

ALGEBRA II - MPG3201  
LISTA DE EJERCICIOS X

OCTUBRE, 2014

EJERCICIO 1. Sea  $K/F$  una extensión galoisiana de grupo  $G$  y sea  $\alpha \in K$ . Demuestre que  $K = F(\alpha)$  ssi para todo  $\sigma, \tau \in G$ , la ecuación  $\sigma(\alpha) = \tau(\alpha)$  implica  $\tau = \sigma$ .

EJERCICIO 2. Demuestre que para cualquier grupo abeliano  $G$  existe una extensión galoisiana con grupo isomorfo a  $G$ .

EJERCICIO 3. Determine el grupo de Galois de los siguientes polinomios:

1.  $x^3 - x^2 - 4$ .
2.  $x^3 - 2x + 4$ .
3.  $x^3 - x + 1$ .
4.  $x^3 + x^2 - 2x - 1$ .
5.  $x^4 - 25$ .
6.  $x^4 + 3x^3 - 3x - 2$ .
7.  $x^4 + 2x^2 + x + 3$ .

EJERCICIO 4. (Fórmulas de Newton) Sea  $f(x)$  polinomio mónico de grado  $n$  con raíces  $\alpha_1, \dots, \alpha_n$ . Sean  $s_i$  las funciones simétricas elementales de grado  $i$  en las raíces y defina  $s_i = 0$  para  $i > n$ . Sea  $p_i = \alpha_1^i + \dots + \alpha_n^i$ ,  $i \geq 0$ . Pruebe las fórmulas:

$$\begin{aligned} p_1 - s_1 &= 0 \\ p_2 - s_1 p_1 + 2s_2 &= 0 \\ p_3 - s_1 p_2 + s_2 p_1 - 3s_3 &= 0 \\ &\vdots = \vdots \\ p_i - s_1 p_{i-1} + s_2 p_{i-2} - \dots + (-1)^{i-1} s_{i-1} p_1 + (-1)^i i s_i &= 0. \end{aligned}$$

EJERCICIO 5. Sea  $f(x)$  un polinomio mónico de grado  $n$  con raíces  $\alpha_1, \dots, \alpha_n$ .

1. Muestre que el discriminante  $D$  de  $f(x)$  es el cuadrado del determinante de Vandermonde

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix} = \prod_{i>j} (\alpha_i - \alpha_j)$$

2. Tomando la matriz de Vandermonde, multiplicando a la izquierda por su traspuesta y tomando el determinante muestre que

$$D = \begin{pmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{pmatrix}$$

donde  $p_i = \alpha_1^i + \dots + \alpha_n^i$ .

EJERCICIO 6. Suponga que los números complejos  $\alpha, \beta, \gamma$  satisfacen las ecuaciones

$$\begin{aligned} \alpha + \beta + \gamma &= 3 \\ \alpha^2 + \beta^2 + \gamma^2 &= 5 \\ \alpha^3 + \beta^3 + \gamma^3 &= 12. \end{aligned}$$

Calcule  $\alpha^4 + \beta^4 + \gamma^4$  (Hint: Utilize los polinomios simétricos  $p_i = \alpha^i + \beta^i + \gamma^i$ ).

EJERCICIO 7. Sea  $\mathbb{F}_2$  el cuerpo con 2 elementos. Muestre que en  $\mathbb{F}_2[x_1, \dots, x_n]$  es imposible expresar  $\sigma_2 = x_1x_2 + x_1x_3 + \dots + x_2x_3 + \dots + x_{n-1}x_n$  como polinomio en  $s_1, \dots, s_n$  para  $n \geq 2$ .

EJERCICIO 1. Probar que para todo  $n$ , el grupo dihedral  $D_n$  es soluble, es decir, encuentre una cadena finita de subgrupos normales  $G_0 = \{1\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$  tales que  $G_i/G_{i-1}$  es abeliano para todo  $i = 1, \dots, n$ .

EJERCICIO 2. Sea  $K_0 = \mathbb{Q}$  y para todo  $n \geq 0$  definir el cuerpo  $K_{n+1}$  como la extensión de  $K_n$  obtenida adjuntando a  $K_n$  todos los elementos radicales en  $K_n$ . Sea  $K$  la unión de los subcuerpos  $K_n$ ,  $n \geq 0$ . Pruebe que  $K/\mathbb{Q}$  es Galois y que no existen extensiones de Galois solubles no triviales de  $K$ .

EJERCICIO 3. **Extensiones Radicales:** Sea  $L$  un cuerpo. Una extensión  $K/L$  se dice *Radical Simple* si  $K = L(\alpha)$  con  $\alpha^n \in L$ . Si el polinomio  $x^n - \alpha^n$  es irreducible en  $L[x]$ , se dice que la extensión  $K/L$  es extensión *Radical Simple e Irreducible*. Una extensión  $L/K$  se llama *Radical* si existe una cadena  $L = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K$  tal que  $K_i/K_{i-1}$  es extensión radical simple.

Mostrar una cadena de extensiones radicales simples e irreducibles desde  $\mathbb{Q}$  a  $\mathbb{Q}(\zeta_{47})$ .

EJERCICIO 4. Sea  $N$  un natural y  $p$  un primo. Mostrar que para  $N$  suficientemente grande el polinomio

$$x(x - Np^2)(x + Np^2)(x^2 + N^2p^4) + p$$

no es soluble por radicales.

EJERCICIO 5. Analizar la solubilidad por radicales sobre  $\mathbb{Q}$  de los polinomios

1.  $x^5 - 6x^2 + 2$
2.  $x^7 - 10x^5 + 15x + 5$
3.  $x^6 + 2x^5 - 5x^4 + 9x^3 - 5x^2 + 2x + 1$ . (*Hint:* Tomar  $u(x) = x + x^{-1}$ ).

EJERCICIO 6. Muestre que el polinomio  $x^3 + x^2 - 2x - 1$  es soluble por radicales sobre  $\mathbb{Q}$  probando que sus raíces son  $2 \cos(2\pi j/7) = \zeta_7^j + \zeta_7^{-j}$ ,  $j = 1, 2, 3$  y que  $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_7)$  es extensión radical.

EJERCICIO 7. Probar que todo grupo  $G$  de orden  $2010 = 2 \cdot 3 \cdot 5 \cdot 67$  es soluble.

EJERCICIO 8. Sea  $F$  cuerpo finito de característica  $p$ . Muestre que todo polinomio  $f(x) \in F[x]$  irreducible de grado menor que  $p$  es soluble por radicales.

EJERCICIO 9. Considere el polinomio  $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ . Sea  $E$  el cuerpo de descomposición de  $f(x)$  sobre  $\mathbb{Q}$ . Pruebe que  $E$  no es una extensión radical de  $\mathbb{Q}$ .

EJERCICIO 10. Sea  $G$  un grupo finito con  $A, B$  subgrupos normales tales que  $G/A$  y  $G/B$  son solubles. Pruebe que  $G/(A \cap B)$  es soluble.

EJERCICIO 1. Encontrar las clausuras normales de las extensiones siguientes:

1.  $\mathbb{Q}(\sqrt[5]{3})/\mathbb{Q}$
2.  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$
3.  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$
4.  $\mathbb{Q}(\gamma)/\mathbb{Q}$  donde  $\gamma$  es una raíz de  $t^3 - 3t^2 + 3$ .
5.  $\mathbb{Q}(\sqrt{3 + \sqrt{5}})/\mathbb{Q}$  y determine el grupo de Galois de la clausura normal sobre  $\mathbb{Q}$ .

EJERCICIO 2. Si  $f(x) \in \mathbb{Q}[x]$  es un polinomio irreducible que posee raíces reales y raíces complejas (no reales), pruebe que el grupo de Galois de  $f$  sobre  $\mathbb{Q}$  no es abeliano.

EJERCICIO 3. Sea  $K = \mathbb{Q}(e^{\frac{2\pi i}{n}})$  y sea  $\alpha \in \mathbb{C}$  tal que  $\alpha^n \in K$ . Demostrar que  $K(\alpha)/K$  es Galois con grupo de Galois cíclico.

EJERCICIO 4. Sea  $\zeta = e^{\frac{2\pi i}{37}}$ . Demuestre que  $\mathbb{Q}(\zeta + \zeta^{10} + \zeta^{26})/\mathbb{Q}$  es Galois y calcule su grupo de Galois.

EJERCICIO 5. Sea  $K/F$  extensión de Galois finita tal que  $\text{Gal}(K/F) \cong S_4$ . Calcule la cardinalidad del conjunto

$$\mathfrak{L} = \{L \mid L \text{ cuerpo intermedio } F \subseteq L \subseteq K, \text{ tal que } [L : F] = 12\}.$$

¿Cuáles  $L \in \mathfrak{L}$  verifican  $L/F$  es Galois?

EJERCICIO 6. Analizar la separabilidad de los siguientes polinomios en los cuerpos  $\mathbb{Q}, \mathbb{C}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{19}$ :

1.  $t^3 + 1$
2.  $t^2 - 2t + 1$
3.  $t^2 + t + 1$
4.  $t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$

EJERCICIO 7. Determinar si las siguientes afirmaciones son verdaderas o falsas:

1. El polígono regular de 771 lados es constructible.
2. El polígono regular de 768 lados es constructible.
3. El polígono regular de 25 lados es constructible.
4. Si  $p$  es un primo impar, el polígono regular de  $p^2$  lados nunca es constructible.

EJERCICIO 8. Demostrar que la clausura algebraica de  $\mathbb{F}_p$  es  $\bigcup_{n \geq 1} \mathbb{F}_{p^n}$ .

EJERCICIO 9. Obtener la correspondencia de Galois para el polinomio  $x^4 - 5x^2 - 5 \in \mathbb{Q}[x]$ .

EJERCICIO 10. Calcular el grupo de Galois de las extensiones  $\mathbb{Q}(\zeta_{22})/\mathbb{Q}$  y  $\mathbb{Q}(\zeta_{60})/\mathbb{Q}$ .

EJERCICIO 11. Utilizar las fórmulas de Cardano para resolver la ecuación  $x^3 + x^2 - 2 = 0$ . En particular, muestre que esta ecuación tiene la raíz real:

$$\frac{1}{3} \left( \sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} - 1 \right).$$

Mostrar directamente que las raíces de esta cúbica son  $\pm 1, \pm i$  probando que

$$\sqrt[3]{26 + 15\sqrt{3}} = 2 + \sqrt{3}, \sqrt[3]{26 - 15\sqrt{3}} = 2 - \sqrt{3},$$

de manera que

$$\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} = 4.$$

EJERCICIO 12. Utilizar las fórmulas de Cardano para resolver la ecuación  $x^3 + x - 2 = 0$ . Note que  $x = 1$  es una raíz. Muestre la fórmula:

$$1 = \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}.$$

EJERCICIO 13. Sea  $\zeta_7$  una raíz primitiva séptima de la unidad y sea  $\alpha = \zeta_7 + \zeta_7^{-1}$ .

1. Mostrar que  $\zeta_7$  es una raíz de  $z^2 - \alpha z + 1$  sobre  $\mathbb{Q}(\alpha)$ .
2. Usando el polinomio minimal para  $\zeta_7$ , muestre que  $\alpha$  es una raíz de la cúbica  $x^3 + x^2 - 2x - 1$ . Encuentre la solución explícita de esta cúbica en términos de radicales.

EJERCICIO 14. Sea  $a$  un número racional no cero.

1. Determine cuándo la extensión  $\mathbb{Q}(\sqrt{a\sqrt{-1}})$  es de grado 4 sobre  $\mathbb{Q}$ .
2. Si  $K = \mathbb{Q}(\sqrt{a\sqrt{-1}})$  es de grado 4 sobre  $\mathbb{Q}$ , mostrar que  $K/\mathbb{Q}$  es Galois con grupo de Galois el grupo 4 de Klein. Determine las extensiones cuadráticas de  $\mathbb{Q}$  contenidas en  $K$ .

EJERCICIO 15. 1. Sea  $D \in \mathbb{Z}$  entero libre de cuadrados y sea  $a \in \mathbb{Q}$  un número racional no cero. Muestre que  $\mathbb{Q}(\sqrt{a\sqrt{D}})$  no puede ser una extensión cíclica de grado 4 sobre  $\mathbb{Q}$ .

2. Sea  $D \in \mathbb{Z}$  entero libre de cuadrados y sea  $a \in \mathbb{Q}$  un número racional no cero. Si  $\mathbb{Q}(\sqrt{a\sqrt{D}})/\mathbb{Q}$  es Galois, entonces  $D = -1$ .

EJERCICIO 16. Analizar la solubilidad por radicales sobre  $\mathbb{Q}$  de los siguientes polinomios:

1.  $x^5 - 4x + 2$
2.  $x^5 - 4x^2 + 2$
3.  $x^5 - 6x^2 + 2$
4.  $x^7 - 10x^5 + 15x + 5$
5.  $x^6 + 2x^5 - 5x^4 + 9x^3 - 5x^2 + 2x + 1$  (tomar  $u = x + x^{-1}$ ).

EJERCICIO 17. Mostrar una cadena de extensiones radicales simples e irreducibles desde  $\mathbb{Q}$  a  $\mathbb{Q}(\zeta_{47})$ .

EJERCICIO 18. Probar que para todo  $n$ , el grupo diédral  $D_n$  es soluble.

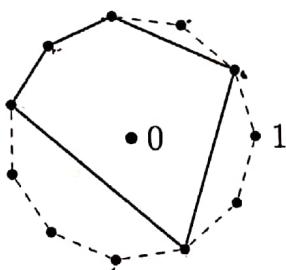
EJERCICIO 19. Muestre directamente que el polinomio  $x^3 + x^2 - 2x - 1$  es soluble por radicales sobre  $\mathbb{Q}$  probando que sus raíces son  $2\cos(2\pi j/7) = \zeta_7^j + \zeta_7^{-j}$  para  $j = 1, 2, 3$  y que  $\mathbb{Q} \subset \mathbb{Q}(\zeta_7)$  es radical.

Álgebra 2 para postgrado Prueba 2  
Martes 21 de Octubre, 2014

1. Para un subconjunto  $S \subset \mu_{11} = \{z \in \mathbb{C} \mid z^{11} = 1\} \subset \mathbb{Q}(e^{2\pi i/11})$  definimos

$$z_S := \sum_{s \in S} s.$$

- a) Demuestre que  $z_S$  es construible con regla y compas comenzando de  $\{0, 1\}$ , donde  $S$  consiste de los vértices de la siguiente 5-ángulo (no regular) en  $\mathbb{C}$ :



- b) Calcula el número de subconjuntos  $S \subset \mu_{11}$  tal que  $z_S$  es construible con regla y compas comenzando de  $\{0, 1\}$ .

