

Por lo tanto, el cuerpo más pequeño donde se puede factorizar $5x^4 - 11x^2 + 2$ es en el cuerpo que contiene a $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{5})$. Tal cuerpo es $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{5})$ y viene dado por

$$\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{5}) = \{ a + b\sqrt{2} + c\sqrt{5} \mid a, b, c \in \mathbb{Q} \}$$

$\sqrt{2}\sqrt{5}?$

¡es cuerpo!

i) $5x^4 - 11x^2 + 2$ es reducible en \mathbb{Q} ?

Sa $y = x^2$ entonces $p(y) = 5y^2 - 11y + 2$. Como en \mathbb{Q} se puede dividir por 2 podemos usar fórmula de 2º grado

$$\Delta = 121 - 40 \quad \text{no es cuadrado perfecto}$$

i. $p(y)$ no se puede reducir en \mathbb{Q}

ii. $p(x)$ no se puede reducir en \mathbb{Q} .

Ejercicios nº1

1. Demuestre que en \mathbb{N} no existen dos operaciones distintas $+$ y $\bar{+}$ que tienen las propiedades mencionadas para la suma en \mathbb{N} .
 2. Demuestre que en \mathbb{N} no existen dos operaciones distintas \cdot y $\bar{\cdot}$ que tienen las propiedades mencionadas para la multiplicación en \mathbb{N} .
 3. Demuestre que en \mathbb{N} la operación $+$ satisface las siguientes propiedades:
 - a) $a + b \neq b \forall a, b \in \mathbb{N}$
 - b) $+$ es asociativa y conmutativa.
 - c) $a + b = a + c \Rightarrow b = c$
 4. Demuestre que en \mathbb{N} la operación \cdot satisface las siguientes propiedades:
 - a) $a \neq 1 \Rightarrow a \cdot b \neq b \forall b \in \mathbb{N}$
 - b) \cdot es asociativa y conmutativa.
 - c) $a \cdot b = a \cdot c \Rightarrow b = c$
 - d) $a(b + c) = a \cdot b + a \cdot c$
 5. Demuestre que dados dos números naturales a, b se verifica uno y solo uno de los siguientes casos: (i) $a = b$, (ii) existe $x \in \mathbb{N}$ tal que $b = a + x$, (iii) existe $y \in \mathbb{N}$ tal que $a = b + y$.
 6. Demuestre que en todo conjunto no vacío S de números naturales existe uno menor que todos los otros números de S (si existen).
 7. Demuestre que $a + c < b + c \Leftrightarrow b < c$ y que $a \cdot c < b \cdot c \Leftrightarrow b < c$ para a, b, c números naturales.
 8. Demuestre que hay una correspondencia biunívoca entre los números naturales y los enteros de la forma $(a + n, n)$. Observe que $(a + n, n) = (b + m, m) \Rightarrow a = b$. $\varphi(a) = [a+n]$
 9. Demuestre que hay una correspondencia biunívoca entre los números naturales y los enteros de la forma $(b, b + n)$.
- ¿Qué le sugieren los últimos dos ejercicios?
10. En el conjunto \mathbb{Z} se define $(a, b) - (c, d) = (a + d, b + c)$. ¿Se puede afirmar que esta igualdad define una operación en \mathbb{Z} ? Si es así estudie propiedades de esta operación.
 11. Demuestre que en \mathbb{Z} se cumple $a \cdot (b + c) = a \cdot b + a \cdot c$.
 12. Demuestre el algoritmo de la división en \mathbb{Z} , esto es, dados $a, b \in \mathbb{Z}, b > 0$ existen enteros $q, r \in \mathbb{Z}, a = bq + r$ y $0 \leq r < b$.

Departamento de Matemáticas
2º Semestre 2011
Licenciatura Matemáticas

Estructuras Algebraicas

Semana nº2: Introducción a la teoría de los grupos.

1. Conjuntos que tienen una operación asociativa, con elemento neutro único y cada elemento tiene un único inverso.
2. Conjuntos con operaciones asociativas, con al menos un neutro por la derecha, digamos e , y cada elemento g tiene al menos un e -inverso por la derecha, es decir, hay g' talque $gg' = e$.
3. Conjuntos con operaciones asociativas que satisfacen las leyes de cancelación, a la derecha y a la izquierda, $\alpha \cdot x = \beta \cdot x \Rightarrow \alpha = \beta$ y $x \cdot \alpha = x \cdot \beta \Rightarrow \alpha = \beta$ y cada una de las ecuaciones $\alpha x = \beta$ y $y\alpha = \beta$ tienen al menos una solución.
4. Para elementos g, g_1, g_2, \dots, g_n de un grupo se tienen:

$$(g^{-1})^{-1} = g$$

$$(g_1 \cdot g_2 \cdot \dots \cdot g_n)^{-1} = (g_n)^{-1} \cdot g_{n-1}^{-1} \cdot \dots \cdot g_1^{-1}$$

5. Subgrupos de un grupo, esto es, subconjuntos de un grupo con la estructura de grupo, respecto de la misma operación del grupo.
6. Grupos cíclicos.
7. Relaciones de equivalencia en un grupo G a partir de un subgrupo S de él: $g \sim h \Leftrightarrow g \cdot h^{-1} \in S$. Condición que debe cumplir una relación de equivalencia para que sea definida por un subgrupo de la manera anterior.
8. Orden e índice de un subgrupo. Teorema de Lagrange. Todo subgrupo del grupo de los enteros es cíclico y consiste de los múltiplos de un entero.
9. El grupo de las permutaciones de un conjunto finito de elementos.

Ejercicios n°2

- Demuestre que en un grupo G , las ecuaciones $a \cdot x = b$ y $y \cdot a = b$ tienen solución para todo par de elementos a y b de G . ¿Qué puede decir sobre la unicidad de estas soluciones?
- Suponga que en un conjunto G está definida una operación \cdot asociativa y tal que para todo par de elementos a y b de G las ecuaciones $a \cdot x = b$ y $y \cdot a = b$ tienen solución. ¿Puede afirmar que esta operación da una estructura de grupo al conjunto G ?
- Demuestre: El conjunto de números racionales $\{\frac{1}{n!}n \in N\}$ genera a cualquier número racional.
- Considere la tabla de multiplicación $*$ en el conjunto $\{e, a, b, c\}$

*	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

¿Es esta multiplicación una multiplicación de grupo para el conjunto $\{e, a, b, c\}$.

- Veamos "el álgebra" de subgrupos de un grupo. Sea G un grupo y S la colección de todos los subgrupos del grupo G . ¿Para qué operaciones entre los conjuntos de esos subgrupos es cerrado esta colección?
- Considere el grupo de permutaciones de n objetos y su subgrupo de las permutaciones pares. (se denotará por A_n). Cuántas clases laterales izquierdas define este subgrupo?
- Si el número de clases laterales de un subgrupo S en el grupo G es n demuestre que si T es otro subgrupo de G que contiene al subgrupo S define un número menor que n de clases laterales en el grupo G . Si ese número es m qué relación satisfacen n y m ?
- Si G es un grupo y S es uno de sus subgrupos, definir el conjunto $C_G(S) = \{x \in G / xsx^{-1} = s \forall s \in S\}$. Demuestre que $C_G(S)$ es un subgrupo del grupo G , ¿qué relación tiene este subgrupo con el subgrupo S ?
- Si G es un grupo y S es uno de sus subgrupos, definir el conjunto $\bar{S} = \{x \in G / xsx^{-1} \in S \forall s \in S\}$. Demuestre que \bar{S} es un subgrupo del grupo G que contiene a S .

10. Considere el conjunto G de todas las matrices de 2×2 sobre los números reales

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Demuestre que G es un grupo. Determine subgrupos de este grupo.

11. Considere el conjunto T de todas las matrices de 2×2 generadas por las multiplicaciones de las matrices

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

Demuestre que T es un grupo que tiene solo 8 elementos y no es conmutativo. Determine subgrupos de este grupo.

12. Considere el conjunto D de todas las matrices de 2×2 generadas por las multiplicaciones de las matrices con coeficientes números complejos dadas por

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \text{ donde } \alpha = e^{\frac{2\pi i}{k}} \text{ y } k \text{ es un número entero positivo. Demuestre que } T \text{ es un grupo que tiene solo } 2k \text{ elementos y no es conmutativo para cada } k > 2. \text{ Determine subgrupos de este grupo.}$$

13. Si H es un subgrupo propio de un grupo finito G , demuestre que existen elementos en G tales que no están en ninguno de los subgrupos de la forma gHg^{-1} cualquiera sea el elemento $g \in G$

14. Si G es el grupo de todas las permutaciones del conjunto $\{1, 2, 3, 4, 5\}$ determine todas las clases de equivalencia definidas por la relación de equivalencia $g \sim h \leftrightarrow \exists x \in G$ tal que $xgx^{-1} = h$.

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

Departamento de Matemáticas
2º Semestre 2011
Licenciatura Matemáticas

Estructuras Algebraicas

Semana nº3: Introducción a la teoría de los grupos. Continuación

1. Subgrupos normales de un grupo G . Dados un grupo G y un subgrupo S : considerar la relación de equivalencia $a \sim b \Leftrightarrow ab^{-1} \in S$. Condiciones necesarias y suficientes del subgrupo S que aseguran la "estabilidad" de la relación \sim esto es, si $a \sim b \Rightarrow \forall g \in G, ga \sim gb, ag \sim bg$.
2. El grupo cuociente G/S para un subgrupo normal del grupo G .
3. Homomorfismos entre grupos. El núcleo de un homomorfismo.
4. Teoremas de isomorfismo.
5. Orden de un grupo; orden de un elemento en un grupo. Determinación del orden de los elementos del grupo de permutaciones de n objetos.

Ejercicios nº3

1. Sea H un subgrupo normal del grupo G . Considere el grupo cuociente $G/H = \bar{G}$. Si \bar{K} es un subgrupo del grupo \bar{G} demuestre que la colección de elementos de G que conforman las distintas clases laterales de H que son elementos de \bar{K} forman un subgrupo de G . Demuestre además que esta es la única manera de formar subgrupos de \bar{G} . ¿y cómo se formaran los subgrupos normales del grupo \bar{G} ?
- ✓ 2. Sean H y K subgrupos normales del grupo G y suponga que $H \subseteq K$. Considere la función $f : G/K \rightarrow G/H$, definida por $gK \mapsto gH$.
 Demuestre que f está bien definida y que es un homomorfismo de grupos. Determine además el núcleo de este homomorfismo y demuestre que esta es una función sobre.
- ✓ 3. Si $f : G \rightarrow H$ es un homomorfismo de grupos ¿qué puede decir de $f(A \cup B)$ y de $f(A \cap B)$?
- ✓ 4. Sean A y B subgrupos de un grupo G , denotar por AB al subconjunto $a \cdot b/a \in A, b \in B$. ¿Es AB un subgrupo de G ? ¿Es $AB = BA$? *Resp. Solo si G es commutativo.*
 Sea H un subgrupo normal del grupo G . demuestre que para cualquier otro subgrupo K se tiene $HK = KH$. ¿Es HK un subgrupo de G ?

10. Considere el conjunto G de todas las matrices de 2×2 sobre los números reales

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Demuestre que G es un grupo. Determine subgrupos de este grupo.

11. Considere el conjunto T de todas las matrices de 2×2 generadas por las multiplicaciones de las matrices

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

Demuestre que T es un grupo que tiene solo 8 elementos y no es commutativo. Determine subgrupos de este grupo.

12. Considere el conjunto D de todas las matrices de 2×2 generadas por las multiplicaciones de las matrices con coeficientes números complejos dadas por

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ y $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ donde $\alpha = e^{\frac{2\pi i}{k}}$ y k es un número entero positivo. Demuestre que T es un grupo que tiene solo $2k$ elementos y no es commutativo para cada $k > 2$. Determine subgrupos de este grupo.

13. Si H es un subgrupo propio de un grupo finito G , demuestre que existen elementos en G tales que no están en ninguno de los subgrupos de la forma gHg^{-1} cualquiera sea el elemento $g \in G$

14. Si G es el grupo de todas las permutaciones del conjunto $\{1, 2, 3, 4, 5\}$ determine todas las clases de equivalencia definidas por la relación de equivalencia $g \sim h \leftrightarrow \exists x \in G$ tal que $xgx^{-1} = h$.

Departamento de Matemáticas
 2ºSemestre 2011
 Licenciatura Matemáticas

Estructuras Algebraicas: Sesión final de Grupos. Temas de trabajo adicional

1. El teorema de Sylow: En la búsqueda de subgrupos de un determinado orden tenemos la siguiente situación:

G es un grupo de orden $p^n m$ donde m es un entero relativamente primo con p . Una demostración de las siguientes afirmaciones descansa en la acción de un grupo sobre un conjunto adecuado.

- a) Existe, al menos, un subgrupo de orden p^n

Demostración: considere el conjunto S de todos los subconjuntos de G que contienen p^n elementos de G .

Este conjunto contiene $\frac{p^n m!}{p^n!(p^n-m)!}$ subconjuntos de G . Una primera observación es que este número es un número relativamente primo con p .

Ahora es claro que el grupo G actúa sobre S , por medio de la acción siguiente: $g \cdot S = \{gs/s \in S\}$. Una segunda observación indica que no todas las órbitas que el grupo G produce en S tienen una cantidad de subconjuntos igual a algún número divisible por el primo p dada la primera observación.

Si A es un subconjunto de G que produce una de esas órbitas, (que tiene un total de elementos relativamente primo con p), entonces podemos afirmar que el subconjunto de G definido por $\{g \in G : g \cdot A = A\}$ es un subgrupo que tiene p^n elementos y que denotaremos por A . Que es un subgrupo es fácil de ver y dado que su orden es $\frac{|G|}{|A|}$, que es relativamente primo con p , debe ser de la forma $p^n m_0$, con m_0 un divisor de m . Que en verdad m_0 es 1 se obtiene de considerar el conjunto $AA = \{\alpha a / \alpha \in A, a \in A\}$ que, a lo menos, contiene $|A| = p^n m_0$ elementos, pero $|A| = p^n$. De aquí entonces A es un subgrupo de p^n elementos.

- b) La colección de todos los subgrupos de p^n elementos tiene una cardinalidad que es un divisor de m y que menos 1 es divisible por p .

Para esto considere la colección de todos los subgrupos de orden p^n . Fije uno de ellos y hágalo actuar sobre la colección toda vía conjugación; esta acción produce órbitas de tamaño un múltiplo de p .

- c) Si P y Q son dos subgrupos de p^n elementos entonces hay $g \in G$ tal que $gPg^{-1} = Q$

Considere la colección de todos los subgrupos de orden p^n . Si supone la existencia de dos órbitas distintas en la acción del grupo vía conjugación obtendrá una contradicción.

2. Algunos ejercicios:

- a) Un grupo G tiene orden 15. Se puede afirmar que existe, al menos, un subgrupo que tiene 3 elementos y al menos uno, que tiene 5 elementos. Sean S y T de esos órdenes, respectivamente. ¿Cuántos de cada uno de ellos son posibles? En cada uno de los casos solo uno es posible; por lo tanto, para cada elemento g del grupo se tiene que $gSg^{-1} = S$ y $gTg^{-1} = T$, esto significa que ellos son subgrupos normales del grupo G y, por lo tanto, el grupo de orden 15 es el producto directo de estos subgrupos. Como claramente cada uno de ellos es un grupo cíclico (de orden 3 y 5, respectivamente) el grupo G es un grupo cíclico de orden 15. Un ejemplo que conocemos de un grupo de orden 15 es \mathbb{Z}_{15} . Como todos los grupos cíclicos del mismo orden son isomorfos podemos afirmar que especialmente hay solo un grupo de orden 15.
- b) Un grupo G tiene orden 6. Se puede afirmar que tiene, al menos, un subgrupo que tiene 3 elementos y al menos uno, que tiene 2 elementos. Sean S y T de esos órdenes, respectivamente. ¿Cuántos de cada uno de ellos son posibles? Es claro que solo hay uno de orden 3, y por lo tanto, debe ser un subgrupo normal. En cambio las posibilidades para los subgrupos de orden 2, que existe solo uno o existen exactamente 3. En el primer caso, este subgrupo de orden 2 debe ser normal en el grupo y en ese caso el grupo será un grupo cíclico de orden 6; un ejemplo de ello es el grupo \mathbb{Z}_6 . En el otro caso, en que existen 3 subgrupos de orden 2, observamos que el grupo de orden 6 es un grupo que consiste de los productos de los elementos de uno de orden 3 y de uno cualquiera de los elementos de un subgrupo de orden 2. Un ejemplo de esta situación es el grupo Σ_3
- c) ¿Qué puede decir de un grupo que contiene 51 elementos?

