ahora bien, en clases de probó que la función $\phi : K \to K$ definida por $\phi(a) = a^p$ es un automorfismos, el cual denominamos automorfismo de Frobenius. Por otro lado sabemos que $K = \{a \in \overline{\mathbb{F}_p} : a^{p^n} = a\}$. Sea $s \in \{1, \cdots, n-1\}$. Si el automorfismo ϕ^s definido por $\phi^s(a) = a^{p^s}$ es la identidad, se tiene que $x^{p^s} - x$ se anula en p^n puntos. Esto nos lleva a una contradicción. Por lo tanto $|\phi| = n$. Concluimos que $G \cong C_n$.

iii.- Por la ciclicidad de G tenemos que todos sus subgrupos son también cíclicos. Es más, todos los subgrupos de G son de la forma $H = \langle\phi^d\rangle$, donde $d|n$. Note que $K^H = \{a \in K : a^{p^d} = a\} = \mathbb{F}_{p^d}$. Esto nos dice que $\{\mathbb{F}_{p^d} : d|n\}$ es el conjunto de los cuerpos fijos por los subgrupos de G.

Ayudantía 9: En esta ayudantía trabajaremos con el teorema principal de Galois.

1.- **Problema 1:** Considere $L = \mathbb{Q}(\zeta_n)$ como el n-ésimo cuerpo ciclotómico y $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

i.- Demuestre que $L/\mathbb{Q}$ es galoisiana y describa $\mathrm{Gal}(L/\mathbb{Q})$.

ii.- Demuestre que $K/\mathbb{Q}$ es galoisiana y describa $\mathrm{Gal}(K/\mathbb{Q})$.

Desarrollo:

i.- Sabemos que L es el cuerpo de descomposición del n-ésimo polinomio ciclotómico $\Phi_n(x)$. Como $\mathrm{car}(\mathbb{Q}) = 0$, tenemos que $\Phi_n(x)$ es separable. Por lo tanto $L/\mathbb{Q}$ es galoisiana. En clases se demostró que la función $\phi : \mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ definida por $\phi(\sigma_i) = \overline{i}$ donde $\sigma_i(\zeta_n) = \zeta_n^i$ es un isomorfismo de grupos. Por lo tanto $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

ii.- Note que $\mathrm{Gal}(L/\mathbb{Q})$ es un grupo abeliano. Por ende todas sus subextensiones son galosianas sobre $\mathbb{Q}$. En particular $K/\mathbb{Q}$ es galoisiana. Por el mismo argumento dado en la prueba 1, tenemos que $[L : K] = 2$. Por lo tanto $\mathrm{Gal}(K/L)$ es un subgrupo de $\mathrm{Gal}(K/\mathbb{Q})$ de orden 2. Note que $\sigma_{-1}(\zeta_n + \zeta_n - 1) = \zeta_n + \zeta_n^{-1}$. Por lo tanto $K \subset L^{\langle \sigma_{-1} \rangle}$. Ahora bien, como $[L : L^{\langle \sigma_{-1} \rangle}] = |\langle \sigma_{-1} \rangle| = 2 = [L : K]$ tenemos que $L^H = K$. Concluimos, del teorema fundamental de Galois, que $\mathrm{Gal}(K/L) = \langle \sigma_{-1} \rangle \cong \{1, -1\} \subset (\mathbb{Z}/n\mathbb{Z})^*$. Por lo tanto $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(K/L) \cong (\mathbb{Z}/n\mathbb{Z})^*/\{1, -1\}$.

2.- **Problema 2:** Sean K_1, K_2 dos extensiones de galois sobre F.

i.- Demuestre que la intersección $K_1 \cap K_2$ es galoisiana sobre F.

ii.- Pruebe que el composito K_1K_2 es galoisino sobre F.

iii.- Demuestre que grupo de galois $\mathrm{Gal}(K_1K_2/F)$ es isomorfo al subgrupo H de $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ formado por los elementos cuyas restricciones a la intersección $K_1 \cap K_2$ sean iguales.

Desarrollo:

i.- Sea $\alpha \in K_1 \cap K_2$ y $p(x) = m_{\alpha,F}(x)$ el polinomio minimal de α. Como K_1/F es separable, tenemos que $p(x)$ es separable y por ende $K_1 \cap K_2/F$ es separable. Para demostrar que $K_1 \cap K_2/F$ es galoisiana basta ver que para todo $\alpha \in K_1 \cap K_2$ el polinomio $m_{\alpha,F}(x)$ tiene toda sus raices en $K_1 \cap K_2$. En efecto, como K_1/F y K_2/F son extensiones normales tenemos que, si $m_{\alpha,F}(\beta) = 0$ entonces $\beta \in K_1 \cap K_2$. Esto demuestra lo pedido.

ii.- Como K_1/F y K_2/F son extensiones galoisianas, sabemos que K_1 es el cuerpo de descomposición del polinomio separable $p(x) \in F[x]$ y que K_2 es el cuerpo de descomposición del polinomio separable $q(x) \in F[x]$. Luego K_1K_2 es el cuerpo de descomposición de la parte libre de cuadrados de $p(x)q(x)$. Esto prueba lo pedido.

iii.- Considere el homomorfismo de grupos $\phi : \mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ definido por $\phi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$. Note que el núcleo de ϕ consiste en $\sigma : K_1K_2 \to K_1K_2$ tales que $\sigma(a) = a$, para todo $a \in K_1 \cup K_2$. Como K_1/F y K_2/F son extensiones separables, por el teorema del elemento primitivo tenemos que $K_1 = F(\alpha)$ y $K_2 = F(\beta)$. Luego $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$ y como $K_1K_2 = F(\alpha, \beta)$ concluimos que $\sigma = \mathrm{id}$. Esto prueba que ϕ es inyectivo. Por otro lado, para todo $(\sigma|_{K_1}, \sigma|_{K_2}) \in \mathrm{Im}(\phi)$, se tiene que

$\sigma|_{K_1}|_{K_1\cap K_2} = \sigma|_{K_1\cap K_2} = \sigma|_{K_1}|_{K_1\cap K_2}$. Sea:

$$H = \{(\tau,\mu) \in \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) : \tau|_{K_1\cap K_2} = \mu|_{K_1\cap K_2}\}.$$

Considere el homomorfismo sobreyectivo:

$$\mathrm{res} : \mathrm{Gal}(K_2/F) \to \mathrm{Gal}(K_1 \cap K_2/F),$$

definido por $\mathrm{res}(\sigma) = \sigma|_{K_1\cap K_2}$, donde $\ker(\mathrm{res}) = \mathrm{Gal}(K_2/K_1 \cap K : 2)$. Entonces, por lo sabido de teoría de grupos, un elemento cualquiera en $\mathrm{Gal}(K_1 \cap K_2/F)$ tiene $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$ preimagenes en $\mathrm{Gal}(K_2/F)$. Equivalentemente, por cada elemento $\tau \in \mathrm{Gal}(K_1/F)$ existen $|\mathrm{Gal}(K_2/K_1\cap K_2)|$ elementos $\mu \in \mathrm{Gal}(K_2/F)$ cuya restricción a $K_1 \cap K_2$ es $\tau|_{K_1\cap K_2}$. Luego tenemos que $|H| = |\mathrm{Gal}(K_1/F)||\mathrm{Gal}(K_2/K_1 \cap K_2)|$ y por lo tanto $H = |\mathrm{Gal}(K_1/F)|\frac{|\mathrm{Gal}(K_2/F)|}{|\mathrm{Gal}(K_2\cap K_2/F)|} = \frac{[K_1:F][K_2:F]}{[K_1\cap K_2:F]}$. Para una extensión K_1/F galoisiana y K_2/F finita se tiene que $\frac{[K_1:F][K_2:F]}{[K_1\cap K_2:F]} = [K_1K_2 : F]$ (ejercicio control 4). Esto implica que $|H| = [K_1K_2 : F] = |\mathrm{Gal}(K_1K_2/F)|$.