2. Sea  $\mathbb{F} := \mathbb{F}_{128}$  el cuerpo con 128 elementos.

- a) Demuestre que para todo  $\alpha \in \mathbb{F} \setminus \mathbb{F}_2$  se tiene  $\mathbb{F}^\times = \langle \alpha \rangle$   
 b) ¿Para cuantos polinomios  $f \in F_2[x]$  se tiene  $F_2[x]/(f) \cong \mathbb{F}$ ?

3. Sea  $K/F$  una extensión finita y separable y sea  $\alpha \in K$ . Sea  $L/F$  una extensión Galois finita con  $K \subset L$ . Define la norma de  $\alpha$  por:

$$N_{K/F}(\alpha) := \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\alpha)$$

donde  $\text{Emb}(K, \bar{F}) := \text{Hom}_F(K, \bar{F})$  son todos los  $F$ -monomorfismos de  $K$  a  $\bar{F}$ .

- a) Demuestre:  $N_{K/F}(\alpha) \in F$  y  $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$   
 b) Suponga que  $K/F$  es Galois con grupo de Galois cíclico  $G = \text{Gal}(K/F) = \langle \sigma \rangle$ . Si  $\alpha \in K$  y  $N_{K/F}(\alpha) = 1$ , entonces existe un  $\beta \in K$ ,  $\beta \neq 0$  tal que  $\alpha = \beta/\sigma(\beta)$   
 (Indicación: use el teorema de Dedekind de la independencia de los caracteres)



FACULTAD DE MATEMÁTICAS  
PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE



NUMERO

NOTA:

60

— FIRMA CORRECTOR —

(Escriba con letra imprenta y lápiz pasta):

APELLIDO PATERNO	APELLIDO MATERNO	NOMBRES
GODOY	VALDEBENITO	MARCO ALEJANDRO

FECHA				
SIGLA	SECCION	DIA	MES	AÑO

CONTROL

INTERROGACIÓN

EXAMEN

Nº

NOMBRE PROFESOR(A)

ERDAL EMSIZ

#### IMPORTANTE

- El artículo N°33 del reglamento del alumno establece.
- "Todo acto realizado por el alumno durante el control académico, que lo viole, será sancionado a lo menos con la suspensión inmediata del control y con la aplicación de la nota mínima. Sin prejuicio de lo anterior, el profesor del curso deberá entregar los antecedentes a la Facultad de que depende el Alumno".
- Por ningún motivo debe arrancar hojas al cuadernillo. Si hay necesidad de hacer cálculos o anotaciones, utilice la contratapa de la última hoja, luego crúcela diagonalmente.

Nota 1 a) 3 b) 3

Nota 2 a) 3 b) 3

Nota 3 a) 3 b) 0

## Problema 2

(a) Por demostrar que para todos  $\alpha \in \mathbb{F} \setminus \mathbb{F}_2$  se tiene

$$\mathbb{F}^x = \langle \alpha \rangle$$

dem.  $\mathbb{F} := \mathbb{F}_{128}$ ,  $\alpha \in \mathbb{F} \setminus \mathbb{F}_2 \Rightarrow \alpha \neq 0, 1$ .

Sabemos que  ~~$\mathbb{F}^x = \mathbb{F}_{127}$~~   $\mathbb{F}^x = C_{127} = \langle \alpha \rangle$

( $C_{127}$  grupo cíclico de 127 elementos). Por otro lado,

$\forall \beta \in \mathbb{F}^x : \langle \beta \rangle \leq \mathbb{F}^x$ , donde si  ~~$d = \text{ord}(\beta)$~~

(orden de  $\beta$ ),  $d \mid 127$ , pero como 127 es primo,  
 $d \in \{1, 127\}$

$\therefore \forall \alpha \in \mathbb{F} \setminus \mathbb{F}_2 : d = \text{ord}(\alpha) = 127$

$\therefore \forall \alpha \in \mathbb{F} \setminus \mathbb{F}_2 : \langle \alpha \rangle = \mathbb{F}^x$

(b) ¿Para cuantos polinomios  $f \in \mathbb{F}_2[x]$  se tiene  $\mathbb{F}_2[x]/(f) \cong \mathbb{F}$ ?

desarrollo.  $128 = 2^7$ , luego  $\mathbb{F} = \mathbb{F}_{2^7}$ .

Como  $\mathbb{F}_{2^7} \cong \mathbb{F}_2[x]/(f) \Rightarrow \deg(f) = 7$

Por otro lado, si  $f$  irreducible y  $\deg(f) = 7$ , entonces

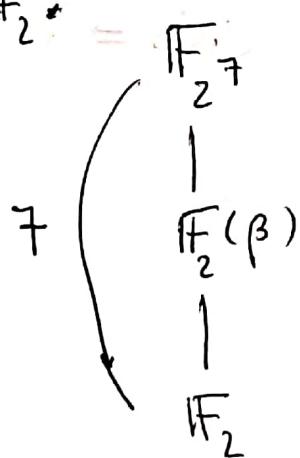
$\forall \alpha \in \overline{\mathbb{F}}_2 : f(\alpha) = 0$ , se tiene que  $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^7}$ .

También sabemos que  $f$  irreducible  $\Rightarrow f$  separable  
 $\Rightarrow f$  tiene raíces distintas.

Sea  $N$  el número de polinomios de grado 7 irreducibles en  $\mathbb{F}_2$ ,

$$N \cdot 7 = \#\{\alpha \in \overline{\mathbb{F}}_2 / \mathbb{F}_2(\alpha) \cong \mathbb{F}_{2^7}\}$$

Sea  $\beta \in \mathbb{F}_{2^7} \setminus \mathbb{F}_2$ :



$$7 = [\mathbb{F}_{2^7} : \mathbb{F}_2] = [\mathbb{F}_{2^7} : \mathbb{F}_2(\beta)] [\mathbb{F}_2(\beta) : \mathbb{F}_2] \quad y \quad [\mathbb{F}_2(\beta) : \mathbb{F}_2] > 1$$

$$\therefore [\mathbb{F}_2(\beta) : \mathbb{F}_2] = 7$$

$$\therefore \mathbb{F}_2(\beta) = \mathbb{F}_{2^7}$$

$$\therefore \#\{\alpha \in \overline{F}_2 \mid F_2(\alpha) \cong F_{2^7}\} = 2^7 - 2$$

$$\therefore N = \frac{2^7 - 2}{7} \quad \checkmark$$

### Problema 1

(a) Si  $\zeta = e^{2\pi i/11}$ , tenemos que para  $S$  dado por la figura

$$Z_S = \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9$$

$Z_S$  es constructible si  $[\mathbb{Q}(Z_S) : \mathbb{Q}] = 2^n$ ,  $n \in \mathbb{N}$ .

Como  $\mathbb{Q}(\zeta)/\mathbb{Q}$  Galoiana, con  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/11\mathbb{Z})^*$ ,

tendremos que encontrar  $H \leq G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  tal que

$$\mathbb{Q}(Z_S) = \mathbb{Q}(\zeta)^H \text{ ; y } [\mathbb{Q}(Z_S) : \mathbb{Q}] = \frac{G}{H}$$

(Recordar que  $\mathbb{Q}(Z_S)/\mathbb{Q}$  también es Galoiana, ya que

$(\mathbb{Z}/11\mathbb{Z})^* \cong C_{10}$  abeliano, es decir, ~~todo~~  $\sigma \in H$  implica que todos sus subgrupos son normales)

$$\text{Sea } \sigma_m \in G : \sigma_m(\zeta) = \zeta^m \quad , \quad m = 0, \dots, 10$$

queremos buscar los  $\sigma_m$  que fijan  $Z_S$ .

$$\begin{aligned} \text{Como } \sigma_m(Z_S) &= \zeta^m + \zeta^{3m} + \zeta^{4m} + \zeta^{5m} + \zeta^{9m} \\ &= \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9 \end{aligned}$$

las opciones son  $m = 1, 3, 4, 5, 9$

$$\sigma_3(\mathbb{Z}_5) = \zeta^3 + \zeta^9 + \zeta^{12} + \zeta^{15} + \zeta^{27}$$

$$= \zeta^3 + \zeta^9 + \zeta + \zeta^4 + \zeta^5$$

$$\sigma_4(\mathbb{Z}_5) = \zeta^4 + \zeta^{12} + \zeta^{16} + \zeta^{20} + \zeta^{36}$$

$$= \zeta^4 + \zeta + \zeta^5 + \zeta^9 + \zeta^3$$

$$\sigma_5(\mathbb{Z}_5) = \zeta^5 + \zeta^{15} + \zeta^{20} + \zeta^{25} + \zeta^{45}$$

$$= \zeta^5 + \zeta^4 + \zeta^9 + \zeta^3 + \zeta$$

$$\sigma_9(\mathbb{Z}_5) = \zeta^9 + \zeta^{27} + \zeta^{36} + \zeta^{45} + \zeta^{81}$$

$$= \zeta^9 + \zeta^5 + \zeta^3 + \zeta + \zeta^4$$

$\therefore H = \{\sigma_3, \sigma_4, \sigma_5, \sigma_9, \text{id}\} \subset \text{fijas } \mathbb{Q}(\mathbb{Z}_5)$

Como  $(\mathbb{Z}/11\mathbb{Z})^*$  es cíclico  $\Rightarrow H$  también debe ser ~~cíclico~~ cíclico

$$\therefore H \cong C_5$$

$$\text{Así } [\mathbb{Q}(\mathbb{Z}_5) : \mathbb{Q}] = \frac{|G|}{|H|} = \frac{10}{5} = 2$$

$\therefore \mathbb{Z}_5$  es constructible

(b) Calcular el número de subconjuntos ~~de~~  
 $S \subset \mu_n$  tal que  $\mathbb{Z}_5$  es constructible con regla y  
compás.

desarrollo: Recordemos que  $\mathbb{Z}_5$  es constructible con regla  
y compás si  $[\mathbb{Q}(\mathbb{Z}_5) : \mathbb{Q}] = 2^n$ ,  $n \in \mathbb{N}$ .

Por lo visto en el punto (a), por segundo teorema  
fundamental de la teoría de Galois, existe  $H_5 \leq G$   
 $= \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  tal que  $\mathbb{Q}(\mathbb{Z}_5) = \mathbb{Q}(\zeta)^{H_5}$ .

Recordemos que  $(\mathbb{Q}(\mathbb{Z}_5)/\mathbb{Q})$  es Galois, ergo

$$\text{Gal}(\mathbb{Q}(\mathbb{Z}_5)/\mathbb{Q}) \cong G/H$$

$$\therefore [\mathbb{Q}(\mathbb{Z}_5) : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(\mathbb{Z}_5)/\mathbb{Q})| = \frac{|G|}{|H|}$$

Como  $|G| = 10 = 2 \cdot 5$ , ~~no~~ necesariamente  $|H| = 5$

~~así~~

Pero  $H = \langle \sigma \rangle$ , luego debemos buscar todos ~~los~~  
los elementos de orden 5 en  $G = C_{10}$

Elemento de $C_{10}$	Orden
0	0
1	10
2	5
3	10
4	5
5	2
6	5
7	10
8	5
9	10

El 2, 4, 6, 8 son de orden 5 ( $C_{10} = \mathbb{Z}/10\mathbb{Z}$ )

- Hay 4 subconjuntos S tales que  $\mathbb{Z}_S$  es constructible

### Problema 3.

(a) Por demostrar que  $N_{K/F}(\alpha) \in F$  y  $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$

dem. Dado  $\alpha \in K$ , sea  $m(x) = \text{irr}_{K/F}(x) \in F[x]$ .

Como  $K/F$  es separable,  $m(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ , donde  $\alpha_i = \alpha$  y  $\alpha_i \neq \alpha_j \quad \forall i \neq j, i, j \in \{1, \dots, n\}$ .

Por otro lado

$$\begin{array}{c} L \\ \text{Gal} \\ | \\ K \\ \text{sep} \\ | \\ F \end{array} \quad \left( \begin{array}{c} L \\ \text{Gal} \\ | \\ K \\ \text{sep} \\ | \\ F \end{array} \right) \quad \text{Gal}$$

entonces, para cada  $\sigma \in \text{Emb}(K, \bar{F})$ , existen  $[L : K]$  tales que  $\tau|_K = \sigma$ .

Pero  $\forall \tau : \tau(m(\alpha_i)) = m(\tau(\alpha_i))$

$\Rightarrow \tau(\alpha_i)$  es una raíz de  $m(x)$ .

Así :  $m(x) = \prod_{\sigma \in \text{Emb}(K, \bar{F})} (x - \sigma(\alpha))$

El término libre de  $m(x)$  es  $(-1)^m \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\alpha) \in F$

algún  $\text{mean}$

$\therefore \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\alpha) \in F$ .

Seien  $\alpha, \beta \in K$

$$\begin{aligned} N_{K/F}(\alpha\beta) &= \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\alpha\beta) \\ &= \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\alpha)\sigma(\beta) \\ &= \left( \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\alpha) \right) \left( \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\beta) \right) \\ &= N_{K/F}(\alpha) N_{K/F}(\beta). \end{aligned}$$

✓

Es ist also  $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$ .  
Wir zeigen  $N_{K/F}(\alpha) = \prod_{\sigma \in \text{Emb}(K, \bar{F})} \sigma(\alpha)$ .

Sei  $\alpha \in K$ . Es sei  $\sigma \in \text{Emb}(K, \bar{F})$ .  
 $\sigma(\alpha) = \sigma(\alpha^{\sigma})$  da  $\sigma$  ein Automorphismus ist.

$\sigma(\alpha) = \sigma(\alpha^{\sigma}) = \sigma(\sigma(\alpha)) = \sigma(\alpha)$ .  
Also ist  $\sigma(\alpha) = \alpha$ .

