Algebra Avanzada

Nociones Introductorias

Aplicación a la Teoría de Códigos

Ejercicios Resueltos

Dr. Cristián Mallol Comandari

APOYO ACADÉMICO A PREGRADO

EDICIONES UNIVERSIDAD DE LA FRONTERA

Algebra Avanzada

Nociones Introductorias

Aplicación a la Teoría de Códigos

Ejercicios Resueltos

Algebra Avanzada

Nociones Introductorias

Aplicación a la Teoría de Códigos

Ejercicios Resueltos

Cristián Mallol Comandari

DEPARTAMENTO DE INGENIERÍA MATEMÁTICA
FACULTAD DE INGENIERÍA CIENCIAS Y ADMINISTRACIÓN

EDICIONES UNIVERSIDAD DE LA FRONTERA

En memoria de Yerko Valderrama,

mi primer maestro.

Estas Notas introductorias son el fruto de enseñar el álgebra por más de una década en el marco de licenciaturas y pedagogías en Matemática así como en el seno de la formación de variadas ingenierías, particularmente la Ingeniería Matemática. Los estudiantes encontrarán aquí la belleza y el rigor propios del álgebra, con sus dificultades y desafíos: les agradezco a ellos, de todo corazón, el interés y la paciencia.

Los temas que presentamos aquí son ineludibles para una introducción formal al estudio del álgebra. Necesitando como requisito el manejo de los conceptos y del lenguaje conjuntista -que se resumen en el comienzo- el lector podrá formarse una idea básica pero exigente de las estructuras algebraicas -grupos, anillos, cuerpos, espacios vectoriales, etc.- y de sus propiedades y ramificaciones. Al respecto hemos incorporado una mirada sobre la teoría de códigos en bloque, como una aplicación de varias de las herramientas algebraicas desarrolladas previamente. Por último, un set de ejercicios resueltos está a disposición, aunque se aconseja utilizarlos solamente como ayuda y en caso alguno para reemplazar la reflexión personal.

Estas Notas no hubieran sido lo mismo sin el trabajo de mis ayudantes Ruben Martínez, Fredna Riquelme, Adrialy Muci y Rodrigo Garcés, quienes aportaron frescura, pasión y candidez en la enseñanza de los conceptos que aquí se exponen: para ellos toda mi gratitud.

Quiero agradecer también a mis colegas por su lectura y sugerencias, particularmente al doctor Richard Varro de la Universidad de Montpellier. Mi reconocimiento, también, a los doctores María Teresa Alcalde, César Burgueño y Raúl Benavides, de la Universidad de La Frontera, por las conversaciones e intercambios de ideas en torno de la enseñanza del álgebra.

Finalmente expreso todo mi agradecimiento a las Ediciones de la Universidad de La Frontera y a su Dirección de Extensión por invitarme a publicar este libro.

Contenidos

C'est difficile de prevoir, surtout l'avenir

Le Sapeur Camember (Francia, 1900)

1. Preambulo Conjuntista

Este capítulo es un recuento de los saberes mínimos, tanto conceptuales como de escritura, relativos a la Teoría de Conjuntos, que son requeridos para el estudio de las materias que se exponen en este cursillo. Es altamente recomendable que las aseveraciones que aquí se exponen sean reflexionadas, demostradas y completamente adquiridas por los lectores.

Un conjunto es una colección de objetos de cualquier naturaleza; este está determinado por los elementos que lo componen, es decir por los elementos que pertenecen a tal conjunto, noción que denotamos por el símbolo $\in$. Darse un conjunto es por tanto conocer la **lista** de los elementos que lo conforman (por ejemplo, $M = \{1, 2, 4, 8\}$) o la **propiedad** que deben satisfacer sus elementos (por ejemplo $S = \{s \ ; \ s \text{ número entero múltiplo de } 4\}$).

A partir de esto, podemos establecer las **operaciones conjuntistas** bien conocidas: sean A y B dos conjuntos

- $A \cup B = \{x \ ; \ x \in A \text{ o } x \in B\}$: la **reunión** de A y B.
- $A \cap B = \{x \ ; \ x \in A \text{ y } x \in B\}$: la **intersección** de A y B. Si A y B no tienen elementos comunes decimos que son disjuntos; en tal caso la intersección es el **conjunto vacío**: $A \cap B = \emptyset$.

De la definición de las operaciones, se infiere que estas son **conmutativas**, es decir que se tiene: $A \cup B = B \cup A$ y $A \cap B = B \cap A$. También son **asociativas**, es decir que $(A \cup B) \cup C = A \cup (B \cup C)$ y $(A \cap B) \cap C = A \cap (B \cap C)$, por lo que podemos escribir sin problemas de ambiguedad $A \cup B \cup C$ y $A \cap B \cap C$. Por último, estas operaciones se **distribuyen** (una respecto de la otra), es decir: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ y $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Otra operación es la siguiente:

- $A \smallsetminus B = \{x \in A \ ; \ x \notin B\}$: la **diferencia** de A y B.

No es dificil demostrar, utilizando ejemplos, que aquí no hay conmutatividad ni asociatividad.

Un conjunto A es **subconjunto** de un conjunto B, cuestión que denotamos por $A \subset B$, si todo elemento de A es también un elemento de B, lo que

escrito en notación matemática se expresa como:

$$A \subset B \overset{\text{si y sólo si}}{\Leftrightarrow} \left(\overset{\text{para todo}}{\forall} x, \text{ si } x \in A \overset{\text{entonces}}{\Rightarrow} x \in B \right).$$

Es claro que se tiene la equivalencia $A = B \Leftrightarrow A \subset B$ y $B \subset A$. También es inmediato que se tiene $A \cap B \subset A, B \subset A \cup B$ y por último no es difícil establecer que la inclusión ($\subset$) es compatible con las operaciones conjuntistas recién señaladas, es decir que si $A \subset B$ se tiene $A \cup C \subset B \cup C$, $A \cap C \subset B \cap C$ y $A \smallsetminus C \subset B \smallsetminus C$, para cualquier conjunto C.

Dado un conjunto E denotamos por $\wp(E)$ el conjunto cuyos elementos son todos los subconjuntos de E; este se denomina conjunto de las **partes** de E. Si $A \in \wp(E)$ se define el **complemento** de A respecto de E por $\complement_E A = E \smallsetminus A$; es claro que $\complement_E A = \{x \in E \ ; \ x \notin A\}$. No presenta problemas ver que se tiene: $A \cup \complement_E A = E$ y $A \cap \complement_E A = \emptyset$. Si no hay ambiguedad posible en cuanto al conjunto respecto del cual se complementa, podemos denotar simplemente $\complement A$. La acción de complementar invierte la inclusión, es decir si A y B son subconjuntos de E y $A \subset B$ entonces $\complement B \subset \complement A$; respecto de las operaciones conjuntistas no es difícil establecer también que si A, $B \in \wp(E)$ entonces se tiene: $\complement(A \cup B) = \complement A \cap \complement B$, $\complement(A \cap B) = \complement A \cup \complement B$ y $A \smallsetminus B = A \cap \complement B$; las dos primeras identidades se conocen como las leyes de De Morgan.

Dados $a \in E$ y $b \in F$ se define el **par ordenado** de estos elementos por la escritura (a, b) y la propiedad: $(a, b) = (c, d) \Leftrightarrow a = c$ y $b = d$. Esto quiere decir que el órden en que aparecen los elementos en la escritura es esencial; no es el caso de $\{a, b\}$ donde el órden de escritura no importa; por lo demás, una definición conjuntista de par ordenado está dada por $(a, b) = \{a, \{a, b\}\}$. El conjunto de todos los pares ordenados, $\{(x, y) \ ; \ x \in E, \ y \in F\}$, se llama el **producto cartesiano** de E y F y se denota por $E \times F$; es claro que en general, salvo si $E = F$, se tiene $E \times F \neq F \times E$. Respecto de las operaciones conjuntistas, si $A, A' \subset E$ y $B, B' \subset F$ se tiene:

- $A \subset A' \subset E$ y $B \subset B' \subset F \ \Rightarrow \ A \times B \ \subset \ A' \times B' \ \subset E \times F$,
- $(A \times B) \cup (A' \times B') \ \subset \ (A \cup A') \times (B \cup B')$,
- $(A \times B) \cap (A' \times B') = (A \cap A') \times (B \cap B')$,
- $\complement A \times \complement B \ \subset \ \complement (A \times B) = \big(\complement A \times F\big) \cup \big(E \times \complement B\big)$.

Una **relación** de E en F es cualquier manera de asociar elementos de E con elementos de F; esto lo denotamos por $R : E \to F$ y decimos que E es el conjunto de salida y F el conjunto de llegada de la relación. No hay restricción alguna para definir una relación, salvo el orden en la escritura: si $a \in E$ está en relación R con $b \in F$ escribimos aRb. Es claro que dado el orden inherente, podemos identificar aRb con (a, b); esto nos lleva a entender que una relación R puede concebirse también como un subconjunto R de $E \times F$ y usar una u otra escritura dependiendo del contexto en que se trabaje.

Un caso particular son las relaciones definidas sobre un conjunto, es decir $R : E \to E$; entre las propiedades que puede tener este tipo de relación destacamos las siguientes:

- Reflexividad: $\forall a \in E$ se tiene aRa.
- Simetría: si $a, b \in E$ y aRb entonces también se tiene bRa.
- Antisimetría: si $a, b \in E,\ a \neq b$ y aRb entonces no se tiene bRa.
- Transitividad: si $a, b, c \in E$ tal que aRb y bRc entonces se tiene aRc.

Ahora bien, la gran mayoría de las relaciones no satisface ninguna de estas propiedades. Sin embargo, aquellas que verifican la primera, tercera y cuarta se llaman **relaciones de orden** y sirven para establecer comparaciones entre los elementos del conjunto. También están las **relaciones de equivalencia**, que son aquellas que verifican la primera, segunda y cuarta propiedad y se utilizan para clasificar objetos (elementos, conjuntos, etc.) que tienen ciertos grados de similaridad; la clasificación es dada por **las clases de equivalencia**, lo que se define $\forall a \in E$ como $cl(a) = \{x \in E \ ; \ xRa\}$. Las clases de equivalencia constituyen una partición de E, es decir son conjuntos no vacíos, disjuntos y cuya reunión da la totalidad de E.

Tanto las relaciones de orden como las de equivalencia aparecen en diversos temás de la matemática (álgebra, análisis, teoría de grafos, etc.) y son herramientas importantes.

Una **función** de E en F es un caso particular de relación, en el sentido de que todo elemento de E tiene un y sólo un elemento asociado en F. Si $\varphi : E \to F$ es una función y $x \in E$, el único elemento de F relacionado con x a través de φ se denota por $\varphi(x)$ y se llama la **imagen** de x. Si

tenemos funciones $\varphi : E \to F$ y $\psi : F \to G$, la función **compuesta** de φ y ψ se define por $\psi \circ \varphi : E \to G$, cuya acción sobre $x \in E$ está dada por $(\psi \circ \varphi)(x) = \psi(\varphi(x))$. La escritura $\psi \circ \varphi$ no es conmutativa: por ejemplo tomemos $\varphi, \psi : \mathbb{N} \to \mathbb{N}$ definidas por $\varphi(n) = 1 + n$ y $\psi(n) = n^2$; se tiene $(\psi \circ \varphi)(n) = (1+n)^2$ y $(\varphi \circ \psi)(n) = 1+n^2$. Más aún, en general, si tenemos la compuesta $\psi \circ \varphi$ escribir $\varphi \circ \psi$ puede no tener sentido alguno, pués la composición de funciones requiere que el conjunto de llegada para una función sea el conjunto de salida para la otra.

Como vimos, todas las funciones salen de la misma manera del conjunto que hace de dominio: de cada elemento sale una y sólo una flecha. En cuanto a como llegan, se puede hacer una clasificación : una función es **inyectiva** si cada elemento del conjunto de llegada recibe a lo más una flecha (dicho de otra manera, elementos distintos de E tienen imágenes distintas en F); es **sobreyectiva** si cada elemento del conjunto de llegada recibe a lo menos una flecha; por último, es **biyectiva** si es inyectiva y sobreyectiva, es decir si cada elemento del conjunto de llegada recibe una y solo una flecha. Escrito en lenjuaje matemático tenemos: sea $\varphi : E \to F$; entonces

- φ es inyectiva $\Leftrightarrow \forall\ a, b \in E,\ \ (a \neq b \Rightarrow \varphi(a) \neq \varphi(b))$.
- φ es sobreyectiva $\Leftrightarrow \forall\ c \in F,\ \exists\ a \in E$ tal que $\varphi(a) = c$.
- φ es biyectiva $\Leftrightarrow \forall\ c \in F,\ \exists!\ a \in E$ tal que $\varphi(a) = c$.

Demás está decir que la mayoría de las funciones no corresponde a ninguno de estos tres grupos. Sin embargo, este tipo de funciones juega un importante rol en cuanto a establecer equivalencias o comparaciones entre estructuras (conjuntistas, topológicas, algebraicas, etc.).

Si entre dos conjuntos existe una biyección, decimos que tienen el mismo **cardinal**; si existe una inyección entre A y B o, lo que es equivalente, una sobreyección entre B y A (ver ejercicios) decimos que $card(A) \leq card(B)$.

El cardinal de $\mathbb{N}$ se denota $\aleph_0$ (alef cero); si $card(A) = \aleph_0$ decimos que A es numerable**.**

Dado un conjunto E le asociamos su **función identidad** $Id_E : E \to E$ definida por $Id_E(x) = x$ para todo $x \in E$; es claro que se tiene $\varphi \circ Id_E = \varphi$ para toda función φ que sale de E y $Id_E \circ \psi = \psi$ para toda función ψ que

llega a E. Si se tiene $E \underset{\psi}{\overset{\varphi}{\rightleftarrows}} F$ de manera que $\psi \circ \varphi = Id_E$ y $\varphi \circ \psi = Id_F$ decimos que φ y ψ son **inversas** una de otra; utilizando la asociatividad de la composición de funciones, no es difícil mostrar que la inversa, de existir, es única, por lo que denotamos $\psi = \varphi^{-1}$ (evidentemente que también se tiene $\varphi = \psi^{-1}$). Es un buen ejercicio demostrar que decir "φ tiene inversa" es equivalente a decir "φ es biyectiva".

Si $\varphi : E \to F$ es una función, $A \subset E$ y $B \subset F$ definimos la **imagen directa** de A por φ y la **imagen recíproca** de B por φ a los respectivos conjuntos $\varphi(A) = \{\varphi(a) \ ; \ a \in A\}$ y $\varphi^{-1}(B) = \{x \in E \ ; \ \varphi(x) \in B\}$; llamamos la atención de que esta escritura no significa que φ tenga inversa (es una notación molesta), sin embargo, cuando existe φ^{-1} hay coincidencia entre la imagen recíproca de φ y la imagen directa de φ^{-1} . Las imágenes directas son subconjuntos de F y las imágenes recíprocas son subconjuntos de E; esto significa que al darse una función de E en F nos damos también aplicaciones de $\wp(E)$ en $\wp(F)$ (la imagen directa) y de $\wp(F)$ en $\wp(E)$ (la imagen recíproca).