3.- **Problema 3:** Sea K/F una extensión finita. Para $\alpha \in K$, sea $L_\alpha : K \to K$ la tranformación F-lineal definida por $L_\alpha(b) = \alpha b$. Definimos $P_\alpha(x)$ como el polinomio caracteristico de L_α y $\mathrm{N}_{K/F}(\alpha)$, $\mathrm{tr}_{K/F}(\alpha)$ como el determinante y la traza de L_α respectivamente.

i.- Pruebe que $P_\alpha(x) = m_{\alpha,F}(x)^m$, donde $m = [K : F(\alpha)]$.

ii.- Sean $\alpha_1, \cdots, \alpha_n$ todas las raices de $P_\alpha(x)$ y suponga que $\alpha_1, \cdots, \alpha_n \in K$. Demuestre que $\mathrm{N}_{K/F}(\alpha) = \prod_{i=1}^n \alpha_i$ y que $\mathrm{tr}_{K/F}(\alpha) = \sum_{i=1}^n \alpha_i$.

iii.- Concluya que si $F(\alpha)/F$ es galoisiana y $G = \mathrm{Gal}(F(\alpha)/F)$ entonces la norma y la traza satisfacen que $\mathrm{N}_{K/F}(\alpha) = \left(\prod_{\sigma\in G}\sigma(\alpha)\right)^m$, $\mathrm{tr}_{K/F}(\alpha) = m\sum_{\sigma\in G}\sigma(\alpha)$.

Desarrollo:

i.- Considere la base $\{1, \alpha, \cdots, \alpha^{k-1}\}$ de $F(\alpha)/F$ y $\{e_1, \cdots, e_m\}$ una base cualquiera de $K/F(\alpha)$. Entonces sabemos que:

$$\beta = \{e_1, \alpha e_1, \cdots, \alpha^{k-1}e_1, \cdots, e_m, \alpha e_m, \cdots, \alpha^{k-1}e_m\},$$

es una base de K/F, la cual en todo lo que sigue consideraremos ordenada como anteriormente. Sea $m_{\alpha,F} = a_0 + a_1x + \cdots + a_kx^k$. Entonces, en la base β tenemos que la tranformación lineal L_α está representada por m bloques diagonales de la forma:

$$B = \begin{bmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & \cdots & 0 & -a_1 \\ \vdots & & & \\ 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Concluimos, de un cálculo directo de los determinantes, que $P_\alpha(x) = \det(B - xI)^m = m_{\alpha,F}(x)^m$.

ii.- Escribimos $P_\alpha(x)) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Es un resultado de álgebra lineal, que $(-1)^n b_0 = \det(L_\alpha)$ y que $-b_{n-1} = \mathrm{tr}(L_\alpha)$. Luego si $P_\alpha(x) = \prod_{i=1}^n(x - \alpha_i)$, se tiene que $\prod_{i=1}^n \alpha_i = \det(L_\alpha)$ y $\sum_{i=1}^n \alpha_i = \mathrm{tr}(L_\alpha)$. El resultado pedido se sigue directamente de este hecho.

iii.- Supongamos que $F(\alpha)/F$ es galoisiana. Entonces como las imágenes de α por los distintos automorfismos $\sigma \in G$ son las otras raices de $m_{\alpha,F}(x)$ se tiene que $m_{\alpha,F}(x) = \prod_{\sigma\in G}(x - \sigma(\alpha))$. Por lo tanto $P_\alpha(x) = \prod_{\sigma\in G}(x - \sigma(\alpha))^m$. De [ii] se sigue que:

$$\mathrm{N}_{K/F}(\alpha) = \left(\prod_{\sigma\in G} \sigma(\alpha)\right)^m, \quad \mathrm{tr}_{K/F}(\alpha) = m\sum_{\sigma\in G} \sigma(\alpha).$$

Ayudantía 10: Sea K un cuerpo de característica distinta de 2 y 3. En esta ayudantía estudiaremos la solubilidad por radicales de la ecuación de grado 3 sobre K.

1.- **Problema 1:** Sea $p(x) \in K[x]$ un polinomio mónico separable. Se define el discriminante de p por $D(p) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j)$, donde $\{\alpha_1, \cdots, \alpha_n\}$ es el conjunto de todas las raices de $p(x)$.

i.- Muestre que $D(p) \in K$.

ii.- Sea $L = K(\alpha_1, \cdots, \alpha_n)$. Pruebe que $\sqrt{D(p)} \in K$ si y solamente si $\mathrm{Gal}(L/K)$ es isomorfo a un subgrupo de A_n.

iii.- Para $p(x) = x^3 + px + q$ demuestre que $D(p) = -4p^3 - 27q^2$.

2.- **Desarrollo:**

i.- Sea $L = K(\alpha_1, \cdots, \alpha_n)$. Note que L es el cuerpo de descomposición del polinomio separable $p(x)$. Por lo tanto L/K es una extensión galoisiana. Sea $G = \mathrm{Gal}(L/K)$. Para demostrar que $D(p) \in K$ basta probar que $\sigma(D(p)) = D(p)$, para todo $\sigma \in G$. En efecto, como $\sigma(\alpha_i)$ es otra raiz de $p(x)$ y $\sigma(\alpha_i) \neq \sigma(\alpha_j)$ para $i \neq j$, tenemos que $\sigma(D(p)) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\sigma(\alpha_i) - \sigma(\alpha_j)) = D(p)$. Esto demuestra lo pedido.

ii.- Considere la función $\pi : G \to S_n$ definida por $\sigma(\alpha_i) = \alpha_{\pi(\sigma)(i)}$. Es un ejercicio probar que π es un homomorfismo inyectivo. Por otro lado, observe que $\sqrt{D(p)} = \prod_{i<j}(\alpha_i - \alpha_j)$. Luego, si identidicamos $\sigma(\alpha_i)$ con $\alpha_{\sigma(i)}$, tenemos que:

$$\sigma(\sqrt{D(p)}) = \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \mathrm{sgn}(\sigma)\sqrt{D(p)}.$$

Por lo tanto $\sigma(\sqrt{D(p)}) = \sqrt{D(p)}$ si y solamente si $\pi(\sigma) \in A_n$. De esto se sigue lo pedido.

iii.- Note que el polinomio $p(x)$ satisface $p(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. De esta forma, la derivada $D_x(p(x))$ de $p(x)$ es:

$$D_x(p(x)) = (x - \alpha_1)(x - \alpha_2) + (x - \alpha_1)(x - \alpha_3) + (x - \alpha_2)(x - \alpha_3).$$

Luego $D_x(p(\alpha_1)) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)$, $D_x(p(\alpha_2)) = (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)$ y $D_x(p(\alpha_3)) = (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$. Por lo tanto tenemos que $D(p) = -D_x(p(\alpha_1))D_x(p(\alpha_2))D_x(p(\alpha_3))$. Por otro lado tenemos que $D_x(p(x)) = 3x^2+p$. Por lo tanto, de un cálculo directo usando las identidades anteriores, se obtiene que $D(p) = -4p^3 - 27q^2$.