El grupo de permutaciones Σ_n

- Suponga que los números a_1, a_2, \dots, a_h son todos distintos y están en el conjunto $I_n = \{1, 2, 3, \dots, n\}$ para $n \geq h$. La permutación de Σ_n , que lleva a_1 en a_2, a_2 en a_3, \dots, a_{h-1} en a_h y a_h en a_1 y al resto de los elementos de I_n los deja fijos se denotará por el símbolo $(a_1 \ a_2 \ \dots \ a_h)$.
Demuestre que $(a_1 \ a_2 \ \dots \ a_h) = (a_1 \ a_h) \cdot (a_1 \ a_{h-1}) \cdot \dots \cdot (a_1 \ a_2)$
- La colección de todos los elementos $(a_i \ a_j) \cdot (a_k \ a_l)$ bajo la composición de permutaciones forma un subgrupo de Σ_n normal y de índice 2, denotado por el símbolo A_n
- Para $n \geq 5$ el subgrupo A_n no tiene subgrupos normales distintos de los subgrupos triviales.



2º Semestre 2010
Licenciatura Matemáticas
Estructuras Algebraicas

~~1652~~
~~2312~~

Examen nº3

Nombre..... Camillo Vera.....
Tiempo 90 minutos

1. De un ejemplo de (y justifique cada una de sus afirmaciones).
 - a) Un anillo de 25 elementos que no sea un cuerpo.
 - b) Un cuerpo de 25 elementos
 - c) Un polinomio irreducible en el anillo de polinomios en X con coeficientes en Z_3 (el cuerpo de los enteros módulo 3), y que tenga grado 3.
2. Justifique cada una de sus afirmaciones.

- 1.5 a) ¿Es constructible el número real $\alpha = \sqrt{1 + \sqrt{1 + \sqrt{2}}}$?
- 1.5 b) Determine un polinomio con coeficientes en Q del cual α es raíz.
- 1.2 c) Demuestre que en $Q(\sqrt{2})$ el número real $1 + \sqrt{2}$ no tiene raíz cuadrada.
- d) Indique la forma que tienen los números reales que están en el menor subcuerpo de los números reales que contiene a los racionales y al número $\sqrt{1 + \sqrt{2}}$)

3. Sea A un anillo comutativo con unidad.

Un elemento $a \in A$ se dice un **elemento primo** si a no es invertible y cada vez que el producto de dos elementos de A , digamos bc , está en el ideal generado por a entonces esto es por que al menos uno de esos elementos está en el ideal generado por a .

Demuestre que si a es un elemento primo de A entonces el anillo cuociente \bar{A} , (de A por el ideal generado por a), es un anillo que cumple la siguiente propiedad :

$$\forall \alpha, \beta \in \bar{A} \quad \alpha\beta = 0_{\bar{A}} \Rightarrow \alpha = 0_{\bar{A}} \quad \vee \quad \beta = 0_{\bar{A}}$$

Departamento de Matemáticas
2º Semestre 2011
Licenciatura Matemáticas

Estructuras Algebraicas

Semana nº5: Ejercicios adicionales de Grupos

1. Demuestre que no todos los subgrupos de Σ_4 , son isomorfos entre sí. Muestre un subgrupo de cada una de las "clases de isomorfía" de estos subgrupos.
2. Demuestre que todos los subgrupos de orden 2 en Σ_3 , son isomorfos entre si. Describa los isomorfismos correspondientes.
3. Considerandola relación de equivalencia $g \sim h \Leftrightarrow \exists p \in G : pgp^{-1} = h$ cualquiera sea el grupo G , demuestre que en Σ_3 , Σ_4 , y Σ_5 no hay elemento, distinto de la unidad, que esté en el centro de esos grupos, es decir, que commute con todos los elementos del grupo.
4. Demuestre que en Σ_4 hay subgrupos normales no triviales y de índice distinto de 2 pero que en Σ_5 no existen ese tipo de subgrupos.
5. Demuestre que una condición necesaria y suficiente para que el producto de dos subgrupos de un grupo sea un subgrupo es que ellos commuten, es decir, $HK = KH \Leftrightarrow HK \leq G$ para $H, K \leq G$.
- 6.

5. Considere las simetrías de un triángulo equilátero y escriba la tabla de multiplicación, cuando la multiplicación entre las simetrías es la composición de funciones.

Determine en ese grupo dos elementos x e y tales que $x^2 = y^3 = Id$, $xyx = y^{-1}$.

Justifique la afirmación: todo elemento de este grupo es de la forma xy^i o y^i

6. Considere el conjunto de las simetrías de un pentágono regular y la composición de esas simetrías. Demuestre que es un grupo que contiene 10 elementos. Determine en ese grupo dos elementos x e y tales que $x^2 = y^5 = Id$ y $xyx = y^{-1}$. Justifique la afirmación: todo elemento de este grupo es de la forma xy^i o de la forma y^i .

En los dos ejercicios anteriores determine las clases de equivalencias que se forman en ambos grupos respecto de la relación: $g \sim h \Leftrightarrow \exists x \in G : xgx^{-1} = h$. ¿Cuántos elementos tienen los centros de aquellos grupos?

7. En general, si H es un subgrupo de un grupo G la clase lateral $Hg \neq gH$. Ahora si H es un subgrupo normal del grupo G esto si es verdadero. En los ejemplos de grupos anteriores muestre ejemplos de ambas situaciones.
8. Determine el orden de la permutación siguiente, primero como elemento del grupo Σ_8 y luego como elemento del grupo Σ_{800} :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 5 & 8 & 2 & 7 \end{pmatrix}$$

9. Si un grupo es abeliano y los elementos g y h de él tienen orden m y n , respectivamente, qué puede afirmar del orden del elemento gh .

10. En Σ_5 considere los elementos $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$ y $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$. Calcule $g \cdot h$ y $h \cdot g$. Compare con el ejercicio anterior. ¿Qué puede afirmar?

11. La notación cíclica de las permutaciones.

Suponga que los números a_1, a_2, \dots, a_h son todos distintos y están en el conjunto

$I_n = \{1, 2, 3, \dots, n\}$ para $n \geq h$. La permutación de Σ_n , que lleva a_1 en a_2, a_2 en a_3, \dots, a_{h-1} en a_h y a_h en a_1 y al resto de los elementos de I_n los deja fijos se denotará por el símbolo $(a_1 \ a_2 \ \dots \ a_h)$.

Demuestre que $(a_1 \ a_2 \ \dots \ a_h) = (a_1 \ a_h) \cdot (a_1 \ a_{h-1}) \cdot \dots \cdot (a_1 \ a_2)$

Escriba la permutación inversa de una tal permutación.

12. Determine el orden del elemento $(a_1 \ a_2 \ \dots \ a_h) \quad (\text{h})$

13. Demuestre que si $\alpha = (a_1 \ a_2 \ \dots \ a_h)$ y $\beta = (b_1 \ b_2 \ \dots \ b_m)$ y ninguno de los números a_i es igual a alguno de los b_j para todos los i y j posibles entonces $\alpha \cdot \beta = \beta \cdot \alpha$.

14. Usando los ejercicios anteriores determine un método para calcular el orden de una permutación.

15. En Σ_5 se define la siguiente relación \sim entre sus elementos: $\alpha \sim \beta \Leftrightarrow \exists \gamma \in \Sigma_5 : \beta = \gamma \cdot \alpha \cdot \gamma^{-1}$. Demuestre que ésta es una relación de equivalencia en Σ_5 . Determine las clases de equivalencia que esta relación produce. ¿Qué tiene en común las permutaciones que están en una misma clase? ¿Es posible hacer la misma pregunta en cualquier otro grupo del tipo Σ_n ?
16. Si H es un subgrupo normal de un grupo G , demuestre que la clase de equivalencia χ de un elemento cualquiera del grupo, respecto de la relación de equivalencia del ejercicio anterior, satisface $\chi \cap H \subseteq H$ o es el conjunto vacío.
17. En Σ_3 , Σ_4 y Σ_5 determine los subgrupos normales.
18. Determine el orden del producto (composición) del elemento $\alpha = (a_1 \ a_2)$ y $\beta = (b_1 \ b_2)$. Análogamente, determine el orden del producto (composición) del elemento $\alpha = (a_1 \ a_2 \ a_3)$ y $\beta = (b_1 \ b_2 \ b_3)$

Ejercicios nº4

Tarea: Ejercicios 1,2 y 3. Fecha entrega: martes Dic. 13

- ✓ 1. Considere los grupos Σ_3 y Σ_4 . Demuestre que en el primero de ellos no hay dos subgrupos (no triviales) cuyo producto sea un producto directo de subgrupos y que si lo hay en el segundo grupo.
- ✓ 2. En el grupo \mathbb{Z} , de los enteros con la adición, no hay un par de subgrupos (no triviales) cuyo producto sea producto directo de ellos.
3. En Σ_4 determine que elementos forman el único subgrupo de 12 elementos que tiene este grupo. Verifique que en ese grupo no hay subgrupo de 6 elementos.
4. Dibuje un hexágono regular con dos de sus vértices en el x-eje y centro en el origen del sistema de coordenadas. Sea α la rotación, en 60° , de los puntos del plano con centro de rotación el origen del sistema. Sea β la reflexión de los puntos del plano respecto del y-eje. Determine el significado geométrico de las composiciones $\alpha \cdot \beta; \beta \cdot \alpha \cdot \beta$. Determine el orden del grupo que generan estas dos transformaciones del plano.
5. Verifique que en los grupos Σ_3 y Σ_4 , se cumple la condición sobre el número total de subgrupos de Sylow.
6. Suponga que un grupo G tiene orden 15.
 - a) Demuestre que G solo tiene un subgrupo de orden 5.
 - b) Demuestre que G solo tiene un subgrupo de orden 3.
 - c) Demuestre que G tiene exactamente 8 elementos de orden 15.
 - d) De un ejemplo concreto de un grupo que tiene 15 elementos.
7. Considere el conjunto de los símbolos $\{1, -1, i, -i, j, -j, k, -k\}$ con la multiplicación

$$i \cdot j = k; j \cdot k = i; k \cdot i = j; j \cdot i = -k; k \cdot j = -i; i \cdot k = -j$$
 el 1 es neutro y -1 "cambia los signos". Verifique que esa operación es una operación de grupo para ese conjunto. Determine la colección de subgrupos de ese grupo.
 Compare este grupo de 8 elementos con el grupo de las simetrías de un cuadrado, que también tiene 8 elementos.
8. Considere el grupo $\mathbb{Z} \times \mathbb{Z}$. Determine las colecciones de elementos de él que son subgrupos. Determine, al menos, tres copias isomorfas de \mathbb{Z} en ese grupo.

Departamento de Matemáticas
2º Semestre 2011
Licenciatura Matemáticas

Estructuras Algebraicas

Semana nº4: Introducción a la teoría de los grupos. Continuación

1. Álgebra de subgrupos de un grupo: productos e intersecciones de subgrupos. El producto directo de subgrupos de un grupo.
2. Producto directo de grupos.
3. Acción de un grupo sobre un conjunto. Acción de un grupo sobre si mismo: la conjugación y la acción regular.
4. Orbitas de una acción. Longitud de una órbita en la acción de un grupo finito.
5. Sea G un grupo de orden $p^\alpha m$: $(p, m) = 1$.
 - a) La acción por multiplicación del grupo G en la colección de subconjuntos que tienen p^α elementos. Existencia de un subgrupo grupo de orden p^α en el grupo G .
 - b) La acción por conjugación del grupo G sobre la colección de subgrupos que tienen p^α elementos. La posible cantidad de subgrupos de ese orden que tiene el grupo G .

Departamento de Matemáticas

2º Semestre 2011

Licenciatura Matemáticas

Estructuras Algebraicas: Ejercicios adicionales de Grupos

- Día*
- Demuestre que no todos los subgrupos de Σ_4 , son isomorfos entre sí. Muestre un subgrupo de cada una de las "clases de isomorfía" de estos subgrupos.
 - Demuestre que todos los subgrupos de orden 2 en Σ_3 , son isomorfos entre si. Describa los isomorfismos correspondientes.
 - Considerando la relación de equivalencia $g \sim h \Leftrightarrow \exists p \in G : pgp^{-1} = h$ cualquiera sea el grupo G , demuestre que en Σ_3 , Σ_4 , y Σ_5 no hay elemento, distinto de la unidad, que esté en el centro de esos grupos, es decir, que commute con todos los elementos del grupo.
 - Demuestre que en Σ_4 hay subgrupos normales no triviales y de índice distinto de 2 pero que en Σ_5 no existe ese tipo de subgrupos.
 - Demuestre que una condición necesaria y suficiente para que el producto de dos subgrupos de un grupo sea un subgrupo es que ellos commuten, es decir, $HK = KH \Leftrightarrow HK \leq G$ para $H, K \leq G$.
 - Sean H y K subgrupos de un grupo G . Considere la colección de elementos en el conjunto HK . Demuestre que $h_1k_1 = h_2k_2 \Leftrightarrow \exists g \in H \cap K : h_2 = h_1g^{-1}, k_2 = gk_1$. Concluya de aquí que si H y K tienen un número finito de elementos entonces $|HK| = \frac{|H||K|}{|H \cap K|}$.
 - Suponga que un grupo G está actuando sobre un conjunto S . Sea s un elemento cualquiera de S y sea O_s la órbita de s bajo G . Demuestre que
 - $\text{Fix}_s = \{g \in G : g \cdot s = s\}$ es un subgrupo del grupo G .
 - El número de clases laterales derechas (o izquierdas) de Fix_s en G es igual a $|O_s|$.
 - Sea G el conjunto de todas las transformaciones lineales biyectivas de un espacio vectorial V en si mismo. Demuestre que la órbita de un vector bajo la "acción natural" de las transformaciones sobre el espacio vectorial es $\{\vec{o}\}$ o $V - \{\vec{o}\}$.
 - Considere el producto directo de los grupos \mathbf{Z}_4 y \mathbf{Z}_6 .
 - ¿Es ese grupo isomorfo a un subgrupo de \mathbf{Z}_{24} ? Explique.
 - ¿Es ese grupo isomorfo a un subgrupo de \mathbf{Z}_{12} ? Explique.
 - Considere el conjunto $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$ provisto de la operación $\star : (a, b, c) \star (m, n, p) = (a+m, 0, c+p)$ Verifique si ese conjunto con esa estructura es un grupo.
 - El conjunto $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$ provisto de la "suma usual" es un grupo isomorfo al producto directo de los grupos $(\mathbf{Z}, +)$ y del grupo producto directo $(\mathbf{Z}, +)$ consigo mismo. Explique.
 - Todo subgrupo normal de un grupo G tiene una copia isomorfa como subgrupo normal en el producto directo $G \times H$ cualquiera sea el grupo H . Explique.

f iso debe cumplir

$$\begin{aligned} f(0, 3) &= 8 \\ f(2, 0) &= 12 \\ \text{No existe} \end{aligned}$$

Basta tomar $f: G \rightarrow G \times H$ para $N \trianglelefteq G$ hay una copia isomorfa $f(N)$ en $G \times H$ y $f(N) \trianglelefteq G \times H$

Departamento de Matemáticas
 2º Semestre 2011
 Licenciatura Matemáticas
 Estructuras Algebraicas

Anillos y Cuerpos, Parte I.