(b)  $K/F$  Galois,  $G = \text{Gal}(K/F) = \langle \sigma \rangle$

Sea  $\alpha \in K$ ,  $N_{K/F}(\alpha) = 1$

$$N_{K/F}(\alpha) = \prod_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha)$$

$$= \sigma(\alpha) \sigma^2(\alpha) \dots \sigma^{n-1}(\alpha) \alpha = 1$$

~~id.~~  
 $\sigma^n = 1$

$$\therefore \alpha = \frac{1}{\sigma(\alpha) \sigma^2(\alpha) \dots \sigma^{n-1}(\alpha)} \stackrel{?}{=} \beta$$

$$\sigma(\beta)$$

# Cuerpos y álgebras (ALGEBRA II).

## Prueba No 1

Octubre 1, 2013

**Escoger 4 preguntas.**

1. Demuestre que si  $L/K$  es una extensión de grado 2, con  $\text{char}(K) \neq 2$ , entonces existe  $a \in K$  tal que  $L = K(\sqrt{a})$ . Muestre con un ejemplo que la restricción a la característica es necesaria (sugerencia: hay un ejemplo finito).
2. Calcule cuantos polinomios mónicos irreducibles de grado 6 hay en el anillo  $\mathbb{F}_5[x]$ .
3. Probar que  $[\mathbb{Q}(\sqrt{2+i}) : \mathbb{Q}] = 4$ .
4. Encuentre el polinomio minimal de la raiz de la unidad  $\rho = e^{2\pi i/7}$  sobre el cuerpo  $L = \mathbb{Q}(\sqrt{-7})$ .
5. Sea  $f(x) \in \mathbb{C}(x)$  una función racional que satisface:
  - (a)  $f(x) = f(1/x)$ ,
  - (b)  $f(x) = f(e^{2\pi i/3}x)$ .

Probar que existe una función racional  $h(x) \in \mathbb{C}(x)$  tal que

$$f(x) = h\left(x^3 + \frac{1}{x^3}\right).$$

(Sugerencia: Consideré el cuerpo  $L \subseteq \mathbb{C}(x)$  formado por todas las funciones racionales que satisfacen (a) y (b)).

# Cuerpos y álgebras (ALGEBRA II).

## Prueba No 3

Diciembre 12, 2013

**Escoger 4 preguntas.**

1. Encuentre las dimensiones de las representaciones irreducibles de  $S_4$ .  $\mathfrak{S}_4$

2. Sean  $A$  y  $B$  álgebras centrales simples de dimensión 4 sobre un cuerpo  $K$ , y sean  $a \in A$ ,  $b \in B$ , dos elementos no centrales que satisfacen  $K(a) \cong K(b)$ . Probar que existe un álgebra central simple  $C$  tal que  $A \otimes_K B \cong M_2(C)$  (Sugerencia: probar que no es un álgebra de división).

~~3.~~ Probar que las álgebras de cuaterniones  $\mathfrak{A} = \left( \frac{-1, -1}{\mathbb{Q}} \right)$  y  $\mathfrak{B} = \left( \frac{2, 3}{\mathbb{Q}} \right)$  no son isomorfas (sugerencia: Considere  $\mathfrak{A}_{\mathbb{R}}$ .)

~~4.~~ Sea  $K$  un cuerpo y  $V$  un espacio vectorial de dimensión 2 sobre  $K$ . Sea  $T : V \rightarrow V$  una transformación lineal.

(a) Pruebe que para toda base  $\{v_1, v_2\}$  de  $V$  se tiene  $T(v_1) \wedge T(v_2) = (\det T)v_1 \wedge v_2$ .

(b) generalice a espacios de  $n$  dimensiones.

# ALGEBRA II.

## Prueba No 2

Octubre 30, 2014

escoger 4 problemas. Justifique todas sus respuestas.

1. Sea  $L = \mathbb{Q}(\alpha)$  donde  $\alpha$  es raíz de  $x^3 + ax + b = 0$ . Sean  $\alpha = \alpha_1, \alpha_2, \alpha_3$ , las tres raíces de esa ecuación y sea  $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ .
  - (a) Probar que  $\delta^2 \in \mathbb{Q}$ .
  - (b) Probar que  $L/\mathbb{Q}$  es una extensión Galoiana si y sólo si  $\delta \in \mathbb{Q}$ .
  - (c) Si  $L = \mathbb{Q}(\sqrt[3]{c})$  con  $c \in \mathbb{Q}$ , entonces  $-3\delta^2$  es un cuadrado en  $\mathbb{Q}$ .
2. Sea  $p = 2^n + 1$  un número primo. Probar que puede escribirse una raíz de la ecuación  $\frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x + 1 = 0$  utilizando números racionales, sumas, productos, restas, cocientes, y raíces cuadradas.
3. Probar que si  $\alpha$  es un entero algebraico, entonces  $\sqrt[3]{3\alpha + 1}$  es un entero algebraico.
4. Sea  $f(x, y)$  un polinomio en dos variables con coeficientes complejos que satisface  $f(x, y) = f(-y, x)$ . Probar que existe un polinomio  $g(x, y)$  en dos variables con coeficientes complejos, tal que  $f(x, y) = g(x^2 + y^2, x^2y^2)$ .
5. Sea  $f(x) \in \mathbb{F}_2[x]$  un polinomio. Sean  $L = \mathbb{F}_2(x)$ , y  $K = \mathbb{F}_2(f)$ . Probar que  $L/L_{t.i.}$  es una extensión separable.
6. Sea  $L = \mathbb{C}(x, \sqrt{1+x^2}, (1+x)\sqrt{2})$  y  $K = \mathbb{R}$ . Calcule el grado de trascendencia de la extensión  $L/K$ .

# ALGEBRA II.

## Prueba No 2

Octubre 30, 2014

**escoger 4 problemas. Justifique todas sus respuestas.**

1. Sea  $L = \mathbb{Q}(\alpha)$  donde  $\alpha$  es raíz de  $x^3 + ax + b = 0$ . Sean  $\alpha = \alpha_1, \alpha_2, \alpha_3$ , las tres raíces de esa ecuación y sea  $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ .
  - (a) Probar que  $\delta^2 \in \mathbb{Q}$ .
  - (b) Probar que  $L/\mathbb{Q}$  es una extensión Galoiana si y sólo si  $\delta \in \mathbb{Q}$ .
  - (c) Si  $L = \mathbb{Q}(\sqrt[3]{c})$  con  $c \in \mathbb{Q}$ , entonces  $-3\delta^2$  es un cuadrado en  $\mathbb{Q}$ .
2. Sea  $p = 2^n + 1$  un número primo. Probar que puede escribirse una raíz de la ecuación  $\frac{x^p-1}{x-1} = x^{p-1} + \dots + x + 1 = 0$  utilizando números racionales, sumas, productos, restas, cocientes, y raíces cuadradas.
3. Probar que si  $\alpha$  es un entero algebraico, entonces  $\sqrt[7]{3\alpha + 1}$  es un entero algebraico.
4. Sea  $f(x, y)$  un polinomio en dos variables con coeficientes complejos que satisface  $f(x, y) = f(-y, x)$ . Probar que existe un polinomio  $g(x, y)$  en dos variables con coeficientes complejos, tal que  $f(x, y) = g(x^2 + y^2, x^2y^2)$ .
5. Sea  $f(x) \in \mathbb{F}_2[x]$  un polinomio. Sean  $L = \mathbb{F}_2(x)$ , y  $K = \mathbb{F}_2(f)$ . Probar que  $L/L_{t.i.}$  es una extensión separable.
6. Sea  $L = \mathbb{C}(x, \sqrt{1+x^2}, (1+x)^{\sqrt{2}})$  y  $K = \mathbb{R}$ . Calcule el grado de trascendencia de la extensión  $L/K$ .

## Tarea

Cuerpos y Álgebras.

Claudio Abraham Bravo Castillo  
Lic. matemáticas.

### Problema 1

Demuestre que si  $L/K$  es una extensión separable de grado 2, entonces es Galoisiana.

Probar que si  $K$  es un cuerpo de característica 2, entonces  $L = K(\alpha)$  donde  $\alpha$  es raíz de un polinomio  $f(x) = x^3 + x + a$ , para algún  $a \in K$ .

Demotación: Si  $L/K$  es separable, con  $[L:K] = 2$ , entonces demostraremos que todo elemento en  $K$  es normal sobre  $K$ .

Sea  $x \in L$ , entonces como  $K \subseteq K(x) \subseteq L$  se tiene que:  $[K(x):K] | [L:K]$

Por lo tanto:  $[K(x):K] \in \{1, 2\}$

Primero, si:  $[K(x):K] = 1$  se tiene que:  $K(x) = K$  por lo tanto  $x \in K$ , en dicho caso:

$\text{irr}_{x,K}(t) = t - x$  (pues se cumple que  $t = x$  no puede tener grado mayor)

Observe que su única raíz es  $t = x \in L$ .

En el otro caso, si:  $[K(x):K] = 2$  entonces existe  $p(t) = \text{irr}_{x,K}(t)$  con  $p(x) = 0$  en  $L$ .

Por lo tanto:  $t - x | p(t)$  en  $L[x]$  y como  $\deg p(t) = 2$

$\Rightarrow \frac{p(t)}{t-x} = t - y$ , donde  $y \in L$ , es decir  $p(t) = (t-y)(t-x)$   $\therefore p(t)$  tiene todas sus

raíces en  $L$ , o sea el elemento  $x \in K$  es normal sobre  $K$ .

$\therefore L/K$  normal y separable, entonces palabras,  $L/K$  Galoisiana.

Un par de observaciones: observe que si  $x \notin K$ , entonces:  $K \subseteq K(x) \subseteq L$  y  $[K(x):K] = 2$

(Si no,  $K(x) = K \Leftrightarrow x \in K$ ), así  $K(x) = L$ .

Y pues si  $p(x) = \text{irr}_{x,K}(t) = t^2 + b$  es de esta forma  $\Rightarrow x^2 + b = 0 \Rightarrow x^2 = b$  pues  $\text{car } K = 2$

y pues si  $p(x) = \text{irr}_{x,K}(t) = t^2 + x^2 = (t+x)^2 \rightarrow p(x)$  no es separable ( $\neq$ )

o sea:  $p(x) = \text{irr}_{x,K}(t) = t^2 + at + b$ , con  $a \neq 0$ .

$\therefore p(x) = \text{irr}_{x,K}(t) = t^2 + at + b$ , con  $a \neq 0$ .

Busquemos ahora un elemento de traza 1.

Un pequeño problema: (realmente pequeño, pues es para dos automorfismos).  $\{ \sigma, \text{id} \} = \text{Gal}(L/K) = G$

son  $K$ -l.i.

Demonstración: Sea por hipótesis, si existe  $k \in K$ :  $\sigma = k \cdot \text{id} \Rightarrow \sigma(xy) = kxy = \sigma(x)\sigma(y) = k^2xy$

$$\therefore k^2 = 1 \quad (\rightarrow k = 1 \text{ o } k = -1)$$

$V_{xy}$

entonces existe  $c \in L$ :  $\sigma(c) + id(c) = r \neq 0$

(Si no tenemos una  $K$ -combinación lineal tal que es nula  $\Rightarrow$  son l.d. ( $\Rightarrow$ ))

Así:  $\sigma\left(\frac{c}{r}\right) + id\left(\frac{c}{r}\right) = \frac{1}{r}(\sigma(c) + c) = 1.$

Sea  $\alpha = \frac{c}{r} \in L - K$  (sino  $\sigma\left(\frac{c}{r}\right) = \frac{c}{r} \Rightarrow \sigma\left(\frac{c}{r}\right) + \frac{c}{r} = 2\frac{c}{r} = 0$  ( $\Rightarrow$ ))

entonces por lo anterior  $L = K(\alpha)$ , donde

$$\begin{aligned} irr_{\alpha, K}(x) &= (x - \alpha)(x - \beta), \text{ donde } \beta = \sigma(\alpha) \quad (\text{por ext. de } \\ &= (x - \alpha)(x - \sigma(\alpha)) \\ &= x^2 - (\alpha + \sigma(\alpha))x + \alpha\sigma(\alpha) \in K(x) \end{aligned}$$

Así  $\alpha, \sigma(\alpha) \in K$ , ojalá  $\alpha = \alpha\sigma(\alpha)$  y  $\alpha + \sigma(\alpha) = 1$  por lo tanto  $\alpha$  es raíz del polinomio:

$$irr_{\alpha, K}(x) = x^2 - x + q = x^2 + x + q, \text{ con } q \in K.$$

Problema 2. Encuentre el menor valor de  $t$  tal que  $x^{t-1}$  tiene un factor irreducible de grado

en  $\mathbb{F}_3(x)$ .

Demostración: queremos que  $x^{t-1}$  tenga un factor irreducible de grado  $7$

o sea queremos que exista  $p(x) \in \mathbb{F}_3[x]$  con  $2f = 7$  y  $p(x) | x^{t-1}$ .

Supongamos que esto sucede (para buscar condiciones). Sea  $\alpha$  raíz de  $p(x)$ . entonces  $\alpha$  es raíz de  $x^{t-1}$

$$\Rightarrow FF_3(\alpha) : FF_3 = 2 \cdot irr_{\alpha, \mathbb{F}_3} = 2p(x) = 7 \Rightarrow FF_3(\alpha) = \mathbb{F}_3^7.$$

$$\therefore \alpha^t = 1 \text{ en } \mathbb{F}_3^7$$

$$\text{Por lo tanto } |\alpha| \mid |\mathbb{F}_3^7| = 3^7 - 1, \text{ luego: } 3^7 \equiv 1 \pmod{|\alpha|}$$

$$\text{pero } 3^7 - 1 = 2186 = 2 \cdot \underbrace{1093}_{\text{nº primo}}, \text{ lo que nos dice que: } |\alpha| = 2, |\alpha| = 1093 \text{ o } |\alpha| = 2186$$

Como buscamos el más pequeño,  $t = 2$  (no hay pol. de grado 7 que lo divida). Tomemos  $t = 1093$  (observa que tomamos  $t = 1093$ , para que  $|\alpha| = t = 1093$ , pero se cumplen  $|\alpha| \mid t \Rightarrow t$  puede ser más grande, pero como buscamos el menor tomaremos este  $t$ )

Observa que entonces:  $3^t - 1 \equiv 0 \pmod{1093} \Rightarrow$  en  $\mathbb{F}_{3^7}$  hay un elemento de orden  $1093$  (y no para  $n < 7$ )

$$\therefore \exists p = irr_{\alpha, \mathbb{F}_3}, 2p = 7 \text{ y } p \mid x^{1093} - 1.$$

$$\therefore t = 1093 \text{ es el número buscado.}$$

Problema 3. Probar que  $[\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5}) : \mathbb{Q}] = 8$ .

Demostración: Sabemos por lo visto en clases que:

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) / \mathbb{Q}$  es una extensión Galoiana

(ya que  $\text{irr}_{\mathbb{Q}}(K/\mathbb{Q}) = X^2 - p = (X - \sqrt{p})(X + \sqrt{p})$  es separable y normal sobre  $K$ , pues sus raíces son  $\sqrt{p}, -\sqrt{p} \in K$  y son diferentes,  $\forall p \in \{2, 3, 5\}$ ).