2.- **Problema 2:** Para L el cuerpo de descomposición de $p(x) = x^3 + px + q$ determine $G = \mathrm{Gal}(L/K)$.

Desarrollo: Si $p(x)$ es reducible sobre K entonces $L = K$ o bien $[L : K] = 2$. En el segundo caso tenemos que $\mathrm{Gal}(L/K) \cong C_2$. En lo que sigue supondremos que $p(x)$ es irreducible, en particular tenemos que $[L : K]$ es divisible por 3. Por el problema 1 parte [iii] tenemos que $G \hookrightarrow S_3$, luego $G \cong A_3$ o bien $G \cong S_3$. Note que por el mismo resultado tenemos que $G \cong S_3$ si y solamente si $D(p) = -4p^3 - 27q^2$ es un cuadrado en K. En dicho caso $[L : K] = 3$ y por lo tanto $K(\alpha_1) = L$. Por otro lado, si $G \cong S_3$, emplenado el mismo argumento anterior con $K(\sqrt{D(p)})$ como cuerpo base

tenemos que $H = \mathrm{Gal}(L/K(\sqrt{D(p)}) \cong A_3$ y que $L = K(\sqrt{D(p)}, \alpha_1)$. Note que un generador de H es $\sigma : K \to K$ tal que $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$ y $\sigma(\alpha_3) = \alpha_1$. Sea $\tau : L \to L$ la función definida por $\tau(\sqrt{D(p)}) = -\sqrt{D(p)}$, $\tau(\alpha_1) = \alpha_1$. Es un ejercicio probar que τ es un isomorfismo. Ahora bien como σ y cualquier elemento de orden 2 de G generan S_3 tenemos que $G = \langle \sigma, \tau \rangle \cong S_3$.

Sea L una extensión cíclica de grado n de K que contiene al conjunto μ_n de las raices n-ésimas de 1 y $\sigma \in \mathrm{Gal}(L/K)$ un generador. Sea $\alpha \in L$ y $\zeta \in \mu_n$ una raiz n-ésima de 1. Se define la resolvende de Lagrange (α, ζ) por $(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$.

3.- **Problema 3:** Para $K = \mathbb{Q}$ deduzca formulas explícitas para las raices de $p(x) = x^3 + px + q$ en términos de los coeficientes p, q.
Desarrollo: En lo que sigue consideraremos $G \cong S_3$. Sea $w = \zeta_3$ una raiz 3-ésima primitiva de la unidad y sea $F = \mathbb{Q}(w)$. Note que $[F(\sqrt{D(p)}) : \mathbb{Q}(\sqrt{D(p)})] \in \{1, 2\}$ y que $[L : \mathbb{Q}(\sqrt{D(p)})] = 3$. Como dichos grados son relativamente primos tenemos que $[L(w) : F(\sqrt{D(p)})] = 3$ y por ende:

$$\mathrm{Gal}(L(w)/F(\sqrt{D(p)}) \cong C_3.$$

Aplicando el resolvente de Lagrange obtenemos que $\theta_1 = (w, \alpha_1) = \alpha_1 + w\alpha_2 + w^2\alpha_3$, $\theta_2 = (w^2, \alpha_1) = \alpha_1 + w^2\alpha_2 + w\alpha_3$ y que $(1, \alpha_1) = \alpha_1 + \alpha_2 + \alpha_3 = 0$. Esto último pues $\alpha_1 + \alpha_2 + \alpha_3$ es el coeficiente de grado 2 en $p(x)$. Observe que:

$$\theta_1 + \theta_2 = 3\alpha_1, w^2\theta_1 + w\theta_2 = 3\alpha_2, w\theta_1 + w^2\theta_2 = 3\alpha_3. \tag{1}$$

En lo que sigue calcularemos θ_1^3 en términos de $D(p)$. En efecto, mediante un cálculo algebraico se obtiene que:

$$\theta_1^3 = \sum_{i=1}^{3} \alpha_i^3 - \frac{3}{2} \sum_{i \neq j} \alpha_i^2 \alpha_j + \frac{3\sqrt{-3}}{2}(D(p)) + 6\alpha_1\alpha_2\alpha_3. \tag{2}$$

Como además como $\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0$, tenemos que:

$$\sigma_1^3 = \sum_{i=1}^{3} \alpha_i^3 - 3 \sum_{i \neq j} \alpha_i^2 \alpha_j + 6\alpha_1\alpha_2\alpha_3 = 0.$$

Sea $\sigma_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3$. Observe que $\sigma_2 = p$ y que $\alpha_1\alpha_2\alpha_3 = -q$. Es un cálculo directo que:

$$0 = \sigma_1\sigma_2 = \sum_{i \neq j} \alpha_i^2 \alpha_j + 3\alpha_1\alpha_2\alpha_3. \tag{3}$$

Sumando las identidades (2) y (3) obtenemos que $\sum_{i=1}^{3} \alpha_i^3 - \frac{3}{2} \sum_{i \neq j} \alpha_i^2 \alpha_j + 6\alpha_1\alpha_2\alpha_3 = \frac{27}{2}\alpha_1\alpha_2\alpha_3 = -\frac{27}{2}q$. Por lo tanto:

$$\theta_1^3 = -\frac{27}{2}q + \frac{3\sqrt{-3}}{2}\sqrt{D(p)} \in \mathbb{Q}(\sqrt{D(p)}).$$

Por un arguemento análogo obtenemos que:

$$\theta_2^3 = -\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\sqrt{D(p)}.$$

Luego, como $\theta_1 + \theta_2 = 3\alpha_1$, tenemos que:

$$\alpha_1 = \frac{1}{3}\left(\sqrt[3]{-\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\sqrt{D(p)}} + \sqrt[3]{-\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\sqrt{D(p)}}\right).$$

De las demás identidades mostradas en (1) se obtiene que:

$$\alpha_2 = \frac{1}{3}\left(w^2\sqrt[3]{-\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\sqrt{D(p)}} + w\sqrt[3]{-\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\sqrt{D(p)}}\right),$$

y que:

$$\alpha_3 = \frac{1}{3}\left(w\sqrt[3]{-\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\sqrt{D(p)}} + w^2\sqrt[3]{-\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\sqrt{D(p)}}\right).$$

5. Álgebras:

Ayudantía 11: En esta ayudantía comenzaremos nuestro estudio de álgebras.