1. Conjuntos que tienen dos operaciones "que se comportan bien". Propiedades básicas. Distintos tipos de anillos: anillos conmutativos, anillos con elemento unidad, dominios de integridad, anillos de división y cuerpos.
2. Subanillos e ideales de un anillo. ¿Por qué un ideal? Anillos cuocientes.
3. Características de los anillos cuocientes según el tipo de ideal que lo produjo.
4. El lema de Zorn.
5. Relaciones de equivalencias "de buen comportamiento" en un anillo y los ideales de un anillo.
6. Clases de elementos: divisores del cero, invertibles,

Ejercicios nº6

Entregar sus soluciones de los ejercicios 1, 3 y 15 el jueves 5 de enero

1. Considere el conjunto \mathbb{Z} de los números enteros y defina las siguientes operaciones en él:
 $a \cdot b = a + b - 1$ y $a * b = a + b - ab$. ¿Qué puede decir de la estructura $\mathbb{Z}, \cdot, *$?
2. Sea I un ideal de un anillo conmutativo A . Defina la relación \sim entre los elementos del anillo como sigue: $a \sim b \Leftrightarrow a - b \in I$.
 Demuestre que la relación es una relación de equivalencia que satisface:
 $(*) : a \sim b, c \sim d \Rightarrow a + c \sim b + d; ac \sim bd, ta \sim tb \forall t \in A$.
3. Sea A un anillo conmutativo y \sim una relación de equivalencia entre sus elementos que satisface:
 $a \sim b, c \sim d \Rightarrow a + c \sim b + d; ac \sim bd$
 Demuestre que el conjunto de elementos de A que están relacionados con el 0 forman un ideal de A .
4. En el anillo \mathbb{Z}_{18} , de los enteros módulo 18 con suma y producto módulo 18 defina una relación de equivalencia que satisface la condición $(*)$.

$$I = \{\overline{0}, \overline{2}, \dots, \overline{14}, \overline{16}\} \quad \text{ideal de } \mathbb{Z}_{18}$$

definir $\forall a, b \in \mathbb{Z}_{18}, a \sim b \Leftrightarrow a - b \in I$

5. Si I y J son ideales de un anillo A demuestre que los conjuntos

$$I + J = \{x + y/x \in I, y \in J\}$$

Preguntar a Ponzi $\rightarrow IJ = \{x_1y_1 + x_2y_2 + \dots + x_r y_r / x_i \in I, y_i \in J, \forall r\}$

$$I \cap J = \{a \in A / a \in I, a \in J\}$$

son ideales del anillo A . Establezca un orden de contención entre ellos y con los ideales I y J .

$$IJ \subseteq I \cap J \subseteq I, J \subseteq I + J$$

6. Dados dos ideales del anillo Z , caracterice los ideales definidos en el ejercicio anterior.

7. En los anillos Z_{18} y Z_{25} determine sus ideales.

8. Demuestre que los elementos invertibles de un anillo forman un grupo.

9. ¿Cuántos elementos invertibles tiene el anillo Z_n ?

10. Si el anillo A es un anillo comutativo con unidad e I es un ideal maximal, respecto de inclusión, demuestre que el anillo cuociente es un cuerpo.

11. Considere el conjunto de todas las matrices de orden $n \times n$ cuyos coeficientes son números reales. Determine ideales de este anillo, tanto izquierdos, como derechos e ideales (biláteros). Ideales izquierdos: Aquellos con columna (s) b's
Ideales derechos: Aquellos con fila (s) 0's

12. Considere el conjunto C de todas las funciones continuas de R en R , ¿Es C ? un anillo respecto de las operaciones suma y composición de funciones usuales? ¿Es C ? un anillo respecto de las operaciones suma y multiplicación de funciones usuales? El subconjunto de funciones continuas que evaluadas en el 0 toman el valor 0 tiene la estructura de ideal, en alguno de los anillos que se puede formar con las funciones continuas? De un ejemplo de un elemento de C que no está en ese subconjunto de funciones continuas. ¿Cuál es el menor ideal que contiene a ese elemento que usted definió y a la colección de funciones continuas que evaluadas en el cero toman el valor 0?

13. Determine los divisores del cero del anillo Z_n .

14. ¿Puede afirmar que en un anillo con unidad si un elemento no es divisor del cero, entonces él es un elemento invertible en el anillo;? y ¿qué puede afirmar del recíproco de esa afirmación?

(\Rightarrow) falso, tomar \mathbb{Z} que es dominio integral pero los únicos invertibles son $-1, 1$

(\Leftarrow) Verdadero. Si a invertible en A , $\exists b \in A$ $a \neq 0$, $ab = 1$, sea $c \in A$ tq $ac = 0 \Rightarrow (ba)c = b0 = 0 \Rightarrow 1 \cdot c = c = 0$
 $\therefore a$ no es divisor de 0.

15. Sea D un dominio de integridad. Forme el conjunto $D \times D^*$, de todos los pares ordenados de elementos de D cuyas segundas componentes son elementos de D distintos de 0. Defina la siguiente relación entre estos elementos: $(a, b) \sim (c, d) \Leftrightarrow ad = bc$

- a) Demuestre que esta relación es una relación de equivalencia en $D \times D^*$, y denote por $\frac{a}{b}$ a la clase de equivalencia de (a, b) .
- b) Considere el conjunto de esas clases de equivalencia y defina las operaciones $+$ y \cdot como sigue:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

y

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Demuestre que el conjunto de las clase de equivalencias tiene la estructura de un anillo respecto de las operaciones $+$ y \cdot .

- c) Compare la anterior situación con la situación de los enteros y los números racionales.

terminal

Departamento de Matemáticas

2º Semestre 2011

Licenciatura Matemáticas

Estructuras Algebraicas

Anillos y Cuerpos: Continuación

1. ¿Cuáles son los equivalentes a los números enteros primos en el anillo $R[x]$? Y si en lugar de R el cuerpo es otro cuerpo K ¿es posible tener un equivalente a los números enteros primos en $K[X]$?
2. Los polinomios irreducibles y los ideales maximales en un anillo $K[x]$ cuando K es un cuerpo.
3. La descomposición de los polinomios similar a la descomposición de los enteros.
4. Algunos casos de caracterización de polinomios irreducibles.

Ejercicios nº8

Entregar sus soluciones de los ejercicios 2 y 6 el jueves 19 de enero.

En los ejercicios siguientes $K[x]$ denota el conjunto de los polinomios en x con coeficientes en un cuerpo K .

- Fail*
1. Sea $p(x)$ un polinomio de grado mayor o igual a 1, en $K[x]$ con la siguiente propiedad:
 $q(x)$ divisor de $p(x) \Rightarrow \delta q(x) = \delta p(x)$ o $q(x) \in K$.
 2. Los ideales maximales de $K[X]$ son los ideales generados por polinomios irreducibles en $K[X]$
 3. De un ejemplo de un ideal I generado por un polinomio $p(x)$ no irreducible en $R[x]$.
 \exists (nunca si $\partial(p(x)) \neq \partial(q(x))$) $f(x) = \alpha q(x)$ para $\alpha \in K$
 4. ¿Es posible tener dos polinomios distintos que generen a un mismo ideal?
 5. Escriba polinomios de grados 2 y 3 que sean irreducibles en $Q[X]$ ¿permanecen irreducibles esos polinomios si los considera como polinomios en $R[X]$?
 6. Sea $p(X)$ un polinomio irreducible en $K[X]$. Suponga que $p(X)$ es un divisor del producto de dos polinomios $a(X)$ y $b(X)$. Demuestre que $p(X)$ es un divisor de $a(X)$ o $p(X)$ es un divisor de $b(X)$. ¿Es necesaria la condición de $p(X)$ ser un polinomio irreducible?

Compare esa propiedad con una propiedad análoga a la de números primos en Z

7. Considere que el cuerpo $K = \mathbb{Z}_5$. Escriba un polinomio de grado 2 y uno de grado 3 irreducibles en ese anillo. $x^2 + x + 1, x^3 + 4x + 2, x^3 + x + 1$
 Para cada ejemplo determine los anillos cuocientes que se forman cuando considera los ideales maximales generados por esos polinomios. ¡Son únicos esos polinomios?
 En caso que escriba dos polinomios de grado 2 compare los correspondientes anillos cuocientes.
8. Considere los anillos cuocientes de $\mathbb{R}[X]$ por cada uno de los ideales generados por los polinomios $X^2 + 1, (X^2 + 1)^2$ y $X^2 + X + 1$. Enuncie afirmaciones y demuéstrelas.
9. ¿Es $x^4 + 2x^3 - x^2 + x + 6$ un polinomio irreducible? Comente.
10. Considere el polinomio $2x^3 - 5x^2 + x + 2$ en el anillo $K[x]$ cuando $K = \mathbb{Q}$ y $K = \mathbb{R}$. Díscrasa una factorización en irreducibles en los correspondientes anillos.
11. Determine el máximo común divisor de los polinomios $2x^3 - 5x^2 + x + 2$ y $x^2 + \frac{x}{2}$
12. Resolver $\begin{cases} p(x) \equiv x^2 + x + 1 \pmod{x^2 + 1} \\ p(x) \equiv x - 1 \pmod{x^2 + 2} \end{cases}$

$$\text{Para } \langle x^2 + 1 \rangle, \text{ o: } \mathbb{C} \rightarrow \mathbb{R}[x]/\langle x^2 + 1 \rangle \quad \therefore \mathbb{C} \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle$$

$$(a, b) \rightarrow a + bx + \langle x^2 + 1 \rangle$$

Departamento de Matemáticas

2ºSemestre 2011

Licenciatura Matemáticas

Estructuras Algebraicas

Anillos y Cuerpos: Continuación

1. Criterio de irreducibilidad de Eisenstein, aplicado a polinomios con coeficientes en \mathbb{Z} .
2. Cuerpos Finitos; construcción de cuerpos finitos. Cardinalidad de los cuerpos finitos.
3. Subcuerpos del cuerpo de los números reales y del cuerpo de los números complejos

Ejercicios nº9

Entregar sus soluciones de los ejercicios 9 y 13 el jueves 26 de enero.

1. Explicite los subanillos que contienen al entero 33 en el anillo \mathbb{Z} . Determine también ideal maximal (respecto de inclusión) en \mathbb{Z} que contiene a este entero, ¿hay solo uno ?
2. Considere el anillo $\mathbb{Q}[x]$ de los polinomios con coeficientes racionales, determine el mayor ideal, no trivial, que contiene al polinomio $x^3 + 2$. $I = \langle x^3 + 2 \rangle$
3. Demuestre que los anillos $\mathbb{Q}[x]$ y $\mathbb{Q}[y]$, de los polinomios en la indeterminada x y de los polinomios en la indeterminada y con coeficientes racionales, respectivamente, son anillos isomorfos, y que también lo son los anillos $\mathbb{Q}[x][y]$ y $\mathbb{Q}[y][x]$, de los polinomios en la indeterminada y con "coeficientes" en el anillo de polinomios en la indeterminada x y de los polinomios en la indeterminada x con "coeficientes" en el anillo de polinomios en la indeterminada y , respectivamente. $(\mathbb{Q}[x][y]) \cong (\mathbb{Q}[y][x])$ *ver después!*
4. Sea p un número entero primo. Considere la siguiente propiedad de los números primos en \mathbb{Z} . Si p es un divisor del producto de dos enteros a y b entonces p es un divisor de a o p es un divisor de b . ¿Puede enunciar y demostrar una propiedad similar en $K[x]$?
5. Sean a y b dos enteros positivos. Considere la siguiente propiedad de los números en \mathbb{Z} : De todos los enteros positivos de la forma $\alpha a + \beta b$ que se pueden formar con estos enteros, el menor de ellos es el máximo común divisor de a y b . ¿Puede enunciar y demostrar una propiedad similar en $K[x]$?
6. Escriba polinomios de grados 2 y 3 que sean irreducibles en $\mathbb{Q}[x]$ ¿permanecen irreducibles esos polinomios si son considerados como polinomios de $\mathbb{Q}(\sqrt{2})[x]$.

$x^2 - 2$ no es reducible en $\mathbb{Q}[x]$ pero sí en $\mathbb{Q}(\sqrt{2})[x]$: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$
 $x^3 + 2$ no es reducible en $\mathbb{Q}[x]$

7. Considere el cuerpo \mathbf{F}_5 y forme el anillo de polinomios con coeficientes en él. Escriba un polinomio de grado 2 y uno de grado 3 que sean irreducibles en ese anillo. Para cada caso determine los anillos cuocientes que se forman cuando considera los ideales maximales generados por esos polinomios. ¿Son únicos esos polinomios? $x^2 + 4x + 1$
8. Considere los cuocientes de $\mathbf{R}[X]$ por los ideales generados por los polinomios $X^2 + 1$, $(X^2 + 1)^2$ y $X^2 + X + 1$. Enuncie afirmaciones y demuéstrelas.
9. Construya un cuerpo K de 9 elementos y presente un polinomio de grado 2 que sea irreducible en $K[x]$
10. ¿Es posible que un cuerpo que tiene 27 elementos tenga un subcuerpo con 9 elementos? y uno que contiene 81 elementos ¿puede tener un subcuerpo de 9 elementos? Elabore.
11. El conjunto de números reales $\{a + b\sqrt{2}/a, b \in Q\}$ tiene la estructura de cuerpo para la suma y el producto usuales de números reales. ¿Puede exhibir este cuerpo en la forma $Q[X]/Q[X]p_0(X)$? $\{a+b\sqrt{2}/a, b \in Q\} \cong Q[\sqrt{2}]/\langle x^2 - 2 \rangle$
12. Sean K un cuerpo y L y M dos de sus subcuerpos. Considere la colección \mathbf{C} de todos los subcuerpos del cuerpo K que contienen, simultáneamente, a ambos L y M . Entonces el cuerpo más pequeño, en K , que contiene a ambos, L y M , es la intersección de todos los subcuerpos en \mathbf{C} .
13. Considere el cuerpo de los números reales \mathbf{R} y en él a los subcuerpos $\{a + b\sqrt{2}/a, b \in Q\}$ y $\{a + b\sqrt{3}/a, b \in Q\}$. Caracterice al menor subcuerpo de \mathbf{R} que contiene a ambos.
14. Considere el cuerpo de los números complejos \mathbf{C} y en él a los subcuerpos $\{a + b\sqrt{2}/a, b \in Q\}$ y $\{a + bi/a, b \in Q\}$. Caracterice al menor subcuerpo de \mathbf{R} que contiene a ambos.
15. Considere el siguiente conjunto de matrices, de entradas reales, de la forma $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. La suma y producto usual de matrices proveen a este conjunto de matrices de la estructura de cuerpo. Determine alguno de los subcuerpos de este cuerpo.
16. Considere el siguiente conjunto de matrices, de entradas reales, de la forma $\begin{pmatrix} a & b \\ -b & a+b \end{pmatrix}$. La suma y producto usual de matrices proveen a este conjunto de matrices de la estructura de cuerpo. Determine alguno de los subcuerpos de este cuerpo.

Grupos de Lie lineales: Prueba 1

16 de Diciembre de 2011

- ✓ 1. Sean $G \subseteq GL_m(\mathbb{C})$ y $H \subseteq GL_k(\mathbb{C})$ dos grupos de Lie de matrices. Se define la función $\phi : G \times H \longrightarrow GL_{m+k}(\mathbb{C})$ tal que

$$\phi(x, y) = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}.$$

Demuestre que $\phi(G \times H) \subseteq GL_{m+k}(\mathbb{C})$ es un grupo de Lie de matrices.
Demuestre que si G y H son camino-conexos, entonces $\phi(G \times H)$ es camino-conexo.

- ✓ 2. Dado dos naturales m, k defina el grupo

$$O_{m,k}(\mathbb{R}) = \{A \in M_m \mathbb{R} \mid AT_{m+k}A^t = T_{m+k}\}$$

donde

$$T_{m+k} = \begin{pmatrix} I_m & 0 \\ 0 & -I_k \end{pmatrix}.$$

Demuestre que es un grupo de Lie y no es compacto.

3. Decimos que una matriz x es nilpotente si $x^k = 0$ para algún k . Decimos que una matriz A es unipotente si $A - I_m$ es nilpotente. Demuestre

- (a) Si x es nilpotente, entonces e^x es unipotente.
(b) Si A es unipotente, entonces existe $\text{Log}(A)$ y es nilpotente.

- Ayuda para 2: Demostrar que dado un real t la matriz

$$\begin{pmatrix} \cosh(t) & \operatorname{senh}(t) \\ \operatorname{senh}(t) & \cosh(t) \end{pmatrix} \in O_{1,1}(\mathbb{R}) \rightarrow M_2(\mathbb{R})$$

Donde $\cosh(t) = \frac{e^t + e^{-t}}{2}$ y $\operatorname{senh}(t) = \frac{e^t - e^{-t}}{2}$.

- Ayuda para 3: Demostrar que si y y z son matrices nilpotentes que comutan, entonces $y + z$ es nilpotente.