Además por lo visto en clases:

$$\text{Gal}(K/\mathbb{Q}) = \langle \{\sigma_2, \sigma_3, \sigma_5\} \rangle \cong C_2 \times C_2 \times C_2, \text{ donde}$$

$$\begin{aligned} \sigma_p: K &\longrightarrow K \\ \sqrt{p} &\longmapsto -\sqrt{p} \end{aligned} \quad \forall p \in \{2, 3, 5\}.$$

Entonces si  $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$ :

$$\text{Orb}_G(\alpha) = \left\{ \sqrt{2} + \sqrt{3} + \sqrt{5}, -\sqrt{2} + \sqrt{3} + \sqrt{5}, -\sqrt{2} - \sqrt{3} + \sqrt{5}, -\sqrt{2} - \sqrt{3} - \sqrt{5}, \right.$$

$$\left. \sqrt{2} - \sqrt{3} + \sqrt{5}, \sqrt{2} - \sqrt{3} - \sqrt{5}, -\sqrt{2} + \sqrt{3} - \sqrt{5}, \sqrt{2} + \sqrt{3} - \sqrt{5} \right\}$$

∴ ningún elemento  $\sigma \in \text{Gal}(L/\mathbb{Q})$  fija a  $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$ , salvo la identidad, así si  $\alpha \in E$ :  $\mathbb{Q} \subseteq E \subset L$ , por lo tanto de la correspondencia de Galois:  $\alpha \in E = L^H$  con  $H \neq \{id\}$

$\Rightarrow \alpha$  es fijado por algún  $\sigma \in G$ ,  $\sigma \neq id$  ( $\not\equiv$ )

$\therefore \alpha \in L$  y no a sus subextensiones menores  $\Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

$$\therefore [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = |G| = 8.$$

∴  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ , donde  $\rho = e^{\frac{\pi i}{12}} = e^{\frac{2\pi i}{24}}$ .

Problema 4. Calcule cuantos cuerpos  $F$  satisfacen que  $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\rho)$ , donde  $\rho = e^{\frac{\pi i}{12}} = e^{\frac{2\pi i}{24}}$ .

Desarrollo: Primero demostremos que la extensión es Galoiana.

Sea  $\Phi_{24}(x)$  el polinomio irreducible de  $\rho$  sobre  $\mathbb{Q}$ .

Se sabemos que las raíces 24-avas de la unidad son de la forma:  $\rho^i$ ,  $i \in \{0, \dots, 23\}$ .

Como sabemos todas las raíces 24-avas de la unidad son de la forma:  $\rho^i$ , pues:

∴ todas las raíces que  $\Phi_{24}(x)$  están en  $\mathbb{Q}(\rho)$ , pues:

$$\Phi_{24}(x) \mid p(x) = x^{24} - 1 = (x-1)(x-\rho) \dots (x-\rho^{23})$$

y  $p(x)$  tiene todas sus raíces en  $\mathbb{Q}(\rho) \Rightarrow \Phi_{24}(x)$  también lo son.

Observa que todas las raíces de  $p(x)$  son distintas  $\Rightarrow$  las raíces de  $\Phi_{24}(x)$  también lo son.

∴  $\mathbb{Q}(\rho)/\mathbb{Q}$  normal y separable  $\Rightarrow \mathbb{Q}(\rho)/\mathbb{Q}$  Galoiana.

$$\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* \text{ para } n = e^{\frac{2\pi i}{12}}$$

Ahora bien se conoce en tales y se vio en Ayudante que:

$$\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) \cong (\mathbb{Z}/24\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/8\mathbb{Z})^* \text{ por teo. Chino de los restos.}$$

Por lo tanto:

$$\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) \cong (\mathbb{Z}/24\mathbb{Z})^*$$

Observemos que  $(\mathbb{Z}/3\mathbb{Z})^*$  es cíclico  $\Rightarrow (\mathbb{Z}/3\mathbb{Z})^* \cong C_2$   
 y que:  $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$  donde  $3^2 = 5^2 = 7^2 \equiv 1 \pmod{8}$   $\therefore$  todo elemento tiene orden 2 en el grupo de 4 elementos.

$$\therefore (\mathbb{Z}/8\mathbb{Z})^* \cong C_2 \times C_2$$

$$\therefore \text{Gal}(\mathbb{Q}(p)/\mathbb{Q}) \cong C_2 \times C_2 \times C_2. \quad \text{(cantidad de}$$

Teorema de la Correspondencia de Galois, el calcular los subcuerpos  $F: \mathbb{Q} \subseteq F \subseteq \mathbb{Q}(p)$ .  $\forall$   $\sigma \in \text{Gal}(\mathbb{Q}(p)/\mathbb{Q})$   $\therefore$  contaremos estos subgrupos.

Es equivalente contar los subgrupos de  $C_2 \times C_2 \times C_2$ .  $\therefore$  contar los subgrupos de  $C_2^3$

Ahora bien como  $C_2 \times C_2 \times C_2 = C_2^3 \in \text{Sub}(C_2 - \text{vectorial})$ , el contar los subgrupos de  $C_2^3$ .

Es equivalente contar los subespacios de  $C_2^3/C_2$  y de estos hay:

de dim 0: Solo hay 1:  $\langle (0,0,0) \rangle = \{(0,0,0)\}$ .

de dim 1: Son generados un vector no nulo y hay  $2^3 - 1$  de estos, pero como vectores su ponderado generan el mismo subespacio, hay en total:

$$\frac{2^3 - 1}{2 - 1} = 7 \text{ subespacios}$$

$$\text{de dim 2: hay } \frac{(2^3 - 1)(2^3 - 2)}{(2^2 - 1)(2^2 - 2)} = 7 \text{ subespacios (son gen. por 2 vectores)}$$

$$\text{de dim 3: hay solo uno: } C_2^3$$

$\therefore$  en total hay 16 subespacios

$\therefore$  en total hay 16 cuerpos  $F: \mathbb{Q} \subseteq F \subseteq \mathbb{Q}(p)$ .

Problema 5. Sea  $p$  un número primo. Sea  $h = h(x) = x^p - x \in \mathbb{F}_p[x]$ . Probar que la extensión  $\mathbb{F}_p(x)/\mathbb{F}_p(h)$  es galoiana y existen isomorfismos de grupo  $\tau: \text{Gal}(\mathbb{F}_p(x)/\mathbb{F}_p(h)) \rightarrow \mathbb{F}_p$  que satisfacen  $\tau(x) = x + \tau(\sigma)$  para todo  $\sigma \in \text{Gal}(\mathbb{F}_p(x)/\mathbb{F}_p(h))$ .  $\mathbb{F}_p(x)/\mathbb{F}_p(h)$  es Galoiana.

Demonstración: Primero demostraremos que la extensión:

$$irr_{\mathbb{F}_p(h)}(t) = t^p - t - h \in \mathbb{F}_p[h]$$

Observemos:  $irr_{\mathbb{F}_p(h)}(t) = t^p - t - h = 0$  y es irreducible ya que, en general, si  $h = \frac{f}{g}$

Esto pues:  $irr_{\mathbb{F}_p(h)}(x) = x^p - x - h = 0$  y es irreducible ya que, en general, si  $h = \frac{f}{g}$

$[\mathbb{F}_p(x): \mathbb{F}_p(h)] = \max\{2f, 2g\}$  (visto en clase)

$\therefore irr_{\mathbb{F}_p(h)}(t)$  tiene el grado correcto y anula a  $x$ .  $\therefore$  es el polinomio irreducible.

Suposición: Raíces de  $\text{irr}_{x \in \mathbb{F}_p(n)}(t)$  enteras.

$$\begin{aligned} \text{irr}_{x \in \mathbb{F}_p(n)}(x+i) &= (x+i)^p - (x+i) - h \quad \text{si } i \in \mathbb{F}_p \\ &= x^p - i^p - x - i - h \\ &= x^p - i - x - i - h \\ &= x^p - x - h = 0 \end{aligned}$$

∴ todas las raíces de  $\text{irr}_{x \in \mathbb{F}_p(n)}(t)$  son:  $\{x, x+1, \dots, x+p-1\}$  todas diferentes, todas en  $\mathbb{F}_p$

$\mathbb{F}_p(x)/\mathbb{F}_p(n)$  es Galoiana.

$\mathbb{F}_p(x)/\mathbb{F}_p(n)$  es separable y normal. ∴  $\mathbb{F}_p(x)/\mathbb{F}_p(n)$  es Galoiana, estos automorfismos de los automorfismos de Galois, estos Algunas de las raíces de  $\text{irr}_{x \in \mathbb{F}_p(n)}$  y como todas son de la forma  $x+i$ ,  $i \in \mathbb{F}_p$  deben llevar raíces de  $\text{irr}_{x \in \mathbb{F}_p(n)}$  a raíces de  $\text{irr}_{x \in \mathbb{F}_p(n)}$ . Los automorfismos están completamente determinados por su comportamiento en  $X$ .

$$G = \text{Gal}(\mathbb{F}_p(x)/\mathbb{F}_p(n)) = \{\sigma_i\}_{i=0}^{p-1} \quad \text{donde:}$$

$$\sigma_i : \begin{cases} \mathbb{F}_p(x) \longrightarrow \mathbb{F}_p(x) \\ x \mapsto x+i \end{cases}, \quad i \in \mathbb{F}_p.$$

Así tenemos que:

(y hay  $p$  de estos pues):  $|G| = [\mathbb{F}_p(x) : \mathbb{F}_p(n)] = p$  por lo dicho anteriormente).

Sea  $T : G \longrightarrow (\mathbb{F}_p, +)$

$$\sigma_i \mapsto i$$

Es un isomorfismo pues  $T(\sigma_i \circ \sigma_j^{-1}) = T(\sigma_{i+j}) = \overline{i-j} = T(\sigma_i) \circ T(\sigma_j^{-1})$  (pues

$$\sigma_i \circ \sigma_j^{-1}(x) = x+i-j = \sigma_{i-j}(x)$$

Además:

$\text{Ker } T = \{\sigma_i \in G : i = 0\} = \{\sigma_i \in G : \text{pli}\} = \{\sigma_0\} = \{\text{id}\}$ .

Además se cumple que:  $T$  es isomorfismo. Además se cumple que:

y como  $T$  es inyección de conjuntos finitos  $\Rightarrow T$  es isomorfismo.

y como  $T$  es inyección de conjuntos finitos  $\Rightarrow T$  es isomorfismo.

$$\forall \sigma_i \in G : \sigma_i(x) = x+i = x+T(\sigma_i) \quad \text{y esto demuestra lo pedido.}$$



Sebastian. trahansen@ alumnos. vsm. cl.

## ALGEBRA II- Tarea 4

Noviembre 26, 2013

1. Sea  $K$  un cuerpo y sea  $V$  un espacio vectorial sobre  $K$ . Sea

$$T(V) = \bigoplus_{n=0}^{\infty} V^{\otimes n}, \quad V^{\otimes 0} = K, \quad V^{\otimes k+1} = V^{\otimes k} \otimes_K V.$$

Nótese que cualquier producto del tipo  $V^{\otimes r} \otimes_K V^{\otimes s}$  puede identificarse canónicamente con  $V^{\otimes r+s}$ . Bajo esta identificación,  $T(V)$  es un álgebra asociativa con un producto que extiende por linealidad el producto tensorial. El álgebra  $T(V)$  se conoce como el álgebra tensorial de  $V$ . Probar que si  $A$  es cualquier  $K$ -álgebra, y  $\phi : V \rightarrow A$  es una función lineal, existe un único homomorfismo de  $K$ -álgebras  $\tilde{\phi} : T(V) \rightarrow A$  que extiende  $\phi$ .

2. Sea  $\Lambda(V)$  el mayor cociente de  $T(V)$  que cumple  $\bar{v} \wedge \bar{w} = -\bar{w} \wedge \bar{v}$  para todo par de vectores  $v, w \in V$ , donde  $\wedge$  denota el producto en el álgebra cociente.

- (a) Enuncie y demuestre, para  $\Lambda(V)$  una propiedad universal similar a la de  $T(V)$ .
- (b) Probar que  $\bar{v} \wedge \bar{v} = 0$  para todo vector  $v \in V$ , y que para toda permutación  $\sigma \in S_k$  se tiene que

$$\bar{v}_{\sigma(1)} \wedge \bar{v}_{\sigma(2)} \wedge \cdots \bar{v}_{\sigma(k)} = \pm \bar{v}_1 \wedge \bar{v}_2 \wedge \cdots \wedge \bar{v}_n.$$

- (c) Si  $V$  es un espacio vectorial de dimensión  $n$ , calcule la dimensión de  $\Lambda(V)$ .

El álgebra  $\Lambda(V)$  se conoce como el álgebra de Grassmann de  $V$ .

3. Sea  $D = \begin{pmatrix} \alpha & \beta \\ \gamma & K \end{pmatrix} = K \oplus Ki \oplus Kj \oplus Kij$  un álgebra de cuaterniones, definida como en clases.

1

$$i^2 = \alpha, \quad j^2 = \beta, \quad ij = -ji$$

(a) Sea  $L = K(i)$ . Probar que  $D = L \oplus Lj$ , y que para cada cuaternión  $q = \lambda + \mu j$  se tienen las identidades

$$\bar{q} = \bar{\lambda} - \mu j, \quad N(q) = N(\lambda) - \beta N(\mu).$$

(b) Probar que si  $\beta$  no es la norma de un elemento de  $L$ , entonces  $D$  es un álgebra de división.

(c) Probar que si  $\beta$  es la norma de un elemento de  $L$ , entonces  $D$  es isomorfo al álgebra de matrices  $M_2(K)$  (Sugerencia: si  $\beta = N(\mu)$  reducir el problema al caso  $\beta = 1$ , remplazando  $j$  por  $\mu^{-1}j$  y luego encontrar una base apropiada del álgebra de matrices).

$$(J\mu^{-1})^2 = J\mu^{-1}J\mu^{-1} = J\overline{J\mu^{-1}\mu^{-1}} = J^2\beta^{-1} = 1.$$

y si llamamos  $\hat{J} = J\mu^{-1}$ , buscamos matriz  $J^T q$

$$\hat{J} \rightarrow J \text{ y } J^2 = I \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 & ab \\ ca & da \end{pmatrix}$$

$$\text{Definiendo } J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Además queremos que si  $i \rightarrow Y$ , entonces:

$$YJ = -JY$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\begin{pmatrix} b & a \\ d & c \end{pmatrix} = \begin{pmatrix} -c & -d \\ -a & -b \end{pmatrix} \Leftrightarrow \begin{cases} b = -c \\ a = -d \end{cases} \quad \begin{cases} \text{Si } a = 1 \Rightarrow d = -1 \\ b = 0 \Rightarrow c = 0 \end{cases}$$

$$Y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$I \rightarrow I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$i \rightarrow Y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\hat{J} \rightarrow J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$ij \rightarrow YJ = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$q = a+bi+cj+dij.$$

$$q_f \rightarrow \begin{pmatrix} a+b & c+d \\ c-d & a-b \end{pmatrix}, \quad \begin{cases} a-b \Rightarrow \\ d-b \end{cases}$$

$$Q(qq_f) =$$

Cápsulas y Álgebra  
Desarrollo Tarea N°4  
Marco Godoy V.