El comportamiento de estas nuevas aplicaciones respecto de las operaciones conjuntistas es disímil: la imagen directa es solo compatible con la reunión, es decir, si A_1 y A_2 son subconjuntos de E se tiene entonces que $\varphi(A_1 \cup A_2) = \varphi(A_1) \cup \varphi(A_2)$; en cambio, con respecto a la intersección sólo se tiene la inclusión $\varphi(A_1 \cap A_2) \subset \varphi(A_1) \cap \varphi(A_2)$. La imagen recíproca funciona bien con todas las operaciones conjuntistas, es decir, si $B_1, B_2 \subset F$ se tiene $\varphi^{-1}(B_1 \cup B_2) = \varphi^{-1}(B_1) \cup \varphi^{-1}(B_2)$, $\varphi^{-1}(B_1 \cap B_2) = \varphi^{-1}(B_1) \cap \varphi^{-1}(B_2)$ y $\varphi^{-1}(B_1 \smallsetminus B_2) = \varphi^{-1}(B_1) \smallsetminus \varphi^{-1}(B_2)$.

Terminamos este capítulo con el concepto de **familia**: una familia de objetos (conjuntos, elementos, estructuras, etc.) está dada por la escritura $(Objeto_i)_{i \in I}$; el conjunto I se llama el conjunto de índices; este conjunto puede ser finito o infinito, ordenado o sin orden. En definitiva una familia no es más que las imágenes de una función del conjunto de índices al conjunto que contiene los objetos que se quieren indiciar; así por ejemplo, $(b_j)_{j \in J}$ es una aplicación $f : J \to B$ y $f(j) = b_j$. Si el cónjunto de índices es $\mathbb{N}$ en vez de familia también comunmente se habla de sucesión

Si $(A_i)_{i \in I}$ es una familia de conjuntos (o subconjuntos de un conjunto) la reunión y la intersección de los elementos de la familia se denotan y definen por: $\bigcup_{i \in I} A_i = \{a \ ; \ a \in A_i, \text{ algún } i \in I\}$, $\bigcap_{i \in I} A_i = \{a \ ; \ a \in A_i, \ \forall i \in I\}$.

No presenta dificultad ver que se tiene: $B \cap \left(\bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} (B \cap A_i)$ y también $B \cup \left(\bigcap_{i \in I} A_i \right) = \bigcap_{i \in I} (B \cup A_i)$; luego $\left(\bigcup_{i \in I} A_i \right) \cap \left(\bigcup_{j \in J} B_j \right) = \bigcup_{i \in I, j \in J} (A_i \cap B_j)$ y $\left(\bigcap_{i \in I} A_i \right) \cup \left(\bigcap_{j \in J} B_j \right) = \bigcap_{i \in I, j \in J} (A_i \cup B_j)$.

Por último, las leyes de De Morgan respecto de los complementos:

$$\complement \left(\bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} \complement A_i \text{y} \complement \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} \complement A_i.$$

Ejercicios

1. Sea U un conjunto y definamos los conjuntos: $\{n \in \mathbb{N} \ / \ n^2 < 0\}$; $\{A \subset U \ / \ A = \complement A\}$; $\{u \in U \ / \ u \neq u\}$; $\{x \in \mathbb{R} \ / \ x^3 \leq 125\}$. Dé razones y argumentos que prueben que los tres primeros son iguales y que están contenidos estrictamente en el último.

2. Sean $A, B \subset U$.

   a) Demuestre las leyes de De Morgan:
   $\complement(A \cup B) = \complement A \cap \complement B$; $\complement(A \cap B) = \complement A \cup \complement B$

   b) Demuestre las siguientes expresiones son equivalentes a $A \subset B$:
   $\complement B \subset \complement A$; $\wp(A) \subset \wp(B)$; $A \cap B = A$; $A \cup B = B$;
   $A \cap X \subset B \cap X$, $\forall\ X \in \wp(U)$; $A \cup X \subset B \cup X$, $\forall\ X \in \wp(U)$.

3. Sean E, F dos conjuntos y $E * F = \{A \times B \ / \ A \subset E \text{ y } B \subset F\}$. Compare y estudie condiciones para que haya igualdad, entre los conjuntos: $E * F$, $\wp(E \times F)$ y $\wp(E) \times \wp(F)$.

4. Sean $A, B \subset E$, $C, D \subset F$ y $f : E \to F$ una función.

   a) Estudie si hay relación entre: $f(\complement A)$ y $\complement f(A)$.

   b) Demuestre que: $A \subset B \Rightarrow f(A) \subset f(B)$; $f(A \cup B) = f(A) \cup f(B)$; $f(A \cap B) \subset f(A) \cap f(B)$.

c) Pruebe que f es inyectiva si y sólo si $f(A \cap B) = f(A) \cap f(B)$ para todo $A, B \subset E$.

d) Además demuestre que:

1) f es inyectiva si y sólo si $f(\complement A) \subset \complement f(A)$ para todo $A \subset E$.

2) f es sobreyectiva si y sólo si $\complement f(A) \subset f(\complement A)$ para todo $A \subset E$.

5. Sean $f : E \to F$ una función y $C, D \subset F$.

   Demuestre que:

   a) $C \subset D \Rightarrow f^{-1}(C) \subset f^{-1}(D)$;

   b) $f^{-1}(\complement D) = \complement f^{-1}(D)$;

   c) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

   d) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

6. Demuestre que para todo $A \subset E$, y $D \subset F$ se tiene:

   a) $A \subset f^{-1}(f(A))$ y $f(f^{-1}(D)) \subset D$.

   b) f es inyectiva si y sólo si $A = f^{-1}(f(A))$ para todo $A \subset E$.

   c) f es sobreyectiva si y sólo si $f(f^{-1}(D)) = D$ para todo $D \subset F$.

7. Sean $f : E \to F$ y $h : E \to H$ funciones.

   Demuestre que se tiene:

   a) Si $h \circ f$ es inyectiva entonces f es inyectiva .

   b) Si $h \circ f$ es sobreyectiva entonces g es sobreyectiva.

8. Sean $f : E \to F$ y $h, k : E \to F$ funciones tales que $h \circ f = Id_E$ y $f \circ k = Id_F$. Demuestre que f es biyectiva y $h = k$.

9. Concluya del ejercicio anterior que f es biyectiva si y solamente si admite una función inversa, es decir, $f^{-1} : F \to E$ tal que

$$f^{-1} \circ f = Id_E \quad \text{y} \quad f \circ f^{-1} = Id_F.$$

10. Sea $f : E \to F$ una función. Demuestre que se tiene:

    a) Si f es inyectiva entonces existe $g : F \to E$ sobreyectiva tal que $g \circ f = Id_E$.

    b) Si f es sobreyectiva entonces existe $g : F \to E$ inyectiva tal que $f \circ g = Id_F$.

11. Sean F un conjunto finito totalmente ordenado y $f : F \to F$ una función. Demuestre que:

    a) Si f es creciente, entonces existe $a \in F$, tal que $f(a) = a$ (es decir, f tiene un punto fijo).

    b) Si f es decreciente, entonces tiene un punto fijo o existen $a, b \in F$, tales que $f(a) = b$ y $f(b) = a$ (es decir, un ciclo de orden 2).

12. Estudie el ejercicio anterior en el caso en que F sea infinito.

13. Sean E un conjunto y $\varphi : \wp(E) \to \wp(E)$ creciente (según el orden dado por la inclusión). Demuestre que φ admite un punto fijo.

14. Demuestre que no existe una función sobreyectiva de E en $\wp(E)$.

15. Sea F un conjunto finito. Si $|F| = n$ demuestre que $|\wp(F)| = 2^n$.

16. Demuestre o dé una idea de demostración de los enunciados siguientes:

    a) Dados dos conjuntos, existe una función inyectiva o una sobreyectiva de uno en el otro (primera parte del teorema de Cantor-Schröder-Bernstein).

    b) Si dados dos conjuntos existen funciones inyectivas de uno en el otro, entonces existe una biyección entre ellos (segunda parte del teorema de Cantor-Schröder-Bernstein).

2. Sobre Inducción y Conteo

Los números naturales o enteros nos acompañan desde los albores de la organización humana y nos brindaron los primeros saltos hacia la abstracción: la formalización de reglas de cálculo y la infinitud.

Este conjunto que denotamos por $\mathbb{N}$ y que contiene a los números $0, 1, 2, \ldots$ (aunque en algunos textos va sin el cero, pues en realidad tal número nos llega mucho después) es totalmente ordenado y es inmediato aceptar que "*todo subconjunto de* $\mathbb{N}$ *tiene un elemento mínimo*" (o un menor elemento), enunciado que se conoce como Axioma del Buen Orden. Este axioma permite establecer el Principio de Recurrencia o de Inducción Matemática, herramienta eficaz para demostrar propiedades que digan relación, de una manera o de otra, con los números enteros, siempre y cuando tales propiedades sean inductivas. Ahora bien, decimos que una propiedad P relacionada con números enteros es **inductiva** (o recursiva) si cada vez que es válida en un entero n (lo que generalmente se escribe como "$P(n)$ es verdadera") entonces también es válida en el entero que sigue. Resumiendo, una propiedad P es inductiva si se tiene la implicación: $P(n)$ es verdadera $\Rightarrow P(n+1)$ es verdadera.

El enunciado que sigue establece el Principio de Inducción:

Teorema 1 *Si P es una propiedad inductiva y existe un entero α para el cual P es válida, entonces la propiedad es verdadera en todo elemento del conjunto* $\mathbb{N}_\alpha = \{\alpha, \alpha+1, \alpha+2, \ldots\}$.

Demostración. En definitiva, lo que tenemos que demostrar es que el conjunto $F = \{n \in \mathbb{N}_\alpha;\ P(n) \text{ es falso}\}$ es vacío. En efecto, si no lo fuera F tendría un elemento mínimo μ para el cual obviamente se tiene que $\alpha < \mu$ (pues $P(\alpha)$ es verdadera y $P(\mu)$ es falsa). Se infiere entonces que $\mu - 1$ es un elemento de $\mathbb{N}_\alpha \setminus F$ y por tanto verifica la propiedad P. Pero, así las cosas, la inductividad de P nos lleva a que $P(\mu)$ es verdadera lo que contradice la definición de μ. ■

La manera de realizar una demostración por inducción se organiza con los siguientes pasos: primero, escoger el menor elemento para el cual una propiedad P es válida; este será el elemento que **inicializa la recurrencia**. Segundo, demostrar la inductividad de la propiedad en cuestión; esto pasa suponer la validez de $P(n)$ - lo que se llama **hipótesis de inducción** - para luego establecer la implicación: $P(n) \Rightarrow\ P(n+1)$.

Veamos dos ejemplos:

- Para todo entero natural n se tiene: $n^3 + 5n$ es múltiplo de 6.

  Obviamente 0 y 1 satisfacen la expresión. Veamos si la propiedad es inductiva: suponemos que n^3+5n es múltiplo de 6 (hipótesis de recurrencia) y estudiamos la expresión para el entero siguiente; para ello escribimos $(n+1)^3 + 5(n+1) = (n^3 + 5n) + 3(n^2 + n + 2)$. Bastaría entonces demostrar que $3(n^2 + n + 2)$ es múltiplo de 6, o sea que $n^2 + n + 2 = n(n+1) + 2$ es múltiplo de 2, lo que es inmediato pues $n(n+1)$ es el producto de dos enteros consecutivos y por tanto un número par. Luego, la afirmación es verdadera para todo entero.

- Para todo $n \neq 3$ se tiene $2^n \geq n^2$.

  Hacemos notar que esta propiedad es verificada por el 0, 1, 2 y 4, con lo que tenemos suficiente para iniciar la recurrencia. Ahora supongamos que para un $n > 4$ la aserción se cumple, y demostremos que entonces también se cumple para $n+1$. La hipótesis de inducción nos dice que $2^n \geq n^2$ y por tanto $2^{n+1} \geq 2n^2 = (n+1)^2+(n^2-2n-1)$; luego bastaría establecer que $n^2 - 2n - 1 \geq 0$ o, lo que es lo mismo, que $n^2 - 2n \geq 1$, lo que es verdadero si $n > 4$ pues $n^2 - 2n = n(n-2)$ es el producto de dos enteros no nulos.

Como vemos, generalmente se trata de trabajar con cálculo y escritura lo que entrega la hipótesis de recurrencia para n de manera llegar a establecer la propiedad al nivel $n+1$.

Pasemos ahora a indagar un poco en eso del conteo.....

El arte de contar o *Ars Combinatoria* es el arte de organizar el conteo de objetos interrelacionados por definiciones o exigencias restrictivas.

Una regla básica e inmediata en lo que al conteo respecta, es que si los conjuntos R y T son **disjuntos** entonces $|R \cup T| = |R| + |T|$, donde la notación $|...|$ significa "número de elementos". Por lo demás, es inmediato establecer que en general se tiene $|A \cup B| = |A| + |B| - |A \cap B|$.

Apliquemos lo anterior a un ejemplo, determinar el número de subconjuntos de un conjunto dado: si X un conjunto y $a \in X$, escoger un subconjunto A de X que contenga al elemento a es equivalente a escoger, sin ambigüedad,

un subconjunto $B \subset X$ que no contenga tal elemento, a la sazón $B = X - A$. Esto significa que hay una biyección entre los conjuntos:

$$S_a = \{A \subset X,\, a \in A\} \text{ y } N_a = \{B \subset X,\, a \notin B\}$$

por lo que se tiene, en el caso finito, $|S_a| = |N_a|$. Como es claro que S_a y N_a constituyen una partición de $\wp(X)$, por lo que acabamos de ver se tiene: $|\wp(X)| = 2\,|S_a| = 2\,|N_a|$. Una consecuencia inmediata de esto es que si $X = Y \cup \{a\}$, con $a \notin Y$, (o, dicho de otro modo, $Y = X - \{a\}$), entonces $|\wp(X)| = 2\,|\wp(Y)|$. Luego, como $|\wp(\emptyset)| = 1$, inductivamente se infiere de lo anterior que si se tiene $|X| = n$ entonces $|\wp(X)| = 2^n$.

Veamos ahora a otro problema clásico de conteo.

Representar un conjunto finito por extensión es exhibir la lista de sus elementos, cuestión que hacemos de la forma siguiente: $\{a,\, b,\, \ldots, z\}$. Según esta convención, el conjunto vacío es representado por $\{\ \ \}$.

Puesto que un conjunto está determinado por los elementos que lo conforman, la presentación por extensión de este no depende, obviamente, de como escribimos sus elementos entre los dos paréntesis, y es inmediato que el "saco" podemos llenarlo de diversas maneras: $\{a,\, c,\, b,\, d,\, \ldots\}$, $\{z,\, y,\, \ldots\}$, $\{a,\, z,\, b,\, y, \ldots\}$, etc.

Necesitamos introducir ciertas definiciones y notaciones: dado un conjunto A, $|A| = n \geq 0$, denotamos por **n!** (que llamamos **ene factorial**) el número de formas posibles **de describir** al conjunto A por extensión.

Es inmediato por la definición que se tiene: $0! = 1! = 1$.

Ahora bien, si $n \geq 2$, es claro que cuando estamos en el proceso de presentación del conjunto por extensión, al cabo de un momento habremos escrito $n - 1$ elementos. Según nuestra definición la lista de estos primeros $n - 1$ elementos podemos hacerla de $(n - 1)!$ maneras.

Para cada una de estas $(n - 1)!$ escrituras tenemos n posibilidades de incluir el último elemento, a la sazón, antes del primero, entre el primero y el segundo, entre el segundo y el tercero, y asi sucesivamente, hasta llegar a ubicarlo después del último. Este raciocinio nos ha llevado a probar que $n! = (n-1)!\cdot n$. Como se tiene que $1! = 1$, inductivamente podemos establecer que $n! = 1 \cdot 2 \cdot \ldots \cdot n$.

Otro problema tipo de la combinatoria es el siguiente:

Si n y k son enteros no negativos, ¿cuántos subconjuntos de k elementos admite un conjunto de n elementos?

Digamos primero que es claro que tal número no puede depender de la naturaleza del conjunto dado, es decir, la cantidad buscada no varía si cambiamos de conjunto.