Fórmulas útiles:

1. Definición de e^x

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

2. Definición de $\operatorname{Log}(A)$

$$\operatorname{Log}(A) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(A - I_m)^n}{n}.$$

3. Para todo t real se cumple

$$\cosh(t)^2 - \operatorname{senh}(t)^2 = 1$$

4. Si y y z comutan, entonces

$$(y + z)^s = \sum_{j=0}^s \binom{s}{j} x^{s-j} y^j$$

Problema 1. Sea F un cuerpo y sea V un F -espacio vectorial. Demuestre que $T^2(V) \cong S^2(V) \oplus \Lambda^2(V)$.

Dem. Sea $B: V \times V \rightarrow W$ una función F -bilineal, donde W es un F -espacio vectorial. Asumiendo que $\dim(F) \neq 2$, entonces B puede descomponerse como una suma

$$B(x, y) = B_1(x, y) + B_2(x, y)$$

donde $B_1(x, y) := \frac{B(x, y) + B(y, x)}{2}$ es una función F -bilineal simétrica ($B_1(x, y) = B_1(y, x)$) y $B_2(x, y) = \frac{B(x, y) - B(y, x)}{2}$ es F -bilineal antisimétrica ($B_2(x, y) = -B(y, x)$).

Obs. La descomposición anterior es única. Pero, si \bar{B}_1 simétrica y \bar{B}_2 antisimétrica tales que

$$B(x, y) = \bar{B}_1(x, y) + \bar{B}_2(x, y) \quad \forall x, y \in V.$$

entonces $B_1(x, y) + B_2(x, y) = \bar{B}_1(x, y) + \bar{B}_2(x, y)$, o de manera equivalente,

$$B_1(x, y) - \bar{B}_1(x, y) = \bar{B}_2(x, y) - B_2(x, y)$$

$$(B_1 - \bar{B}_1)(x, y) = (\bar{B}_2 - B_2)(x, y) \quad \forall x, y \in V$$

$$\Leftrightarrow B_1 - \bar{B}_1 = \bar{B}_2 - B_2$$

donde $B_1 - \bar{B}_1$ es simétrico y $\bar{B}_2 - B_2$ antisimétrica. Pero,

$$(\bar{B}_2 - B_2)(x, y) = (B_2 - \bar{B}_1)(x, y) = (B - \bar{B}_1)(y, x) = (\bar{B}_2 - B_2)(y, x) = -(\bar{B}_2 - B_2)(x, y)$$

$$\Rightarrow (B_1 - \bar{B}_1)(x, y) = (\bar{B}_2 - B_2)(x, y) = -(\bar{B}_2 - B_2)(x, y)$$

$$\Rightarrow (B_1 - \bar{B}_1)(x, y) = 0 \quad \forall x, y \in V$$

$$\therefore B_1 - \bar{B}_1 = 0$$

$$\therefore B_1 = \bar{B}_1$$

De lo anterior se desprende que $B_2 = \bar{B}_2$.

Ahora, como $B = B_1 + B_2$ (única descomposición)

$B_1 : V \times V \rightarrow W$ simétrico, entonces existe única $h : S^2(V) \rightarrow W$ lineal tal que $\forall x, y \in V : h(x \otimes y) = B_1(x, y)$. Análogamente,

al ser $B_2 : V \times V \rightarrow W$ antisimétrico, existe única $j : \Lambda^2(V) \rightarrow W$ lineal tal que $j(x \wedge y) = B_2(x, y) \quad \forall x, y \in V$.

Definimos ahora $k : T^2(V) \rightarrow W$ por $k = h + j$, i.e.,

$\forall x, y \in V : k(x \otimes y) = h(x \otimes y) + j(x \wedge y)$. Notar que k es

F -lineal tal que $k(x \otimes y) = h(x \otimes y) + j(x \wedge y)$
 $= B_1(x, y) + B_2(x, y) = B(x, y)$.

Así, se ve que $S^2(V) \oplus \Lambda^2(V)$ satisface la propiedad universal del producto tensorial,

$$\therefore S^2(V) \oplus \Lambda^2(V) \cong T^2(V).$$

abs. Para el problema hubo que assumir que $\text{char}(F) \neq 2$.

1/5

Problema 3

Sea D un dominio de integridad y sea F su cuerpo de cocientes.

(a) Considera a F como D -módulo y demuestra que $\Lambda^2 F = 0$.

(b) Sea I un D -submódulo de F . Demuestra que $\Lambda^i I$ es un módulo de torsión.

(c) Encuentra un ejemplo de un dominio D y un submódulo I de F tal que $\Lambda^n I \neq 0$ para todo n natural.

dem. (a) $\Lambda^2 F$ está generado, como D -módulo, por $a \wedge b$, donde $a \in F, b \in F$. Como $F = \text{Quot}(D)$, $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}$, $a_i, b_i \in D$, ($i=1, 2$) ($a_2, b_2 \neq 0$)

$$\Rightarrow a \wedge b = \frac{a_1}{a_2} \wedge \frac{b_1}{b_2} = \frac{a_1 b_2}{a_2 b_2} \wedge \frac{b_1 a_2}{b_2 a_2} = a_1 b_2 a_2 b_1 \left(\frac{1}{a_2 b_2} \wedge \frac{1}{a_2 b_2} \right)$$

Como $\frac{1}{a_2 b_2} \wedge \frac{1}{a_2 b_2} = 0$, se tiene que $a \wedge b = 0 \quad \forall a, b \in F$

$$\therefore \Lambda^2 F = 0$$

(b) Para $i \in \mathbb{N}$, $\Lambda^i I$ está generado como D -módulo, por los elementos de la forma $a_1 \wedge \dots \wedge a_i$, donde $a_j \in I$ ($j=1, \dots, i$). Como

$I \subseteq F$ (D -submódulo), $a_j = \frac{a_{j1}}{a_{j2}}$, donde $a_{j1}, a_{j2} \in D$ ($a_{j2} \neq 0$)

Tomando $r \in D$ como $r = \prod_{j=1}^i a_{j2}$, se tiene que

$$\begin{aligned} \text{en } r(a_1 \wedge \dots \wedge a_i) &= \prod_{j=1}^i a_{j2} (a_1 \wedge \dots \wedge a_i) \\ &= a_{12} \dots a_{i2} (a_1 \wedge \dots \wedge a_i) \end{aligned}$$

$$= \alpha_{i_1} \wedge \alpha_{i_2} \wedge \dots \wedge \alpha_{i_k}$$

$$= \alpha_{i_1} \dots \alpha_{i_k} (1 \wedge \dots \wedge 1)$$

pero $1 \wedge \dots \wedge 1 = 0$

$$\therefore r(\alpha_{i_1} \wedge \dots \wedge \alpha_{i_k}) = 0$$

$\therefore N^i I$ es de torsión $\forall i \in N$.

7, 6

Problema 9.

Demonstre que existe una extensión Galoisiana $(\mathbb{Q} \subseteq L)$ con $[\mathbb{L} : \mathbb{Q}] = 15$.

dem. Sea ζ una raiz-31-ava primitiva de la unidad ($\zeta^{31} = 1, \zeta \neq 1$)

Sabemos que $(\mathbb{Q}(\zeta)/\mathbb{Q})$ es Galoisiana, con $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(31) = 30$ (31 es primo en \mathbb{Z}).

Como $2 \mid 30$, por el teorema de Cauchy, $\exists \sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ tal que $|\sigma| = 2$. Como $(\mathbb{Q}(\zeta)/\mathbb{Q})$ es una extensión abeliana ($\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/31\mathbb{Z})^*$ y $(\mathbb{Z}/31\mathbb{Z})^*$ es abeliano), $\langle \sigma \rangle \trianglelefteq \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

$$\langle \sigma \rangle \trianglelefteq \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \iff (\mathbb{Q}(\zeta)^{\langle \sigma \rangle}/\mathbb{Q}) \text{ Galoisiana}$$

(teo. fundamental de la teoría de Galois)

Como $|\sigma| = 2 \Rightarrow [(\mathbb{Q}(\zeta) : (\mathbb{Q}(\zeta))^{\langle \sigma \rangle}] = |\langle \sigma \rangle| = |\sigma| = 2$ y en particular $[(\mathbb{Q}(\zeta))^{\langle \sigma \rangle} : \mathbb{Q}] = 15$.

∴ Basta tomar $L \subseteq (\mathbb{Q}(\zeta))$ como $L = (\mathbb{Q}(\zeta))^{\langle \sigma \rangle}$

Problema 2 Sea $K \subseteq \mathbb{C}$ el cuerpo de descomposición sobre $F = \mathbb{Q}(\sqrt{-5})$ del polinomio $x^4 - 5$.

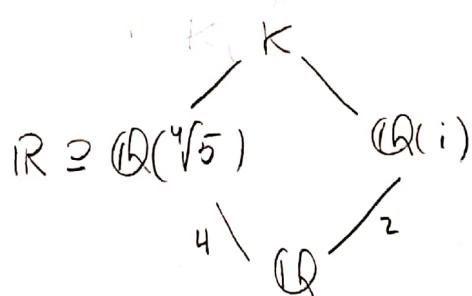
Determine explícitamente y abstractamente el grupo $\text{Gal}(K/F)$
 (Dé generadores de K sobre F , describa explícitamente cómo actúa $\text{Gal}(K/F)$ sobre los generadores de K . Describa el grupo abstracto al cual $\text{Gal}(K/F)$ es isomorfo).

desarrollo: Primero veamos que si $x^4 - 5 \in \mathbb{Q}[x]$, entonces sus raíces son $\sqrt[4]{5}, \sqrt[4]{5}\zeta, \sqrt[4]{5}\zeta^2, \sqrt[4]{5}\zeta^3$, donde $\zeta = e^{2\pi i/4} = e^{\pi i/2} = i$ una raíz 4-ta primitiva de la unidad ($\zeta = i \Rightarrow \zeta^2 = -1, \zeta^3 = -i$)

Como $\sqrt[4]{5}, i\sqrt[4]{5} \notin \mathbb{Q}(\sqrt{-5})$, entonces el cuerpo de descomposición K de $x^4 - 5 \in \mathbb{Q}(\sqrt{-5})[x]$ es el mismo al polinomio $x^4 - 4 \in \mathbb{Q}[x]$.

$$\begin{aligned} \text{En particular } K &= \mathbb{Q}(\sqrt{-5})(\sqrt[4]{5}, i\sqrt[4]{5}) = \mathbb{Q}(\sqrt{-5})(\sqrt[4]{5}, i) = \mathbb{Q}(\sqrt{-5}, \sqrt[4]{5}, i) \\ &= \mathbb{Q}(\sqrt[4]{5}, i) \quad (\sqrt{-5} = i\sqrt{5} = i(\sqrt[4]{5})^2) \\ \therefore K &= \mathbb{Q}(\sqrt[4]{5}, i) \end{aligned}$$

Ahora,



Como $\mathbb{Q}(\sqrt[4]{5}) \subseteq R \Rightarrow i \notin \mathbb{Q}(\sqrt[4]{5}) \Rightarrow [K : \mathbb{Q}(\sqrt[4]{5})] = 2$

$$\therefore [K : \mathbb{Q}] = 2$$

Como no hay una dependencia \mathbb{R} -lineal entre $\sqrt[4]{5}$ e i , juntas con K/\mathbb{Q} es Galoisiana y $[K:\mathbb{Q}] = 8$, entonces

$$\begin{cases} \sqrt[4]{5} \mapsto \zeta^a \sqrt[4]{5}, & a = 0, 1, 2, 3 \\ i \mapsto \pm i \end{cases}, (\zeta = i)$$

Son todos los automorfismos de $\text{Gal}(K/\mathbb{Q})$ (contienen 8, justo el grado de K/\mathbb{Q}). Como $[K:\mathbb{Q}(\sqrt{-5})] = 4$, entonces $\mathbb{Q}(\sqrt{-5}) = K^H$, donde $H \trianglelefteq \text{Gal}(K/\mathbb{Q})$ ($\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ es Galoisiana por T.F.T.G.) y $|H| = 4$

Busquemos los elementos de H :

$$\sigma: \begin{cases} \sqrt[4]{5} \mapsto i\sqrt[4]{5} \\ i \mapsto i \end{cases}, \quad \tau: \begin{cases} \sqrt[4]{5} \mapsto \sqrt[4]{5} \\ i \mapsto -i \end{cases}$$

$$\sigma^4 = \tau^2 = 1. \text{ Además:}$$

$$\sigma\tau: \begin{cases} \sqrt[4]{5} \mapsto -i\sqrt[4]{5} \\ i \mapsto -i \end{cases}$$

$$\sigma\tau^2: \begin{cases} \sqrt[4]{5} \mapsto \sqrt[4]{5} \\ i \mapsto -i \end{cases}$$

$$\sigma\tau^3: \begin{cases} \sqrt[4]{5} \mapsto i\sqrt[4]{5} \\ i \mapsto -i \end{cases}$$

$$\therefore \sigma\tau = \sigma\tau^3$$

$$\sigma\tau^3: \begin{cases} \sqrt[4]{5} \mapsto i\sqrt[4]{5} \\ i \mapsto -i \end{cases}$$

Como $\sqrt{-5} = i(\sqrt[4]{5})^2$, es fácil verificar que $H = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$.

En efecto,

$$\begin{aligned}\sigma^2(i(\sqrt{5})^2) &= \sigma(\sigma(i(\sqrt{5})^2)) = \sigma(i(i(\sqrt{5})^2)) = \sigma(-i(\sqrt{5})^2) = -i(i(\sqrt{5}))^2 \\ &= i(\sqrt{5})^2 = \sqrt{5}\end{aligned}$$

$$\sigma_6(i(\sqrt{5})^2) = \sigma(\sigma_6(i(\sqrt{5})^2)) = \sigma(-i(\sqrt{5})^2) = -i(i(\sqrt{5})^2) = i(\sqrt{5})^2 = \sqrt{5}$$

$$\sigma^3\sigma(i(\sqrt{5})^2) = \sigma^2(\sigma_6(i(\sqrt{5})^2)) = \sigma^2(i(\sqrt{5})^2) = i(\sqrt{5})^2 = \sqrt{5}$$

$$\therefore \text{Gal}(K/F) = H = \{\iota, \sigma^2, \sigma_6, \sigma^3\}$$

Como K/\mathbb{Q} es abeliana y $|\sigma^2| = |\sigma_6| = |\sigma^3| = 2 \Rightarrow H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problema 3. Sea $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ y sea $\alpha \in \mathbb{Q}(\zeta_n)$ tal que el polinomio irreducible de α sobre \mathbb{Q} sólo tiene raíces reales. Demuestre que $\alpha \in \mathbb{Q}(\cos(2\pi/n))$.

dem. Primero veamos que $\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ implica $\zeta_n + \zeta_n^{-1} = 2 \cos\left(\frac{2\pi}{n}\right)$

$$\Rightarrow \mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}(2 \cos(2\pi/n)) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$$

También, $\zeta_n^{-1} = \bar{\zeta}_n$ (porque $\zeta_n \bar{\zeta}_n = |\zeta_n|^2 = 1 \Rightarrow \bar{\zeta}_n = \zeta_n^{-1}$)

Entonces $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es Galoisiana, dado $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que

$$\sigma(\zeta_n + \zeta_n^{-1}) = \zeta_n + \zeta_n^{-1}, \quad (\sigma \neq 1);$$

$$\sigma(\zeta_n + \zeta_n^{-1}) = \sigma(\zeta_n) + \sigma(\zeta_n^{-1}) = \sigma(\zeta_n) + \sigma(\zeta_n)^{-1}$$

$$\Rightarrow \zeta_n + \zeta_n^{-1} = \sigma(\zeta_n) + \sigma(\zeta_n)^{-1}$$

$$\begin{aligned} \Rightarrow \zeta_n - \sigma(\zeta_n) &= \sigma(\zeta_n)^{-1} - \zeta_n^{-1} = \frac{1}{\sigma(\zeta_n)} - \frac{1}{\zeta_n} \\ &= \frac{\zeta_n - \sigma(\zeta_n)}{\sigma(\zeta_n) \zeta_n} \end{aligned}$$

$$\Rightarrow 1 = \frac{1}{\sigma(\zeta_n) \zeta_n}, \quad \text{ya que } \sigma \neq 1$$

$$\therefore \sigma(\zeta_n) = \zeta_n^{-1}$$

Es decir, la conjugación es el único automorfismo que fije a $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$,

$$\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n)^{\langle \sigma \rangle} \quad \checkmark$$

1.5. Producto tensorial de álgebras

Primero recordemos el producto tensorial de módulos.