1.- **Problema 1:** Sea F cuerpo tal que $\text{car}(F) \neq 2$. Sea $A = \left(\frac{a,b}{F}\right)$ un álgebra de cuaterniones sobre F y considere $x = c + z$, donde $c \in F$ y $z \in Fi + Fj + Fij$. Se define el conjugado de x por $\bar{x} = c - z$ y su norma $N(x) = x\bar{x}$, además x se dice puro si $c = 0$. Pruebe que:

i.- $\forall x \in A$ se tiene que $N(x) \in F$ y que $N(x) = N(\bar{x})$, $\bar{\bar{x}} = x$.

ii.- Muestre que si $x^2 \in F$ entonces x es un cuaternión puro o bien $x \in F$.

iii.- Pruebe que $N(xy) = N(x)N(y)$, para todo $x, y \in A$.

1.- **Desarrollo:**

i.- Sea $x \in A$ escrito como en el enunciado. Es sencillo notar que si $\bar{x} = c - z$ entonces $\bar{\bar{x}} = c+z = x$. Escribimos ahora $x = a_0+a_1i+a_2j+a_3ij$. Mediante un cálculo directo podemos concluir que $N(x) = x\bar{x} = a_0^2-aa_1^2-ba_2^2+aba_4^4 \in F$. Por el mismo cálculo concluimos que $N(\bar{x}) = a_0^2 - aa_1^2 - ba_2^2 + aba_4^4 = N(x)$.

ii.- Escribimos $x = c + z$ como en el enunciado. Entonces, como $z^2 = -N(z)$ y $cz = zc$ tenemos que $x^2 = c^2 + cz + zc - N(z) = c^2 + 2cz - N(z) \in F$. De esto se sigue que $cz = 0$. Por la independencia lineal del conjunto $\{i, j, ij\}$ la igualdad anterior implica que $c = 0$ o bien $z = 0$. Esto nos permite concluir que x es un cuaternión puro o bien $x \in F$.

iii.- Se sigue de un cálculo directo (Ejercicio).

2.- **Problema 2:** Sea $A = \left(\frac{a,b}{F}\right)$ un álgebra de cuaterniones sobre F tal que $\text{car}(F) \neq 2$. Pruebe que son equivalentes:

i.- A es un álgebra de división.

ii.- Para todo $x \in A$ no nulo se tiene que $N(x) \neq 0$.

iii.- Si $a_0, a_1, a_2 \in F$ satisfacen la ecuación $x_0^2 = ax_1^2 + bx_2^2$ entonces $a_0 = a_1 = a_2 = 0$.

2.- **Demostración:** Primero mostremos que [i] y [ii] son equivalentes. Sea $x \in A$ tal que $N(x) = 0$. Si A es álgebra de división tenemos que existe $y \in A$ tal que $yx = xy = 1$. De la identidad $N(xy) = N(x)N(y)$ se sigue que $1 = N(xy) = N(x)N(y) = 0$. Esto nos lleva a una contradicción. Invsersamente, si $N(x) \neq 0$, para todo $x \neq 0$ se tiene que $y = \frac{\bar{x}}{N(x)}$ es un elemento tal que $xy = yx = 1$. Esto último es un resultado directo del problema 1 parte [i]. Utilizando la igualdad $N(a_0 + a_1i + a_2j + a_3ij) = a_0^2 - aa_1^2 - ba_2^2 + aba_4^4$ se concluye facilmente que [ii] implica [iii]. Por último mostremos que [iii] implica [ii]. En efecto, supongamos que $a_0^2 - aa_1^2 - ba_2^2 + aba_4^4 = 0$, es decir $a_0^2 - ba_2^2 = a(ba_4^2 - a_1^2)$. Por lo tanto:

$$(ba_4^2 - a_1^2)^2 = (ba_4^2 - a_1^2)(a_0^2 - ba_2^2) = (a_0a_1 + ba_2a_3) - b(a_0a_3 + a_1a_2).$$

Por [iii] tenemos que $ba_4^2 - a_1^2 = a_0a_1 + ba_2a_3 = a_0a_3 + a_1a_2 = 0$. Esto implica que $a_0 = a_1 = a_2 = a_3 = 0$. Concluimos lo pedido.

3.- **Problema 3:** Sea K un cuerpo de característica distinta de 2. Considere $a, b \in K^*$ y $A = \left(\frac{a,b}{K}\right)$ el álgebra de cuaterniones asociada.

i.- Para $K = \mathbb{R}$ muestre que A es un álgebra de división si y solamente si $a, b < 0$.

ii.- Muestre que $\left(\frac{1,1}{K}\right) \cong \mathbb{M}_2(K)$.

iii.- Pruebe que $B = \left(\frac{a,b}{\mathbb{C}}\right) \cong \mathbb{M}_2(\mathbb{C})$, para todo $a, b \in \mathbb{C}$.

3.- **Desarrollo:**

i.- Usamos el criterio [iii] del problema 2. En efecto, supongamos que $a, b < 0$. Si $a_0^2 = aa_1^2 + ba_2^2$ tenemos que $a_0^2 < 0$. Por lo tanto $a_0 = 0$ y $aa_1^2 + ba_2^2 =$. Esto implica que $a_1 = a_2 = 0$. Concluimos que A es un álbegra de división. Ahora bien, si $a > 0$ entonces $a \in \mathbb{R}^2$. Como $a \neq 0$ tenemos que la ecuación $aa_1^2 + ba_2^2 =$ tiene una solución a $(\sqrt{a}, 1, 0)$ y por ende A no es un álgebra de división. Análogamente deducimos que si $b > 0$ entonces A no es un álgebra de división. Esto prueba lo pedido.

ii.- Considee $A = \left(\frac{1,1}{K}\right)$ y la función $\varphi : A \to \mathbb{M}_2(F)$ definida por:

$$\varphi(i) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \varphi(j) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note que $\varphi(i)^2 = \varphi(j)^2 = \text{id} \in \mathbb{M}_2(K)$. Esto implica que, expandiendo φ lineal y multiplicativamente, se tiene que φ es un homomorfismo de K-álgebras (Ejercicio). Note que $\varphi(ij) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Por lo tanto $\{\varphi(1), \varphi(i), \varphi(j), \varphi(ij)\}$ es un conjunto linealmente independiente en $\mathbb{M}_2(K)$. De esto se sigue que φ es sobreyectiva. Como $\dim_K(A) = \dim_K(\mathbb{M}_2(K)) = 4$, concluimos que φ es un isomorfismo. Esto prueba lo pedido.

iii.- Como $\mathbb{C}$ es algebraicamente cerrado, podemos hacer el cambio de variable $i \mapsto \frac{i}{\sqrt{a}}$ y $j \mapsto \frac{j}{\sqrt{b}}$. Note que dicho cambio de variable está bien definido pues $\frac{i}{\sqrt{a}}\frac{j}{\sqrt{b}} + \frac{j}{\sqrt{b}}\frac{i}{\sqrt{a}} = \frac{1}{\sqrt{ab}}(ij + ji) = 0$. Por lo tanto $B \cong \left(\frac{1,1}{\mathbb{C}}\right)$ y por el item [ii] concluimos que $B \cong \mathbb{M}_2(\mathbb{C})$.