Como no hay ninguna ambigüedad posible, denotemos por C_n^k **el número de subconjuntos de k elementos** que admite un conjunto B de n elementos.

De la definición se deduce, naturalmente, que $C_n^0 = 1$ y $C_n^n = 1$, como también que $C_n^k = 0$ si $k > n$.

Asimismo, se infiere que $C_n^k = C_n^{n-k}$, pues como ya vimos anteriormente, escoger un subconjunto es determinar también su complemento.

Ahora bien, si $a \notin B$ y $A = B \cup \{a\}$, los subconjuntos de k elementos de A se dividen en dos clases: los que no poseen al elemento a y aquellos que lo poseen.

Evidentemente que los de la primera clase no son otros que los subconjuntos de B que tienen k elementos; igualmente inmediato es que los otros provienen de los subconjuntos de B que tienen $k-1$ elementos, a los cuales se le ha agregado el elemento a.

Sin conocer aún la expresión concreta de los números C_n^k, el análisis anterior permite establecer la hermosa relación recursiva:

$$C_{n+1}^k = C_n^k + C_n^{k-1}$$

Esta relación, que debemos al matemático francés Blaise Pascal, permite ir construyendo estos números (en la literatura especializada los números C_n^k se llaman **combinaciones**).

Calculemos, ahora, el valor de C_n^k. Para ello veamos que para formar un subconjunto de k elementos comenzamos pòr elegir un elemento b_1 de B; para ello tenemos n posibilidades. El segundo elemento, b_2, lo escogemos obviamente entre los $n-1$ elementos restantes y como $\{b_1, b_2\} = \{b_2, b_1\}$ hay $n(n-1)/2$ maneras de formar un subconjunto de B con dos elementos. Siguiendo con el mismo tipo de análisis, tenemos $n-2$ opciones para escoger un tercer elemento lo que nos entrega $n(n-1)(n-2)$ posibilidades de haber elegido b_1, b_2 y b_3 en ese orden; dado que para formar un conjunto el orden de

escritura de sus elementos no importa y podemos describirlo por extensión de 3! maneras, tendremos en definitiva $n(n-1)(n-2)/3!$ subconjuntos de tres elementos. Así sucesivamente, podemos establecer que

$$C_n^k = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Ahora bien, las expresiones $\frac{n!}{k!(n-k)!}$ también se conocen como **coeficientes binomiales** y aparecen con la notación $\binom{n}{k}$. Esta denominación viene de la necesidad de encontrar una expresión utilizable para calcular $(a+b)^n$ con $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Para ello, lo primero es observar que, si no reordenamos los productos resultantes por acción de la conmutatividad, el desarrollo de tal expresión es un larga suma de términos, cada uno formado de n factores formados por letras a y/o b, del tipo $aababbaa\cdots$, etc.

Asi por ejemplo, se tiene:

$$\begin{aligned}(a+b)^2 &= aa + ba + ab + bb \\ (a+b)^3 &= aaa + baa + aba + bba + aab + bab + abb + bbb\end{aligned}$$

Obviamente, utilizando la conmutatividad, una expresión que tiene k factores a lo terminamos escribiendo $a^k b^{n-k}$. Pero al hacer esto perdemos de vista una cuestión fundamental, que es la que en definitiva nos permite contar cuantas expresiones con k factores a aparecen en la suma. En efecto, si reflexionamos vemos que cuando trabajamos con la escritura no modificada por la conmutatividad, lo que ocurre de una expresión a otra (con k factores a) es que escogemos otro conjunto de k "lugares" (de un conjunto de n "lugares") para poner las letras a. O sea, se manifiestan aquí las combinaciones C_n^k. Dicho de otro modo, hay $\binom{n}{k}$ expresiones con k factores a, con lo que podemos escribir la formula que se conoce como el binomio de Newton:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Terminamos este capítulo con un comentario necesario y un ejemplo ad-hoc: La acción de enumerar o contar sólo puede realizarse una vez que hayamos entendido las definiciones y relaciones que unen a los objetos en juego. En la mayoría de los casos estas son de una complejidad tal, que sin herramientas matemáticas poderosas (como las series generadoras, temas que están lejos de ser tratados en este nivel), los problemas combinatorios

son altamente disuasivos y debemos contentarnos con el conteo de algunos casos particulares, generalmente con ayuda de la computación, que puedan ayudarnos en nuestra intuición del problema. Pero en general, es muy difícil llegar a resultados tan específicos como los que hemos desarrollado hasta aquí. Algunas veces, con suerte, podemos establecer una formula recursiva: eso ya es tocar el cielo...

Para ilustrar lo recién dicho, estudiemos el problema siguiente: dado un conjunto A con n elementos, ¿cuantas relaciones de equivalencia se pueden definir sobre A?

Como sabemos, darse una relacion de A en A es en definitiva escoger un subconjunto R de A^2 y que la relación es de equivalencia si tiene las siguientes propiedades:

- Reflexividad: para todo $a \in A$, $(a, a) \in R$.
- Simetría: si $(a, b) \in R$, entonces $(b, a) \in R$.
- Transitividad: si (a, b) y $(b, c) \in R$, entonces $(a, c) \in R$.

El conteo de las relaciones reflejas, así como el de las simétricas y, por ende, el de las reflejas y simétricas, no presenta mayor dificultad, siempre y cuando nos ubiquemos en una posición apta para organizar el conteo.

Primero convengamos que cuando representamos A^2 como un plano cartesiano, lo hacemos dando implícitamente un orden total a los elementos de A. Para los fines que aquí nos ocupan, ello no produce distorsiones.

Teniendo claro lo anterior, si nos situamos en el plano cartesiano A^2, las relaciones reflejas son aquellos subconjuntos de A^2 que contienen la diagonal $D = \{(a, a),\ a \in A\}$. Esto quiere decir que las relaciones reflejas son de la forma $D \cup S$ donde $S \subset A^2 - D$; concluimos que el número de relaciones reflejas es $|\wp(A^2 - D)|$, es decir $2^{n(n-1)}$.

En cuanto a las relaciones simétricas, notemos que los puntos (a, b) y (b, a) se ubican en el plano A^2 en simetría axial con respecto a la diagonal D. Dicho de otra manera, si en el triángulo inferior de A^2, es decir el conjunto $A^2_{Inf} = \{(a_i, a_j) \in A^2,\ i \leq j\}$, la relación simétrica tiene un cierto subconjunto de puntos, entonces tendrá el reflejo de este a través de la diagonal en el triágulo superior.

Todo esto nos dice que el número de relaciones simétricas es exactamente el número de subconjuntos posibles de A^2_{Inf} ; dada la configuración triangular, no presenta dificultad ver que $\left|A^2_{Inf}\right| = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$, por lo cual el número de relaciones simétricas es $2^{\frac{n(n+1)}{2}}$.

Por último el lector podrá convencerse que el número de relaciones reflejas y simétricas está dado por $\left|\wp(A^2_{Inf} - D)\right| = 2^{\frac{n(n-1)}{2}}$.

Tratar de trabajar la transitividad en el plano cartesiano A^2 es ruda tarea; con unos pocos bocetos y algo de observación racional, nos convencemos rapidamente que ello está ligado a la clasificación y conteo de los conjuntos convexos que puedan allí dibujarse.

Esta no es por tanto la buena óptica para organizar el conteo de las relaciones de equivalencia.

Cambiemos pues el punto de vista.

Sabemos que toda relación de equivalencia determina (y es determinada) por las clases que ella genera. El conjunto de clases de equivalencia es una partición del conjunto A y es evidente que toda partición de A induce trivialmente una relación de equivalencia (aquella definida por "a esta en relación con b si pertenecen al mismo pedazo de la partición").

Todo esto quiere decir que darse una relación de equivalencia en A es similar a darse una partición de A.

Denotemos ahora por $\pi(n, k)$ el número de particiones de un conjunto de n elementos en k pedazos, $k \geq 1$; es inmediato que se tiene: $\pi(n, 1) = 1$ y $\pi(n, n) = n$. Aunque quizás ya no sea necesario, reiteramos que este tipo de número no depende de la naturaleza del conjunto en juego. Esto significa que el número total de particiones de un conjunto de n elementos esta dado por la suma: $\pi(n) = \pi(n, 1) + \pi(n, 2) + \cdots + \pi(n, n)$.

Ahora bien, pese a las apariencias en nada hemos avanzado para responder al propósito que nos hemos impuesto.

Para poder dar herramientas de conteo que nos permitan avanzar, aunque sea paso a paso, necesitamos saber un poco más sobre el comportamiento estructural de los números $\pi(n, k)$.

En lo que sigue buscaremos explicitar una relación recursiva entre estos números.

Si $B = A \cup \{b\}$, con $b \notin A$, el número de particiones de B en k pedazos está dado por $\pi(n+1, k)$. Con un poco de observación concluimos que estas particiones de B son de dos tipos:

- Aquellas en que aparece el singleton $\{b\}$ y que corresponden a las particiones de A en $k-1$ pedazos a las cuales les agregamos $\{b\}$. Son, por tanto, $\pi(n, k-1)$ particiones.
- Aquellas en que b aparece en un subconjunto estrictamente más grande que $\{b\}$. Cada una de estas corresponde a una partición de A en k subconjuntos en la cual hemos escogido un pedazo para agregar al elemento b. Como por cada una de estas particiones tenemos k maneras de agregar b y hay en total $\pi(n, k)$ particiones distintas, el número de particiones que refleja la situación que estamos describiendo es $k\pi(n, k)$.

Con lo analizado en los dos puntos anteriores hemos logrado establecer la relación recursiva: $\pi(n+1, k) = \pi(n, k-1) + k\pi(n, k)$.

Como se puede apreciar, la estructura de la relación encontrada no es en nada simple. No es recomendable perder el tiempo buscando la expresión concreta de $\pi(n)$ en función de n, .

Ejercicios

1. Demuestre que

   - $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$.
   - $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.
   - $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.

   Encuentre una expresión en función de n para $1^4 + 2^4 + 3^4 + \cdots + n^4$

2. Sean E y F dos conjuntos finitos, $|E| = n$ y $|F| = m$. Encuentre el número de funciones de E en F. Si $n \leq m$ ¿cuantas de estas funciones son inyectivas?

3. Sea A un conjunto, $|A| = m$ y k tal que $2 \leq k \leq m$. Si $a_1, a_2, \ldots, a_k$, son elementos distintos de A, cuente el número de subconjuntos de A que no contienen ningun a_i, $1 \leq i \leq k$.

4. Si a, $b \in A$, cuente el número de subconjuntos de A que contienen a lo más uno de los elementos a o b. La misma situación anterior, pero cambiando la frase "a lo más uno" por la frase "al menos uno".

5. Sea A un conjunto finito, $|A| = n$. Demuestre que

$$|\{P \ / \ P \subset A, \ |P| \ \text{ par}\}| = |\{I \ / \ I \subset A, \ |I| \ \text{ impar}\}| = 2^{n-1}.$$

6. Establezca los números C_n^k, para $0 \leq k \leq n$, en los casos $n = 3$, 4, 5, 6 y 7. Para ello utilice la relación de Pascal (dicho de otra manera, construya lo que se conoce como el Triángulo de Pascal).

7. Calcule en función de n las sumas $\sum_{k=0}^{n} \binom{n}{k}$, $\sum_{k=0}^{n} \binom{n}{2k}$ y $\sum_{k=0}^{n} \binom{n}{2k+1}$.

3. Leyes de Composición y Estructuras

Las ideas y expresiones algebraicas surgen a través de los tiempos como una necesidad de conceptualizar y formalizar estructuralmente operaciones cuyas propiedades y comportamiento tienen una cierta similitud.

Más allá de las escrituras y notaciones utilizadas, el ser humano ha estado confrontado a problemas de cálculo y las operaciones "basicas" entre números (suma, resta, multiplicación y división) aparecen temprano en la historia, aunque no algoritmicamente pues la representación decimal surge tarde, con la aparición del cero por el siglo XI.

Poco a poco, impulsada por el aumento en número y complejidad de los intercambios comerciales y fundamentalmente por el desarrollo de la física y de la astronomía, va tomando forma, paulatinamente, la escritura formal (uso de letras y símbolos) para expresar distintos tipos de operaciones, resolución de ecuaciones, comportamiento de objetos geométricos (simetrías), etc.

Basicamente, para comenzar, necesitamos precisar lo siguiente: dados a y b, dos objetos o elementos de un mismo tipo, ¿cómo producir un tercero, sin ambiguedad, a partir de ellos? (por ejemplo el 5, con el 2 y el 3 a partir de la suma).

En lo que viene formalizamos esta idea; tenemos:

Definición 2 *Sea E un conjunto no vacío: llamamos* ***ley de composición interna*** *a toda función $\Lambda : E \times E \to E$. Así mismo, dado otro conjunto no vacío F, llamamos* ***ley de composición externa*** *de F sobre E a toda función $\Theta : F \times E \to E$.*

En vez de ley de composición, también podemos hablar de **operación** (interna o externa) entre elementos. Por razones de escritura eficiente, el elemento $\Lambda(a, b)$,que resulta de la composición de a con b, lo denotaremos en general por ab o $a + b$, pudiéndose utilizar también, si fuera necesario, expresiones tales como: $a \circledast b$, $a \triangle b$, etc..

En caso alguno debe pensarse que estamos trabajando exclusivamente con números, situación que corresponde, como se verá, a un importante pero pequeño caso particular.

Definición 3 *Llamamos* ***estructura algebraica*** *a un conjunto E provisto de una o más operaciones; en tal caso, expresamos eso por $(E, +)$, $(E, \cdot)$ o $(E, +, \cdot)$ etc., según el caso.*

Además, se dice que una estructura $(E, \cdot)$:

- *es* ***conmutativa****, si $ab = ba$ para todo $a, b \in E$;*
- *es* ***asociativa****, si $a(bc) = (ab)c$ para todo $a, b, c \in E$;*
- *admite* ***neutro****, si existe $e \in E$ tal que $ae = ea = a$, $\forall a \in E$;*
- *admite* ***absorbente****, si existe $z \in E$ tal que $az = za = z$, $\forall a \in E$;*

Asi las cosas, el conjunto de los enteros naturales con la suma usual, que denotamos por $(\mathbb{N}, +)$, es una estructura conmutativa, asociativa y con neutro (el 0); por otro lado, $(\mathbb{N}, \cdot)$, es también una estructura conmutativa, asociativa y con neutro (el 1), pero además con absorbente (el 0). Otro ejemplo, menos usual pero muy importante, es el siguiente: dado un conjunto A consideremos la estructura $(\mathcal{F}(A), \circ)$ donde $\mathcal{F}(A) = \{f;\ f : A \to A\}$ y la operación "$\circ$" es la composición de funciones; esta estructura es asociativa, no es conmutativa y tiene neutro (la función identidad, Id_A).

Proposición 4 *Si una estructura admite un elemento neutro (o un absorbente) este es único.*

Demostración. En efecto, si e y ε son neutros de $(E, \cdot)$ se tiene $ae = ea = a$ y $a\varepsilon = \varepsilon a = a$, para todo $a \in E$; en particular, $\varepsilon \overset{e \text{ neutro}}{=} \varepsilon e \overset{\varepsilon \text{ neutro}}{=} e$. La unicidad del absorbente se trata de la misma forma. ■

En general, en una escritura multiplicativa, si la estructura $(E, \cdot)$ admite neutro, este será denotado por 1_E; si además tiene absorbente utilizaremos la notación 0_E.