Definición 1.5.1. Sea R anillo comunitativo y M, N dos R -módulos. Un producto tensorial de M y N es un R -módulo que denotaremos por $M \otimes_R N$ junto con una aplicación bilineal $\varphi : M \times N \rightarrow M \otimes_R N$ denotada por $(m, n) \mapsto m \otimes n$ tal que

- (i) $M \otimes_R N$ está generado como R -módulo por $\{x \otimes y \mid x \in M, y \in N\}$.
- (ii) **Propiedad universal.** Sean P un R -módulo, $\psi : M \times N \rightarrow P$ una aplicación bilineal, entonces existe una única aplicación lineal

$$f : M \otimes_R N \rightarrow P \text{ tal que } f \circ \varphi = \psi$$

$$\text{Luego } f(x \otimes y) = \psi(x, y) \quad \forall x, y \in M \times N;$$

Teorema 1.5.1. El producto tensorial de dos R -módulos M y N existe y es único, salvo isomorfismo.

Demostración. Existencia: Consideremos el R -módulo libre

$$R^{(M \times N)} = \left\{ \sum_{(x_j, y_j) \in M \times N} \alpha_j (x_j, y_j) \mid \alpha_j \in R \right\}$$

de base $M \times N$.

Sea S es el sub-módulo de $R^{(M \times N)}$ generado por elementos del tipo

$$\begin{aligned} & (x + x', y) - (x, y) - (x', y) \\ & (x, y + y') - (x, y) - (x, y') \\ & \alpha(x, y) - (\alpha x, y) \\ & \alpha(x, y) - (x, \alpha y) \\ & \forall x, x' \in M, y, y' \in N, \alpha \in R \end{aligned}$$

Definamos

$$M \otimes_R N = R^{(M \times N)} / S$$

y consideremos las aplicaciones

$$i : M \times N \rightarrow R^{(M \times N)}, (x, y) \mapsto (x, y) \quad \text{y } \pi : R^{(M \times N)} \rightarrow R^{(M \times N)} / S \text{ epimorfismo canónico}$$

Definamos

$$\varphi : M \times N \rightarrow M \otimes_R N, \text{ tal que } \varphi = \pi \circ i,$$

Luego,

$$\varphi : M \times N \rightarrow M \otimes_R N, \quad (x, y) \rightarrow (x, y) + S = x \otimes y$$

Se tiene que

$$\varphi : M \times N \rightarrow M \otimes_R N, \quad (x, y) \rightarrow (x, y) + S$$

es bilineal.

Sean $x, x' \in M, y \in N, \alpha \in R$. Entonces $(x + x', y) - (x, y) - (x', y) \in S \iff (x + x', y) + S = (x, y) + (x', y) + S \iff (x + x', y) + S = (x, y) + S + (x', y) + S \iff \varphi(x + x', y) = \varphi(x, y) + S + \varphi(x', y) + S$. Además $\alpha(x, y) - (\alpha x, y) \in S \iff \alpha(x, y) + S = (\alpha x, y) + S \iff \alpha((x, y) + S) = (\alpha x, y) + S \iff \alpha\varphi(x, y) = \varphi(\alpha x, y)$. Por lo tanto, φ es lineal en la primera variable. En forma similar se ve que φ es lineal en la segunda variable. Luego φ es bilineal.

Denotemos para cada $x \in M, y \in N$, $\varphi(x, y) + S = x \otimes y$ y se tiene que $M \otimes_R N$ está generado como R -módulo por $\{\varphi(x, y) + S = x \otimes y \mid x \in M, y \in N\}$.

Veamos que se cumple la Propiedad Universal. Sean P un R -módulo, $\psi : M \times N \rightarrow P$ una aplicación bilineal. Por ser $R^{(M \times N)}$ un módulo libre existe $h : R^{(M \times N)} \rightarrow P$ lineal tal que $h \circ i = \psi$, es decir, para cada $x \in M, y \in N$, $h \circ i(x, y) = \psi(x, y)$ o bien para cada $x \in M, y \in N$, $h(x, y) = \psi(x, y)$.

Para demostrar que existe $f : R^{(M \times N)} / S \rightarrow P$, lineal tal que $f \circ \pi = h$ se necesita probar que $\text{Ker}(\pi) \subseteq \text{Ker}(h)$, es decir, que $S \subseteq \text{Ker}(h)$ y aplicar proposición 1.1.2 que también es válida para módulos y aplicaciones lineales. Basta trabajar con los generadores de S . Tomemos por ejemplo $(x, y+y') - (x, y) - (x, y')$. Entonces como h es lineal, $h((x, y+y') - (x, y) - (x, y')) = h(x, y+y') - h(x, y) - h(x, y') = \psi(x, y+y') - \psi(x, y) - \psi(x, y') = \psi((x, y+y') - (x, y) - (x, y')) = 0$, pues ψ es bilineal. Similarmente se procede con los otros generadores.

Finalmente veamos que $f \circ \varphi = \psi$. Para ello usaremos que $h \circ i = \psi$ y que $f \circ \pi = h$. En efecto, $f \circ \varphi = f \circ (\pi \circ i) = (f \circ \pi) \circ i = h \circ i = \psi$.

Unicidad: Sea (T, φ') otro producto tensorial para M y N . Probemos que $T \simeq M \otimes_R N$.

Como (T, φ') es producto tensorial para M y N y φ es bilineal, existe

$$g : T \rightarrow M \otimes_R N \text{ lineal, tal que } g \circ \varphi' = \varphi.$$

Usando ahora que $(M \otimes_R N, \varphi)$ es producto tensorial para M y N y φ' es bilineal, existe

$$f : M \otimes_R N \rightarrow T \text{ lineal, tal que } f \circ \varphi = \varphi'.$$

Falta sólo probar que $g = f^{-1}$. Probaremos que $f \circ g = id_T$ y que $g \circ f = id_{M \otimes_R N}$.

En efecto, como $g \circ \varphi' = \varphi$ se tiene que $f \circ (g \circ \varphi') = f \circ \varphi = \varphi'$, es decir $(f \circ g) \circ \varphi' = \varphi'$.

Luego $f \circ g = id_T$. En forma similar se prueba que $g \circ f = id_{M \otimes_R N}$.

□

Observación 1.5.1. Como $M \otimes_R N$ es el producto tensorial de M y N , de (i) se tiene que para todo $z \in M \otimes_R N$, $z = \sum_{\text{finita}} x_i \otimes y_i$, con $x_i \in M$, $y_i \in N$, cada i . De (ii) tenemos que para todo R -módulo P , $\text{Bil}_R(M \times N, P) \simeq \mathcal{L}_R(M \otimes N, P)$.

Como $(m, n) \rightarrow m \otimes n$ es bilineal se tiene

1. $\forall x \in M, y \in N, x \otimes 0 = 0 \otimes y = 0$.
2. $\forall \alpha \in R, x \in M, y \in N, \alpha x \otimes y = \alpha(x \otimes y) = x \otimes \alpha y$.
3. $\forall \alpha, \beta \in R, x_i \in M, y \in N, (\alpha x_1 + \beta x_2) \otimes y = \alpha x_1 \otimes y + \beta x_2 \otimes y$.
4. $\forall \alpha, \beta \in R, x \in M, y_i \in N, x \otimes (\alpha y_1 + \beta y_2) = \alpha x \otimes y_1 + \beta x \otimes y_2$.

Se tiene además

1. Si $\{a_i\}_{i \in I}$ es una base de M y $\{b_j\}_{j \in J}$ es una base de N entonces $\{a_i \otimes b_j\}_{(i,j) \in I \times J}$ es una base de $M \otimes_R N$.
2. $M \otimes_R N \simeq N \otimes_R M; R \otimes_R N \simeq N; (M \otimes_R N) \otimes_R T \simeq M \otimes_R (N \otimes_R T)$.

Proposición 1.5.1. Sean A, B dos R -álgebras, $A \otimes_R B$ el producto tensorial de los R -módulos A y B entonces existe una única aplicación bilineal $\phi : A \otimes_R B \times A \otimes_R B \rightarrow A \otimes_R B$ definida por $\phi(x \otimes y, m \otimes n) = xm \otimes yn; \forall x, m \in A, \forall y, n \in B$. En particular se tiene que

$$(x \otimes y)(m \otimes n) = xm \otimes yn, \quad \forall x, m \in A, \quad \forall y, n \in B.$$

Demostración. Para cada $m \in A, n \in B$ se define:

$$\psi_{m,n} : A \times B \rightarrow A \otimes_R B \text{ por } \psi_{m,n}(x, y) = xm \otimes yn \quad \forall x \in A, \forall y \in B.$$

Entonces $\psi_{m,n}$ es bilineal. Luego existe una única aplicación lineal

$$f_{m,n} : A \otimes_R B \rightarrow A \otimes_R B \text{ tal que } f_{m,n}(x \otimes y) = \psi_{m,n}(x, y) = xm \otimes yn \quad \forall (x, y) \in A \times B.$$

Además se tiene:

$$f_{m+m',n} = f_{m,n} + f_{m',n} \quad \forall m, m' \in A, \forall n \in B$$

$$f_{m,n+n'} = f_{m,n} + f_{m,n'} \quad \forall m \in A, \forall n, n' \in B$$

$$f_{\alpha m,n} = \alpha f_{m,n} = f_{m,\alpha n} \quad \forall m \in A, \forall n \in B, \forall \alpha \in R$$

Teorema 2.4.1. (*Teorema de Wedderburn*) Sea A una R -álgebra semi-simple. Entonces:

1. Existen números naturales n_1, \dots, n_k y D_1, \dots, D_k álgebras de división sobre R tales que

$$A \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k).$$

2. Los pares (n_i, D_i) , $i = 1, \dots, k$ son únicos salvo isomorfismo.

*Demuestra*ción. 1. Sea A semi-simple, luego $A = N_1^{n_1} \oplus \cdots \oplus N_t^{n_t}$ con N_i ideales izquierdos minimales de A , N_i no isomorfo a N_j si $i \neq j$.

Sea $M_i = N_i^{n_i}$, $i = 1, \dots, t$ entonces M_i es semi-simple para cada i . Como N_i no es isomorfo a N_j si $i \neq j$, se tiene que $\text{Hom}_A(M_j, M_i) = \{0\}$. Luego

$$\begin{aligned} A^\circ &\simeq \text{End}_A(A) = \text{End}_A(N_1^{n_1} \oplus \cdots \oplus N_t^{n_t}) \\ &\simeq \text{End}_A(N_1^{n_1}) \oplus \cdots \oplus \text{End}_A(N_t^{n_t}) \\ &\simeq M_{n_1}(\text{End}_A(N_1)) \oplus \cdots \oplus M_{n_t}(\text{End}_A(N_t)) \end{aligned}$$

Para cada $i = 1, \dots, t$ sea $D'_i = \text{End}_A(N_i)$, entonces D'_i es un álgebra de división, pues N_i es ideal izquierdo minimal de A . Luego,

$$A^\circ \simeq M_{n_1}(D'_1) \oplus \cdots \oplus M_{n_t}(D'_t),$$

de donde

$$A = (A^\circ)^\circ \simeq (M_{n_1}(D'_1))^\circ \oplus \cdots \oplus (M_{n_t}(D'_t))^\circ.$$

Examinando cada sumando se tiene que, $(M_{n_i}(D'_i))^\circ \simeq (M_{n_i}(R) \otimes_R D'_i)^\circ \simeq (M_{n_i}(R))^\circ \otimes_R (D'_i)^\circ$, pero $(M_{n_i}(R))^\circ \simeq M_{n_i}(R)$, aplicando la matriz B a la matriz transpuesta B^t . Luego

$$(M_{n_i}(D'_i))^\circ \simeq M_{n_i}(R) \otimes_R (D'_i)^\circ \simeq M_{n_i}(D'^{\circ o}_i).$$

Por lo tanto,

$$A \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k),$$

y se tiene la primera parte del teorema.

2. Sean $n_1, \dots, n_t \in \mathbb{N}$, $s_1, \dots, s_t \in \mathbb{N}$, y C_i, D_j álgebras de división para $i = 1, \dots, k$, $j = 1, \dots, t$ tales que

$$A \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_t}(D_t),$$

$$A \simeq M_{s_1}(C_1) \oplus \cdots \oplus M_{s_k}(C_k).$$

Como

$$M_{n_1}(D_1) \oplus \cdots \oplus M_{n_t}(D_t) \simeq M_{s_1}(C_1) \oplus \cdots \oplus M_{s_k}(C_k)$$

y A es semi-simple se tiene que $t = k$ (reordenando si fuera necesario), luego $n_t = s_k \forall t$. Sea $A_i = M_{s_i}(C_i)$, $i = 1, \dots, k$. Luego A_i es semi-simple. Por lo tanto hay ideales izquierdos minimales $P_{i,j}$ para cada j tales que

$$A_j = \sum_{i=1}^n P_{ij} \text{ y } \text{End}_{A_j}(P_{ij}) \simeq C_j \forall j = 1, \dots, t.$$

Además,

$$C_j \simeq \text{End}_{A_j}(P_{ij}) \simeq \text{End}_A(P_{ij}) \simeq \text{End}_A(N_j) \simeq D_j, \quad \forall j = 1, \dots, t.$$

□

Observación 2.4.2. Si n_1, \dots, n_k y D_1, \dots, D_k son álgebras de división sobre R entonces

$M_{n_1}(D_1) \oplus \dots \oplus M_{n_k}(D_k)$ es semi-simple.

*Demuestra*ción. Se tiene que $M_{n_i}(D_i)$ es simple para cada i , luego $M_{n_1}(D_1) \oplus \dots \oplus M_{n_k}(D_k)$ es semi-simple.

□

Corolario 2.4.4. Una R -álgebra A , artiniana es simple sí y sólo sí $A \simeq M_n(D)$ cierto $n \in \mathbb{N}$ y D un álgebra de división, únicamente determinados.

Corolario 2.4.5. Una R -álgebra A , de dimensión finita es simple sí y sólo sí $A \simeq M_n(D)$ cierto $n \in \mathbb{N}$ y D un álgebra de división, únicamente determinados.

Lema 2.4.1. Sea F un cuerpo algebraicamente cerrado. Si D es un álgebra de división, de dimensión finita sobre F , entonces $D = F$.

*Demuestra*ción. Sea $a \in D$ y sea $\dim_F(D) = m$. Luego $\{1, a, \dots, a^m\}$ es linealmente dependiente. Sea $q(x)$ el polinomio de grado mínimo y mónico del cual a es raíz. Como F es algebraicamente cerrado, $q(x) = \prod_{i=1}^k (x - \lambda_i)$, $\lambda_i \in F$.

$$q(a) = 0 \implies \prod_{i=1}^k (a - \lambda_i) = 0.$$

Luego $a - \lambda_j = 0$ para algún j y $a = \lambda_j \in F$.

□

Usando el lema anterior y el teorema de Wedderburn se prueba:

Proposición 2.4.2. Sea F un cuerpo algebraicamente cerrado. Si A es un álgebra de dimensión finita sobre F entonces A es semi-simple sí y sólo sí $A \simeq M_{n_1}(F) \oplus \dots \oplus M_{n_k}(F)$ donde n_1, \dots, n_k están únicamente determinados. En particular A es simple sí y sólo sí $A \simeq M_n(F)$ y $\dim_F(A) = n^2$.

Ejercicio 2.4.1. Sea F un cuerpo algebraicamente cerrado, A un álgebra semi-simple de dimensión finita sobre F , $A \simeq M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$. Pruebe que $\dim_F(Z(A)) = k$.

Teorema 2.4.2. Sean G grupo finito de orden n , F cuerpo algebraicamente cerrado, tal que $\text{car}(F)$ no es un divisor de n . Entonces $F[G] \simeq M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$ donde $k =$ número de clases de conjugación de G .

Demostración. Por teorema de Maschke, $F[G]$ es semi-simple y de dimensión finita. Luego $F[G] \simeq M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$. Falta probar que $k =$ es el número de clases de conjugación de G . Por ejercicio anterior, $\dim_F(Z(M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F))) = k$. Probaremos que $\dim_F(Z(F[G])) =$ número de clases de conjugación de G .

Sean H_1, \dots, H_t las distintas clases de conjugación de G . Luego $G = \bigcup_{i=1}^t H_i$ (unión disjunta). Si $h_i \in H_i$, $H_i = \{y^{-1}x_iy \mid y \in G\}$.