6,7

1	20
2	19
3	13

### Problema 1.

Sea  $K$  un campo y sea  $V$  un espacio vectorial sobre  $K$ . Sea

$$T(V) = \bigoplus_{n=0}^{\infty} V^{\otimes n}, \quad V^{\otimes 0} = K, \quad V^{\otimes k+1} = V^{\otimes k} \otimes_K V$$

Notese que cualquier producto del tipo  $V^{\otimes r} \otimes_K V^{\otimes s}$  puede identificarse canónicamente con  $V^{\otimes r+s}$ . Dado esta identificación,  $T(V)$  es un álgebra asociativa con un producto que extiende por linealidad el producto tensorial. El álgebra  $T(V)$  se conoce como el álgebra tensorial de  $V$ . Probar que si  $A$  es cualquier  $K$ -álgebra, y  $\phi: V \rightarrow A$  es una función lineal, existe un único homomorfismo de  $K$ -álgebras  $\tilde{\phi}: T(V) \rightarrow A$  que extiende  $\phi$ .

#### - Demostración -

Dada  $\phi: V \rightarrow A$  lineal, podemos definir naturalmente la función bilineal

$$b: V \times V \rightarrow A \text{ por}$$

$$b(v, w) = \phi(v)\phi(w)$$

Verifiquemos que  $b$  es efectivamente bilineal:

$$\begin{aligned} b(v_1 + v_2, w) &= \phi(v_1 + v_2)\phi(w) = (\phi(v_1) + \phi(v_2))\phi(w) = \phi(v_1)\phi(w) + \phi(v_2)\phi(w) \\ &= b(v_1, w) + b(v_2, w) \end{aligned}$$

$$\begin{aligned} b(v, w_1 + w_2) &= \phi(v)\phi(w_1 + w_2) = \phi(v)(\phi(w_1) + \phi(w_2)) = \phi(v)\phi(w_1) + \phi(v)\phi(w_2) \\ &= b(v, w_1) + b(v, w_2) \end{aligned}$$

$$b(kv, w) = \phi(kv)\phi(w) = k\phi(v)\phi(w) = kb(v, w)$$

$$b(v, kw) = \phi(v)\phi(kw) = \phi(v)(k\phi(w)) = kb(v)\phi(w).$$

$$v_1, v_2, w_1, w_2, v, w \in V, \quad k \in K.$$

Ahora por la propiedad universal del producto tensorial, existe única  $\phi_2 : V \otimes V \rightarrow A$  lineal tal que

$$b(v, w) = \phi_2(v \otimes w) ; \quad b = \phi_1 \circ \otimes$$

$$= \phi \cdot \phi$$

$$\otimes : V \times V \rightarrow V \otimes V$$

$$(v, w) \mapsto v \otimes w$$

Ahora, al igual que en el paso anterior, podemos definir la función bilineal  $b_2 : (V \otimes V) \times V \rightarrow A$ ,  $b_2(v_1 \otimes v_2, w) = \phi_2(v_1 \otimes v_2) \phi(w)$ , luego por la propiedad universal del producto tensorial, existe única  $\phi_3 : (V \otimes V) \otimes V \rightarrow A$  lineal tal que  $b_2 = \phi_3 \circ \otimes = \phi_2 \cdot \phi$ . Se sigue por inducción que podemos conseguir,  $\forall n \in \mathbb{N}$ , una única  $\phi_{n+1} : V^{\otimes n+1} \rightarrow A$  lineal tal que  $\phi_{n+1} \circ \otimes = \phi_n \cdot \phi$  ( $\phi_1 = \phi$ ).

Dado  $T(V) = \bigoplus_{n=0}^{\infty} V^{\otimes n}$  definimos  $\tilde{\phi}$  por

$$\tilde{\phi}(k + v^{(1)} + v^{(2)} + v^{(3)} + \dots + v^{(n)} + \dots) = k + \phi_1(v^{(1)}) + \phi_2(v^{(2)}) + \phi_3(v^{(3)}) + \dots + \phi_n(v^{(n)}) + \dots$$

donde  $\forall n \in \mathbb{N}$ ,  $v^{(n)} \in V^{\otimes n}$ . Es claro que  $\tilde{\phi}$  extiende  $\phi$  ya que  $V \hookrightarrow T(V)$  mediante  $v \xrightarrow{i} 0 + v + 0^{(2)} + 0^{(3)} + \dots$ ,

$$\Rightarrow \tilde{\phi}(v) = \phi(v)$$

Demostremos que  $\tilde{\phi}$  es un homomorfismo de álgebras. Claramente  $\tilde{\phi}$  es lineal ya que es suma de funciones lineales, y para comprobar que respeta producto, es suficiente con ver que  $v^{(r)} v^{(s)} \in V^{\otimes r+s}$ ,

$$\tilde{\phi}(v^{(r)} v^{(s)}) = \phi_{r+s}(\underbrace{v^{(r)} v^{(s)}}_{r+s - \text{productos tensoriales de elementos de } V}) = \phi_r(v^{(r)}) \phi_s(v^{(s)}) = \tilde{\phi}(v^{(r)}) \tilde{\phi}(v^{(s)})$$

r+s - productos tensoriales de elementos de  $V$

Notar que aquí se ha ocupado el hecho de que  $\tilde{\phi}$  extiende a toda  $\Phi_n$  y que  $\Phi_{r+s} = \phi_r \cdot \phi_s$  (el punto es el producto en el álgebra  $A$ , en donde exigimos implícitamente que este producto sea asociativo...)

$\therefore \tilde{\phi}$  homomorfismo de álgebras.

Falta ver la unicidad de  $\tilde{\phi}$ . Para ello primero veamos que tenemos la colección de inclusiones  $i_m$  tales que

$$V^{\otimes n} \xrightarrow{i_n} A ; \quad \tilde{\phi} \circ i_n = \phi_n$$

de la misma manera que  $V \xrightarrow{i} A$  ( $i_1 = i$ ). Como  $i_n$  es inyectiva, entonces para otra función  $\hat{f}$  que cumpliese

$$\hat{f} \circ i_n = \phi_n$$

entonces  $\hat{f} = \tilde{\phi}$  (propiedad de las funciones inyectivas). Todo lo anterior queda resumido en el siguiente diagrama comutativo

$$\begin{array}{ccc} T(V) & \xrightarrow{\tilde{\phi}} & A \\ i_n \downarrow & \swarrow \phi_n & \checkmark \\ V^{\otimes n} & & \end{array}$$

## Problema 2

Sea  $\Lambda(V)$  el mayor cociente de  $T(V)$  que cumple  $\bar{v} \wedge \bar{w} = -\bar{w} \wedge \bar{v}$  para todo par de vectores  $v, w \in V$ , donde  $\wedge$  denota el producto en el álgebra cuociente.

(a) Enuncie y demuestre, para  $\Lambda(V)$  una propiedad universal similar a la de  $T(V)$ .

(b) Pruebe que  $\bar{v} \wedge \bar{v} = 0$  para todo vector  $v \in V$ , y que para toda permutación  $\sigma \in S_k$  se tiene que

$$\bar{v}_{\sigma(1)} \wedge \bar{v}_{\sigma(2)} \wedge \dots \wedge \bar{v}_{\sigma(k)} = \pm \bar{v}_1 \wedge \bar{v}_2 \wedge \dots \wedge \bar{v}_k$$

(c) Si  $V$  es un espacio de dimensión  $n$ , calcule la dimensión de  $\Lambda(V)$

-Demostración-

(a) Sea  $X \leq T(V)$  tal que  $\Lambda(V) = T(V)/X$  (después intentemos de describir su forma). Es obvio que dado un cuociente, tenemos la proyección canónica  $p$  dada por

$$p : T(V) \longrightarrow \Lambda(V)$$

$$p(\bar{v}) = \bar{v} + X$$

el cual cumple la propiedad universal de que dada cualquier función  $f : T(V) \rightarrow A$ , existe única  $\hat{f}$  tal que el siguiente diagrama commute

que respete  $p$ , es decir, si  $p(\bar{v}) = p(\bar{w}) \Rightarrow f(\bar{v}) = f(\bar{w})$

$$\begin{array}{ccc} T(V) & \xrightarrow{p} & \Lambda(V) \\ & \searrow f & \downarrow \hat{f} \\ & A & \end{array}; \quad f = \hat{f} \circ p$$

Esto se debe al hecho de que  $p$  es sobreyectiva.

Además  $p$  es un homomorfismo de álgebras, entonces si  $f$  es un homomorfismo de álgebra,  $\hat{f}$  es un homomorfismo de álgebras. En efecto,

$$\begin{aligned}\hat{f}(\alpha(\vec{v}+X)+\beta(\vec{w}+X)) &= \hat{f}((\alpha\vec{v}+X)+(\beta\vec{w}+X)) \\ &= \hat{f}((\alpha\vec{v}+\beta\vec{w})+X) \\ &= f(\alpha\vec{v}+\beta\vec{w}) \\ &= \alpha f(\vec{v})+\beta f(\vec{w}) \\ &= \alpha \hat{f}(\vec{v}+X)+\beta \hat{f}(\vec{w}+X)\end{aligned}$$

$$\begin{aligned}\hat{f}((\vec{v}+X)(\vec{w}+X)) &= \hat{f}(\vec{v}\vec{w}+X) = f(\vec{v}\vec{w}) = f(\vec{v})f(\vec{w}) \\ &= f(\vec{v}+X)f(\vec{w}+X)\end{aligned}$$

Ahora combinemos esta propiedad universal con la del problema 1, dada una  $\phi: V \rightarrow A$  lineal, entonces el siguiente diagrama comutativo

$$\begin{array}{ccc} \Lambda(V) & \xrightarrow{\exists! \hat{\phi}} & \text{Ker } \tilde{\phi} \cong X \\ p \downarrow & \nearrow \hat{\phi} & \\ T(V) & \xrightarrow{\tilde{\phi}} & A \\ i \downarrow & \nearrow \phi & \\ V & & \end{array}$$

indica que existe una única función  $\hat{\phi}$  (homomorfismo de álgebra) tal que extienda  $\phi$ . Pero aquí falta un hecho que no hemos considerado: el hecho de que  $\hat{\phi}$  debe respetar la relación de equivalencia que determina  $\Lambda(V)$

En este caso se ve claramente que si  $\Lambda(V) = T(V) \setminus X$ , entonces decir lo anterior es equivalente a decir que  $\tilde{\phi}(X) = 0$ . Antes de encontrar otra condición equivalente veamos que  $X$  puede escribirse como la siguiente suma directa

$$X = \bigoplus_{r=1}^{\infty} X_r, \text{ donde}$$

$X_r = \langle x_1 \otimes \dots \otimes x_r \mid \begin{array}{l} x_i = x_j \\ \text{algun } i \neq j \end{array} \rangle_K$ . Luego  $\tilde{\phi}$  debe mandar a cero a todos los elementos de  $X_r$ , en particular a los productos tensoriales  $e_1 \otimes \dots \otimes e_r$  donde  $e_i$  es un elemento de la base de  $V$ .

$$\therefore \tilde{\phi}(e_i \otimes e_i) = 0 \quad \forall i$$

Como definimos  $\tilde{\phi}$  a partir de  $\phi$ , tenemos que  $\tilde{\phi}(e_i \otimes e_i) = \phi(e_i)\phi(e_i) = 0$ , más generalmente,

$$\tilde{\phi}(e_1 \otimes \dots \otimes e_r) = \phi(e_1) \dots \phi(e_r) = 0$$

Por lo tanto, una buena condición es pedir que el álgebra cumpla la siguiente propiedad

$$\forall a \in A, \quad a^2 = 0.$$

Esto último calza con el hecho de que  $\tilde{\phi}(X) = 0$ .

Conclusión: Dada  $\phi: V \rightarrow A$  lineal, existe  $\tilde{\phi}: N(V) \rightarrow A$  homomorfismo de álgebras que extiende  $\phi$  siempre que para todo  $a \in A$ ,  $a^2 = 0$ .

↑  
Basta pedir que  $\phi(v)^2 = 0$  para todo  $v \in V$ . (Esta condición,  $a^2 = 0 \forall a \in A$  es vacía si las álgebras tienen 1).

(b) Por demostrar que  $\bar{v} \wedge \bar{v} = 0$  para todo  $v \in V$ , y que para toda permutación  $\sigma \in S_k$  se tiene que

$$\bar{v}_{\sigma(1)} \wedge \bar{v}_{\sigma(2)} \wedge \dots \wedge \bar{v}_{\sigma(k)} = \pm \bar{v}_1 \wedge \bar{v}_2 \wedge \dots \wedge \bar{v}_k$$

- Demostración -

Del hecho de que  $\bar{v} \wedge \bar{v} = -\bar{v} \wedge \bar{v}$ , se tiene que,  $\forall v \in V$ :

$$\bar{v} \wedge \bar{v} = -\bar{v} \wedge \bar{v}$$

$$\Rightarrow 2(\bar{v} \wedge \bar{v}) = 0 \quad (\text{en el cuádrante } N(V) = T(V)/X)$$

$$\Leftrightarrow 2(\bar{v} \wedge \bar{v}) \in X$$

$$\Leftrightarrow \bar{v} \wedge \bar{v} \in X$$

$$\Leftrightarrow \bar{v} \wedge \bar{v} = 0 \quad \forall v \in V.$$

Ahora recordando que toda permutación  $\sigma \in S_k$  es un producto de trasposiciones  $\tau$ , entonces sólo basta estudiar este caso:

Sean  $i, j \in \{1, \dots, k\}$ ,  $i < j$ ,  $\tau = (ij)$  (la trasposición que cambia el índice  $i$  por el índice  $j$ ). Tenemos que

$$\bar{v}_1 \wedge \bar{v}_2 \wedge \dots \wedge \bar{v}_{j-1} \wedge \bar{v}_j \wedge \bar{v}_{i+1} \wedge \dots \wedge \bar{v}_{j+1} \wedge \bar{v}_i \wedge \bar{v}_{j+1} \wedge \dots \wedge \bar{v}_k$$

$$= (-1) \left( \bar{v}_1 \wedge \bar{v}_2 \wedge \dots \wedge \bar{v}_{j-1} \wedge \bar{v}_{i+1} \wedge \bar{v}_j \wedge \dots \wedge \bar{v}_{j-1} \wedge \bar{v}_i \wedge \bar{v}_{j+1} \wedge \dots \wedge \bar{v}_k \right)$$

$$=(-1)^{|i-j|} \left( \bar{v}_1 \wedge \bar{v}_2 \wedge \dots \wedge \bar{v}_{i-1} \wedge \bar{v}_{i+1} \wedge \dots \wedge \bar{v}_i \wedge \bar{v}_j \wedge \bar{v}_{j+1} \wedge \dots \wedge \bar{v}_k \right)$$

$$=(-1)^{|i-j| + |i-j-1|} \left( \bar{v}_1 \wedge \bar{v}_2 \wedge \dots \wedge \bar{v}_{i-1} \wedge \bar{v}_i \wedge \bar{v}_{i+1} \wedge \dots \wedge \bar{v}_{j-1} \wedge \bar{v}_j \wedge \bar{v}_{j+1} \wedge \dots \wedge \bar{v}_k \right)$$