Consideremos ahora a $\mathbb{Z}$, el conjunto de los enteros, con la suma. La estructura $(\mathbb{Z}, +)$, es conmutativa, asociativa y con neutro (el 0), pero además, dado $x \in \mathbb{Z}$ existe $y \in \mathbb{Z}$ tal que $x + y = 0$. Esto nos lleva a:

Definición 5 *Sea $(E, \cdot)$ una estructura con neutro 1_E. Decimos que $a \in E$ admite un* ***inverso*** *si existe $b \in E$ tal que $ab = ba = 1_E$.*

Dada la definición, el neutro siempre es inverso de si mismo. Por otro lado, en una estructura con neutro pueden haber elementos con inverso y otros que no lo admiten: por ejemplo en $(\mathcal{F}(A), \circ)$ las funciones biyectivas tienen inversas pero sabemos que no toda función de A en A es biyectiva. En cuanto

a notación, cuando un elemento a tiene un **único inverso**, denotamos este por $-a$ si la escritura utilizada es la aditiva, y por a^{-1} cuando la escritura es multiplicativa (la composición de funciones es una escritura multiplicativa).

Si $(E,\cdot)$ es una estructura y $A \subset E$ es un subconjunto no vacío, la exigencia mínima para que A sea una estructura con la operación de E y pueda ser considerada una sub-estructura de E, cuestión que se denota por $A < E$, es que necesariamente se tenga $xy \in A$ para todo $x, y \in A$; sin embargo en muchas situaciones esto no es suficiente: si tomamos los enteros módulo 20, $\mathbb{Z}_{20} = \{0, 1, \ldots, 19\}$, en donde operamos simbólicamente con la multiplicación de $\mathbb{Z}$, pero utilizando la regla de cálculo $20 = 0$, podemos constatar que $A = \{0, 5, 10, 15\}$ es estable para el producto y que el 5 hace de neutro; esto nos dice que si bien $(A,\cdot)$ es una estructura asociativa con neutro, no es una sub-estructura de $(E,\cdot)$ cuyo neutro no es el 5 sino el 1.

De la misma manera, si $(F,\cdot)$ es otra estructura y $f : E \to F$ una aplicación, la mínima exigencia de compatibilidad de f con las estructuras en juego es que se tenga $f(xy) = f(x)f(y)$ para todo $x, y \in E$; obviamente que en muchos casos esto no es suficiente y haya que agregar, por ejemplo, que $f(1_E) = 1_F$. Pasemos ahora al estudio de ciertas estructuras; tenemos:

Definición 6 *Llamamos* ***monoide*** *a una estructura $(M,\cdot)$ asociativa y con neutro; si la operación es conmutativa, hablamos de un monoide conmutativo. Además, si $A \subset M$ decimos que $(A,\cdot)$ es un* ***submonoide*** *de $(M,\cdot)$, cuestión que denotamos por $A < M$, si $1_M \in A$ y para todo $x, y \in A$, $xy \in A$. Por último, si $(N,\cdot)$ es otro monoide decimos que $f : M \to N$ es un* ***morfismo*** *(de monoides) si $f(1_M) = 1_N$ y $f(ab) = f(a)f(b)$ para todo $a, b \in M$.*

A un morfismo de monoides $f : M \to N$ le asociamos los conjuntos $Ker(f) = \{m \in M;\ f(m) = 1_N\}$ y $Im(f) = \{f(m);\ m \in M\}$, llamados respectivamente el **nucleo** y la **imagen** de f. No es difícil establecer que $Ker(f)$ es un submonoide de M y que $Im(f)$ es un submonoide de N.

Como sabemos, $(\mathbb{N},+)$, $(\mathbb{N},\cdot)$ y $(\mathcal{F}(A),\circ)$ son monoides; notemos que si el conjunto A es finito, también lo es $\mathcal{F}(A)$; el lector puede calcular el cardinal de $\mathcal{F}(A)$ cuando A tiene n elementos. Por otro lado, si a es un entero positivo la función $\mathbb{N} \to \mathbb{N}$ definida por $n \mapsto a^n$ es un morfismo del monoide $(\mathbb{N},+)$ al monoide $(\mathbb{N},\cdot)$: compruébelo. Respecto de todo esto tenemos:

Proposición 7 *En un monoide $(M,\cdot)$ si un elemento a admite un inverso este es único. Además, si $f : M \to N$ es un morfismo de monoides, $f(a)$ es invertible y $f(a)^{-1} = f(a^{-1})$.*

Demostración. Sea $a \in M$ y supongamos que b y β son inversos de a; se tiene entonces $ab = ba = 1_E$ y $a\beta = \beta a = 1_E$; utilizando la asociatividad, $b \cdot 1_E = b\,(a\beta) \overset{asociatividad}{=} (ba)\,\beta = 1_E \cdot \beta = \beta$. En cuanto a la segunda afirmación, ella se infiere de

$$1_N = f(1_M) \overset{a\ invertible}{=} f(aa^{-1}) = f(a^{-1}a) \overset{f\ morfismo}{=} f(a)f(a^{-1}) = f(a^{-1})f(a).$$

y de la unicidad de un inverso en un monoide. ■

Proposición 8 *Sea $(E, \cdot)$ una estructura asociativa con neutro 1_E. Si a, b tienen inversos entonces: $(a^{-1})^{-1} = a$ y $(ab)^{-1} = b^{-1}a^{-1}$ lo que en escritura aditiva entrega: $-(-a) = a$ y $-(a+b) = -b + -a$*

Demostración. Se desprende de la unicidad del inverso. Hágalo. ■

3.1. Sobre los Grupos

Entre las estructuras determinadas por una sóla operación, la de grupo es sin lugar a dudas la más importante; esta aparece en varias ramas de la Matemática, como también en la Física y en ciencias afines. Sirve además de sustento a definiciones de estructuras más complejas, que veremos más adelante.

En lo que sigue desarrollamos las definiciones, nomenclaturas y propiedades básicas de esta estructura, que serán utilizadas permanentemente a lo largo de este libro.

Definición 9 *Llamamos **grupo** a un monoide $(G, \cdot)$ en el cual todo elemento admite un inverso; si la operación es conmutativa, hablaremos de un grupo **abeliano**. Además, si $H \subset G$ decimos que $(H, \cdot)$ es un **subgrupo,** cuestión que denotamos por $H < G$, si es un submonoide de $(G, \cdot)$ y si además para todo $x \in H$ se tiene $x^{-1} \in H$. Finalmente, si $(L, \cdot)$ es otro grupo decimos que $f : G \to L$ es un **morfismo** (de grupos) si $f(1_G) = 1_L$, $f(a^{-1}) = f(a)^{-1}$ y $f(ab) = f(a)f(b)$ para todo $a, b \in G$.*

Hacemos notar que para $g \in G$, dada la existencia de g^{-1}, las aplicaciones $G \to G$ definidas por $l_g(x) = gx$ y $r_g(x) = xg$ son biyectivas pero en caso alguno morfismos. El resultado siguiente simplifica los test definitorios:

Proposición 10 *Sean G, L grupos, $H \subset G$ y $f : G \to L$ una aplicación. Entonces:*

- *H es un subgrupo de G si y sólo si H es no vacío y si para todo $a, b \in H$ se tiene $ab^{-1} \in H$.*
- *f es un morfismo de grupos si y sólo si $f(ab) = f(a)f(b)$ para todo $a, b \in G$.*

Demostración. Es claro que en ambos casos basta demostrar los recíprocos. Como $H \neq \emptyset$ sea $a \in H$: por un lado, $1_G = aa^{-1} \in H$; por el otro $a^{-1} = 1_G a^{-1} \in H$; finalmente, si b es otro elemento de H, puesto que ya sabemos que en tal caso $b^{-1} \in H$, se tiene $a(b^{-1})^{-1} = ab \in H$. La segunda equivalencia se deja al lector. ■

Un **isomorfismo** entre estructuras E y F (entre monoides o entre grupos, etc.) es un morfismo biyectivo $f : E \to F$. Usted puede demostrar que f^{-1}, la inversa de f, es también un morfismo. Así las cosas, las estructuras E y F son **algebraicamente indistinguibles**, es decir, todo lo que suceda con la estructura de E (propiedades, elementos singulares, etc.) sucederá sin diferencia alguna con F; esto significa que conociendo cabalmente a una se conoce absolutamente a la otra, y por tanto ellas se pueden **identificar**.

En el caso que entre E y F exista un **monomorfismo**, es decir un morfismo inyectivo $\iota : E \hookrightarrow F$, esto significa que E será isomorfa con una subestructura de F, a saber $\iota(E) < F$, puesto que ι pensado de E en $\iota(E)$ es obviamente sobreyectivo. Cuando trabajamos con grupos, la inyectividad de un morfismo es equivalente a que se tenga $Ker(\iota) = \{1_E\}$; usted puede demostrar esto como ejercicio.

El teorema que viene es importante y generaliza la construcción del grupo $(\mathbb{Z}, +)$ a partir del monoide $(\mathbb{N}, +)$:

Teorema 11 *Dado un monoide conmutativo $(M, +)$ con cancelación existe siempre el menor grupo abeliano $Gr(M)$ que contiene al monoide en cuestión.*

Menor en el sentido siguiente: $M < Gr(M)$ y no existe subgrupo de $Gr(M)$ que contenga a M; usted puede demostrar que esto es equivalente a decir que todo grupo que contiene a M contiene también a $Gr(M)$.

Demostración. Sea $(M,+)$ un monoide conmutativo con cancelación. De lo que se trata es de construir los opuestos de los elementos de M; ahora bien, por ejemplo en $\mathbb{Z}$ tenemos $15-11=23-19$ o $14-18=2-6$ lo que se expresa en $\mathbb{N}$ por $15+19=11+23$ y $14+6=18+2$, es decir, estamos trabajando con pares ordenados de enteros naturales que verifican sumas equivalentes (hechas de cierta manera).

Esto nos inspira para definir sobre $M\times M$ la relación :

$$(x,y)\backsim(z,t)\Leftrightarrow x+t=y+z.$$

Mostremos que esta relación es de equivalencia: en efecto, la reflexividad y la simetría son inmediatas (aquí se utiliza la conmutatividad de M); en cuanto a la transitividad, si $(x,y)\backsim(z,t)$ y $(z,t)\backsim(k,l)$ quiere decir que tenemos $x+t=y+z$ y $z+l=t+k$; sumando estas identidades y reordenándolas (gracias a la conmutatividad) se llega a $(x+l)+(z+t)=(y+k)+(z+t)$; utilizando la cancelación, obtenemos $x+l=y+k$, es decir $(x,y)\backsim(k,l)$ como queríamos demostrar.

Sea $Gr(M)=M\times M/\backsim$, el conjunto cociente (es decir, el conjunto de las clases de equivalencia). Utilizando la operación del monoide M, se postula la siguiente ley de composición para $Gr(M)$:

$$\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)}$$

Obviamente que tenemos que cerciorarnos de que esta operación está bien definida (es decir que no depende de los representantes de las clases en juego).

Si $\overline{(a,b)}=\overline{(a',b')}$ y $\overline{(c,d)}=\overline{(c',d')}$ debemos establecer que se tiene

$$\overline{(a+c,b+d)}=\overline{(a'+c',b'+d')}$$

es decir que $a+c+b'+d'=b+d+a'+c'$. Ahora bien, como por hipótesis $(a,b)\backsim(a',b')$ y $(c,d)\backsim(c',d')$, lo que significa que $a+b'=a'+b$ y $c+d'=c'+d$, basta sumar estas igualdades para obtener lo pedido.

No es difícil chequear que $(Gr(M),+)$ es un grupo conmutativo: en efecto, es claro que $\overline{(0_M,0_M)}$ es el neutro y trivialmente se verifica que la conmutatividad y la asociatividad se heredan de la estructura de M. Por otro lado, para cualquier $a\in M$ se tiene $\overline{(a,a)}=\overline{(0_M,0_M)}$; esto nos dice que $\overline{(a,b)}+\overline{(b,a)}=\overline{(a+b,a+b)}=\overline{(0_M,0_M)}$, es decir que $\overline{(b,a)}=-\overline{(a,b)}$ lo que prueba que $(Gr(M),+)$ es un grupo abeliano.

Finalmente, la función $\iota : M \to Gr(M)$, $\iota(a) = \overline{(a, 0_M)}$ es trivialmente un monomorfismo de monoides; como entonces M es isomorfo a $\iota(M)$ y por tanto son dos estructuras algebraicamente indistinguibles, podemos considerar a M como un submonoide de $Gr(M)$). En tal caso, conviene aligerar la escritura, identificando a con $\iota(a) = \overline{(a, 0_M)}$; así las cosas, naturalmente denotamos $\overline{(0_M, a)} = -a$ y por tanto, $\overline{(a, b)} = a - b$.

El lector puede hacer una pequeña reflexión que lo lleve a establecer que $Gr(M)$ es el menor grupo abeliano que contiene a M. ■

Veamos ahora una propiedad que en general se repite en las estructuras algebraicas:

Proposición 12 *Si G es un grupo y $(H_i)_{i\in I}$ es cualquier familia de subgrupos de G, entonces $H = \bigcap_{i\in I} H_i$ es un subgrupo de G.*

Demostración. Para esto utilicemos el test enunciado en la Proposición 10: primero, para todo $i \in I$, $1_G \in H_i$ pues cada uno es un subgrupo de G y por tanto $1_G \in H$; además, si $x, y \in H$ entonces x, y están en cada H_i y por tanto, pues se trata de subgrupos, $xy^{-1} \in H_i$ para todo $i \in I$ y así, $xy^{-1} \in \bigcap H_i$, lo que establece que H es un subgrupo de G. ■

Así las cosas, las propiedades algebraicas son generalmente estables por intersección de estructuras que las poseen. En ese sentido, es claro que si distintos subgrupos contienen a un cierto subconjunto S la intersección de ellos también lo contendrá, obteniéndose así un subgrupo menor que contiene a S. Esto nos lleva a:

Definición 13 *Sean G un grupo y S un subconjunto de G. Llamamos **subgrupo engendrado** por S al menor subgrupo de G que contiene a S y que denotamos por $\langle S\rangle$.*

Proposición 14 *Se tiene: $\langle S\rangle$ es la intersección de todos los subgrupos de G que contienen S, es decir, $\langle S\rangle = \bigcap_{S\subset H<G} H$.*

Demostración. Inmediata. ■

De acuerdo a la definición, es claro que $\langle\emptyset\rangle = \{1_G\}$ y que el subgrupo engendrado por $\{g\}$ con $g \in G$, que denotamos simplificadamente por $\langle g\rangle$ es $\{g^k;\ k \in \mathbb{Z}\}$ acordando que $g^0 = 1_G$.