4.- **Problema 4:** Sea G grupo y sea F un cuerpo. Se define el F-álgebra de grupo $F[G]$ por:

$$F[G] = \left\{ \sum a_g g : g \in G, a_g \in F \right\}.$$

Donde la suma y el producto por escalar se define puntualmente y la multiplicación como la extensión lineal del producto $g.h = gh$, $\forall g, h \in G$. Sea $g \in G$ un elemento cualquiera.

i.- Demuestre que el ideal izquierdo (g) generado por g es $F[G]$.

ii.- Para $G = C_2$, demustre que existen ideales de $F[g]$ no triviales.

4.- **Desarrollo:**

i.- Sea $g \in G$ un elemento arbitrario. Note que el producto por izquierda de g con hg^{-1} es h. Por lo tanto $h \in (g)$, para todo $h \in H$. Esto implica que todas las sumas finitas $\sum_{h \in G} a_h h \in (g)$. Concluimos que $(g) = F[G]$.

ii.- Considere un elemento generador $g \in C_2$. Note que $(1-g)^2 = 0$ y que $x = 1 - g$ es un elemento no trivial. En particular dicho elemento es no invertible. Por lo tanto $(x) \neq F[G]$ y $(x) \neq \{0\}$. Esto concluye lo pedido.

Ayudantía 12: En esta ayudantía comenzaremos a estudiar la estructura del producto tensorial de módulos y álgebras.

1.- **Problema 1:** Sea M un R-módulo y $S \subset R$ un conjunto multiplicativo con uno. Se define el módulo localizado $S^{-1}M$ por:

$$S^{-1}M = \left\{ \frac{m}{s} : m \in M,\ s \in S \right\},$$

con la identificación $\frac{m}{s} = \frac{m'}{s'} \Leftrightarrow \exists t \in S : t(s'm - sm') = 0$.

i.- Pruebe que $S^{-1}M$ es un $S^{-1}R$-módulo.

ii.- Muestre que $M \otimes_R S^{-1}R \cong S^{-1}M$.

iii.- Concluya que si R es un DI y $K = \text{Quot}(R)$ entonces $M \otimes_R K$ es un K-módulo libre.

1.- **Desarrollo:**

i.- Definimos la acción de $S^{-1}R$ sobre $S^{-1}M$ por $\frac{a}{s}.\frac{m}{t} = \frac{am}{st}$, donde $a \in R$, $s, t \in S$ y $m \in M$. Observe que si $\frac{a}{s} = \frac{a'}{s'}$ y $\frac{m}{t} = \frac{m'}{t'}$ entonces existen $s'', t'' \in S$ tales que $s''(as' - a's) = 0$ y $t''(t'm - tm') = 0$. Luego tenemos que $s''t''(s't'am - sta'm') = 0$. Por lo tanto la acción está bien definida. Es relativamente sencillo demostrar que se cumplen los axiomas de módulo en este caso (Ejercicio).

ii.- Considere el R-morfismo bilineal $\phi : M \times S^{-1}R \to S^{-1}M$ definido por $\phi\left(m, \frac{a}{s}\right) = \frac{am}{s}$. Se sigue, de un argumento análogo al dado en [i], que ϕ está bien definido. Por la propiedad universal del producto tensorial tenemos que existe un único homomorfismo de R-módulos $\psi : M \otimes_R S^{-1}R \to S^{-1}M$ tal que $\psi\left(m \otimes \frac{a}{s}\right) = \phi\left(m, \frac{a}{s}\right) = \frac{am}{s}$. Por otro lado, considere la función $\varphi : S^{-1}M \to M \otimes_R S^{-1}R$ definida por $\varphi\left(\frac{m}{s}\right) = m \otimes \frac{1}{s}$. Observe que φ está bien definida, pues si $\frac{m'}{s'} = \frac{m}{s}$ entonces existe $t \in S$ tal que $ts'm = tsm'$, luego tenemos que $m \otimes \frac{1}{s} = ts'm \otimes \frac{1}{ts's} = tsm' \otimes \frac{1}{ts's} = m' \otimes \frac{1}{s'}$. Observe que $\varphi \circ \psi = id_{M \otimes S^{-1}R}$ y $\psi \circ \varphi = id_{S^{-1}M}$. Luego tenemos que ψ es un homomorfismo biyectivo. Concluimos que ψ es un isomorfismo.

iii.- Se deduce de lo mostrado en [i] e [ii] que $M \otimes_R K$ es un K-módulo. Luego tenemos que $M \otimes_R K$ es un K-espacio vectorial. Por lo tanto $M \otimes_R K$ es libre sobre K.

2.- **Problema 2:** Sean A, B, C, D cuatro R-módulos y $f : A \to B$, $g : C \to D$ dos R-homomorfismos cualquiera.

i.- Pruebe que existe un homomorfismo de $R-$módulos $t : A \otimes_R C \to B \otimes_R D$ tal que $t(a \otimes c) = f(a) \otimes g(c)$, para todo $a \in A, c \in C$.

ii.- Muestre que si f y g son invertible entonces t también lo es.

2.- **Desarrollo:**

i.- Considere la aplicación $h : A \times C \to D \otimes_R B$ definida por $h(a, c) = f(a) \otimes g(c)$. Dicha función es R-bilineal pues f y g son lineales y el tensor es bilineal. Por la propiedad universal del producto tensorial tenemos que existe una único R-homomorfismo $t : A \otimes_R C \to B \otimes_R D$ tal que $t(a \otimes c) = f(a) \otimes g(c)$, para todo $a \in A, c \in D$.

ii.- Considere $\tau : B \otimes_R D \to A \otimes_R C$ definida por $\tau(b,d) = f^{-1}(b) \otimes g^{-1}(d)$. Note que $\tau \circ t = \mathrm{id}_{A\otimes_R C}$ y que $t \circ \tau = \mathrm{id}_{B\otimes_R D}$. Esto nos permite concluir que t es invertible.

3.- **Problema 3:** Sea R un anillo conmutativo con uno y M un R-ḿodulo cualquiera.

i.- Muestre que $M \otimes_R R^n \cong M^n$.

ii.- Sean M, N dos K-espacios vectoriales de dimensión m y n respetivamente. Pruebe que $M \otimes_K N \cong K^{nm}$.

iii.- Suponga que $\{v_i\}_{i=1}^m$ y $\{w_j\}_{j=1}^n$ son K-bases de M y N respectivamente. Pruebe que $\beta = \{v_i \otimes w_j\}_{i,j=1}^{n,m}$ es una K-base de $M \otimes_K N$.