Ahora para una permutación cualquiera  $\sigma \in S_k$ , tenemos

$$\sigma = (i_1 j_1) (i_2 j_2) \dots (i_r j_r) \quad , \quad i_1 < i_2 < \dots < i_r \\ = z_1 z_2 \dots z_r$$

$$\Rightarrow \bar{V}_{\sigma(1)} \wedge \bar{V}_{\sigma(2)} \wedge \dots \wedge \bar{V}_{\sigma(k)} = (-1)^{|i_1 - j_1| + |i_1 - j_1 - 1|} \bar{V}_{z_2 \dots z_{r(1)}} \wedge \bar{V}_{z_2 \dots z_{r(2)}} \wedge \dots \wedge \bar{V}_{z_2 \dots z_{r(k)}} \\ = (-1)^{|i_1 - j_1| + |i_1 - j_1 - 1| + |i_2 - j_2| + |i_2 - j_2 - 1|} \bar{V}_{z_3 \dots z_{r(1)}} \wedge \bar{V}_{z_3 \dots z_{r(2)}} \wedge \dots \wedge \bar{V}_{z_3 \dots z_{r(k)}} \\ = (-1)^{|i_1 - j_1| + |i_1 - j_1 - 1| + \dots + |i_r - j_r| + |i_r - j_r - 1|} \bar{V}_1 \wedge \bar{V}_2 \wedge \dots \wedge \bar{V}_k$$

✓

19  
20

Obs:  $|k| + |k-1|$  es siempre impar.

c) Dado  $V$  espacio vectorial de dimensión finita, calcular la dimensión de  $\Lambda(V)$ .

Primero veamos que el conjunto  $X$  consiste en todos los productos posibles  $x_1 \otimes \dots \otimes x_r$  en donde al menos dos se repiten. Además que los productos  $e_1 \otimes \dots \otimes e_r$  son l.i., donde  $e_i$  son vectores de la base de  $V$  (de dimensión  $n$ ). Por otro lado, el producto  $\bar{v}_1 \wedge \dots \wedge \bar{v}_r$  se puede ver de la forma<sup>(4)</sup>:

$$\bar{v}_1 \wedge \dots \wedge \bar{v}_r = \overline{e_1 \otimes \dots \otimes e_r} = e_1 \otimes \dots \otimes e_r + \langle e_1 \otimes \dots \otimes e_r / \begin{matrix} e_i = e_j \\ \text{digo } i \neq j \end{matrix} \rangle$$

También, por álgebra lineal, tenemos que si dos vectores en el espacio cociente son l.i., entonces sus representantes son l.i.. Luego basta buscar vectores l.i. en su forma de producto  $\bar{v}_1 \wedge \dots \wedge \bar{v}_r$ .

Veamos que un producto  $\bar{v}_1 \wedge \dots \wedge \bar{v}_j \wedge \bar{v}_j \wedge \dots \wedge \bar{v}_r$  no puede ser l.i. ya que  $\bar{v}_1 \wedge \dots \wedge \bar{v}_j \wedge \bar{v}_j \wedge \dots \wedge \bar{v}_r = 0$ . También, por problema anterior

$$\bar{v}_1 \wedge \dots \wedge \bar{v}_r = \pm \bar{v}_{\sigma(1)} \wedge \dots \wedge \bar{v}_{\sigma(r)}$$

Entonces basta tomar productos no repetidos y con índices ordenados de manera creciente. Como este es un ~~un~~ menor problema de conteo, se tiene que

$$\dim X_r = n^r - \binom{n}{r}$$

donde  $n^r$  son las maneras de elegir un producto de  $r$  términos con  $m$  elementos de la base y  $\binom{n}{r}$  la cantidad de productos de  $r$  términos (distintos) se puede considerar de un conjunto de  $n$  elementos. Antes de seguir, notemos que

$$\Lambda^r(V) = V^{\otimes r} / X_r$$

$$\Rightarrow \Lambda(V) = \bigoplus_{r=0}^{\infty} \Lambda^r(V)$$

Otro hecho a considerar, es que cuando  $r > n$ , el cuociente se trivializa, es decir,  $\Lambda^r(V) = 0$ , porque  $X_r$  contiene productos con elementos repetidos.

$$\therefore \dim \Lambda(V) = \sum_{r=0}^n \binom{n}{r} = 2^n$$

$$(1) \quad V \times V \xrightarrow{\otimes} V \otimes V$$

$$\downarrow f \quad \downarrow p$$

$$V \otimes V / X_2$$

$$f = p \circ \otimes$$

$p$  es la proyección canónica. Este diagrama se puede generalizar para cualquier producto  $V^{\otimes r}$ ,  $r \in \mathbb{N}$ .

### Problema 3

Sea  $D = \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) = k \oplus k_i \oplus k_j \oplus k_{ij}$ , un álgebra de cuaterniones, definida como en clases.

- (a) Sea  $L = k(i)$ . Probar que  $D = L \oplus L_j$ , y que para todo cuaternion  $q = \lambda + \mu j$  se tienen las identidades

$$\bar{q} = \bar{\lambda} - \mu j, \quad N(q) = N(\lambda) - \beta N(\mu)$$

- (b) Probar que si  $\beta$  no es la norma de un elemento en  $L$ , entonces  $D$  es un álgebra de división.
- (c) Probar que si  $\beta$  es la norma de un elemento de  $L$ , entonces  $D$  es isomorfo a un álgebra de matrices  $M_2(k)$ .

- Demostración -

- (a) Tenemos que  $i$  es raíz de  $x^2 - \alpha = 0$ , luego

$$L = k \oplus k_i$$

$$\therefore D = k \oplus k_i \oplus k_j \oplus k_{ij}$$

$$\cong (k \oplus k_i) \oplus (k \oplus k_i)j$$

$$\cong L \oplus L_j$$

Tenemos que  $q = \lambda + \mu j$ , donde  $\lambda, \mu \in L$ . Es decir

$$\lambda = \lambda_1 + \lambda_2 i$$

$$\mu = \mu_1 + \mu_2 i$$

$$\Rightarrow q = \lambda_1 + \lambda_2 i + (\mu_1 + \mu_2 i)j = \lambda_1 + \lambda_2 i + \mu_1 j + \mu_2 ij$$

$$\begin{aligned} \Rightarrow \bar{q} &= \lambda_1 - \lambda_2 i - \mu_1 j - \mu_2 ij \\ &= \lambda_1 - \lambda_2 i - (\mu_1 + \mu_2 i)j \\ &= \bar{\lambda} - \bar{\mu} j \end{aligned}$$

$$N(q) = q\bar{q} = (\lambda_1 + \lambda_2 i + \mu_1 j + \mu_2 ij)(\lambda_1 - \lambda_2 i - \mu_1 j - \mu_2 ij)$$

$$= \lambda_1^2 - \lambda_1 \lambda_2 i - \lambda_1 \mu_1 j - \lambda_1 \mu_2 ij$$

$$- \lambda_2 \lambda_1 i - \lambda_2^2 i^2 - \lambda_2 \mu_1 ij - \lambda_2 \mu_2 ij^2$$

$$+ \lambda_1 \mu_1 j - \lambda_2 \mu_1 ji - \mu_1^2 j^2 - \mu_1 \mu_2 jiij$$

$$- \lambda_2 \mu_2 ij - \lambda_2 \mu_2 iji - \mu_1 \mu_2 ij^2 - \mu_2^2 ijiij$$

$$= \lambda_1^2 - \lambda_2^2 i^2 - \mu_1^2 j^2 - \mu_2^2 ijiij$$

$$= \lambda_1^2 - \lambda_2^2 \alpha - \mu_1^2 \beta + \mu_2^2 i^2 j^2$$

$$= \lambda_1^2 - \lambda_2^2 \alpha - \mu_1^2 \beta + \mu_2^2 \alpha \beta$$

$$= \lambda_1^2 - \lambda_2^2 \alpha - \beta(\mu_1^2 - \mu_2^2 \alpha) = N(\lambda) - \beta N(\mu) \quad \checkmark$$

$$\boxed{iij = -ji}$$

(b) Por contraposición lógica. Supongamos que  $D$  no es un álgebra de división, entonces existe  $q \in D$ ,  $q \neq 0$  y

$$N(q) = 0$$

pero

$$N(q) = N(\lambda) - \beta N(\mu) = 0$$

Afirmamos que  $N(\lambda), N(\mu) \neq 0$ , ya que en caso contrario

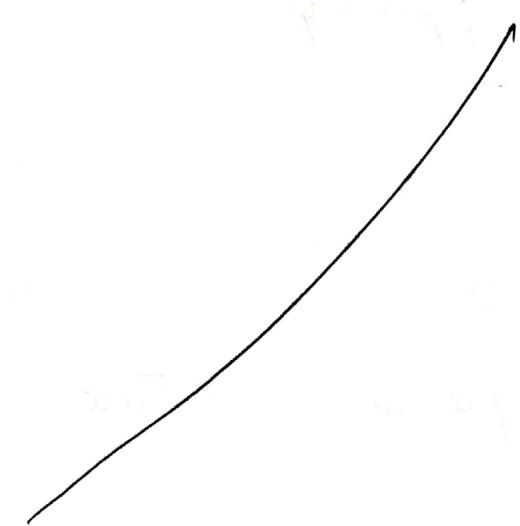
$$\begin{aligned} & \lambda, \mu = 0 \\ \Rightarrow & q = 0 \quad (\Leftrightarrow) \end{aligned}$$

Asumiendo lo anterior

$$\begin{aligned} \beta &= \frac{N(\lambda)}{N(\mu)} = N(\lambda) N(\mu)^{-1} \\ &= N(\lambda) N(\mu^{-1}) \\ &= N(\lambda \underbrace{\mu^{-1}}_{\in L}) \end{aligned}$$

$\therefore \beta$  es la norma de un elemento de  $L$ .

(c) Sin resolver



$$y = mx + b \quad m > 0 \quad b < 0$$

$$m = \frac{y_2 - y_1}{x_2 - x_1} > 0$$

$$(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$$

$$\text{Máximo } X = \frac{b - y_1}{m}$$

$$\text{Mínimo } X =$$

$$\frac{b - y_2}{m}$$

$$x_1 < x_2$$

• El trazo es de recta.

• La pendiente es constante.

• La recta no tiene punto de corte con el eje de las abscisas.

• La recta no tiene punto de corte con el eje de las ordenadas.

**Novena Guía de Ejercicios y tarea.  
Grupos y Anillos. Primer semestre 2012**

Entregar los ejercicios marcados con \* el miércoles 20 de junio.

- ✓ 1. \* Sea  $F$  un cuerpo y  $I = (Y^2 - X)$ ,  $J = (Y^2 - X^2)$  los ideales en  $F[X, Y]$  generados por los polinomios indicados. Demuestre que los anillos  $F[X, Y]/I$  y  $F[X, Y]/J$  no son isomorfos.

- §. 2. 1 2. Sea  $F$  un cuerpo y  $f(X) \in F[X]$  un polinomio de grado  $n \geq 1$ . Si la barra en  $\bar{g}(X)$  denota la imagen de  $g(X) \in F[X]$  en el cuociente  $F[X]/(f(X))$ , demuestre que  $\{\bar{1}, \bar{X}, \bar{X^2}, \dots, \bar{X^{n-1}}\}$  es base del  $F$ -esp. vectorial  $F[X]/(f(X))$ .

- §. 2. 2 3. Sea  $F$  un cuerpo finito de  $q$  elementos y  $f(X) \in F[X]$  un polinomio de grado  $n \geq 1$ . Muestre que  $F[X]/(f(X))$  tiene  $q^n$  elementos.

4. Sea  $F$  un cuerpo y  $f(X) \in F[X]$  un polinomio de grado  $n \geq 1$ . Demuestre que  $F[X]/(f(X))$  es cuerpo si y solo si  $f(X)$  es irreducible.

5. \* Encuentre los polinomios irreducibles de grado 4 y 5 en  $\mathbb{F}_2[x]$ . Factorice los de grado 4 en  $\mathbb{F}_4[x]$ . ( $\mathbb{F}_4$  es el cuerpo de 4 elementos, no es  $\mathbb{Z}_4$ .)

- §. 2. 3 6. \* Determine el máximo común divisor de los polinomios  $a(X) = X^5 + 2X^3 + X^2 + X + 1$  y  $b(X) = X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1$  en  $\mathbb{Q}[X]$  y escriba su resultado como combinación lineal de  $a(X)$  y  $b(X)$ .

- §. 3. 2 7. Sean  $f(X)$  y  $g(X)$  en  $\mathbb{Q}[X]$  tal que el producto  $f(X)g(X)$  pertenece a  $\mathbb{Z}[X]$ . Demuestre que el producto de cualquier coeficiente de  $f(X)$  con cualquier coeficiente de  $g(X)$  debe ser un entero.

- §. 3. 3 8. Sea  $F$  un cuerpo y  $R$  el subconjunto de polinomios en  $F[X]$  tal que el coeficiente de  $X$  es cero. Pruebe que  $R$  es un subanillo de  $F[X]$  y que  $R$  no es DFU. (Sug.:  $X^6 = (X^2)^3 = (X^3)^2$  son dos factorizaciones distintas de  $X^6$  en irreducibles).

- §. 3. 4 9. \* Sea  $R = \mathbb{Z} + X\mathbb{Q}[X]$  el conjunto de polinomios en  $\mathbb{Q}[X]$  cuyo término constante es un entero.

- a) Pruebe que  $R$  es un dominio de integridad y sus elementos invertibles son  $\pm 1$ .

- b) Pruebe que los elementos irreducibles de  $R$  son  $\pm p$  donde  $p$  es un primo en  $\mathbb{Z}$  y los polinomios  $p(X)$  que son irreducibles en  $\mathbb{Q}[X]$  con término constante  $\pm 1$ . demuestre que estos irreducibles son primos en  $R$ .