Mas generalmente, usted puede verificar que

$$\langle g_1, g_2, \ldots, g_m \rangle = \left\{ g_{i_1}^{k_1} g_{i_2}^{k_2} \cdots g_{i_n}^{k_n};\ k_j \in \mathbb{Z},\ n \in \mathbb{N}^*,\ i_j = 1, 2, \ldots, m \right\}$$

Definición 15 *Un grupo G se llama **monógeno** si es engendrado por un sólo elemento, es decir, si existe $g \in G$ tal que $G = \langle g \rangle$. Si además G es finito, se dice que G es **cíclico**.*

El generador de un grupo monógeno o cíclico no tiene porqué ser único; así por ejemplo, el grupo aditivo $(\mathbb{Z}, +)$ es engendrado por 1 y -1; analogamnete, usted podrá comprobar que el grupo aditivo $(\mathbb{Z}_{20}, +)$, de los enteros módulo 20 ($\mathbb{Z}_{20} = \{0, 1, \ldots, 19\}$), es cíclico, generado obviamente por el 1, pero también por el 3 o el 7, etc.. Lo que viene requiere del resultado siguiente:

Teorema 16 *(Teorema de la División Euclidiana para enteros) Sea $d \in \mathbb{N}^*$. Entonces para todo $n \in \mathbb{Z}$ existen $q \in \mathbb{Z}$ y $r \in \mathbb{N}$, únicos, tales que $n = qd + r$ con la condición $0 \leq r < d$.*

Demostración. Basta demostrar el enunciado para $n \geq 0$ (¿porqué?). Si se tuviera $n = qd + r = q'd + r'$ con $q \geq q'$, entonces $(q - q')d = r' - r < d$, lo que es posible sólo si $(q - q')d = r' - r = 0$; luego, $q = q'$ y $r = r'$, lo que muestra la unicidad. En cuanto a la existencia, la propiedad es trivial para los enteros menores o iguales a d; sea A el conjunto de los enteros mayores que d que no verifican el enunciado. Demostremos que A es vacío: en efecto, en caso contrario, sea m el elemento mínimo de A; luego existen existen $q, r \in \mathbb{N}$, tales que $m - 1 = qd + r$ con $0 \leq r < d$ (¿porqué?). Como $r + 1 \leq d$, se infiere que $m = qd + (r + 1)$ o $m = (q + 1)d$. Contradicción. ■

Proposición 17 *Todo subgrupo de un grupo monógeno es monógeno.*

Demostración. Sea $G = \langle g \rangle$ tal grupo y $H < G$. Sea ahora p el menor entero positivo tal que $g^p \in H$ y mostremos que $H = \langle g^p \rangle$, es decir que todo elemento de H es potencia de g^p: en efecto, como $H < G = \langle g \rangle$ todos sus elementos son de la forma g^n con $n \in \mathbb{Z}$; efectuando la división euclidiana de n por p obtenemos $n = pq + r$ con $0 \leq r < p$. Así las cosas tenemos $g^n = g^{pq+r} = (g^p)^q g^r$ de donde $g^r = g^n \left((g^p)^q\right)^{-1}$ es un elemento de H (puesto que es un subgrupo) por lo que, so pena de contradecir la opción de p, obligadamente $r = 0$, o sea, $g^n = (g^p)^q$ como se quería establecer. ■

Obviamente que todo subgrupo de un grupo cíclico es cíclico.

Corolario 18 *Los únicos subgrupos de* $(\mathbb{Z}, +)$ *son los conjuntos* $n\mathbb{Z}$, $n \in \mathbb{N}$.

Demostración. Esto sale de la Proposición anterior pues es inmediato que en $(\mathbb{Z}, +)$ si $n \in \mathbb{N}$ se tiene $\langle n \rangle = \langle -n \rangle = n\mathbb{Z}$. ■

Veamos ahora lo siguiente, que nos llevará a conocer mejor a los grupos finitos y, más adelante, a la construcción de grupos que satisfagan ciertas propiedades: si G es un grupo y $H < G$ es un subgrupo cualquiera, podemos definir una relación sobre G, que llamamos $modH$ (módulo H), de la manera siguiente: si $g, k \in G$ decimos que g está en relación $modH$ con k, que denotamos por $g = k\ modH$, si $g^{-1}k \in H$. Esta relación es de equivalencia; en efecto: es reflexiva pues $g^{-1}g = 1_G \in H$; simétrica ya que si $g = k\ modH$, entonces $g^{-1}k \in H$ y, como H es un subgrupo, $k^{-1}g = (g^{-1}k)^{-1} \in H$, luego $k = g\ modH$. Finalmente, si $g = k\ modH$ y $k = l\ modH$, se tiene $g^{-1}k, k^{-1}l \in H$ de donde $(g^{-1}k)(k^{-1}l) = g^{-1}l \in H$ o sea, $g = l\ modH$.

Denotamos el conjunto cociente por G/H. ¿Como son las clases de equivalencia?

Sabemos que la clase de g está dada por el conjunto $\{x \in G; x = g\ modH\}$; ahora bien, si $g = x\ modH$ tenemos $g^{-1}x \in H$ es decir, existe $h \in H$ tal que $g^{-1}x = h$ y finalmente $x = gh$. Concluimos por tanto que las clase de equivalencia de g está dada por el conjunto $\{gh;\ h \in H\}$ que denotamos naturalmente por gH.

Obviamente que podemos invertir la escritura en la definición de la relación obteniendo una nueva equivalencia, la relación $Hmod$; en tal caso diríamos que $g = k\ Hmod$ si $kg^{-1} \in H$; en tal situación el cociente lo denotamos por $H\backslash G$ y la clases evidentemente son los conjuntos Hg. Como $gH = l_g(H)$ y $Hg = r_g(H)$ y l_g, r_g son biyecciones, los conjuntos H, gH y Hg tienen el mismo cardinal (como ejercicio demuestre que $card(G/H) = card(H\backslash G)$).

Respecto de todo lo anterior, tenemos:

Teorema 19 *(Lagrange) Sean* G *un grupo finito y* H *un subgrupo de* G. *Entonces* $|H|$ *divide a* $|G|$, *más precisamente,* $|G| = |G/H|\,|H|$ *(donde* $|X|$ *denota el número de elementos de* X*).*

Demostración. Como G es finito es claro que G/H también lo es. Supongamos que $|G/H| = n$ y sean $g_1H, g_2H, \ldots, g_nH$ los elementos (las clases) de G/H. Sabemos que los conjuntos g_kH, $1 \leq k \leq n$, constituyen

una partición de G es decir $G = \bigcup_{1\leq k\leq 1} g_k H$, reunión disjunta de conjuntos no vacíos.

Así las cosas se infiere que $|G| = \sum_{1\leq k\leq n} |g_k H| = \sum_{1\leq k\leq n} |H| = n\,|H|$, es decir que se tiene $|G| = |G/H|\,|H|$, que es lo que queríamos demostrar. ■

Llamamos **orden de un grupo** G a su cardinal y lo denotamos por $o(G)$; en ese sentido, hablamos de **orden de un elemento** $g \in G$, que denotamos por $o(g)$, al orden de $\langle g\rangle$. Estas apelaciones son sobretodo utilizadas en el ámbito de lo finito. Tenemos:

Proposición 20 *Si $\langle g\rangle$ es finito, entonces $o(g)$ es el menor entero n que verifica $g^n = 1_G$. Más aun, si $g^m = 1_G$ entonces $o(g) \mid m$.*

Demostración. Si $g = 1_G$ no hay nada que demostrar, por lo que consideramos a g distinto del elemento neutro. Es claro que al ser $\langle g\rangle$ finito existen potencias de g iguales a 1_G : en efecto, al tomar las potencias sucesivas de g tienen que haber repeticiones, es decir, en cierto momento tendremos $g^i = g^j$ con $i < j$; esto significa que $g^{j-i} = 1_G$, con $j - i > 1$ pues sabemos que $g \neq 1_G$. Luego si n es el menor entero positivo tal que $g^n = 1_G$ se tiene $\langle g\rangle = \{g, g^2, \ldots, g^{n-1}, g^n = 1_G\}$, de donde se infiere que $o(g) = n$. Para la última aseveración, realizando la división euclidiana de m por $o(g)$ se tiene $m = o(g)q + r$ con $0 \leq r < o(g)$; el resultado se infiere por el mismo tipo de raciocinio utilizado en la Proposición 17, concluyendo que $r = 0$. ■

Corolario 21 *Sea G un grupo finito. Entonces $o(G)$ es un entero primo si y solamente si G no posee más subgrupos que los triviales. En tales condiciones G es cíclico.*

Demostración. Queda para el lector. ■

3.2. Subgrupos Normales y Grupos Cocientes

Sean G un grupo y $H < G$. Retomemos aquí la construcción del conjunto cociente G/H a partir de la relación de equivalencia $modH$; ¿existe la posibilidad de proveer al cociente de una estructura de grupo inducida naturalmente por la estructura de G?

Para contestar a esta pregunta, recordemos que dada una relación de equivalencia siempre existe un función sobreyectiva natural (la proyección) que a cada elemento le asocia su clase de equivalencia. En nuestro caso tenemos $\pi : G \to G/H$, $x \mapsto xH$ y obviamente una estructura de grupo sobre el cociente G/H impone como exigencia mínima que π sea un morfismo de grupos, es decir que $\pi(g_1)\pi(g_2) = \pi(g_1 g_2)$ para todo $g_1, g_2 \in G$, o sea que se debería definir el producto en el cociente por: $g_1 H \cdot g_2 H = g_1 g_2 H$. ¿Es siempre eso posible? Lo que tenemos que ver, como cada vez que se trabaja con conjuntos cocientes y se quiere definir operaciones o verificar propiedades con las clases de equivalencia, es constatar si lo que se está definiendo no depende de los representantes de las clases.

En lo que aquí nos convoca, debemos por tanto ver si la situación $u_1 H = g_1 H$ y $u_2 H = g_2 H$ implica que $u_1 u_2 H = g_1 g_2 H$. Es decir, tenemos $u_1 = g_1 h_1$ y $u_2 = g_2 h_2$ $(*)$ para ciertos $h_1, h_2 \in H$, y debemos estudiar las condiciones para que de estas dos igualdades podamos inferir que exite $h \in H$ tal que $u_1 u_2 = g_1 g_2 h$. Ahora bien, multiplicando las dos igualdades $(*)$ sólo obtenemos $u_1 u_2 = g_1 h_1 g_2 h_2$; es claro que si G es conmutativo no habría problemas pues tendríamos $u_1 u_2 = g_1 g_2 h_1 h_2$ y bastaría tomar $h = h_1 h_2$. Sin embargo, no tenemos para que exigir tanto: para lograr nuestro cometido bastaría asegurar que existe $k_1 \in H$ tal que $h_1 g_2 = g_2 k_1$. Concluimos este análisis estableciendo que lo que se requiere es que para todo $g \in G$ y para todo $h \in H$ existe $k \in H$ (que depende de g y h) tal que $gh = kg$. Dicho de otra manera, que se tenga $gH = Hg$ para todo $g \in G$.

Proposición 22 *Sean G un grupo y $H < G$. Las afirmaciones siguientes, válidas para todo $g \in G$, son equivalentes:*

(a) $gH = Hg$ *(b)* $gH \subset Hg$ *(c)* $gHg^{-1} = H$ *(d)* $gHg^{-1} \subset H$.

Demostración. Demostremos $(b) \Rightarrow (a)$: si $gH \subset Hg$ para todo $g \in G$, entonces $g^{-1}H \subset Hg^{-1}$ de donde, multiplicando a la izquierda y a la derecha por g, obtenemos $Hg \subset gH$. Etc., etc. ■

Definición 23 *Un subgrupo $H < G$ se llama **normal** (o invariante o distinguido) si para todo $g \in G$ se tiene $gH = Hg$. Denotamos esto por $H \lhd G$.*

Como vimos, si $H \lhd G$ el conjunto G/H hereda de G una estructura de grupo definida por $gH \cdot g'H = gg'H$; $(G/H, \cdot)$ se llama grupo cociente

y obviamente se tiene $1_{G/H} = 1_G H = H$ y $(gH)^{-1} = g^{-1}H$. Para esta estructura de grupo, la proyección canónica $g \overset{\pi}{\mapsto} gH$ es un morfismo (un epimorfismo pues sabemos que es sobreyectiva) y se tiene $Ker(\pi) = H$.

Terminamos esta sección haciendo notar que los enteros *módulo* n, estudiados en primer año, no son otra cosa que los grupos $\mathbb{Z}_n$, cocientes del grupo aditivo $(\mathbb{Z}, +)$ por los subgrupos $n\mathbb{Z}$, es decir, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$; como sabemos, allí se opera formalmente como en $(\mathbb{Z}, +)$ pero con la regla de cálculo $n = 0$, pués es claro que $n\mathbb{Z}$, la clase de equivalencia de n, es el cero del cociente $\mathbb{Z}/n\mathbb{Z}$.

3.3. El Grupo Simétrico

Lo que sigue, para terminar esta breve caminata por el tópico de los grupos, se afirma en la importancia de los grupos de biyecciones, es decir, aquellos definidos por $Biy(A) = \{f;\, f : A \to A,\, f \textit{ biyectiva}\}$, con la composición de funciones como operación interna. El siguiente resultado nos explica porqué:

Teorema 24 *(Cayley-Hamilton). Todo grupo puede ser considerado subgrupo de un grupo de biyecciones.*

Demostración. De lo que se trata es de establecer que todo grupo es isomorfo a un subgrupo de algún grupo de biyecciones, y por tanto identificable a él. Sea pues G un grupo: sabemos que para todo $g \in G$ las aplicaciones (multiplicación a la izquierda) l_g son biyectivas, es decir que se tiene, $L_G = \{l_g;\ g \in G\} \subset Biy(G)$; como es inmediato que $l_{1_G} = Id_G$, $l_g \circ l_h = l_{gh}$ (pues, $g(hx) = (gh)\,x$) y $l_{g^{-1}} = l_g^{-1}$), en definitiva L_G es un subgrupo de $Biy(G)$. Ahora bién, la aplicación $l : G \to L_G$, $l(g) = l_g$ es trivialmente inyectiva (pues si $l_g = l_h$ entonces $g = l_g(1_G) = l_h(1_G) = h$); como además $l(gh) = l_{gh} = l_g \circ l_h = l(g) \circ l(h)$ y $l(G) = L_G$, la aplicación l es un morfismo que establece una isomorfía entre G y L_G. ■

Veamos ahora lo siguiente:

Proposición 25 *Sean A y B dos conjuntos. Si A y B son equipotentes (mismo cardinal) entonces sus grupos de biyección son isomorfos.*

Demostración. Sea $f : B \to A$ biyectiva. La aplicación Φ_f de $Biy(A)$ en $Biy(B)$ definida por $\Phi_f(\alpha) = f^{-1} \circ \alpha \circ f$, para $\alpha \in Biy(A)$, es biyectiva pués es inmediato que su inversa está dada por la función $\beta \mapsto f \circ \beta \circ f^{-1}$,

con $\beta \in Biy(B)$ (por lo demás, Φ_f^{-1} no es otra cosa que $\Phi_{f^{-1}}$). Como es evidente que $\Phi_f(Id_A) = Id_B$ y además como se tiene: $\Phi_f(\alpha_1) \circ \Phi_f(\alpha_2) = (f^{-1} \circ \alpha_1 \circ f) \circ (f^{-1} \circ \alpha_2 \circ f) = f^{-1} \circ (\alpha_1 \circ \alpha_2) \circ f = \Phi_f(\alpha_1 \circ \alpha_2)$, tal aplicación es un morfismo. ■

Lo anterior nos dice que para estudiar los grupos de biyecciones, podemos escoger un conjunto referencial por cardinalidad. En el caso finito, que es el que nos interesa aquí, evidentemente que tomaremos como refencia al conjunto $\mathbb{I}_n = \{1, 2, \ldots, n\}$.

Definición 26 *Llamamos* ***grupo simétrico*** *de orden n, que denotamos por* $\mathbf{S}_n$, *al grupo* $Biy(\mathbb{I}_n)$; *sus elementos se llaman* ***permutaciones****.*

No está demás en recordar que se tiene $|S_n| = n!$ (hágalo)

Las permutaciones las denotaremos, en general, con letras minúsculas griegas ($\alpha, \beta, \sigma, \pi$, etc) y la composición la escribiremos $\alpha\beta$ en vez de $\alpha \circ \beta$.