3.- **Desarrollo:**

i.- Sabemos que $M \otimes_R \bigoplus_{i=1}^n N_i \cong \bigoplus_{i=1}^n M \otimes_R N_i$. Además, como se vió en clase, tenemos que $M \otimes_R R \cong M$. De esto se sigue lo pedido.

ii.- Note que si M, N son dos K-espacios vectoriales de dimensión m y n respetivamente, entonces $M \cong K^m, N \cong K^n$ y en particular por el problema [2ii] tenemos que $M \otimes_K N \cong K^m \otimes_K K^n$. Del item [i] se sigue que $M \otimes_K N \cong (K^m)^n$. Concluimos que $M \otimes_K N \cong K^{nm}$.

iii.- De la construcción de $M \otimes_K N$ se desprende que β es un conjunto generador. Ahora bien, como $\dim_K(M \otimes_K N) = mn$, se concluye que β es una K-base de $M \otimes_K N$.

4.- **Problema 4:** Sea A una K-álgebra y L/K una extensión de cuerpos.

i.- Pruebe que $A_L = L \otimes_K A$ es una L-álgebra. A_L se denomina extensión escalar de A.

ii.- Pruebe que si $\{a_1, a_2, \cdots, a_n\}$ es una base de A entonces $\beta = \{1 \otimes a_1, 1 \otimes a_2, \cdots, 1 \otimes a_n\}$ es una base de A_L, vista como L-álgebra.

4.- **Desarrollo:**

i.- Sea $\lambda \in L$ fijo. Definimos la aplicación K-bilineal $h_\lambda : L \times A \to A_L$ por $h_\lambda(r,a) = \lambda r \otimes a$. El hecho de que h sea K-bilineal queda como ejercicio. Por la propiedad universal del producto tensorial tenemos que existe una única función K-lineal $f_\lambda : A_L \to A_L$ tal que $f_\lambda(r \otimes a) = (\lambda r, a)$. De esto se sigue que el producto escalar $\lambda(r \otimes a) = (\lambda r) \otimes a$ dota a A_L de estructura de L-álgebra, pues es relativamente sencillo demostrar que se cumplen los axiomas de requeridos (Ejercicio).

ii.- Por un lado sabemos que existe un isomorfismo K-lineal tal que $A \cong K^n$. Por lo tanto $A_L \cong L \otimes_K K^n \cong K^n \otimes_K L \cong L^n$, por lo mostrado en el problema 3. Luego, para probar lo pedido, basta probar que el conjunto β genera A_L. En efecto sabemos que $\{r \otimes a_n : r \in L, i = 1, \cdots, n\}$ genera A_L como K-espacio vectorial. De la definción del producto escalar en A_L dada en [i] tenemos que $\{1 \otimes a_n : i = 1, \cdots, n\}$ genera A_L como L-espacio vectorial.

Ayudantía 13: En esta ayudantía estudiaremos el álgebra $T(M)$. En particular, estudiaremos productos tensoriales iterados de módulos.

1.- **Problema 1:** Sea M un R-módulo. Pruebe que $T(M)$ está generada como R-álgebra por $T^1(M)$.

1.- **Demostración:** Sabemos que $\beta = \{m_1 \otimes \cdots \otimes m_k : k \in \mathbb{Z}_{>0}\} \cup \{1\}$ genera $T(M)$ como R-módulo, en particular como R-álgebra. Además el producto en $T(M)$ está definido por:

$$(m_1 \otimes \cdots \otimes m_k) \otimes (n_1 \otimes \cdots \otimes n_l) = m_1 \otimes \cdots \otimes m_k \otimes n_1 \otimes \cdots \otimes n_l \in T^{k+l}(M).$$

Por lo tanto, tomando productos de elementos $m \in M$ podemos generar $\beta - \{1\}$. Luego $\gamma = \{m \in M\} \cup \{1\}$ genera $T(M)$ como R-álgebra. Como $\gamma \subset T^1(M)$ concluimos que $T(M)$ está generada como R-álgebra por $T^1(M)$.

2.- **Problema 2:** Sabemos que el producto tensorial $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ es libre de rango 4 como módulo sobre $\mathbb{R}$, con base:

$$\beta = \{e_1 = 1 \otimes 1,\ \ e_2 = 1 \otimes i,\ \ e_3 = i \otimes 1,\ \ e_4 = i \otimes i\}.$$

i.- Sea $\varepsilon_1 = \frac{1}{2}(e_1 + e_4)$ y $\varepsilon_2 = \frac{1}{2}(e_1 - e_4)$. Pruebe que $\varepsilon_1\varepsilon_2 = 0$, $\varepsilon_1 + \varepsilon_2 = 1$, $\varepsilon_j^2 = \varepsilon_j$, para $j = 1, 2$. Deduzca que A es isomorfa como anillo al producto directo de dos ideales principales, a saber, $A \simeq \varepsilon_1 A \times \varepsilon_2 A$.

ii.- Demuestre que $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$.

iii.- Concluya que el $\mathbb{R}$-álgebra $T(\mathbb{C})$ es un $\mathbb{C}$-espacio vectorial de dimensión infinita.

2.- **Desarrollo:**

i.- Note que $\varepsilon_1^2 = \frac{1}{4}(e_1^2 + e_1e_4 + e_4e_1 + e_4^2) = \frac{1}{4}(1 \otimes 1 + 2i \otimes i + (-1) \otimes (-1)) = \varepsilon_1$. Análogamente se prueba que $\varepsilon_2^2 = \varepsilon_2$. Por otro lado $\varepsilon_1 + \varepsilon_2 = 1 \otimes 1$ y $\varepsilon_2\varepsilon_2 = \varepsilon_1\varepsilon_2 = \frac{1}{4}(e_1^2 - e_4^2) = 0$. Ahora bien, como $A = (1 \otimes 1)A = \varepsilon_1 A + \varepsilon_2 A$, se tiene que el anillo A es suma de los subanillos $\varepsilon_1 A$ y $\varepsilon_2 A$. Por otro lado, si $z \in \varepsilon_1 A \cap \varepsilon_2 A$, se tiene que $z = \varepsilon_1 t_1 = \varepsilon_2 t_2$ donde $t_1, t_2 \in A$. Luego $\varepsilon_1 z = \varepsilon_1^2 t_1 = z$ y $\varepsilon_1 z = \varepsilon_1\varepsilon_2 z = 0$. Concluimos que $z = 0$ y por ende $A = \varepsilon_1 A \oplus \varepsilon_2 A \cong \varepsilon_1 A \times \varepsilon_2 A$.