- c) Muestre que  $X$  no es el producto de irreducibles en  $R$  (en particular  $X$  no es irreducible en  $R$ ), y concluya que  $R$  no es DFU.

- d) Demuestre que  $X$  no es primo en  $R$  y describa el anillo  $R/(X)$ .

**Duodécima Guía de Ejercicios y tarea.  
Grupos y Anillos. Primer semestre 2012**

Entregar los ejercicios marcados con \* el miércoles 4 de julio.

1. \* Suponga que  $I$  es un ideal monomial con generadores monomiales  $g_1, \dots, g_m$ . Use el criterio de Buchberger para demostrar que  $\{g_1, \dots, g_m\}$  es una base de Gröbner para  $I$ .
2. \* Suponga que  $I$  es un ideal monomial en  $R = \mathbb{F}[x_1, \dots, x_n]$  y suponga que  $m_1, \dots, m_k$  es un conjunto minimal de generadores para  $I$  (es decir que ningún subconjunto propio genera  $I$ ). Demuestre que los  $m_i$  son únicos.
3. \* Fije un orden monomial en  $\mathbb{F}[x_1, \dots, x_n]$  y suponga  $g_1, \dots, g_m$  es un conjunto de generadores para el ideal  $I$ . Demuestre que si  $S(g_i, g_j) \not\equiv 0 \pmod{G}$  entonces el ideal  $(LT(g_1), \dots, LT(g_m), LT(S(g_i, g_j)))$  es estrictamente mayor que el ideal  $(LT(g_1), \dots, LT(g_m))$ . Concluya que el algoritmo de Buchberger para calcular bases de Gröbner termina en un número finito de pasos.
4. \* Muestre que  $\{x - y^3, y^5 - y^6\}$  es la base de Gröbner reducida para el ideal  $I = (x - y^3, -x^2 + xy^2)$  con respecto al orden lexicográfico definido por  $x > y$  en  $\mathbb{F}[x, y]$ .
5. \* Encuentre la base de Gröbner reducida para el ideal del ejercicio anterior con respecto al orden lexicográfico definido por  $y > x$  en  $\mathbb{F}[x, y]$ .
6. \* Demuestre que los ideales  $I = (x^2y + xy^2 - 2y, x^2 + xy - x + y^2 - 2y, xy^2 - x - y + y^3)$  y  $J = (x - y^2, xy - y, x^2 - y)$  en  $\mathbb{F}[x, y]$  son iguales

CAMI

Prueba N° 3 Grupos y Anillos  
I Semestre 2012

Resuelva 4 de las siguientes preguntas:

- Demuestre que  $\mathbb{Z}[i]$  es un dominio euclídeo.
- Enuncie el criterio de Eisenstein y úselo para demostrar que el polinomio  $y^3 + x^3y^2 + (x)y^2 + (x^2 + 1) \in \mathbb{Q}[x, y]$  es irreducible.
- Sea  $f(x) \in \mathbb{F}_3[x]$  un polinomio de grado  $n$ . Demuestre que  $\mathbb{F}_3[x]/(f(x))$  tiene  $3^n$  elementos.
- Factorice completamente el polinomio  $x^{10} + 1$  en  $\mathbb{F}_4[x]$ .
- Encuentre una base de gröbner reducida para el ideal

$$(x^2y + y^3, xy^2 - y - 1) \subseteq \mathbb{Q}[x, y]$$

usando el orden monomial que prefiera (debe especificarlo).  $x > y$ .

$$\underbrace{\mathbb{Q}[x][y]}_{\text{DE}} \quad 1025:4 \quad x^{10} + 1 \in \mathbb{F}_4[x]$$

$$z^{10} + 1$$

$$z^{10} \quad z^{5 \cdot 2} \quad z^{5 \cdot 3}$$

$$(x^2+1)(x^3+x)$$

$$x^2 (x^8 +$$

$$(x^2 + 1)(x^8 + Bx^2 + 1)$$

~~$x^{10} + 1$~~

$x^2 + 1$

$$(x^2+1) \quad \overline{(x^2+1)} \quad 6562:4 = 1640$$

$$\begin{aligned} x^2+1 &\in (\mathbb{F}_4) \\ (\Rightarrow) \quad pd &- x^2+1 \\ (x, 1) &= \boxed{(\mathbb{F}_4[x, y])} \end{aligned}$$

$$\frac{\mathbb{Q}[x]}{(x-1)} = \mathbb{Q}$$

$$\begin{array}{|c|} \hline \text{Zapato} \\ \hline (x^2+1)(x) \\ \hline \end{array}$$

semestre Oficios.

# Algebra Lineal

17. 10. 2012.

Práctica N° 3

Nombre  
Marco Godoy Valdebenito

Tiempo 90 minutos.

~~1 5 5  
2 4  
3 3  
4 1 5~~

$$\varphi(v, w) = \sum_{i=1}^n \alpha_i \beta_j \varphi(v_i, w_j)$$

$$+ \beta_{j+1} \varphi(v_i, w_{j+1})$$

1. Sea  $\varphi : V \times W \rightarrow K$  una forma bilineal definida para los  $K$ -espacios vectoriales

$V$  y  $W$ , de dimensiones finitas.

a) Si  $\dim V < \dim W$ , demuestre que existe  $\vec{w}_0 \neq \vec{0} \in W$  tal que  $\varphi(\vec{v}, \vec{w}_0) = 0 \forall \vec{v} \in V$

b) Demuestre que si  $\varphi$  es una forma no degenerada

entonces  $\dim V = \dim W$

1.5. 2. Enuncie el recíproco de la afirmación en a)

2. ¿Es verdadera? Justificar

Desarrollo.

a) Para  $\varphi(\vec{v}, \vec{w})$  bilineal, fijando  $\vec{w}$  sabemos que se define un funcional lineal  $f_{\vec{w}} : V \rightarrow K \in V^*$ . Entonces cada  $\vec{w} \in W$  define un elemento en  $V^*$  dado por la función  $f_{\vec{w}} : \vec{v} \in V \mapsto \varphi(\vec{v}, \vec{w}) \in K$ .

Como  $\dim V < \dim W$  entonces la función no es un isomorfismo

$$\varphi(\vec{v}, \vec{w}) = \sum_{i=1}^n \alpha_i \beta_i \varphi(v_i, w_i) + \sum_{i=n+1}^{m+1} \beta_i \varphi(v_i, w_i)$$

El teorema de la dimensión nos dice que  $\dim W = \dim \ker f + \dim \text{Im } f$  pero como  $\dim \text{Im } f \leq \dim V$  y  $\dim \ker f \geq 0 \Rightarrow$

Por lo tanto existe  $\vec{w}_0 \neq \vec{0} \in W$  tal que  $L(\vec{w}_0) = 0$   
 Si  $L(\vec{w}_0) = f_{\vec{w}_0} : V \rightarrow K$ ,  $f_{\vec{w}_0} = \vec{0}$  tiene la  
 forma  $f_{\vec{w}_0} + \vec{v} = \varphi(\vec{v}, \vec{w}_0) = 0$   $\forall \vec{v} \in V$

Para que  $\varphi$  sea una forma bilineal no degenerada, entonces  
 $\forall \vec{v} \in V$  tal que  $\varphi(\vec{v}, \vec{w}_0) = 0$ ,  $\vec{w}_0 = \vec{0}$ . En otras palabras,  
 $\forall \vec{w} \in W$  implicó que  $L$  es inyectiva. Por otro lado, podemos  
 hacer el análogo  $R : V \rightarrow W^*$  que satisface las propiedades  
 de  $L$  (TODAS), fijando  $\vec{v} \in V$ . Nuevamente, si  $\dim W < \dim V$   
 entonces  $R$  no es inyectiva, con lo que tenemos:

$$\text{Si } L \text{ es inyectiva} \Rightarrow \dim W \leq \dim V$$

$$\text{Si } R \text{ es inyectiva} \Rightarrow \dim V \leq \dim W$$

$$\therefore \dim V = \dim W$$

Enunciado recíproco: Sean  $V, W$  espacios vectoriales de dimensión finita, con  $\dim V = \dim W$ , (sobre el cuerpo  $K$ ), entonces la forma bilineal  $f : V \times W \rightarrow K$  es no degenerada. Es verdad?

Demonstración por contrapositivo. Basta ver que  $L : W \rightarrow V^*$  y  $R : V \rightarrow W^*$  ... ?

Nombre

Marco Godoy - - -

2.

La matriz de un producto escalar definido en el espacio vectorial  $\mathbb{R}^3$ , respecto de la base canónica es

$$\begin{bmatrix} 1 & 3 & 0 \\ 3 & 2 & -4 \\ 0 & -4 & 8 \end{bmatrix},$$

- ✓ a) Determine la signatura de ese producto.  
 ✓ b) Es posible hablar de base cartesiana de  $\mathbb{R}^3$  respecto de este producto escalar? Justificar

Hacemos operaciones elementales a la matriz

$$\begin{array}{c}
 \left( \begin{array}{ccc} 1 & 3 & 0 \\ 3 & 2 & -4 \\ 0 & -4 & 8 \end{array} \right) \xrightarrow{f_2 \leftarrow f_2 - 3f_1} \left( \begin{array}{ccc} 1 & 3 & 0 \\ 0 & -7 & -4 \\ 0 & -4 & 8 \end{array} \right) \xrightarrow{c_2 \leftarrow c_2 - 3c_1} \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -7 & -4 \\ 0 & -4 & 8 \end{array} \right) \\
 \xrightarrow{f_2 \leftarrow \frac{1}{\sqrt{7}}f_2} \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -\frac{1}{\sqrt{7}} & -\frac{4}{\sqrt{7}} \\ 0 & -4 & 8 \end{array} \right) \xrightarrow{c_2 \leftarrow \frac{1}{\sqrt{7}}c_2} \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & -\frac{4}{\sqrt{7}} \\ 0 & -\frac{4}{\sqrt{7}} & 8 \end{array} \right) \\
 \xrightarrow{c_3 \leftarrow c_3 - \frac{4}{\sqrt{7}}f_2} \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & -\frac{4}{\sqrt{7}} & \frac{72}{\sqrt{7}} \end{array} \right) \xrightarrow{f_3 \leftarrow -\frac{4}{\sqrt{7}}f_2} \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \frac{72}{\sqrt{7}} \end{array} \right) \\
 \xrightarrow{f_3 \leftarrow \frac{\sqrt{7}}{\sqrt{72}}f_3} \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{array} \right) \xrightarrow{c_3 \leftarrow \frac{\sqrt{7}}{\sqrt{72}}c_3} \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{array} \right)
 \end{array}$$

La signatura de la matriz es 1 ✓

Respuesta (b)

Como la matriz contiene un -1 dentro de sus entradas diagonales y como esta representación es única (salvo cambio de orden) entonces para cualquier base  $B = \{\vec{v}_i / i=1,2,3\}$  de  $\mathbb{R}^3$  que diagonalice el producto escalar debe satisfacer  $g(\vec{v}_i, \vec{v}_i) = -1$  para algún  $i = 1, 2, 3$  (donde  $g$  es el producto escalar). Por lo tanto no podemos hablar de base cartesiana en esta ocasión.

2

Nombre:

Marco Godoy

3.

En  $\mathbb{C}^3$ , la matriz de una forma hermitiana en la base (ordenada)  $\{\hat{e}_1 = (1, 0, 0), \hat{e}_1 + \hat{e}_2 = (1, 1, 0), \hat{e}_3 + \hat{e}_2 + \hat{e}_3 = (1, 1, 1)\}$

esta dada por

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

- a) Determine la colección de vectores isotrópicos  
b) Si a ese colección le agrega el vector  $\vec{0}$  es la nueva colección un subespacio vectorial de  $\mathbb{C}^3$ .

Desarrollo.

a) Tenemos que: Sea  $g: \mathbb{C}^3 \times \mathbb{C}^3 \rightarrow \mathbb{C}$  una forma hermitiana que satisface los enunciados anteriores.

Isotropos

$$g(\hat{e}_1, \hat{e}_1) = 1$$

$$g(\hat{e}_1 + \hat{e}_2, \hat{e}_1 + \hat{e}_2) = g(\hat{e}_1, \hat{e}_1) + g(\hat{e}_1, \hat{e}_2) + g(\hat{e}_2, \hat{e}_1) + g(\hat{e}_2, \hat{e}_2) = 0 + g(\hat{e}_1, \hat{e}_2) + \overline{g(\hat{e}_1, \hat{e}_2)} + 1 = 1$$

$$g(\hat{e}_1 + \hat{e}_2 + \hat{e}_3, \hat{e}_1 + \hat{e}_2 + \hat{e}_3) = g(\hat{e}_1, \hat{e}_1 + \hat{e}_2 + \hat{e}_3) + g(\hat{e}_2, \hat{e}_1 + \hat{e}_2 + \hat{e}_3) + g(\hat{e}_3, \hat{e}_1 + \hat{e}_2 + \hat{e}_3)$$

$$= g(\hat{e}_1, \hat{e}_1) + g(\hat{e}_1, \hat{e}_2) + g(\hat{e}_1, \hat{e}_3) + g(\hat{e}_2, \hat{e}_1) + g(\hat{e}_2, \hat{e}_2) + g(\hat{e}_2, \hat{e}_3) + g(\hat{e}_3, \hat{e}_1) + g(\hat{e}_3, \hat{e}_2) + g(\hat{e}_3, \hat{e}_3) = 1 + 0 + 0 + 0 + 1 + 0 + 0 + 0 + 1 = 3$$

$$\left\{ \begin{array}{l} g(\hat{e}_1 + \hat{e}_2, \hat{e}_2) = 1 \\ g(\hat{e}_1, \hat{e}_1) = 1 \end{array} \right.$$

$$g(\hat{e}_2 + \hat{e}_3, \hat{e}_1 + \hat{e}_2 + \hat{e}_3) = -1$$

Departamento de Matemáticas  
2º Semestre 2011  
Licenciatura Matemáticas  
Estructuras Algebraicas

~~1~~  
~~2~~  
~~3~~  
~~4~~  
~~5~~

Prueba nº 2

Tiempo (90 minutos) Nombre..... Marco Godoy Valdebenito

1. Sea  $(A, +, \cdot)$  un anillo conmutativo con unidad 1 ( $\neq 0$ ).

Definir para  $n \geq 1$  el símbolo  $U_n$  como la suma  $1+1+\dots+1$  de  $n$  sumandos iguales al 1. Suponga que existen enteros  $r$  tal que  $U_r = 0$  y que cierto  $s > 1$  es el menor entero positivo tal que  $U_s = 0$ .

- a) Considere la afirmación:  $s$  es un número primo.