Generalmente, una permutación se puede representar por la notación operacional:

$$\sigma = \begin{pmatrix} 1 & 2 & & n \\ \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

Con este tipo de escritura, tenemos por ejemplo :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

Si $\alpha \in S_n$ definimos el **soporte** de a como $Sop(\alpha) = \{k \in \mathbb{I}_n;\ \alpha(k) \neq k\}$, es decir es el conjunto constituido por los elementos de $\mathbb{I}_n$ sobre los cuales actúa efectivamente α; claro es que $Sop(\alpha) = \mathbb{I}_n \setminus Fix(\alpha)$, donde $Fix(\alpha)$ denota al conjunto de los puntos fijos de α.

Respecto de estos conceptos tenemos:

Proposición 27 *a) Si* $k \in \mathbb{I}_n$, *entonces* $k \in Sop(\alpha) \Leftrightarrow \alpha(k) \in Sop(\alpha)$ *(obviamente, este enunciado equivale a:* $Sop(\alpha) = \alpha\,(Sop(\alpha))$*). b) Para todo* $m \in \mathbb{N}$ *se tiene* $Sop(\alpha^m) \subset Sop(\alpha)$. *c) Si* $Sop(\alpha) \cap Sop(\beta) = \emptyset$ *entonces* $\alpha\beta = \beta\alpha$ *(es decir, permutaciones con soportes disjuntos conmutan; en tal caso hablamos de permutaciones disjuntas).*

Demostración. Las afirmaciones (a) y (b) se dejan de ejercicio. En cuanto a (c), debemos mostrar que $(\alpha\beta)(k) = (\beta\alpha)(k)$ para todo $k \in \mathbb{I}_n$; como $Sop(\alpha) \cap Sop(\beta) = \emptyset$, ello resulta inmediatamente, utilizando (a) cuando corresponda, del análisis de los casos: $k \notin Sop(\alpha) \cup Sop(\beta)$, $k \in Sop(\alpha)$ y $k \in Sop(\beta)$ en los cuales se tiene, respectivamente, $\alpha(k) = k = \beta(k)$, $\alpha(k) \neq k = \beta(k)$ y $\alpha(k) = k \neq \beta(k)$. Hágalo. ■

Definición 28 *Una permutación γ se llama* ***ciclo de largo k*** *(con $k \geq 2$) si $Sop(\gamma) = \{c_1, c_2, \ldots, c_k\}$, $\gamma(c_i) = c_{i+1}$ si $1 \leq i \leq k-1$ y $\gamma(c_k) = c_1$. Los ciclos de largo 2 se denominan* ***transposiciones.***

Dada la estructura de los ciclos, podemos aligerar la notación utilizada y, en vez de

$$\gamma = \begin{pmatrix} 1 & 2 & & n \\ & & & \\ \gamma(1) & \gamma(2) & & \gamma(n) \end{pmatrix}, \text{ optamos por } (c_1, c_2, \ldots, c_k).$$

Ahora bien, no es difícil ver que dada la definición para todo $1 \leq j \leq k$ se tiene $(c_1, c_2, \ldots, c_k) = (c_j, c_{j+1,} \ldots, c_k, c_1, c_2, \ldots, c_{j-1})$ por lo que la notación de un ciclo admite varias expresiones. Podemos admitir que Id es un ciclo de largo cero; por lo demás tal suposición es coherente con la afirmación que sigue:

Lema 29 *Un ciclo de largo k es de orden k (o sea, $(c_1, c_2, \ldots, c_k)^k = Id$). En particular se infiere que para toda transposición τ se tiene $\tau = \tau^{-1}$.*

Demostración. Se deja al lector (obviamente que el recíproco no es válido: es decir una permutación de orden k no tiene porqué ser un ciclo: encuentre un ejemplo que ilustre esto). ■

Respecto de los ciclos tenemos:

Proposición 30 *Todo ciclo de largo $k \geq 2$ se descompone en producto de $k-1$ transposiciones. Tal descomposición no es única, salvo la minimalidad del número de factores (es decir no admite descomposición con un menor número de transposiciones)*

Demostración. Se hace recursivamente, pues para $k = 2$ se trivializa y para $k > 2$ no es difícil ver que $(c_1, c_2, \ldots, c_k) = (c_1, c_2, \ldots, c_{k-1})(c_{k-1}, c_k)$; esto nos lleva a que $(c_1, c_2, \ldots, c_k) = (c_1, c_2)(c_2, c_3) \cdots (c_{k-1}, c_k)$. En cuanto a la no unicidad, usted puede constatar que también se tiene $(c_1, c_2, \ldots, c_k) = (c_{k-1}, c_k) \cdots (c_2, c_k)(c_1, c_k)$, descomposición que utiliza también $k - 1$ transposiciones. ■

Lo que sigue requiere de lo siguiente: si $\sigma \in S_n, \sigma \neq Id$, y $x \in \mathbb{I}_n$ es claro que $C_{\sigma,x} = \{x, \sigma(x), \sigma^2(x), \sigma^3(x), \ldots\}$ es finito y por el hecho de haber repeticiones y de existir σ^{-1} siempre podemos escoger el menor entero positivo m (que depende de σ y de x) tal que $C_{\sigma,x} = \{x, \sigma(x), \sigma^2(x), \sigma^3(x), \ldots, \sigma^m(x)\}$.

Tenemos:

Teorema 31 *Toda permutación (distinta de la identidad) se descompone en producto de ciclos disjuntos. Esta descomposición en su minimalidad es única salvo escritura.*

Demostración. La palabra *minimalidad* se refiere al número mínimo necesario de ciclos para la descomposición

Sea $\sigma \in S_n, \sigma \neq Id$ y escojamos $x_1 \in Sop(\sigma)$; le asociamos a x_1 el conjunto $C_1 = \{x_1, \sigma(x_1), \ldots, \sigma^{m_1}(x_1)\}$; tomemos ahora $x_2 \in Sop(\sigma) \setminus C_1$ y le asociamos el conjunto $C_2 = \{x_2, \sigma(x_2), \ldots, \sigma^{m_2}(x_2)\}$; es claro que si continuamos con esta construcción sucesiva conseguiremos una partición de $Sop(\sigma)$ por conjuntos $C_1, C_2, , \ldots, C_r$.

Así las cosas, basta ahora asociar a estos conjuntos, de manera obvia y natural, los ciclos $\gamma_i = (x_i, \sigma(x_i), \ldots, \sigma^{m_i}(x_i))$; estos ciclos conmutan pues sus soportes son disjuntos y un pequeño test permite establecer que $\sigma = \gamma_1\gamma_2 \cdots \gamma_r$ (hágalo). ■

Es inmediato que el método (paso a paso) empleado en la demostración garantiza no sólo encontrar los ciclos disjuntos sino que la minimalidad de la descomposición.

Asi por ejemplo, si consideramos la permutación:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \\ 7 & 1 & 5 & 6 & 3 & 9 & 2 & 4 & 8 \end{pmatrix}$$

tomando $x_1 = 1$ logramos $\gamma_1 = (1, 7, 2)$; con $x_2 = 3$ logramos $\gamma_2 = (3, 5)$; etc. Obtenemos finalmente: $\sigma = (1, 7, 2)(3, 5)(4, 6, 9, 8)$.

Corolario 32 *Toda permutación (distinta de la identidad) se descompone en producto de transposiciones.*

Demostración. Es consecuencia inmediata de la Proposición y el Teorema anteriores. ■

Podemos ahora introducir el siguiente concepto:

Definición 33 *Una permutación σ es **par** si su descomposición (mínimal) en transposiciones utiliza un número par de factores. En caso contrario, decimos que σ es una permutación **impar**.*

*Por último, con lo anterior, definimos **el signo** de σ, que denotamos por $sg(\sigma)$, como **positivo** (o $+1$) si σ es par y como **negativo** (o -1) si σ es impar (o sea que, en definitiva, se tiene $sg(\sigma) = (-1)^{paridad\ de\ \sigma}$).*

Así las cosas, tenemos que un ciclo de largo impar es una permutación par y otro de largo impar es una permutación par (parece juego de palabras, pero no lo es).

Sea $A_n = \{\sigma;\ \sigma \in S_n,\ \sigma \text{ par}\}$ (o, lo que es lo mismo, $A_n = \{\sigma;\ sg(\sigma) = +\}$):

Teorema 34 *A_n es un subgrupo normal del grupo simétrico de orden n y se llama el **grupo alterno** de orden n. Además, $|A_n| = n!/2$*

Demostración. Es claro que $Id \in A_n$ y además no es difícil establecer que si $\sigma \in A_n$ su inverso σ^{-1} también pertenece a A_n : esto sale de que una transposición es igual a su inversa y por tanto si $\tau_1, \ldots, \tau_k$ son transposiciones se tiene $(\tau_1 \cdots \tau_k)^{-1} = \tau_k \cdots \tau_1$.

Por otro lado, si $\alpha, \beta \in A_n$ entonces tienen descomposiciones en transposiciones: $\alpha = \tau_1 \cdots \tau_{2r}$ y $\beta = \pi_1 \cdots \pi_{2s}$ de manera que $\alpha\beta = \tau_1 \cdots \tau_{2r}\pi_1 \cdots \pi_{2s}$; ahora bien si hay supresión de factores fronteras, esto se hara por pares, es decir, si $\tau_{2r} = \pi_1$ nos quedará $\alpha\beta = \tau_1 \cdots \tau_{2r-1}\pi_2 \cdots \pi_{2s}$ y así sucesivamente, manteniendose la condición de tener siempre un número par de factores. Con lo anterior se demuestra que A_n es un subgrupo de S_n.

Para lo que sigue, notemos que si τ es una transposición, las biyecciones $S_n \to S_n, \sigma \mapsto \tau\sigma$ y $\sigma \mapsto \sigma\tau$ transforman permutaciones pares en impares y vice-versa $(*)$; esto nos dice, entre otras cosas, que $|A_n| = |S_n \setminus A_n| = n!/2$ y además como $\tau = \tau^{-1}$ se infiere de inmediato que $\tau A_n \tau^{-1} = A_n$. Luego, si σ es una permutación y su descomposición en trasposiciones es $\sigma = \tau_1 \cdots \tau_r$,

sabiendo que $\sigma^{-1} = \tau_r \cdots \tau_1$, se tiene $\sigma A_n \sigma^{-1} = \tau_1 \cdots \tau_r A_n \tau_r \cdots \tau_1 = \tau_1 \cdots \tau_{r-1} A_n \tau_{r-1} \cdots \tau_1 = \tau_1 \cdots \tau_{r-2} A_n \tau_{r-2} \cdots \tau_1 = \ldots = A_n$, lo que prueba que A_n es un subgrupo normal. ■

Ejercicios

1. Sea E una estructura algebraica. Demuestre que:

   a) Si E admite un neutro ($ea = ae = a, \forall a \in E$) este es único.

   b) Si E admite un absorbente ($za = az = z, \forall a \in E$) este es único.

   c) Caracterize el conjunto E si el neutro es igual al absorbente (que tambien se llama anulador).

   d) Si E es asociativa y admite neutro, entonces cada elemento tiene a lo mas un inverso.

2. Sean $(E, \cdot)$ una estructura asociativa, $e \in E$ un elemento idempotente y M_e el conjunto definido por $M_e = eEe$. Demuestre que M_e es un monoide y es el mayor submonoide de E cuyo neutro es el elemento e.

3. Sea F una estructura asociativa finita. Demuestre que F tiene un elemento idempotente (es decir, existe x tal que $x^2 = x$).

4. Sea $(A, \boxtimes, \boxplus)$ una estructura en la cual la operación $\boxtimes$ tiene cancelación (o sea, $a \boxtimes x = a \boxtimes y \Rightarrow x = y$) y la ley $\boxplus$ se distribuye con respecto a $\boxtimes$, es decir, para todo $a, b, c \in A : (a \boxtimes b) \boxplus c = (a \boxplus c) \boxtimes (b \boxplus c)$. Demuestre que si $\boxtimes$ tiene neutro entonces $\boxplus$ tiene absorbente. Determine A cuando además $\boxplus$ tiene cancelación.

5. Sea $s : \mathbb{N} \to \mathbb{N}$ definida por $s(n) = n + 1$. Determine el conjunto F_s de las funciones $f : \mathbb{N} \to \mathbb{N}$ que conmutan con s y demuestre que es un monoide conmutativo equipotente a $\mathbb{N}$.

6. Sea E una estructura asociativa que verifica las propiedades siguientes: existe e tal que para todo $a \in E$ se tiene $ea = a$ (neutro izquierdo) y para todo $a \in E$ existe b tal que $ba = e$ (inverso izquierdo).Demuestre que E es un grupo.

7. Sea F una estructura asociativa finita que verifica las cancelaciones a la izquierda y a la derecha, ($xy = xz \Longrightarrow y = z$; $yx = zx \Longrightarrow y = z$). Muestre que F es un grupo. Dé un ejemplo en el cual, teniendo las propiedades de cancelación, no tengamos un grupo.

8. Construir cuatro subgrupos no triviales de $(\mathbb{R}^*, \cdot)$.

9. En un grupo demuestre las siguientes identidades de escritura:
   $(ab)^{-1} = b^{-1}a^{-1}$, $(a^{-1})^{-1} = a$ y $(a^{-1}ba)^n = a^{-1}b^n a$. Además, si el grupo es abeliano, $(ab)^n = a^n b^n$.

10. Encontrar todos los grupos con dos, tres, cuatro elementos.

11. En $\mathbb{Z}$ se define la operación " $\oplus$" de la manera siguiente: $a \oplus b = a+b+1$.

    a) Demuestre que $(\mathbb{Z}, \oplus)$ es un grupo abeliano.

    b) Determine $a \ominus b$ según las operaciones de $(\mathbb{Z}, +)$ y $a + b$ según las operaciones de $(\mathbb{Z}, \oplus)$.

12. Si $(G, \cdot)$ y $(H, \star)$ son grupos, demuestre que $G \times H$ con la operacion $(g, h)(g', h') = (g \cdot g', h \star h')$ es un grupo (llamado producto directo).

13. Demuestre que si $G' < G$ y $H' < H$ entonces $G' \times H' < G \times H$. ¿ Todo subgrupo de $G \times H$ es producto de un subgrupo de G con uno de H ?.

14. Se considera $E = \mathbb{R}^* \times \mathbb{R}$ con el producto: $(x, y) \cdot (z, t) = (xz, xt + y)$. Muestre que $(E, \cdot)$ es un grupo no conmutativo. De tres subgrupos no triviales de E.

15. Demuestre que si la reunion de dos subgrupos (de un grupo G) es un subgrupo, entonces uno de los subgrupos en cuestión contiene al otro.

16. Muestre que un grupo es conmutativo si y sólo si para todo a, b se tiene una de las condiciones siguientes: (a) $(ab)^{-1} = a^{-1}b^{-1}$ (b) $(ab)^2 = a^2b^2$ (c) $(ab)^n = a^n b^n$, para tres enteros consecutivos.

17. Muestre que si en un grupo G se tiene $a^2 = 1_G$ para todo a, entonces es conmutativo.

18. Sea $n \geq 1$ un entero dado y E una estructura asociativa que verifica la identidad siguiente: $yxy = x^n$ para todo $x, y \in E$. Demuestre que:

    a) Si $n = 1$, E es un grupo conmutativo.

    b) E tiene un idempotente ($a^2 = a$) que se precisará.

    c) Si E es un grupo no trivial, n es impar.

d) Si E tiene cancelación (izquierda o derecha) entonces es un grupo conmutativo.

19. Muestre que si un grupo G tiene un número par de elementos, entonces existe por lo menos un elemento $a \neq 1_G$ que verifica $a = a^{-1}$.

20. Sean G un grupo finito y H un subconjunto no vacio tal que $HH \subset H$. Demuestre que H es un subgrupo de G.

21. Sea G un grupo y $a \in G$. Demuestre que si G tiene más de dos elementos, $G - \{a\}$ no es un subgrupo. Además, si para todo $x, y \in G - \{a\}$ se tiene $xy = yx$ entonces G es abeliano.