ii.- Basta probar que $\varepsilon_1 A, \varepsilon_2 A \cong \mathbb{C}$. En efecto note que $\varepsilon_1 e_1 = \varepsilon_1$, $\varepsilon_1 e_2 = -\varepsilon_1 e_3$ y $\varepsilon_1 e_4 = \varepsilon_1$. Como β es una $\mathbb{R}$-base de A se tiene que $\varepsilon_1 A = \varepsilon_1\mathbb{R} \oplus \varepsilon_1 e_2\mathbb{R} = \varepsilon_1(e_1\mathbb{R} \oplus e_2\mathbb{R})$, donde $e_1 = 1_A$ y $e_2^2 = -e_1 = -1_A$. Considere la función $\phi : \varepsilon_1 A \to \mathbb{C}$ definida por $\phi(\varepsilon_1(ae_1 + be_2)) = a + ib$. Dicha función es un homomorfismo de anillos pues $\varepsilon_1^2 = \varepsilon_1$ (Ejercicio). Además tiene por inversa a la función $\psi : \mathbb{C} \to \varepsilon_1 A$ definida por $\psi(a + ib) = \varepsilon_1(ae_1 + be_2)$. Esto nos permite concluir que $\varepsilon_1 A \cong \mathbb{C}$. Análogamente podemos deducir que $\varepsilon_2 A \cong \mathbb{C}$. Esto demuestra lo pedido.

iii.- Observe que $T^3(\mathbb{C}) \cong \mathbb{C} \otimes_{\mathbb{R}} (\mathbb{C} \times \mathbb{C}) \cong (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}) \times (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}) \cong \mathbb{C}^4$. Por indución se prueba que $T^k(\mathbb{C}) \cong \mathbb{C}^{2^{k-1}}$. Esto implica que $T(M) \cong \bigoplus_{k=0}^{\infty} \mathbb{C}^{2^{k-1}}$, donde $T(M)$ es un $\mathbb{C}$-espacio vectorial de dimensión infinita.

3.- **Problema 3:** Pruebe que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = \{0\}$. Concluya que $T(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

3.- **Demostración:** Primero demostremos que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ es trivial. En efecto sabemos que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ está generado por $\overline{\frac{p}{q}} \otimes \overline{\frac{r}{s}}$, donde $\overline{\frac{p}{q}}, \overline{\frac{r}{s}} \in \mathbb{Q}/\mathbb{Z}$. Luego si demostramos que estos elementos son triviales tenedremos que el módulo en cuestión lo es. En efecto:

$$\overline{\frac{p}{q}} \otimes \overline{\frac{r}{s}} = \overline{\frac{p}{q}} \otimes \overline{\frac{qr}{qs}} = \overline{\frac{qp}{q}} \otimes \overline{\frac{r}{qs}} = \overline{p} \otimes \overline{\frac{r}{qs}} = 0$$

Concluimos que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = \{0\}$. Ahora bien, como $T^k(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$, tenemos que $T^k(M) = \{0\}$ para todo $k \geq 2$. Esto implica que $T(\mathbb{Q}/\mathbb{Z}) = T^0(M) \oplus T^1(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

4.- **Problema 4:** Sea R un anillo conmutativo y unitario, I un ideal de R y $M = R/I$ un R-módulo. Pruebe que $T(M)/I \cong R/I[x]$.

4.- **Demostración:** Por el ejercicio 14 del control 5 tenemos que $M \otimes M \cong R/I$. Esto prueba por inducción que $T^k(M) \cong R/I$, para todo $k > 0$. Por lo tanto tenemos que:

$$T(M)/I \cong R/I \oplus R/I \oplus R/I \cdots$$

En lo que sigue denotamos a la suma directa de la derecha como un conjunto de tuplas cuyo soporte es finito. Considere el homomorfismo $\phi : T(M)/I \to R/I[x]$ definido por $\phi((r_i)_{i=1}^{\infty}) = \sum_{i=1}^{\infty} r_i x^i$, donde $r_i \in R/I$. Dicha función esta bien definida pues $r_i = 0$ para casi todo $i \in \mathbb{N}$. Es sencillo demostrar que ϕ es un isomorfismo R-lineal. Por otro lado tenemos que:

$$(\cdots, 0, r_i, 0, \cdots)(\cdots, 0, r_j, 0, \cdots) = (\cdots, 0, r_i r_j, 0, \cdots),$$

donde $r_i r_j$ está en la posición $i + j$-ésima. Utilizando esta identidad y escribiendo cada elemento $(r_i)_{i=1}^{\infty}$ como:

$$(r_i)_{i=1}^{\infty} = \sum_{i=0}^{\infty} (\cdots, r_i, 0 \cdots),$$

se prueba que ϕ es un homomorfismo de anillos. Concluimos que ϕ es un isomorfismo de R-álgebras. Esto prueba lo pedido.

Ayudantía 14: En esta ayudantía estudiaremos el álgebra simética y exterior. Además incluiremos un pequeño análisis de álgebras centrales simples.

1.- **Problema 1:** En el anillo $R = \mathbb{Z}[x]$, sea $I = (2, x)$ el ideal generado por 2 y por x. Entonces el anillo $\mathbb{Z}/2\mathbb{Z} \cong R/I$ es un $R-$ módulo aniquilado por x y por 2.

i.- Pruebe que $\varphi : I \times I \to \mathbb{Z}/2\mathbb{Z}$, definida por:

$$\varphi(a_0 + \cdots + a_n x^n, b_0 + \cdots + b_m x^m) = \frac{a_0}{2} b_1 \pmod 2,$$

es R-bilineal.

ii.- Pruebe que hay un homomorfismo de $R-$ módulos de $I \otimes_R I \to \mathbb{Z}/2\mathbb{Z}$, que lleva $p(x) \otimes q(x)$ en $\frac{p(0)}{2} q'(0)$, donde $q'(x)$ es el polinomio derivado de $q(x)$.

iii.- Pruebe que $2 \otimes x \neq x \otimes 2$.

1.- **Desarrollo:**

i.- Observe que φ está bien definido pues $a_0 \in 2\mathbb{Z}$. Ahora bien, tenemos que:

$$\varphi(r(x)(a_0 + \cdots + a_n x^n), q(x)) = r_0 \frac{a_0}{2} b_1 = r(x)\varphi(a_0 + \cdots + a_n x^n, q(x)) \pmod 2,$$

donde $q(x) = b_0 + \cdots + b_m x^m$, $r(x) = r_0 + \cdots + r_k x^k$ y donde identificamos $\mathbb{Z}/2\mathbb{Z}$ con R/I. Análogamente tenemos que:

$$\varphi(p(x), r(x)(b_0 + \cdots + b_m x^m)) = r_0 \frac{a_0}{2} b_1 = r(x)\varphi(p(x), b_0 + \cdots + b_m x^m),$$

donde $p(x) = a_0 + \cdots + a_n x^n$. Esto demuestra que φ es R-bilineal.

ii.- Con las notaciones de la parte [i] tenemos que $a_0 = p(0)$ y que $b_1 = q'(0)$. Luego, de la propiedad universal del producto tensorial, deducimos que existe un homomorfismo de $R-$ módulos de $\psi : I \otimes_R I \to \mathbb{Z}/2\mathbb{Z}$, definido por $\psi(p(x) \otimes q(x)) = \frac{p(0)}{2} q'(0)$.

iii.- Si $2 \otimes x = x \otimes 2$ entonces su imagenes bajo ψ son iguales. Pero $\psi(2 \otimes x) = 1$, mientras que $\psi(x \otimes 2) = 0$ en $\mathbb{Z}/2\mathbb{Z}$. Concluimos que $2 \otimes x \neq x \otimes 2$.