Demuestre esa afirmación o de un contraejemplo de ella e indique alguna hipótesis adicional sobre el anillo para que sea verdadera.

- b)  $\{U_1, U_2, \dots, U_s\}$  es un grupo respecto de la operación  $+$  del anillo  $A$ .

Demostración,

Por hipótesis,  $\forall n \geq 1$ ,  $U_n = \underbrace{1+1+\dots+1}_{n-\text{veces}}$

Sea  $s > 1$  (el más pequeño) tal que  $U_s = 0$

Por demostrar que  $s$  es primo.

Supongamos que  $s = s_1 s_2$  ( $s_1, s_2 \leq s$ ,  $s_1, s_2 \neq 1$ )

$$U_s = U_{s_1 s_2} = \underbrace{1+1+1+\dots+1}_{s_1 s_2 - \text{veces}} = (\underbrace{1+\dots+1}_{s_1 - \text{veces}})(\underbrace{1+1+\dots+1}_{s_2 - \text{veces}}) \\ = U_{s_1} U_{s_2} = 0$$

Podemos tomar como ejemplo el anillo  $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$  donde  $6 \cdot 1 = 1+1+1+1+1+1 = 0$ , y además  $6 = 2 \cdot 3 = 0$ .

En este caso  $\mathbb{Z}_6$  es anillo conmutativo con unidad, y 6 es el menor número  $\geq 1$  que satisface  $6 \cdot 1 = 0$

Como hipótesis adicional, podemos pedir que  $(A, +, \cdot)$  sea dominio de integridad, así

$$U_S = U_{S_1} U_{S_2} = 0$$

(Continuación de la demostración)

$$\therefore U_{S_1} = 0 \quad \text{o} \quad U_{S_2} = 0 \quad (\Rightarrow \Leftarrow)$$

$\therefore S$  es número primo



(b) Por demostrar que  $\{U_1, U_2, \dots, U_s\}$  es grupo respecto a  $+$ .  
Demostración. Sea  $\mathcal{C} = \{U_1, U_2, \dots, U_s\}$ . Evidentemente  $\mathcal{C} \neq \emptyset$  ya que  $U_S \in \mathcal{C}$

Sean  $a, b \in \mathcal{C} : a = U_r, b = U_{\tilde{r}}$  viéndose  $r, \tilde{r} \leq s$

$$\Rightarrow a+b = U_r + U_{\tilde{r}} = \underbrace{(1+\dots+1)}_{r-\text{veces}} + \underbrace{(1+\dots+1)}_{\tilde{r}-\text{veces}} = \underbrace{1+1+\dots+1}_{r+\tilde{r}-\text{veces}}$$

$$= U_{r+\tilde{r}}$$

$\therefore r+\tilde{r} \leq s$ , entonces  $U_{r+\tilde{r}} \in \mathcal{C}$

$\therefore r+\tilde{r}=0$ , entonces  $U_{r+\tilde{r}} = U_s = 0 \in \mathcal{C}$

$\therefore r+\tilde{r}>0$ , entonces  $U_{r+\tilde{r}} = U_{s-(r+\tilde{r})}$ , donde  $s-(r+\tilde{r}) < s$   
 $\therefore U_{r+\tilde{r}} \in \mathcal{C}$

Para  $a \in \mathcal{C}$ ,  $a = U_r$  sabemos que  $U_r + U_{s-r} = U_s = 0$   
donde  $U_{s-r} \in \mathcal{C}$ , tomando  $-a = U_{s-r}$  vemos que  $-a \in \mathcal{C}$

$$\therefore \mathcal{C} \leq A$$

$\therefore \mathcal{C}$  es un grupo con respecto a  $+$

2. Considere el anillo  $(\mathbb{Z}, +, \cdot)$  de los enteros con la suma y el producto usual. Si en  $\mathbb{Z}$  se definen las operaciones  $\star, \diamond$  como sigue:

$$a \star b = a + b - 1 \quad +$$

$$a \diamond b = a + b - a \cdot b \quad \cdot$$

entonces  $\mathbb{Z}$ , con esas operaciones, también tiene estructura de anillo ¡no lo demuestre!

Considere la afirmación: ambos estructuras de anillo sobre  $\mathbb{Z}$  son isomorfas, ¿es verdadera o falsa? Demuestre que es verdadera o de una razón justificada para afirmar que es falsa.

Demonstración

Sea  $f$  un homomorfismo entre  $(\mathbb{Z}, +, \cdot)$  y  $(\mathbb{Z}, \star, \diamond)$   
 entonces  $\forall a, b \in \mathbb{Z}$ ;  $f(a+b) = f(a) \star f(b)$ ,  $f(a \cdot b) = f(a) \diamond f(b)$

$$f(a+b) = f(a) \star f(b) = f(a) + f(b) - 1$$

$$\underline{f(a \cdot b) = f(a) \diamond f(b) = f(a) + f(b) - f(a) \cdot f(b)}$$

Por condición, debe cumplirse que  $f(0) = 0_a$ ,  $f(-a) = -a \quad \forall a \in \mathbb{Z}$   
 para  $b=0$ :  $f(a+0) = f(a+0) = f(a) + f(0) - 1 = f(a) - 1$   
 pero  $f(a+0) = f(a) \quad \therefore f(a) = f(a) - 1 \quad \therefore 1 = 0 \Leftrightarrow$

Lo anterior quiere decir que si existiera un homomorfismo  $f$  entre  $(\mathbb{Z}, +, \cdot)$  y  $(\mathbb{Z}, \star, \diamond)$  se tendría  $1 = 0$   
 pero en la estructura de anillo  $(\mathbb{Z}, +, \cdot)$  el elemento neutro para la suma "0" es siempre distinto al elemento unidad "1"

3. Escoger uno de los siguientes

a) Resolver en  $\mathbb{Z}$ .

$$\begin{cases} -x \equiv 1 \pmod{3} \\ 3x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{7} \end{cases}$$

b) Resolver en  $\mathbb{Q}[x]$ .  $\begin{cases} p(x) \equiv x^2 + x + 1 \pmod{x^2 + 1} \\ p(x) \equiv x - 1 \pmod{x^2 + 2} \end{cases}$

Desarrollo

$$(b) \begin{cases} p(x) \equiv x^2 + x + 1 \pmod{x^2 + 1} \\ p(x) \equiv x - 1 \pmod{x^2 + 2} \end{cases}$$

$$p(x) \equiv x - 1 \pmod{x^2 + 2} \Rightarrow p(x) = x - 1 + (x^2 + 2)q(x), \text{ cierto } q(x) \in \mathbb{Q}[x]$$

completando en la primera ecuación

$$x - 1 + (x^2 + 2)q(x) \equiv x^2 + x + 1 \pmod{x^2 + 1}$$

$$(x^2 + 2)q(x) \equiv x^2 + 2 \pmod{x^2 + 1}$$

$$(x^2 + 2)q(x) \equiv 1 \pmod{x^2 + 1}$$

X como  
dividendo  
de 1 en 0

$$1 \equiv (x^2 + 2)q(x) \pmod{x^2 + 1}$$

$$1 \equiv (x^2 + 1)q(x) + q(x) \pmod{x^2 + 1}$$

$$1 \equiv q(x) \pmod{x^2 + 1}$$

$$\Rightarrow 1 = q(x) + (x^2 + 1)\tilde{q}(x), \text{ cierto } \tilde{q}(x) \in \mathbb{Q}[x]$$

$$(x^2 + 2) = (x^2 + 2)q(x) + (x^2 + 1)(x^2 + 2)\tilde{q}(x)$$

$$(x^2 + 2) = p(x) - x + 1 + (x^2 + 1)(x^2 + 2)\tilde{q}(x)$$

$$\therefore x^2 + 2 \equiv p(x) - x + 1 \pmod{(x^2 + 1)(x^2 + 2)}$$

$$\begin{array}{c} x^2 + x + 1 \equiv p(x) \pmod{(x^2 + 1)(x^2 + 2)} \\ \hline \therefore p(x) \equiv x^2 + x + 1 \pmod{(x^2 + 1)(x^2 + 2)} \end{array}$$

4. a) De un ejemplo de un anillo  $A$  y dos de sus ideales  $I, J$  tales que

$$I \cdot J \subset I \cap J \subset I, J \subset I + J \subset A$$

- b) Determine cuántos polinomios monicos irreducibles de grado 4 existen en  $\mathbb{F}_3[x]$

Desarrollo.

$$\text{Sea } A = \mathbb{Z}, \quad I = 3\mathbb{Z} = \{3n \mid n \in \mathbb{Z}\}$$

$$J = 6\mathbb{Z} = \{6m \mid m \in \mathbb{Z}\}$$

Evidentemente  $(\mathbb{Z}, +, \cdot)$  anillo y  $2\mathbb{Z}, 6\mathbb{Z} \leq \mathbb{Z}$

$$I \cdot J = \left\{ \sum_{i=1}^r a_i b_i \mid a_i \in 2\mathbb{Z}, b_i \in 6\mathbb{Z}; r \in \mathbb{N} \right\}$$

$$= \left\{ \sum_{i=1}^r (3n_i)(6m_i) \mid 3n_i \in 3\mathbb{Z}, 6m_i \in 6\mathbb{Z}, r \in \mathbb{N} \right\}$$

$$= \left\{ \sum_{i=1}^r 18p_i \mid p_i \in \mathbb{Z}, r \in \mathbb{N} \right\} = 18\mathbb{Z}$$

$$I \cap J = 3\mathbb{Z} \cap 6\mathbb{Z} = 6\mathbb{Z}$$

$$I + J = 3\mathbb{Z} + 6\mathbb{Z} = \{3n + 6m \mid n, m \in \mathbb{Z}\}$$

Evidentemente se tiene que

$$18\mathbb{Z} \subset 6\mathbb{Z} \subset 3\mathbb{Z}, 6\mathbb{Z} \subset 3\mathbb{Z} + 6\mathbb{Z} = \mathbb{Z}$$

(b) Sea  $\mathbb{F}_3[x]$  anillo de polinomios con coeficientes en  $\mathbb{F}_3 = \{0, 1, 2\}$

Sea  $p(x) \in \mathbb{F}_3[x]$  un polinomio monico,  $\deg(p(x))=4$ , ✓ verdadero

$$\text{o sea, } p(x) = x^4 + ax^3 + bx^2 + cx + d$$

$x$	$x^2$	$x^3$	$x^4$
0	0	0	0
1	1	1	1
2	1	2	1

Tipos de factorizaciones

$$(x+a)^3(x+\beta)^2 \quad (x+a)(x+\beta)(x^2+mx+\sigma)$$

$$x+a \quad x+\beta \quad x^2+mx+\sigma \quad \text{verdadero}$$

$$(x+\alpha)^2(x^2+nx+\beta)$$

$$\dots$$

Supongamos que

$$\begin{aligned} x^4 + ax^3 + bx^2 + cx + d &= (ax + \beta)(bx^3 + dx^2 + px + r) \\ &= ax^4 + \cancel{\alpha}x^3 + \cancel{\alpha}px^2 + \cancel{\alpha}rx + \cancel{\beta}x^3 + \cancel{\beta}dx^2 + \cancel{\beta}px + \cancel{\beta}r \\ &= ax^4 + (\cancel{\alpha} + \beta)x^3 + (\alpha p + \beta d)x^2 + (\alpha r + \beta p)x + \beta r \end{aligned}$$

$$\begin{aligned} x^4 + ax^3 + bx^2 + cx + d &= (mx^2 + nx + \sigma)(px^2 + qx + r) \\ &= mp x^4 + mq x^3 + mr x^2 + np x^3 + nq x^2 + nr x \\ &\quad + \sigma px^2 + \sigma qx + \sigma r \\ &= mp x^4 + (mq + np)x^3 + (mr + nq + \sigma p)x^2 \\ &\quad + (\sigma q + nr)x + \sigma r \end{aligned}$$

Con lo anterior

$$\begin{cases} \alpha = m \\ \alpha + \beta = a \\ \alpha p + \beta d = b \\ \alpha r + \beta p = c \\ \beta r = d \end{cases}$$

$$\begin{cases} mp = 1 \\ mq + np = a \\ mr + nq + \sigma p = b \\ \sigma q + nr = c \\ \sigma r = d \end{cases}$$

$$(\sqrt{2})^4 = 2^2 = 4$$

$$\sqrt{2} \text{ es raíz de } 5x^4 - 11x^2 + 2$$

5

5. Determinar un menor cuerpo  $F$ , contenido en el cuerpo de los números reales, que permite factorizar al polinomio  $5x^4 - 11x^2 + 2$  en polinomios de  $F[x]$  de primer grado. ¿Puede afirmar que ese polinomio es irreducible sobre el cuerpo de los números racionales? Justifique su respuesta.

Desarrollo.

Sea el cuerpo  $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} / a, b \in \mathbb{Q}\}$ , entonces en  $\mathbb{Q}(\sqrt{2})[x]: 5x^4 - 11x^2 + 2 = (x - \sqrt{2})(5x^3 + 5\sqrt{2}x^2 - x - \sqrt{2})$ .

En efecto:

$$(x - \sqrt{2})(5x^3 + 5\sqrt{2}x^2 - x - \sqrt{2}) = 5x^4 + 5\sqrt{2}x^3 - x^2 - \sqrt{2}x \\ - 5\sqrt{2}x^3 - 10x^2 + \sqrt{2}x + 2 \\ = 5x^4 - 11x^2 + 2$$

$$5x^3 + 5\sqrt{2}x^2 - x - \sqrt{2} : x + \sqrt{2} = 5x^2 - 1$$

$$\begin{array}{r} 5x^3 + 5\sqrt{2}x^2 \\ \hline -x - \sqrt{2} \\ \hline -x - \sqrt{2} \\ \hline 0 \end{array}$$

$$\therefore 5x^3 + 5\sqrt{2}x^2 - x - \sqrt{2} = (x + \sqrt{2})(5x^2 - 1)$$

$$\therefore 5x^4 - 11x^2 + 2 = (x - \sqrt{2})(x + \sqrt{2})(5x^2 - 1)$$

$$\text{Además: } 5x^2 - 1 : x - \frac{\sqrt{5}}{5} = 5x + \sqrt{5}$$

$$\begin{array}{r} 5x^2 - \sqrt{5}x \\ \hline \sqrt{5}x - 1 \\ \hline \sqrt{5}x - 1 \\ \hline 0 \end{array}$$

$$\therefore 5x^4 - 11x^2 + 2 = (x - \sqrt{2})(x + \sqrt{2})(x - \frac{\sqrt{5}}{5})(5x + \sqrt{5})$$

donde la última factorización se hizo en  $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} / a, b \in \mathbb{Q}\}$