22. Sea G un grupo y $S, T \subset G$. Demuestre que $\langle S \cap T \rangle \subset \langle S \rangle \cap \langle T \rangle$; de un ejemplo en donde $\langle S \cap T \rangle \neq \langle S \rangle \cap \langle T \rangle$. Establezca $\langle S \cup T \rangle = \langle \langle S \rangle \cup \langle T \rangle \rangle$. Compare los subgrupos de G^2 : $\langle S \rangle \times \langle T \rangle$ y $\langle S \times T \rangle$.

23. Sean G un grupo, $H < G$ y $A \subset G$. Determine $\langle G \setminus H \rangle$. ¿Que puede decir de A si $G \setminus A$ es un subgrupo de G?.

24. Sea $G = \{a_1, ..., a_n\}$ un grupo abeliano. Si $g = a_1 \cdot a_2 \cdot ... \cdot a_n$, demuestre que $g^2 = 1_G$ y, si n es impar, que $g = 1_G$. Establezca además que: (a) Si existe un único $x \neq 1_G$, tal que $x^2 = 1_G$, entonces $x = g$; (b) Si existe mas de un elemento $x \in G$, $x \neq 1_G$, tal que $x^2 = 1_G$ entonces $g = 1_G$.

25. Sean G un grupo y $g, h \in G$ tales que: $gh = hg$, $o(g), o(h) < \infty$ y $\langle g \rangle \cap \langle h \rangle = \{1_G\}$. Demuestre que $o(gh) = mcm(o(g), o(h))$.

26. Sean H, $L < G$. Entonces $HL < G$ si y solamente si $HL = LH$.

27. Sean H y L dos subgrupos de un grupo G; demuestre que si se tiene $h^{-1}Lh \subset L$ para todo $h \in H$, entonces HL es un subgrupo de G.

28. Sean G un grupo y H un subgrupo. Demuestre que:

    a) Dados $g, l \in G$, entonces $Hg = Hl$ o $Hg \cap Hl = \emptyset$.

    b) Para todo $g, l \in G$ se tiene $card(gH) = card(Hl) = card(H)$.

    c) $card(G/H) = card(H\backslash G)$.

    d) $gH = Hg$ para todo $g \in G \Leftrightarrow G/H = H\backslash G$

29. Sean G un grupo y H un subgrupo. Demuestre que si $|G/H| = 2$ entonces H es normal.

30. De un subgrupo normal no trivial del grupo $E = \mathbb{R}^* \times \mathbb{R}$ provisto de la multiplicación : $(x, y) \cdot (z, t) = (xz, xt + y)$.

31. Sea G un grupo. Demuestre que si H y L son dos subgrupos normales de G, también lo son los subgrupos $H \cap L$ y HL.

32. Sean G un grupo y H un subgrupo: ¿ Si $xH \neq yH$ se tiene $Hx \neq Hy$? Si cada vez que se tiene $xH = yH$ entonces $Hx = Hy$, demuestre que H es normal.

33. Sean G un grupo y H un subgrupo de G tal que $xHx \subset H$ para todo $x \in G$.

    a) Demuestre que $x^{2k} \in H$ para todo $x \in G$. Deduzca que si $y \in G$ tiene orden impar entonces $y \in H$.

    b) Demuestre que el subgrupo H es normal

    c) Utilizando (a) y (b), demuestre que el grupo cociente G/H es conmutativo.

    d) De un ejemplo que muestre que el reciproco de (b) no es válido (es decir, H normal no implica $xHx \subset H$ para todo $x \in G$).

34. Sean G un grupo, $n \in \mathbb{N}$ y H un subgrupo de G tal que $x^n Hx \subset H$ para todo $x \in G$. Demuestre que H es un subgrupo normal.

35. Sean G un grupo y S un conjunto generador de G (es decir, se tiene $S \subset G$ y $\langle S \rangle = G$). Muestre que un subgrupo H es normal si y solo si $s^{-1}Hs = H$ para todo $s \in S$.

36. Si $x \in G$, demuestre que xHx^{-1}es un subgrupo de G (llamado el conjugado de H por x).

    Demuestre que $N(H) = \bigcap_{x \in G} x^{-1}Hx$ es un subgrupo normal de G.

37. Sea G un grupo; se define a $Z(G)$, **el centro de** G, de la manera siguiente: $Z(G) = \{x \in G \ / \ gx = xg \ \text{ para todo } g \in G\}$.

    a) Demuestre que $Z(G)$ es un subgrupo normal de G.

b) Muestre además que $G/Z(G)$ es monógeno si y solo si G es abeliano.

38. Si H y L son dos subgrupos normales de G tales que $H \cap L = \{1_G\}$, muestre que $hl = lh$ para todo $h \in H$ y $l \in L$.

39. Si G es un grupo tal que todo subgrupo es normal, demuestre que para todo $x, y \in G$ se tiene $yx = x^n y$ para algún entero n.

40. Sean G un grupo no necesariamente finito y H un subgrupo de G, tal que G/H es finito.

    a) Demuestre que todo $x \in G$ tiene una potencia en H

    b) Consideremos ahora que $|G/H| = 3$. Si existe $x \in G$, $x^2 \notin H$, tal que $xH = Hx$, demuestre que H es un subgrupo normal. De un ejemplo en donde $|G/H| = 3$ y H no sea normal.

41. Consideremos el grupo cociente aditivo $\mathbb{Q}/\mathbb{Z}$. Sean p, q dos enteros positivos primos entre si.

    Demuestre que si $\frac{a}{p} \equiv \frac{b}{q}\ mod(\mathbb{Z})$ entonces $\frac{a}{p}$ y $\frac{b}{q}$ son enteros.

    Deduzca que $\mathbb{Q}/\mathbb{Z}$ es un grupo infinito.

42. Sea G un grupo. Si $g \in G$ se define el centralizador de g en G de la manera siguiente: $C(g) = \{x \in G : gx = xg\}$. Demuestre que: (a) Para todo $g \in G$, $C(g)$ es un subgrupo de G. (b) Se tiene $Z(G) = \bigcap_{g \in G} C(g)$.

43. Sean G y H dos grupos y $f : G \to H$ una función. Demuestre que si para todo $x, y \in G$ se tiene $f(x^{-1}y) = f(x)^{-1}f(y)$ entonces f es un morfismo.

44. Mas simple aún, si G y H son dos grupos y $f : G \to H$ una función, demuestre que si para todo $x, y \in G$ se tiene $f(xy) = f(x)f(y)$ entonces f es un morfismo.

45. Sean G y $f : G \to G$, definida por $f(x) = x^{-1}$. Demuestre que f es un morfismo si y solo si G es conmutativo.

46. Igual situación y pregunta que en el ejercicio anterior, pero ahora con $f(x) = x^2$.

47. Sean G y H dos grupos y $f : G \to H$ un morfismo. Demuestre que f es inyectivo si y solo si $Ker(f) = \{1_G\}$.

48. Sean G y H dos grupos y $f : G \to H$ un morfismo. Demuestre que $Ker(f)$ es un subgrupo normal de G, $Im(f)$ es un subgrupo de H y que el grupo cociente $G/Ker(f)$ es isomorfo a $Im(f)$.

49. Encuentre el orden de $(1, 2)$ en los siguientes grupos:

    a) $\mathbb{Z}_3 \times \mathbb{Z}_3$ b) $\mathbb{Z}_2 \times \mathbb{Z}_3$ c) $\mathbb{Z}_2 \times \mathbb{Z}_6$ d) $\mathbb{Z}_4 \times \mathbb{Z}_3$ e) $\mathbb{Z}_5 \times \mathbb{Z}_{10}$.

50. Establezca todos los morfismos entre: $(\mathbb{Z}, +)$ y $(\mathbb{Z}, +)$; $(\mathbb{Z}, +)$ y $(\mathbb{Z}_5, +)$; $(\mathbb{Z}_3, +)$ y $(\mathbb{Z}_6, +)$; $(\mathbb{Z}_3, +)$ y $(\mathbb{Z}_5, +)$; $(\mathbb{Z}_8, +)$ y $(\mathbb{Z}_4, +)$; $(\mathbb{Z}_4, +)$ y $(\mathbb{Z}_8, +)$.

51. Establezca los automorfismos de los grupos siguientes:

$$(\mathbb{Z}, +);\ (\mathbb{Z}_4, +);\ (\mathbb{Z}_5, +);\ (\mathbb{Z}_6, +);\ (\mathbb{Z}_2^2, +);\ (\mathbb{Z}_2 \times \mathbb{Z}_4, +)$$

52. Demuestre que todo grupo cíclico de orden n es isomorfo al grupo $(\mathbb{Z}_n, +)$ (el cual será tomado como modelo).

53. Sabemos que los conjuntos $\mathbb{Z}$ y $\mathbb{Z} \times \mathbb{Z}$ son equipotentes (es decir, que existe una biyección entre ellos). ¿ Cree usted que los grupos aditivos $\mathbb{Z}$ y $\mathbb{Z} \times \mathbb{Z}$ son isomorfos? Argumente su respuesta.

54. Si p y q son primos entre si, demuestre que los grupos aditivos $\mathbb{Z}_{pq}$ y $\mathbb{Z}_p \times \mathbb{Z}_q$ son isomorfos.

55. Si G es un grupo finito tal que $x^2 = 1_G$ para todo $x \in G$ entonces G es isomorfo a $\mathbb{Z}_2^n$ para algún entero n.

56. Demuestre que la composición de morfismos es un morfismo, es decir, si $\alpha : G \to H$ y $\beta : H \to L$ son morfismos de grupos, entonces la aplicación $\beta \circ \alpha : G \to L$ es también un morfismo.

57. Si G es un grupo demuestre que $Aut(G)$, el conjunto de los automorfismos de G, es un grupo.

58. Sea G un grupo finito. Demuestre que $|G| = 1, 2$ si y sólo si $Aut(G) = \{Id_G\}$.

59. Sea G un grupo tal que $Z(G) = \{1_G\}$. Demuestre que entonces se tiene $Z(Aut(G)) = \{Id_G\}$.

60. Sea G un grupo finito y $f \in Aut(G)$, una involución con un único punto fijo (es decir, $f^2 = Id$ y $\exists!\ x \in G,\ f(x) = x$). Demuestre que $f(x) = x^{-1}$ y deduzca que G es abeliano (se sugiere con entusiasmo estudiar la función $x \longmapsto x^{-1}f(x)$).

61. Determine los grupos simétricos y alternos que son abelianos.

62. Explicite la estructura de los grupos S_2, S_3, S_4 , A_2, A_3 y A_4.

63. Demuestre que si $n \geq 3$ entonces $Z(S_n) = \{Id\}$.

64. Determine la paridad de una permutación de orden 14 sobre 10 letras.

65. La misma pregunta anterior pero referida a permutaciones de ordenes 20 y 42 sobre un conjunto de 13 letras.

66. Para cada caso, estudie la existencia de una permutación σ tal que:
    (a) $\sigma(1,2)\sigma^{-1} = (1,3)$.
    (b) $\sigma(1,2)\sigma^{-1} = (1,2,3)$.
    (c) $\sigma(1,2,3)\sigma^{-1} = (4,5,6)$.
    (d) $\sigma(1,2,3)\sigma^{-1} = (1,2,4)(5,6,7)$.
    (e) $\sigma(1,2) = (1,2,3,4)\sigma$.
    (f) $(1,2)\sigma = \sigma(1,3)(2,4)$.
    (g) $\sigma(1,2)\sigma^{-1} = (1,3)$.

67. Demuestre que una permutación σ de orden 30 sobre 13 letras:

    a) Tiene a lo más 3 puntos fijos (k es punto fijo si $\sigma(k) = k$).
    b) Si tiene mas de un punto fijo σ es una permutación impar.
    c) Si tiene un sólo punto fijo es una permutación par.

68. ¿Cual es el orden posible de la composición de dos transposiciones?

69. Si α, β y γ son transposiciones, pruebe que $\alpha\beta\gamma \neq Id$.

70. Demuestre que una transposición no puede expresarse como composición de ciclos disjuntos de largo 3.

71. Demuestre que toda permutación par puede expresarse como composición de ciclos de largo 3.

72. Demuestre que los siguientes conjuntos de permutaciones generan S_n :

    a) $\{(1,2,3,...,n-1),\ (n-1,n)\}$

    b) $\{(1,2),\ (2,3),\ (3,4),...,\ (n-1,n)\}$

73. Demuestre que todo elemento de A_n puede expresarse como producto de ciclos de orden n.

4. La Estructura de Anillo

Iniciamos aquí el estudio, aunque somero, de estructuras definidas por dos leyes de composición internas, una suma y un producto. Las referencias están dadas por $\mathbb{Z}$, $\mathbb{Q}$ y, por ejemplo, $M_n(\mathbb{Z})$ las matrices cuadradas de orden n a coeficientes enteros.

Definición 35 *Se dice que $(A,+,\cdot)$ es un **anillo** si $(A,+)$ es un grupo abeliano, $(A,\cdot)$ es un monoide y además se tiene la **distribuitibidad** del producto con respecto de la suma, es decir, $a(b+c)=ab+ac$ y $(b+c)a=ba+ca$. Diremos que un anillo es **conmutativo** si su producto lo es.*

Detallando tenemos:

- *La estructura aditiva de A es asociativa y conmutativa.*
- *A admite un neutro aditivo que denotamos por 0_A.*
- *Para todo $a \in A$ existe su opuesto (inverso aditivo) $-a$*
- *La estructura multiplicativa de A es asociativa.*
- *A admite un neutro multiplicativo que denotamos por 1_A.*
- *Las operaciones suma y producto se relacionan por la distribuitibidad.*

*Diremos además que un anillo es un **cuerpo**, si es conmutativo y si todo elemento no nulo es invertible (si $a \neq 0_A$ existe a^{-1}), o sea, dicho de otra manera, si $(A \setminus \{0_A\},\cdot)$ es un grupo abeliano.*

Como lo dejamos entrever, ejemplos de anillos conmutativos son dados por $(\mathbb{Z},+,\cdot),(\mathbb{Z}_n,+,\cdot)$ y no conmutativos por $M_n(\mathbb{Z})$ entre otros. Es claro que si $(A,+,\cdot)$ es un anillo podemos considerar igualmente a $M_n(A)$, el conjunto de las matrices cuadradas con coeficientes en A. Si S es un conjunto, otro ejemplo de anillo está dado por $F=\{f;\ f:S\to A\}$ con las operaciones (heredadas de A) siguientes: si $f,g\in F$ entonces $f+g$ se define por $(f+g)(s)=f(s)+g(s)$ y $f\cdot g$ por $(fg)(s)=f(s)g(s)$; es inmediato que con estas operaciones $(F,+,\cdot)$ es un anillo con propiedades similares al anillo A (usted puede precisar cuales son los neutros de tal estructura, así como los opuestos). ¿Que puede decir de F si A es un cuerpo?.