Para cada $i = 1, \dots, t$ sea $z_i = \sum_{h \in H_i} h$. Entonces $z_i \in Z(F[G])$ pues para todo $g \in G$, $g^{-1}z_ig = g^{-1}\sum_{h \in H_i} hg = \sum_{h \in H_i} g^{-1}hg = \sum_{h' \in H_i} h' = z_i$. Por lo tanto, $Fz_1 \oplus \cdots \oplus Fz_t \subseteq Z(F[G])$.

Sea ahora, $w \in Z(F[G])$ Entonces $w = \sum_{g \in G} a_g g$ y para todo $y \in G$, $y^{-1}wg = w$. Esta última condición impone la condición $a_{y^{-1}gy} = a_g$ sobre los coeficientes de w . Por lo tanto, w se escribe como una suma $\sum_{i=1}^t b_i z_i$, con $b_i \in F$. Luego $Z(F[G]) = \bigoplus_{i=1}^t Fz_i$, y $\dim_F(Z(F[G])) = t =$ número de clases de conjugación de G , que es lo que se quería probar. \square

Proposición 2.4.3. Sean F cuerpo y A una F -álgebra central simple de dimensión finita, entonces $\dim_F(A) = n^2$, cierto $n \in \mathbb{N}$.

Demostración. Sea \overline{F} la cerradura algebraica de F , entonces $A \otimes_F \overline{F}$ es simple, más aún, es central simple. Luego existe una \overline{F} -álgebra de división D tal que $A \otimes_F \overline{F} \simeq M_n(D)$ cierto $n \in \mathbb{N}$. Como \overline{F} es algebraicamente cerrado, se tiene por lema 2.4.1 que $D = \overline{F}$, luego $\dim_F(A) = \dim_{\overline{F}}(A \otimes_F \overline{F}) = n^2$. \square

Ejercicio 2.4.2. Sean F cuerpo y A una F -álgebra central simple de dimensión n . Entonces

$$A \otimes_F A^\circ \simeq M_n(F) \simeq \text{End}_F(A).$$

Sugerencia: Como $\dim_F(A \otimes_F A^\circ) = \dim_F(M_n(F))$ y $M_n(F) \simeq \text{End}_F(A)$ basta definir un morfismo biyectivo $f : A \otimes_F A^\circ \rightarrow \text{End}_F(A)$.

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
FACULTAD DE MATEMÁTICAS
DEPARTAMENTO DE MATEMÁTICA

MAT2218 (Álgebra II)

Interrogación N° 2 Lunes, 21 de Octubre, 2013

Importante: Motive su respuesta, mencione el teorema, proposición, lema, etc. que usted utiliza.

1. Considerar $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_3[x]$. Sea $K \subset \overline{\mathbb{F}}_3$ el cuerpo de descomposición de $f(x)$ sobre \mathbb{F}_3 . Determinar el tamaño $|K|$ de K . Demostrar que $x^2 + 1 \in K[x]$ se descompone sobre K .
2. Determinar si los siguientes elementos en \mathbb{R} son construibles con regla y compas de $X = \{0, 1\}$:
 - a) $\sqrt{2 + \sqrt{3 + \sqrt{5}}}$
 - b) $\cos(2\pi/9)$
3. Sea $K = \mathbb{Q}(e^{2\pi i/n}) \subset \mathbb{C}$. Sea $\alpha \in \mathbb{C}$ tal que $\alpha^n \in K$ y define $L = K(\alpha)$. Demostrar que L/K es Galois. Demostrar que el grupo de Galois G de L/K es un grupo cíclico. Demostrar que $|G|$ divide a n .
4. Sea K un cuerpo que contiene \mathbb{F}_q , donde $q = p^n$, p un primo y $n \geq 1$. Sea $a \in K$. Considerar $h(x) = x^q - x + a \in K[x]$. Sea L un cuerpo de descomposición para h sobre K . Sea $\beta \in L \subset \overline{\mathbb{F}}_p$ un cero de h .
 - a) Demostrar que existe un homomorfismo de grupos $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_q$ (es decir de $\text{Gal}(L/K)$ al grupo aditivo \mathbb{F}_q) tal que $\psi(\sigma) = \sigma(\beta) - \beta$.
 - b) Asumir que h es irreducible. Demostrar que ψ es un isomorfismo.
 - c) Asumir que K es un cuerpo finito y $n > 1$. Demostrar que h es reducible.

Duración: 2 horas

$\begin{array}{c} * \\ F \\ \downarrow \\ L \\ \downarrow \\ K \\ \downarrow \\ \mathbb{F}_q \end{array}$

$\begin{array}{c} \text{Si } x \in L \\ \text{entonces } x \in K \\ \text{y } x \in \mathbb{F}_q \end{array}$

$(x^q - x + a) \in K[x]$

$x^q - x + a \in \mathbb{F}_q[x]$

$x^q - x + a \in \mathbb{F}_p[x]$

MAT2218 (Álgebra Abstracta II)

Examen Martes, 3 de Diciembre, 2013

Importante: Motive su respuesta, mencione el teorema, proposición, lema, etc. que usted utiliza.

- Calcular el número de factores irreducibles de $x^{255} - 1 \in \mathbb{F}_2[x]$ y sus grados. 35 -
 Calcular el número de factores irreducibles de $x^{255} - 1 \in \mathbb{Q}[x]$ y sus grados.

Sea $\alpha = \sqrt{3 + \sqrt{5}} \in \mathbb{R}$ y sea $K = \mathbb{Q}(\alpha)$. Sea L un cuerpo de descomposición para el polinomio mínimo $m_\alpha(x)$ de α sobre \mathbb{Q} . Encuentre $\text{Gal}(L/\mathbb{Q})$.

Determine el grupo de Galois de $f(x) = x^3 - 2x^2 + x + 1 \in \mathbb{Q}[x]$ sobre \mathbb{Q} . 2

3. a) Sea $f(x) \in \mathbb{Q}[x]$ irreducible sobre \mathbb{Q} y tal que $f(x)$ tiene raíces en \mathbb{R} y en $\mathbb{C} \setminus \mathbb{R}$. Demuestre que el grupo de Galois $\text{Gal}(f/\mathbb{Q})$ no es abeliano.

- b) Sea σ un automorfismo de un cuerpo F . Supongamos que $\sigma^4 = 1$ y

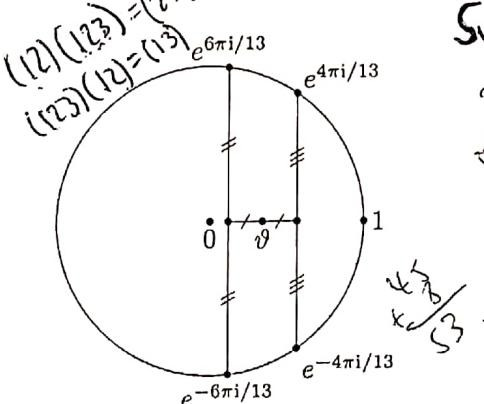
$$\sigma(\alpha) + \sigma^3(\alpha) = \alpha + \sigma^2(\alpha) \quad \forall \alpha \in F$$

$$\text{Demuestre que } \sigma^2 = 1. \quad \sigma(\alpha + \sigma^2(\alpha)) = \alpha + \sigma^4(\alpha)$$

4. Sea $\vartheta \in \mathbb{C}$ definida como en la figura.

- a) Calcule $[\mathbb{Q}(\vartheta) : \mathbb{Q}]$.

Investigar si es posible construir el punto $\zeta := e^{2\pi i/13}$ con regla y compás desde $X = \{0, 1, \vartheta\}$.



Duración: $2\frac{1}{2}$ horas

$$x^4 - 6x^2 - 4$$

$$x^2 = -6 \pm \sqrt{52}$$

$$x^4 + 2$$

$$-4+6=2$$

$$x^2 = 1$$

$$\frac{1}{5} \times 5 = 1$$

Guía de Ejercicios y tarea 2.
Álgebra II, segundo semestre 2013

1. Demuestre que $X^3 - 2X - 2$ es irreducible sobre \mathbb{Q} . Si θ es una raíz de este polinomio, calcule $(1 + \theta)(1 + \theta + \theta^2)$ y $\frac{1+\theta}{1+\theta+\theta^2}$ en $\mathbb{Q}(\theta)$.
2. * Encuentre los valores de $a \in \mathbb{Z}$ tal que $X^5 - aX - 1$ sea irreducible en $\mathbb{Z}[X]$.
3. * Sea K/F una extensión de cuerpos. Si $u \in K$ es un elemento algebraico de grado impar sobre F , entonces u^2 también lo es y $F(u) = F(u^2)$.
4. Sea K/F una extensión de cuerpos y $X^n - a \in F[X]$ irreducible. Si $u \in K$ es una raíz de este polinomio y $m|n$, demuestre que el grado de u^m sobre F es n/m . ¿Cuál es el polinomio irreducible de u^m sobre F ?
5. En el cuerpo de funciones racionales $F(X)$, sea $u = \frac{X^3}{X+1}$. Demuestre que $F(X)$ es una extensión simple de $F(u)$. Calcule $[F(X) : F(u)]$.
6. * Sea K/F una extensión de cuerpos, sean L/F y M/F subextensiones finitas de K/F (es decir, $F \subset L \subset K$, $F \subset M \subset K$, $[L : F] < \infty$, $[M : F] < \infty$). Sea LM el compósito de L y M dentro de K (es decir, el mínimo subcuerpo de K que contiene a L y a M).
 - a) Demuestre que $[LM : F] < \infty$, y que $[L : F][LM : F]$.
 - b) Demuestre que $[LM : F] = [L : F][M : F]$ implica $L \cap M = F$.
 - c) Demuestre que el recíproco se verifica cuando $[L : F] = 2$ o $[M : F] = 2$.
 - d) Dé un ejemplo de extensiones F, L, M, K tal que $[L : F] = [M : F] = 3$, $[LM : F] < 9$, $L \cap M = F$.
7. Sea p un primo y \mathbb{F}_p el cuerpo de p elementos. Demuestre que la función $x \rightarrow x^p - x$ es la función nula sobre \mathbb{F}_p , pero el polinomio $x^p - x$ no es nulo.
8. Sea F un cuerpo infinito y $P(X) \in F[X]$ un polinomio no nulo. Demuestre que la función $f : F \rightarrow F$ dada por $f(\alpha) := P(\alpha)$ no es la función nula.
9. * Un cuerpo de característica p se dice perfecto si la función $\alpha \mapsto \alpha^p$ es sobreyectiva.
 - a) Demuestre que todo cuerpo finito es perfecto.
 - b) Demuestre que Si F es un cuerpo cualquiera de característica p , entonces $F(x)$ no es perfecto.
10. Sea $f(x) \in F[x]$ un polinomio irreducible de grado p y sea $E \supseteq F$ con $|E : F| < \infty$. Si $f(x)$ no es irreducible en $E[x]$, demuestre que $p | |E : F|$. Ayuda: Considere un cuerpo $L \supseteq E$ en el que f tenga una raíz.

Guía de Ejercicios y tarea 3.
Álgebra II, segundo semestre 2013

Entregar los ejercicios marcados el miércoles 4 de septiembre.

1. Determine el cuerpo de descomposición y su grado sobre \mathbb{Q} para cada uno de los polinomios siguientes:
a) $x^4 - 2$ b) $x^4 + 2$ c) $x^4 + x^2 + 1$
2. *Sea K una extensión finita de F . Demuestre que K es un cuerpo de descomposición sobre F si y solo si todo polinomio irreducible en $F[x]$ que tiene una raíz en K se descompone completamente en $K[x]$.
3. *Sean K_1, K_2 extensiones finitas de F contenidas en K y suponga que ambas son cuerpos de descomposición sobre F . Demuestre que $K_1 \cap K_2$ es cuerpo de descomposición sobre F .
4. Sea $\overline{\mathbb{Q}} \subset \mathbb{C}$ la clausura algebraica de \mathbb{Q} en \mathbb{C} .
 - a) Demuestre que $\overline{\mathbb{Q}}$ es denumerable.
 - b) Demuestre que $\overline{\mathbb{Q}}/\mathbb{Q}$ es una extensión algebraica infinita.
 - c) Sea $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ y $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Demuestre que el conjunto de racionales p/q (con $p, q \in \mathbb{Z}$) tales que $|\alpha - p/q| < 1/q^{n+1}$ es finito (o vacío). Concluya (como Liouville alrededor de 1829) que $\sum_{j=0}^{\infty} 10^{-j!}$ es un número real no algebraico.
SUGERENCIA. Sea $P(X) \in \mathbb{Z}(X)$ de grado n y tal que $P(\alpha) = 0$. Considere $|P(p/q)| = |P(p/q) - P(\alpha)|$ y piense en el teorema del valor medio.
5. Sea F , un cuerpo y $g(x) \in F[x]$. Demuestre $D(g(x))$ es el polinomio nulo ssi $g(x)$ es constante, o F es de característica p y $g(x) = f(x^p)$, con $f(x) \in F[x]$.
6. * Sea \mathbb{F}_q el cuerpo finito de q elementos, de modo que $q = p^k$ para algún primo p y algún $k \in \mathbb{N}$. ¿Cuándo se cumple que hay una inyección $\mathbb{F}_q \rightarrow \mathbb{F}_{q'}$?
7. * Calcule el grupo de automorfismos del cuerpo \mathbb{F}_q .
8. Sea p primo y $a \neq 0 \in \mathbb{F}_p$. Demuestre que $x^p - x + a$ es irreducible y separable sobre \mathbb{F}_p .
9. Demuestre que el único automorfismo del cuerpo \mathbb{R} es la identidad.
10. Demuestre que la clausura algebraica $\overline{\mathbb{Q}}$ tiene infinitos automorfismos. Más aún, demuestre que el grupo de automorfismos (de cuerpo) de $\overline{\mathbb{Q}}$ no es denumerable.

Guía de Ejercicios y tarea 4.
Álgebra II, segundo semestre 2013

Entregar los 4 ejercicios marcados el miércoles 11 de septiembre (o cuando se pueda).

1. Sea $F = \mathbb{F}_p(T)$ el cuerpo de funciones racionales sobre un cuerpo primo finito y sea K/F el cuerpo de descomposición del polinomio $X^p - T$. Demuestre que $[K : F] = p$ y que hay un único F -automorfismo del cuerpo K .
2. Determine el polinomio minimal sobre \mathbb{Q} para el elemento $1 + \sqrt[3]{2} + \sqrt[3]{4}$.
3. * Determine todos los subcuerpos del cuerpo de descomposición de $x^8 - 2$ que son Galois sobre \mathbb{Q} .
4. Muestre que $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ es una extensión de grado 4 de \mathbb{Q} con grupo de Galois cíclico.
5. * Demuestre que el cuerpo de descomposición de $x^4 - 2x^2 - 2$ sobre \mathbb{Q} es de grado 8 con grupo de Galois dihedral. Ayuda: ejercicio 16 página 582 Dummit.
6. * Sea K/F una extensión finita de cuerpos. Para $\alpha \in K$, sea $L_\alpha : K \rightarrow K$ dada para $x \in K$ por $L_\alpha(x) := \alpha x$. Como L_α es F -lineal, definamos su polinomio característico $P_\alpha(X) \in F[X]$ como $P_\alpha(X) = \det(XI - L_\alpha)$, donde $I(x) = x$ es la función identidad de K a K . Demuestre las siguientes aseveraciones.
 - a) Si $K = F(\alpha)$, entonces $P_\alpha(X) = \min_{\alpha, F}(X)$, el polinomio minimal de α sobre F .
 - b) $P_\alpha(X) = (\min_{\alpha, F}(X))^m$, donde $m = [K : F(\alpha)]$.
7. * Con la nomenclatura del ejercicio anterior, definamos la norma $N_{K/F} : K \rightarrow F$ (resp., la traza $\text{Tr}_{K/F} : K \rightarrow F$) de K a F de α como $N_{K/F}(\alpha) := \det(L_\alpha)$ (resp., $\text{Tr}_{K/F}(\alpha) := \text{Traza}(L_\alpha)$).
 - a) Sean $\alpha_1, \dots, \alpha_n$ todas las raíces (en alguna extensión de F) de $P_\alpha(X) = \prod_{i=1}^n (X - \alpha_i)$. Demuestre

$$N_{K/F}(\alpha) = \prod_{i=1}^n \alpha_i, \quad \text{Tr}_{K/F}(\alpha) = \sum_{i=1}^n \alpha_i,$$
 - b) Si K/F es separable, y $K \subset L$ con L algebraicamente cerrado, entonces $P_\alpha(X) = \prod_{\tau} (X - \tau(\alpha))$, donde τ recorre todas las F -incrustaciones de K en L .
 - c) Demuestre, para $\alpha \in F$, que $\text{Tr}_{K/F}(\alpha) = [K : F]$, $N_{K/F}(\alpha) = \alpha^{[K:F]}$.