2.- **Problema 2:** Sea V un K-espacio vectorial y $\{v_1, \cdots, v_n\} \subset V$. Considere $\sigma \in S_n$ una permutación cualquiera. Pruebe que $v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(n)} = \operatorname{sgn}(\sigma)(v_1 \wedge \cdots \wedge v_n)$, donde sgn es la función signo de permutaciones.

Demostración: Primero demostramos este hecho para una trasposición $\tau = (ij)$, donde $i < j$. En efecto, el elemento:

$$z = v_1 \wedge \cdots \wedge (v_i + v_j) \wedge \cdots \wedge (v_i + v_j) \wedge \cdots \wedge v_n,$$

donde los factores $v_i + v_j$ van en las posiciones i y j, cumple con:

$$z = v_1 \wedge \cdots \wedge v_i \wedge \cdots \wedge v_j \wedge \cdots \wedge v_n + v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_i \wedge \cdots \wedge v_n,$$

pues cada vez que se repite un factor en la cuna, esta es nula. Por el mismo argumento $z = 0$. De esto se sigue que:

$$v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_i \wedge \cdots \wedge v_n = -v_1 \wedge \cdots \wedge v_n.$$

Por lo tanto:

$$v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_i \wedge \cdots \wedge v_n = \operatorname{sgn}(\tau)(v_1 \wedge \cdots \wedge v_n).$$

Ahora bien, como toda permutación es un producto de trasposiciones, tenemos que $\sigma = \tau_1 \circ \cdots \circ \tau_r$, donde $\text{sgn}(\sigma) = (-1)^r$. Aplicando inductivamente el resultado anterior obtenido sobre las trasposiciones se sigue que:

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(n)} = (-1)^r (v_1 \wedge \cdots \wedge v_n),$$

es decir:

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(n)} = \text{sgn}(\sigma)(v_1 \wedge \cdots \wedge v_n).$$

3.- **Problema 3:** Sea V espacio vectorial de dimensión finita sobre un cuerpo F con base $B = \{v_1, \cdots, v_n\}$. Pruebe que los vectores:

$$v_{i1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_k}, \quad \text{para } 1 \leq i_1 < i_2 \cdots < i_k \leq n,$$

son una base de $\Lambda^k(V)$, y que $\Lambda^k(V) = \{0\}$ si $k > n$.

Demostración: En clases de probó que los tensores $v_{i_1} \otimes \cdots \otimes v_{i_n}$, donde $i_j \in \{0, \cdots, n\}$ forman una base de $T^k(V)$. Ahora bien, como cualquier permutación en los subindices de dichos vectores cambia a lo más en un signo al tensor alternante, se tiene que

$$\beta = \{v_{i_1} \wedge v_{i2} \wedge \cdots \wedge v_{i_k} : 1 \leq i_1 < i_2 \cdots < i_k \leq n\},$$

genera $\Lambda^k(V)$. Para demostrar que son linealmente independientes basta encontrar una función k-lineal alternante de V^k a F la cual es 1 en un elemento dado:

$$(v_{i_1}, v_{i_2}, \cdots, v_{i_k}), \quad \text{para } 1 \leq i_1 < i_2 \cdots < i_k \leq n,$$

y es nulo en los vectores $(v_{j_1}, v_{j_2}, \cdots, v_{j_k})$ con la misma propiedad de orden en los subíndices. Esto último pues, por la propiedad universal del producto exterior, si lo anterior se cumple, se tiene una función F-lineal que vale 1 en $v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_k} \in \beta$ y cero en los demás elementos de β. Considere la base $\gamma = \{(v_{j_1}, v_{j_2}, \cdots, v_{j_k}) : j_l \in \{1, \cdots, n\}\}$ de $V^k(V)$ y la función k-lineal $f : V^k \to F$ definida en γ por $f((v_{j_1}, v_{j_2}, \cdots, v_{j_k})) = \text{sgn}(\sigma)$ para $(j_1, \cdots, j_k)$ la permutación por σ de $(i_1, \cdots, i_k)$, es decir si $\sigma(i_l) = j_l$ para todo $l \in \{0, \cdots, k\}$. Definimos $f((v_{j_1}, v_{j_2}, \cdots, v_{j_k})) = 0$ si es que $(j_1, \cdots, j_k)$ no es una permutación de $(i_1, \cdots, i_k)$. Note que f es cero en todo vector con las entradas repetidas, pues sus tuplas de subíndices no pueden ser una permutación de $(i_1, \cdots, i_k)$. Esto implica que f es una función alternante. Además esta función es 1 en $(v_{i_1}, v_{i_2}, \cdots, v_{i_k})$ y cero en de demás vectores con la misma propiedad de orden en los subíndices, pues dichos subíncices nos son permutaciones de $(i_1, \cdots, i_k)$ (para mayor detalle ver un libro de teoría de grupos y permutaciones). Esto concluye que β es base de $\Lambda^k(V)$. Observe que si $k > n$ entonces todo elemento de la base $v_{i1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_k}$ cumple con $v_{i_j} = v_{i_l}$ para $j \neq l$. Por lo tanto $\beta = \{0\}$. Esto implica que $\Lambda^k(V) = \{0\}$ si $k > n$.

4.- **Problema 4:** Sea K un cuerpo y A una K-álgebra simple de dimensión finita.

i.- Pruebe que $\text{End}_K(A)$ es una K-álgebra de división.

ii.- Muestre que si $K = \mathbb{C}$ entonces $\text{End}_K(A) \cong \mathbb{C}$.

Desarrollo:

i.- Considere $T \in \mathrm{End}_K(A)$ un endomorfismo cualquiera no nulo. Para demostrar lo requerido debemos probar que T es invertible. En efecto, como $\ker(T)$ es un ideal de A y A es un álgebra simple, tenemos que $\ker(T) = \{0\}$. Esto implica que T es una aplicación K-lineal e inyectiva. Como T es una función entre espacios de igual dimensión, concluimos que T es invertible. Esto prueba lo pedido.

ii.- Basta probar que para todo $T \in \mathrm{End}_K(A)$ existe $\lambda \in \mathbb{C}$ tal que $T = \lambda\mathrm{id}$. Esto ya que en dicho caso $\mathrm{End}_K(A) = \{\lambda\mathrm{id} : \lambda \in \mathbb{C}\} \cong \mathbb{C}$ como $\mathbb{C}$-álgebras. En efecto, sea $\lambda \in \mathbb{C}$ un autovalor de T, el cual existe pues $\mathbb{C}$ es algebraicamente cerrado. Por defínción $T - \lambda I$ no es invertible. Por otro lado $T - \lambda I \in \mathrm{End}_K(A)$. De [i] concluimos que $T - \lambda I = 0$. Esto prueba lo pedido.