- d) Demuestre, para $\alpha, \beta \in K$, que $\text{Tr}_{K/F}(\alpha + \beta) = \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta)$,
 $\text{N}_{K/F}(\alpha\beta) = \text{N}_{K/F}(\alpha) \cdot \text{N}_{K/F}(\beta)$.
- e) Si $F \subset K \subset H$ son extensiones finitas sucesivas de cuerpos, demuestre para
 $\beta \in H$, $\text{N}_{H/F}(\beta) = \text{N}_{K/F}(\text{N}_{H/K}(\beta))$ y $\text{Tr}_{H/F}(\beta) = \text{Tr}_{K/F}(\text{Tr}_{H/K}(\beta))$.
- f) Démuestre que si K/F es una extensión de cuerpos finitos, entonces $\text{N}_{K/F}$
y $\text{Tr}_{K/F}$ son funciones epiyectivas.

GUIA 6 TOPICOS EN TEORIA DE ALGEBRAS

SEGUNDO SEMESTRE 2014

1. Sea A un álgebra de división. Pruebe que el A -módulo A es indecomponible.
2. Sean M, N dos A -módulos y sea $f : M \rightarrow N$ lineal. Pruebe que hay $g : N \rightarrow M$ lineal con $g \circ f = Id_M \iff f$ es inyectiva y $Im(f)$ tiene complementario en N .
3. Sean M, N dos A -módulos y sea $f : M \rightarrow N$ lineal. Pruebe que hay $g : N \rightarrow M$ lineal con $f \circ g = Id_N \iff f$ es inyectiva y $Ker(f)$ tiene complementario en M .
(μ jil)
4. Sean M, N, P A -módulos. Considere la sucesión exacta $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$. Pruebe que son equivalentes:
 - (a) $Im(f)$ tiene complementario en N .
 - (b) Hay $r : N \rightarrow M$ lineal con $r \circ f = Id_M$.
 - (c) Hay $s : P \rightarrow N$ lineal con $g \circ s = Id_P$.

Si una de ellas se verifica se tiene que $N = Im(f) \oplus Im(s)$ y la función $M \times P \rightarrow N, (x, p) \rightarrow f(x) + s(p)$ es un isomorfismo de A -módulos.

5. Sea M un A -módulo. Pruebe que existe una sucesión exacta $L \xrightarrow{f} M \longrightarrow 0$, donde L es un A -módulo libre.
6. La sucesión $0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$, donde f está definida por $f(x) = 2x \forall x \in \mathbb{Z}$, es exacta. Sea $N = \mathbb{Z}/2\mathbb{Z}$, un \mathbb{Z} -módulo. ¿Es $0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} N \xrightarrow{f \otimes I_N} \mathbb{Z} \otimes_{\mathbb{Z}} N$, una sucesión exacta?
7. Pruebe que el anillo $R = \mathbb{Q}^{\mathbb{Q}} = \{f : \mathbb{Q} \rightarrow \mathbb{Q} \mid f \text{ función}\}$, no es noetheriano ni artiniano. Sugerencia: Considere para cada $q \in \mathbb{Q}, q > 0$, $I_q = \{u \in R \mid u(x) = 0, \forall x \in [-q, q] \cap \mathbb{Q}\}$.

GUIA 6 TOPICOS EN TEORIA DE ALGEBRAS
SEGUNDO SEMESTRE 2014

- ✓ 1. Sea A un álgebra de división. Pruebe que el A -módulo A es indescomponible.
- ✓ 2. Sean M, N dos A -módulos y sea $f : M \rightarrow N$ lineal. Pruebe que hay $g : N \rightarrow M$ lineal con $g \circ f = Id_M \iff f$ es inyectiva y $Im(f)$ tiene complementario en N .
- ✓ 3. Sean M, N dos A -módulos y sea $f : M \rightarrow N$ lineal. Pruebe que hay $g : N \rightarrow M$ lineal con $f \circ g = Id_N \iff f$ es inyectiva y $Ker(f)$ tiene complementario en M .
Sobrejetiva
- ✓ 4. Sean M, N, P - A módulos. Considere la sucesión exacta $0 \xrightarrow{\text{iny.}} M \xrightarrow{f} N \xrightarrow{g} P \xrightarrow{\text{lineal}} 0$. Pruebe que son equivalentes:
 - $Im(f)$ tiene complementario en N .
 - Hay $r : N \rightarrow M$ lineal con $r \circ f = Id_M$.
 - Hay $s : P \rightarrow N$ lineal con $g \circ s = Id_P$.

Si una de ellas se verifica se tiene que $N = Im(f) \oplus Im(s)$ y la función $M \times P \rightarrow N, (x, p) \rightarrow f(x) + s(p)$ es un isomorfismo de A -módulos.
5. Sea M un A -módulo. Pruebe que existe una sucesión exacta $L \xrightarrow{f} M \rightarrow 0$, donde L es un A -módulo libre.
- ✓ 6. La sucesión $0 \rightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$, donde f está definida por $f(x) = 2x \forall x \in \mathbb{Z}$, es exacta. Sea $N = \mathbb{Z}/2\mathbb{Z}$, un \mathbb{Z} -módulo. ¿Es $0 \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}} N \xrightarrow{f \otimes I_N} \mathbb{Z} \otimes_{\mathbb{Z}} N$, una sucesión exacta? *No!*
- ✓ 7. Pruebe que el anillo $R = \mathbb{Q}^{\mathbb{Q}} = \{f : \mathbb{Q} \rightarrow \mathbb{Q} \mid f \text{ función}\}$, no es noetheriano ni artiniano. Sugerencia: Considere para cada $q \in \mathbb{Q}, q > 0$, $I_q = \{u \in R \mid u(x) = 0, \forall x \in [-q, q] \cap \mathbb{Q}\}$.

problemat. $R = \mathbb{W}^U$ woshoetheridnoi artinidha.

$f \in \mathbb{W}$. Soz $I_f = \{u \in R : u(x) = 0, \forall x \in [-f, f] \cap \mathbb{W}\} \neq \emptyset$ i Pwes

$$u_{f_i}(x) = \begin{cases} 0, & \text{si } x \in (-f_i, f_i) \cap \mathbb{W} \\ 1, & \text{sin } \end{cases} \in I_{f_i}.$$

g es idealza pue $I_f \subseteq R$ s: $f \in R, u \in I_f : f_n(x) = f(x_1 \cdot 0) = 0, \forall x \in [-f, f] \cap \mathbb{W}$.

$\therefore f \in I_f$.

Aleatoris indenendo \mathbb{W} por \mathbb{N} : $I_{f_1} \subset I_{f_2} \subset \dots$ si $f_1 < f_2 < \dots$

yza pue $u_{f_i} \in I_{f_i} - I_{f_{i+1}}$. $I_{f_1} \supset I_{f_2} \supset \dots$ s: $f_1 > f_2 > \dots$

Adlegamente:

glarcadenas noson estacionarias

$\therefore R$ woshoetheridnoi artinidha.

problemas. $\xrightarrow{f} \mathbb{N} \rightarrow 0$ Nun A-modulo.
exacto si f sobreyectiva, L A-modulo libre.

considere: $\{e_i\}_{i \in \mathbb{Z}}$ base del $\Rightarrow m \in \mathbb{N} \Rightarrow m = f(l) = f(\sum x_i e_i) = \sum x_i f(e_i)$
 $\therefore \{f(e_i)\}_{i \in \mathbb{Z}}$ sevan \mathbb{N} , pero pueden waterbate. (pueden ser l.d.)

Problema 1. A alg. dedivisión. el A -módulo B es indecomponible.

$$\text{Sea } B \leq A \Rightarrow B \text{ ideal de } A \Rightarrow B = (0) \quad B = A$$

$\therefore B$ tiene complementario nulo trivial.

Problema 2. M, N A -módulos : $f: M \rightarrow N$ lineal. Probar que: $f: N \rightarrow M$ lineal con $f \circ f = \text{id}_N$ ssi f inyectiva $\eta \text{ Im } f$ tiene complementario en N .

Dem: $\exists p: p \circ f = \text{id}_M$

$$\text{Sea } f(x) = f(y) \Rightarrow p(f(x)) = p(f(y)) = y \quad \therefore f \text{ inyectiva.}$$

$$\text{Sea } p(n) \in N \Rightarrow f(p(n)) = p(f(n)) \in M$$

$$\eta \text{ Im } f = S, T = \text{Ker } f \Rightarrow \text{Sea } n \in N \Rightarrow f(n) \in M \Rightarrow f(p(n)) \in S$$

$$\text{Así: } n - f(p(n)) = t \text{ es la p.e.: } p(t) = p(n) - p(f(n)) = p(n) - p(n) = 0.$$

$$\therefore N = S + T \text{ y si } n \in S \cap T \Rightarrow \exists u: n = f(u) \Rightarrow p(f(u)) = n = 0 \quad \therefore N = S \oplus T.$$

$$\text{Al final, si } f \text{ inyectiva} \Rightarrow \exists p: p \circ f = \text{id}_N \text{ y } \begin{matrix} p: N \rightarrow M \\ n \mapsto m: f(m) = n \end{matrix}$$

$$\eta p(h_1 + h_2) = h_1 + h_2 \text{ p.e.s } f(h_1 + h_2) = h_1 + h_2. \quad \therefore p \text{ es lineal.}$$

$$\text{Problema 3. } f: M \rightarrow N \text{ lineal. } \exists p: N \rightarrow M \text{ s.t. } p \circ f = \text{id}_N \text{ ssi } f \text{ sobreyectiva y Ker } f \text{ tiene complementario.}$$

Dem: Si $\exists p: f \circ p = \text{id}_N$ $\therefore f$ sobreyectiva.

$$\text{Sea } x \in N \Rightarrow p(x) \in M \Rightarrow f(p(x)) = x \quad \therefore x \in \text{Im } f. \quad \therefore f \text{ sobreyectiva.}$$

$$\text{Sea } S = \text{Ker } f, T = \text{Im } f. \quad \text{Sea } m \in N \Rightarrow f(m) \in M \Rightarrow p(f(m)) \in N \quad \text{Sea } m - f(m) = t$$

$$\therefore N = S + T \quad \text{y si } x \in S \cap T \Rightarrow f(x) = 0 \quad \exists y \in N: f(y) = x$$

$$f(m - p(f(m))) = f(m) - f(p(f(m))) = 0$$

$$\Rightarrow f(p(y)) = y = f(x) = 0 \Rightarrow x = 0$$

$$\therefore N = S \oplus T$$

$$\text{y si } f \text{ sobre} \Rightarrow \exists p \text{ lineal: } p \circ f = \text{id}_N.$$

Problema 4. a) \Rightarrow b)

$$(r \circ f = \text{id}_M)$$

$$M = \text{Im } f \oplus T. \quad \text{Sea } r: N \rightarrow M, \text{ con } f(m) = m \quad \text{(biunív.) p.e.s: } h_1 = h_2 \Rightarrow f(h_1) = h_1 = h_2 = f(h_2) \Rightarrow h_1 = h_2.$$

$$n = h_1 + t \text{ únicos.} \quad \begin{matrix} m+t \mapsto f(m) \\ m \in M \end{matrix}$$

$$\text{Así: } r(h_1 + h_2 + \lambda(h_2 - h_1)) = r(h_1 + h_2 + (\lambda + 1)(h_2 - h_1)) = m + \lambda m_2 = r(h_1) + r(h_2), \text{ p.e.s } f(m_1 + \lambda m_2) = f(m_1) + \lambda f(m_2).$$

$$\therefore r(1 \cdot 1 \cdot 1) = r(h_1) - m_1 \Rightarrow r \circ f = \text{id}_M.$$

(c) $r: N \rightarrow N$ lineal : $r \circ f = \text{id}_N$

Sea $S: P \rightarrow N$ lineal
 $R \mapsto S_1 : p(S) = R$, se puede probar que es posible.
 $S_1 : q(S_1) = p(S_2) \Rightarrow S_1 - S_2 \in \ker p = \text{Im } f$

y tiene sentido pues:

$$\Rightarrow \exists t : f(t) = S_1 - S_2$$

$$\Rightarrow r \circ f(t) = t = r(S_1) - r(S_2)$$

Otro camino. Por 2 y 3.
 $\text{Im } f$ tiene complementario, $f \circ g \Leftrightarrow \exists r: r \circ f = \text{id}_N$

$\text{Im } f = \ker g$ tiene complementario, $g \circ f \text{ posible} (\Leftrightarrow \exists S: p \circ S = \text{id}_P)$.

Por lo tanto (a) ss; (b) ss; (c).

$$\text{Así: } N = \text{Im } f \oplus \text{Im } S$$

es isomorfo a A -módulos.

Observa que: $N = \ker f \oplus \text{Im } S = \text{Im } f \oplus \text{Im } S$ (por definición 3).
 Como $N = \text{Im } f \oplus \text{Im } S$ y $f \circ g = \text{id}_N$.

$$\psi(x_1y) = 0 \Rightarrow 0 = f(x_1) + S(p) \Rightarrow f(x_1) = 0 \Rightarrow x_1 = 0, \text{ pues } f \text{ iny.}$$

$$S(p) = 0 \Rightarrow p = p \cdot S(p) = f(0) = 0$$

Observa que $\psi \notin \text{lineal}$, con

$\therefore \ker \psi = \{0\}$ y todo $n \in N$: $n = f(x) + S(p)$

$\therefore \psi$ isomorfismo.

Problema 6. $0 \rightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}_2$, $f(x) = 2x$. exacto pues

inyectiva: $2x = 2y \Rightarrow x = y$.

$$S: 0 \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{f \otimes \text{id}} \mathbb{Z}/2\mathbb{Z}$$

No es exacto (ta pone)

$$f(x \otimes \bar{y}) = (2x \otimes \bar{y}) = 2(x \otimes \bar{y}) = (x \otimes 2\bar{y}) = 0$$

pero: $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \Rightarrow f \text{ no es inyectora}$

$$(x \otimes \bar{y}) = (x, \bar{y}) \rightarrow \bar{x}\bar{y}$$

bilineal

(x) pones: $\psi: \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ lineal

$$(x, \bar{y}) \rightarrow \bar{x}\bar{y}$$

lineal

$$\Rightarrow \exists! f: \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$$

$$x \otimes \bar{y} \mapsto \bar{x}\bar{y}$$

\therefore es sobre \therefore es inyectora $\therefore \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

$$\text{y } f(1 \otimes \bar{1}) = \bar{1}$$

$$f(0 \otimes \bar{1}) = 0$$

GUIA 5 TOPICOS EN TEORIA DE ALGEBRAS

PRIMER SEMESTRE 2014

1. Sean F cuerpo, A una F -álgebra, K una extensión de F . Considere $A_K = K \otimes_F A$, la extensión escalar de A por K . Si A es de dimensión finita y $\{a_1, a_2, \dots, a_n\}$ es una base de A entonces $z \in A_K$, $z = \sum_{i=1}^n \alpha_i \otimes a_i$.
 - a) Si J es de Jordan $\text{car}(F) \neq 2$, entonces J_K es de Jordan.
 - b) Si L es de Lie, entonces L_K es de Lie.
 - c) Si A es alternativa, entonces A_K es alternativa.
2. Sea K una extensión algebraica de F , $K \neq F$. Pruebe que $K \otimes_F K$ no es un álgebra de división. Sugerencia: Como $F \subset K$, existe $a \in K, a \notin F$. Pruebe que $a \otimes 1_K - 1_K \otimes a \neq 0$ es un divisor de cero de $K \otimes_F K$. Use que $\{1_k, a, \dots, a^{n-1}\}$ es una base de la extensión $F(a)$ sobre F y $\{a^i \otimes a^j\}_{i,j \in \{0,1,\dots,n-1\}}$ es una base de $F(a) \otimes_F F(a)$, donde $n = \text{grado de } \text{irr}(a, F)$.
3. Si M es un módulo se llama proyector sobre M a todo endomorfismo f del módulo M tal que $f^2 = f$. Sea P submódulo de M . Pruebe P tiene complementario en M , \iff hay proyector sobre M cuyo núcleo es P , \iff hay proyector sobre M cuya imagen es P .
4. Pruebe que todo submódulo y cada cuociente de un módulo semi-simple es semi-simple.
5. Pruebe que el \mathbb{Z} -módulo \mathbb{Z} no es semi-simple.
6. Pruebe que si el A -módulo A es semi-simple entonces todo ideal por la izquierda J de A contiene un elemento e , $e^2 = e$ y $Je = J = Ae$.
7. Sea $(M_i)_{i \in I}$ una familia de módulos semi-simples. Pruebe que $M = \bigoplus_{i \in I} M_i$ es un módulo semi-simple.

GUIA 5 TOPICOS EN TEORIA DE ALGEBRAS

PRIMER SEMESTRE 2014

1. Sean F cuerpo, A una F -álgebra, K una extensión de F . Considere $A_K = K \otimes_F A$, la extensión escalar de A por K . Si A es de dimensión finita y $\{a_1, a_2, \dots, a_n\}$ es una base de A entonces $z \in A_K$, $z = \sum_{i=1}^n \alpha_i \otimes a_i$.

- a) Si J es de Jordan $\text{car}(F) \neq 2$, entonces J_K es de Jordan.
- b) Si L es de Lie, entonces L_K es de Lie.
- c) Si A es alternativa, entonces A_K es alternativa.

- ✓ 2. Sea K una extensión algebraica de F , $K \neq F$. Pruebe que $K \otimes_F K$ no es un álgebra de división. Sugerencia: Como $F \subset K$, existe $a \in K, a \notin F$. Pruebe que $a \otimes 1_K = 1_K \otimes a \neq 0$ es un divisor de cero de $K \otimes_F K$. Use que $\{1_k, a, \dots, a^{n-1}\}$ es una base de la extensión $F(a)$ sobre F y $\{a^i \otimes a^j\}_{i,j \in \{0,1,\dots,n-1\}}$ es una base de $F(a) \otimes_F F(a)$, donde $n = \text{grado de } \text{irr}(a, F)$.

- ✓ 3. Si M es un módulo se llama proyector sobre M a todo endomorfismo f del módulo M tal que $f^2 = f$. Sea P submódulo de M . Pruebe P tiene complementario en $M \iff$ hay proyector sobre M cuyo núcleo es $P \iff$ hay proyector sobre M cuya imagen es P .

- ✓ 4. Pruebe que todo submódulo y cada cuociente de un módulo semi-simple es semi-simple.

- ✓ 5. Pruebe que el \mathbb{Z} -módulo \mathbb{Z} no es semi-simple.

- ✓ 6. Pruebe que si el A -módulo A es semi-simple entonces todo ideal por la izquierda J de A contiene un elemento e , $e^2 = e$ y $Je = J = Ae$.

- ✓ 7. Sea $(M_i)_{i \in I}$ una familia de módulos semi-simples. Pruebe que $M = \bigoplus_{i \in I} M_i$ es un módulo semi-simple.

A un \mathbb{Z} -módulo, con multiplicación usual.

$$0 \subseteq J \subseteq (1), J \neq 0 \Rightarrow \exists p \neq 0, p \in J$$

J ideal por la izquierda

$$\Rightarrow J \text{ es submódulo, semi-simple} \stackrel{1}{\Rightarrow} \exists T : A = J \oplus T$$

problema 3: $P \leq T$. i) P tiene complementario ss. si hay proyector Π cuya imágen es P si
ii) proyector sobre Π cuya imagen es P (iii)

(i) sc. (ii)

Si P es complementario $\Pi = P \oplus T$ sc.: $\Psi: \Pi \rightarrow \Pi$ bien dada pues $\Pi = P \oplus T$

observar que $\ker \Psi = \{m \in \Pi : m_T = 0\} = P$ y $\Psi^2(m) = \Psi(m_T) = m_T = \Psi(m) \Rightarrow \Psi^2 = \Psi$

y si existe $\Psi: \Pi \rightarrow \Pi$: $\ker \Psi = P$, $\Psi^2 = \Psi$

Sea $T = \text{Im } \Psi$, entonces si $m \in M$:

$$\text{homo } \Psi(m+n) = (m+n)_T = m_T + n_T \quad (\text{mismo sum})$$

$$m \mapsto m_T$$

$$0 = \Psi(m) - \Psi(m) = \Psi(m-m), \forall m \in \Pi$$

$\therefore \exists t \in \ker \Psi : t(m) + T = m \quad \therefore \Pi = P + T$.

y si $a \in P \cap T$: $t(a) = 0$, $\exists p \in T : \Psi(p) = a \Rightarrow \Psi^2(p) = \Psi(p) = a = 0 \quad \therefore \Pi = P \oplus T$.

(ii) ss. (iii)

Si P es complementario $\Pi = P \oplus T$ Sea $\Psi: \Pi \rightarrow \Pi$ bien dada y homo pors $\Pi = P \oplus T$,

$$\text{Im } \Psi = P, \quad \Psi^2 = \Psi.$$

Recíprocamente: $\Psi: \Pi \rightarrow \Pi$, $\text{Im } \Psi = P$, $\Psi^2 = \Psi$.

Sea $T = \ker \Psi$; entonces si $m \in \Pi$: $0 = \Psi^2(m) - \Psi(m) = \Psi(\Psi(m) - m) \quad \forall m \in \Pi$

$$\therefore \exists t \in \ker \Psi = T : m = t + \Psi(m) \quad \therefore \Pi = P + T$$

y si $a \in P \cap T$: $\Psi(a) = 0$, $\exists p \in T : \Psi(p) = a \Rightarrow \Psi^2(p) = \Psi(p) = a = 0 \quad \therefore \Pi = P \oplus T$.

problema 4. Pruebe que todo submódulo N card. coíncide de un módulo semi-simple es semi-simple.

Demonstración: 1) Sea $\Pi = \bigoplus_{i \in I} \Pi_i$, Π_i simple, $N \leq \Pi$. Sea $N_i = N \cap \Pi_i$.

$$\text{entonces: } N = \sum_{i \in I} N_i \Pi_i. \quad \text{si: } x \in N_j \cap \bigcap_{i \neq j} \Pi_i \Rightarrow x \in \Pi_i \cap \bigcap_{i \neq j} \Pi_i = \{0\}$$

$$\therefore N = \bigoplus_{i \in I} N_i. \quad \text{Sea } J \text{ submódulo de } \Pi_i \Rightarrow 0 \neq J \subseteq N_i \subseteq \Pi_i \Rightarrow J = \Pi_i$$

$$\Rightarrow J = N_i \quad \because N_i \text{ es simple} \quad \therefore N \text{ es semi-simple.}$$

2) Sea Π/N cociente de Π . Consideremos: En general si Ψ es homo de módulos.

Π semi-simple $\Rightarrow \Psi(\Pi)$ semi-simple.

$$\Pi = \bigoplus_{i \in I} \Pi_i, \quad \text{sea: } N_i = \Psi(\Pi_i), \quad \text{si } m \in \Pi_i \Rightarrow \Psi(m) = \Psi(\sum_{j \in I} m_j) = \sum_{j \in I} \Psi(m_j) = \sum_{j \in I} \Psi(n_j) = \sum_{j \in I} n_j$$

$$\Rightarrow x = \psi(m_{ii}) = \psi(\sum m_j)$$

$$\Rightarrow m_i - \sum m_j \in \text{Ker } \psi \subseteq \cap, \text{ s. } \text{Ker } \psi = \{0\} \Rightarrow u = \sum m_j, m_j \in M_j$$

$$\Rightarrow m_i = \sum m_j + \sum m_j'$$

$\Rightarrow \dots$

$$a \otimes 1_K = 1_K \otimes a$$

Rückbeweis: Sei $(n_i)_{i \in I}$ eine Basis, die den direkten Summanden $N = \bigoplus_{i \in I} n_i$ erzeugt. Seien n_i semisimpliz.

$$\text{dann gilt } n_i = \bigoplus_{j \in J} t_j$$

$$\text{Folgerung: } x \in N \Rightarrow x = \sum_{i \in I} m_i, m_i = \sum_{j \in J} m_{ij} \Rightarrow x = \sum_{i \in I} \sum_{j \in J} m_{ij} \Rightarrow N = \sum_{i \in I, j \in J} n_{ij}$$

$$\text{Akkumulation: } \text{Sei } x \in N \cap N_{k+1} \Rightarrow x \in N \cap \left(\sum_{i \in I} n_{ik} + \sum_{l \neq k} N_l \right)$$

$$\therefore x = m_{ij} = \sum_{k \neq i} m_{ik} + \underbrace{\sum_{l \neq k} m_{il}}_{\in \sum_{l \neq k} N_l} \Rightarrow m_{ij} = \sum_{k \neq i} m_{ik} \Rightarrow m_{ij} = 0 \quad : N = \bigoplus_{i \in I, j \in J} n_{ij}$$

Con N_{ij} simpliz.

oder Form: Sei N ein Submodul von $N \Rightarrow \exists T: N = N \oplus T$

$$\Rightarrow N|N = \frac{N \oplus N}{N} = \frac{N}{N} \cong T \text{ ist semisimpliz. per Induktionshypothese.}$$

$$\text{Oder Form: Sei } N \leq N \Rightarrow N = N \cap N = N \bigoplus_{i \in I} n_i$$

$$\text{Dann } N \cap N \subseteq \bigoplus_{i \in I} (n_i) \cap N$$

$$\Rightarrow \sum_{i \in I} n_i \cap N = \bigoplus_{i \in I} n_i \cap N \subseteq \bigoplus_{i \in I} n_i \cap N \text{ folgt aus Konstruktion der Kontraktionsbündel.}$$

$$\text{Beispiel: } \bigoplus_{i \in I} n_i \cap N = \bigoplus_{i \in I} n_i \cap N'$$

$$\text{Dann } n_i \cap N \leq n_i \Rightarrow n_i \cap N = 0 \text{ & } n_i \cap N = n_i \Rightarrow N = \bigoplus_{i \in I} n_i \Rightarrow N|N = \bigoplus_{k \in I-J} n_k \text{ Semisimpliz.}$$

GUIA 7 TOPICOS EN TEORIA DE ALGEBRAS
SEGUNDO SEMESTRE 2014

1. Sea M un A -módulo semi-simple. Sea $x \in M, x \neq 0$. Pruebe que Ax contiene un A -módulo simple.

Sugerencia: Considere el conjunto $\mathcal{T} = \{N \mid N \text{ submódulo de } Ax, x \notin N\}$.

Vea que tiene elemento maximal N_1 y pruebe que su complementario en Ax es simple.

2. Sea M un A -módulo. Se define el **radical** de M como el conjunto $\text{rad}(M) = \cap\{N \mid N \text{ submódulo de } M, M/N \text{ simple}\}$. Puede suceder que no haya submódulos N de M , tal que M/N sea simple, en este caso diremos por convención que $\text{rad}(M) = M$. Pruebe que:

- (a) $\text{rad}(M)$ es un submódulo de M .
- (b) Sea N es submódulo de M , entonces $\text{rad}(M/N) = 0$ implica que $\text{rad}(M) \subseteq N$.
- (c) $\text{rad}(M/\text{rad}(M)) = 0$.

Note que también $\text{rad}(M) = \cap\{N \mid N \text{ submódulo maximal de } M\}$.

3. Sea M un A -módulo. Si M es semi-simple, pruebe que $\text{rad}(M) = 0$.

4. Sea M un A -módulo. Pruebe que son equivalentes

- (a) M es finitamente generado y semi-simple.
- (b) M es artiniano y $\text{rad}(M) = 0$.

5. El radical de un anillo R es el radical de R considerado como R -módulo a la izquierda. Pruebe que $\text{rad}(R)$ es un ideal bilátero de R .

6. (Lema de Nakayama). Sea M un A -módulo finitamente generado y N submódulo de M tal que $N + \text{rad}(M) = M$. Pruebe que $N = M$.
7. Sea M un A -módulo finitamente generado y $\{x_1, \dots, x_n\}$ un conjunto finito de generadores de M . Una condición necesaria y suficiente para que un elemento $x \in M$ pertenezca a $\text{rad}(M)$ es que cualquiera que sean los elementos $\alpha_1, \dots, \alpha_n$ de A , los elementos $x_1 + \alpha_1 x, \dots, x_n + \alpha_n x$ forman un sistema de generadores de M .
8. Sea M un A -módulo. Se define el **sócalo de M** como el conjunto $\text{soc}(M) = \sum\{N \mid N \text{ submódulo simple de } M\}$. Pruebe que:
- $\text{soc}(M)$ es un submódulo semi-simple de M .
 - Sea N es submódulo semi-simple de M , entonces $N \subseteq \text{soc}(M)$.
 - M es semi-simple sí y sólo sí $\text{soc}(M) = M$.
 - $\text{soc}(\text{soc}(M)) = \text{soc}(M)$.
 - Si $\text{soc}(M) = M$, entonces $\text{rad}(M) = 0$.
9. Pruebe las siguientes implicaciones para \mathbb{Z} -módulos.
- $M = \mathbb{Z}$ implica que $\text{rad}(M) = \text{soc}(M) = 0$.
 - $M = \mathbb{Q}$ implica que $\text{rad}(M) = M$ y $\text{soc}(M) = 0$.
 - $M = \mathbb{Q}/\mathbb{Z}$ implica que $\text{rad}(M) = M$ y $0 \neq \text{soc}(M) \neq M$.

Teoría de Álgebras
Ejercicios Resueltos Apuntes

Ejercicio 1.23 Sea $x \in \left(\frac{a, b}{F}\right) \setminus 10^3$, $x = c + z$ con $c \in F$, $z \in A_+$.

Pruebe que $x \in A_+ \Leftrightarrow x \notin Z(A) \wedge x^2 \in Z(A)$.

Dem. (\Rightarrow) $x \in A_+ \setminus 10^3$: $x = c_1 i + c_2 j + c_3 ij$, $x \neq 0$.

$$\begin{aligned} xi &= (c_1 i + c_2 j + c_3 ij)i = c_1 i^2 + c_2 ji + c_3 iji \\ &= ac_1 + c_2 ji - ac_3 j \end{aligned}$$

$$ix = i(c_1 i + c_2 j + c_3 ij) = c_1 ii + c_2 ij + c_3 i^2 j = ac_1 + c_2 ij + c_3 aj$$

$$xi = ix \Leftrightarrow -c_2 = c_2 \wedge -ac_3 = c_3 a$$

$$\Leftrightarrow c_2, c_3 = 0.$$

$$\cancel{x(i\cancel{j}\cancel{ij})} = (c_1 i + c_2 j + c_3 ij)(ijk) = c_1 i^2 jk + c_2 jik + c_3 ijijk$$

$$x(ijk) \neq abcijk$$

$$= c_1 i^2 ij + c_2 jij ik + c_3 ijijk$$

$$= -abc_1 i - abc_2 j - abc_3 ij$$

~~$$(ijk)x = (ijk)(c_1 i + c_2 j + c_3 ij)$$~~

~~$$= c_1 i jki + c_2 i jkj + c_3 i jkij$$~~

~~$$= c_1 ijiji + c_2 ijijj + c_3 ijiji$$~~

~~$$= -abc_1 i - abc_2 j - abc_3 ij$$~~

(\Rightarrow) $x \in A_+$. Como $x = 0 \Rightarrow x \in Z(A)$

$$x^2 = (c_1 i + c_2 j + c_3 ij)^2 = (c_1 i + c_2 j + c_3 ij)(c_1 i + c_2 j + c_3 ij)$$

$$\begin{aligned} &= c_1^2 i^2 + c_1 c_2 ij + c_1 c_3 ij + c_2 c_1 ji + c_2 c_3 ij + c_3 c_1 ji \\ &\quad + c_3 c_2 ij + c_2 c_3 ij + c_3^2 iji \end{aligned}$$

$$\begin{aligned} &= ac_1^2 + c_1 c_2 ij + ac_1 c_3 j - c_1 c_2 ij + bc_2 - bc_2 c_3 i - ac_1 c_3 j \\ &\quad + bc_2 c_3 i - abc_3^2 = ac_1^2 + bc_2 - abc_3^2 \in F \cong Z(A) \end{aligned}$$