Establezcamos, ahora, ciertas reglas de cálculo muy útiles:

Proposición 36 *Sea $(A,+,\cdot)$ un anillo. Entonces para todo $a,b \in A$ se tiene $a \cdot 0_A = 0_A \cdot a = 0_A$ y $a(-b) = (-a)b = -(ab)$, (por lo que podremos escribir sin ambiguedad $-ab$). De esto último se infiere en particular que $(-1_A)(-1_A) = 1_A$.*

Demostración. Seguros de que no produce confusión, escribiremos 0 y 1 en vez de 0_A y 1_A. Mostraremos que $a \cdot 0 = 0$ y que $a(-b) = -(ab)$; del lado derecho se hace analogamente. Tenemos:

$$a \cdot 0 \overset{\substack{0 \text{ neutro} \\ \text{aditivo}}}{=\!=\!=} a \cdot (0+0) \overset{\text{distribuitividad}}{=\!=\!=\!=} (a \cdot 0) + (a \cdot 0)\,;$$

luego, sumando a ambos lados el opuesto de $a\cdot 0$ (es decir, $-(a \cdot 0)$) obtenemos $0 = a \cdot 0$. Para la otra aserción tenemos: $0 = a \cdot 0 = a(b + (-b)) = ab + a(-b)$ y sumando a ambos lados el opuesto de ab se obtiene $-(ab) = a(-b)$. De esto último sale que $-(-(ab)) = -(a(-b)) = (-a)(-b)$; como en cualquier grupo aditivo se tiene que $-(-x) = x$, llegamos a $(-a)(-b) = ab$ y tomando, en particular, $a = b = 1$ obtenemos $(-1)(-1) = 1$. ■

Respecto de escritura, denotemos por $n_A = 1_A + 1_A + \cdots + 1_A$, n veces; la distribuitividad nos dice que para todo $a \in A$ se tiene $a + a + \cdots + a = n_A a$; por lo anterior, $-n_A = n_A(-1_A)$, lo que significa que expresiones del tipo r_A con $r \in \mathbb{Z}$ tienen absoluto sentido. Si no hay confusión, en vez de n_A podemos escribir simplemente n y lo llamamos *ene*, entendiendo que no se trata de números enteros (por ejemplo, en $(\mathbb{Z}_6,+,\cdot)$ se tiene $4 = 10$).

4.1. Morfismos e Ideales

Veamos ahora los morfismos y subestructuras ad-hoc de los anillos. Si $(A,+,\cdot)$ y $(B,+,\cdot)$ son anillos y $f : A \to B$ es una función, lo exigible para que f sea un morfismo es que sea compatible con las operaciones en juego, es decir entre $(A,+)$ y $(B,+)$ como también entre $(A,\cdot)$ y $(B,\cdot)$. De aquí para adelante consideraremos sólo anillos conmutativos; tenemos:

Definición 37 *Llamamos **morfismo** entre los anillos $(A,+,\cdot)$ y $(B,+,\cdot)$ a toda aplicación $f : A \to B$ que verifica: $f : (A,+) \to (B,+)$ es un morfismo de grupos abelianos y $f : (A,\cdot) \to (B,\cdot)$ un morfismo de monoides.*

Detallando tenemos:

- $f(x+y) = f(x) + f(y)$ *para todo* $x, y \in A$. *De esto, como sabemos se infiere que* $f(0_A) = 0_B$ *y que* $f(-a) = -f(a)$ $\forall a \in A$.

- $f(xy) = f(x)f(y)$ *para todo* $x, y \in A$; *además,* $f(1_A) = 1_B$, *cuestión que exige un morfismo de monoides y que no se infiere de la multiplicatividad de* f.

Al igual que lo realizado en el estudio de monoides y grupos, podemos definir aquí los conjuntos núcleo e imagen: $Ker(f) = \{a \in A;\ f(a) = 0_B\}$ e $Im(f) = \{f(a);\ a \in A\}$; es claro que $Ker(f) \subset A$ y $Im(f) \subset B$. Veamos que tipo de estructuras son estas: la imagen posee el 0_B y el 1_B y es inmediato que es estable para las operaciones de B; es decir $Im(f)$, con las operaciones de B es un anillo. En cuanto al nucleo, este posee al 0_A pero no al 1_A pues $f(1_A) = 1_B$ y no es difícil ver que es estable para las operaciones de A; así las cosas, $Ker(f)$ no es un anillo con las leyes internas de A; sin embargo tiene una fuerte propiedad: $AKer(f) \subset Ker(f)$. Todo lo anterior nos lleva a:

Definición 38 *Sea* $(A, +, \cdot)$ *un anillo,* $S, I \subset A$. *Decimos que:*

- S *es un* ***sub-anillo*** *de* A *si* $(S, +, \cdot)$ *es un anillo y sus neutros aditivo y multiplicativo son los de* A.

- I *es un* ***ideal*** *de* A *si* $(I, +)$ *es un subgrupo de* A *y además se tiene* $AI \subset I$, *es decir, para todo* $a \in A$ *y* $x \in I$ *se tiene* $ax \in I$.

El nucleo de un morfismo es por tanto un ideal del anillo de partida y la imagen un sub-anillo del anillo de llegada. Sabemos que $Ker(f) = f^{-1}(\{0_B\})$ es decir, los nucleos son imagenes recíprocas del ideal nulo; podemos generalizar esto:

Proposición 39 *Si* $f : A \to B$ *es un morfismo de anillos y* J *es un ideal de* B *entonces* $f^{-1}(J)$ *es un ideal de* A.

Demostración. Que $f^{-1}(J)$ es un subgrupo aditivo de A sale directamente de la aditividad de f. Probemos que para todo $a \in A$ y $x \in f^{-1}(J)$ se tiene $ax \in f^{-1}(J)$: en efecto, $f(ax) = f(a)f(x)$ y como $f(x)$ pertenece al ideal J se llega a que $f(ax) \in J$ es decir, $ax \in f^{-1}(J)$ ■

De estas estructuras, la que juega un rol importante es la de ideal; la estructura de subanillo no tiene grandes propiedades ni incide mayormente en el estudio de estos tópicos. Es claro que los ideales triviales de A son obviamente $\{0_A\}$ y A. Tenemos:

Lema 40 *Sea I un ideal de A. Entonces I posee elementos invertibles si y solamente si $I = A$.*

Demostración. El recíproco es inmediato pues $1_A \in A$. Para el directo, veamos que si un elemento $x \in I$ es invertible, entonces $xx^{-1} = 1_A \in I$ y por tanto $a = 1_A a \in I$ para todo $a \in A$, es decir, $A = I$. ■

Corolario 41 $(A, +, \cdot)$ *es un cuerpo si y sólo si sus únicos ideales son los triviales.*

Demostración. En efecto, sea I un ideal de A; si $I \neq \{0_A\}$ existe $a \in A$ no nulo y por lo tanto invertible; luego $I = A$. El recíproco es inmediato. ■

Corolario 42 *Sea $f : A \to B$ un morfismo de anillos. Si A es un cuerpo entonces f es inyectivo.*

Demostración. Sabemos que $Ker(f)$ es un ideal de A. Obligadamente $Ker(f) = \{0_A\}$ pues si se tuviera $Ker(f) = A$ se contradicería con el hecho que $f(1_A) = 1_B \neq 0_B$. Ahora bien, sabemos que $Ker(f) = \{0_A\}$ es equivalente a decir que f es un monomorfismo (un morfismo inyectivo). ■

Con los ideales tenemos las mismas propiedades que hemos visto con los subgrupos:

Proposición 43 *La intersección de cualquier familia de ideales de un anillo es un ideal.*

Demostración. Se deja de ejercicio; como la intersección de subgrupos es un subgrupo, sólo es menester demostrar que se tiene $AI \subset I$. ■

Puesto que también la intersección de submonoides es un submonoide, obviamente que la intersección de sub-anilos es un sub-anillo. Aparte de la intersección, otra operación que produce ideales es la suma, más precisamente, si I, J son ideales de un anillo A definimos $I + J = \{i + j;\ i \in I, j \in J\}$; no presenta dificultad comprobar que $I + J$ es un ideal de A que contiene al conjunto $I \cup J$.

Definición 44 *Sean $(A, +, \cdot)$ y $T \subset A$. Llamamos ideal* ***engendrado*** *por T a la intersección de todos los ideales de A que contienen a T, que denotamos por $\langle T \rangle$. Es claro que $\langle T \rangle$ es el menor ideal de A que contiene a T.*

Un buen ejercicio es probar que $I + J = \langle I \cup J \rangle$. Por otro lado, es inmediato, como en los subgrupos, que $\langle \emptyset \rangle = \{0_A\}$. Además, si $a \in A$ el ideal $\langle a \rangle$ debe contener a todas las expresiones del tipo ax con $x \in A$, es decir $aA \subset \langle a \rangle$; sin embargo, el conjunto aA es trivialmente un ideal que contiene al elemento a y por tanto, dadas las propiedades del engendrado, $\langle a \rangle \subset aA$ o sea que lo que se tiene es $\langle a \rangle = aA$ (más generalmente, usted puede demostrar que $\langle a_1, \ldots, a_n \rangle = a_1 A + \cdots + aA_n$). Así las cosas, tenemos:

Proposición 45 *Los únicos ideales de* $(\mathbb{Z}, +, \cdot)$ *son los conjuntos* $n\mathbb{Z}$.

Demostración. Acabamos de ver que los $n\mathbb{Z}$ son ideales. La unicidad sale del hecho que, como sabemos, todo ideal es un subgrupo aditivo del anillo y los $n\mathbb{Z}$ son, cuestión que también sabemos, los únicos subgrupos aditivos del anillo $(\mathbb{Z}, +, \cdot)$. ■

No está demás en recordar que si $n\mathbb{Z} \neq \{0\}$ entonces n es el menor entero positivo contenido por tal ideal; esto fue establecido cuando tratamos a los grupos.

4.2. AnilIos Integros, Anillos Principales

Como hemos visto, el anillo de los enteros relativos es rico en propiedades. Sabemos, por ejemplo, que todo ideal es monógeno. Pero también hay otra, a la cual estamos culturalmente tan acostumbrados, que no nos damos cuenta, y que generalizamos ahora:

Definición 46 *Sea* $(A, +, \cdot)$ *un anillo. Entonces decimos que:*

- A *es* ***íntegro*** *si* $ab = 0$ *implica que* $a = 0$ *o* $b = 0$. *Dicho de otra manera, si* $a, b \neq 0$ *entonces* $ab \neq 0$.
- A *es* ***principal*** *si todo ideal es engendrado por un elemento.*

La integridad de un anillo es equivalente a decir que la multiplicaciones por un elemento no nulo ($x \mapsto ax$) son funciones inyectivas, o lo que es lo mismo, que hay cancelación cuando trabajamos con $a \in A \setminus \{0\} : ax = ay \Rightarrow x = y$. Obviamente que todo cuerpo es íntegro y además principal (hágalo). Pero además, como sabemos, $(\mathbb{Z}, +, \cdot)$ es principal; esto significa que dados los ideales $p\mathbb{Z}$ y $q\mathbb{Z}$, los ideales que surgen de la intersección y de la suma de ellos son monógenos; al respecto:

Teorema 47 *Se tiene:* $p\mathbb{Z} \cap q\mathbb{Z} = mcm(p,q)\mathbb{Z}$ *y* $p\mathbb{Z} + q\mathbb{Z} = mcd(p,q)\mathbb{Z}$.

Demostración. Es claro que $p\mathbb{Z} \cap q\mathbb{Z}$ es un ideal y está formado por los múltiplos comunes de p y q; sabemos además que existe $n \in \mathbb{N}$ tal que $p\mathbb{Z} \cap q\mathbb{Z} = n\mathbb{Z}$, donde n es el menor positivo del ideal: luego, $n = mcm(p,q)$.

Para lo otro, sea $m \in \mathbb{N}$ tal que $p\mathbb{Z} + q\mathbb{Z} = m\mathbb{Z}$ $(*)$; de ello se infiere que $p, q \in m\mathbb{Z}$ y por tanto existen $l, k \in \mathbb{N}$ tales que $p = lm$ y $q = km$, es decir, m es un divisor común de p y q. Pero de $(*)$ tambien sale que $m \in p\mathbb{Z} + q\mathbb{Z}$ por lo que existen $r, s \in \mathbb{Z}$, $m = rp + sq$ $(**)$. Si $d \in \mathbb{Z}$ es otro divisor de p y q, entonces existen $t, u \in \mathbb{Z}$ tales que $p = td$ y $q = ud$; reemplazando esto en $(**)$ se obtiene $m = (rt + su)d$, es decir, que m es múltiplo de d. Luego, $m = mcd(p,q)$. ■

Corolario 48 *Si* p *y* q *son primos entre sí, existen entonces* $r, s \in \mathbb{Z}$ *tales que se tiene* $pr + qs = 1$.

Demostración. En efecto, si p y y q son primos entre sí, entonces $mcd(p,q) = 1$, es decir $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$. ■

Corolario 49 *Si* p *es un primo, entonces* $p \mid qt$ *y* $p \nmid q$ *implica que* $p \mid t$.

Demostración. Sabemos por lo recién realizado que si p es primo entonces para todo $q \notin p\mathbb{Z}$ (o sea, q no es múltiplo de p), existen $r, s \in \mathbb{Z}$ tales que $1 = rp + sq$: esto significa que se tiene $t = rtp + sqt$, por lo que $p \mid t$. ■

4.3. Ideales Primos, Ideales Maximales

En lo que sigue, una vez más inspirados en la riqueza estructural de $(\mathbb{Z}, +, \cdot)$, estudiaremos nuevos aspectos de los anillos.

Así por ejemplo tomemos p un entero primo:

(a) sean $m, n \in \mathbb{Z}$ tales que $mn \in p\mathbb{Z}$; esto significa que $mn = rp$ es decir que p divide a mn y por el corolario anterior se tiene que p divide a m o que p divide a n, o sea que $m \in p\mathbb{Z}$ o $n \in p\mathbb{Z}$.

(b) supongamos ahora que $p\mathbb{Z} \subsetneq s\mathbb{Z}$: entonces $s \notin p\mathbb{Z}$ y por tanto p, s son primos entre si y, por lo recién visto en los corolarios, $p\mathbb{Z} + s\mathbb{Z} = \mathbb{Z}$; como además se tiene $p\mathbb{Z} + s\mathbb{Z} = s\mathbb{Z}$ (pues $p\mathbb{Z} \cup s\mathbb{Z} = s\mathbb{Z}$) concluimos que la suposición $p\mathbb{Z} \subsetneq s\mathbb{Z}$ nos lleva a que $s\mathbb{Z} = \mathbb{Z}$.

Todo esto nos permite introducir:

Definición 50 *Sean $(A,+,\cdot)$ un anillo y P, M ideales de A. Decimos que:*

- *P es un ideal **primo** si $ab \in P$ implica que $a \in P$ o $b \in P$.*
- *M es un ideal **maximal** si para todo ideal I tal que $M \subsetneq I$ se tiene $I = A$..*

Así las cosas, si p es primo el ideal $p\mathbb{Z}$ es un ideal primo y también maximal del anillo $(\mathbb{Z},+,\cdot)$. Al respecto tenemos:

Proposición 51 *Si M es un ideal maximal si y solamente si para todo elemento $a \in A \setminus M$ se tiene $A = M + aA$.*

Demostración. El directo es inmediato pues $M \subsetneq M + aA$. En cuanto al recíproco, si I es un ideal tal que $M \subsetneq I$ entonces existe $i \in I \setminus M$, es decir (puesto que $i \in A \setminus M$) , $A = M + iA$. Como $M \subset I$ y obviamente $iA \subset I$ se llega a que $A = I$. ■

Corolario 52 *Todo ideal maximal es primo.*

Demostración. Sale de lo anterior pues si $ab \in M$ y $a \notin M$ entonces $A = M + aA$ y por tanto existen $m \in M$ y $c \in A$ tales que $1 = m + ac$; luego $b = mb + abc$ y como $mb, abc \in M$ se llega a que $b \in M$. ■

4.4. El Anillo Cociente, el Cuerpo de Fracciones

Introduzcamos ahora la estructura de anillo cociente, la cual, entre otras cosas nos brinda una caracterización muy hermosa de los ideales primos y maximales.

Sabemos que dado un anillo A y un ideal I, A/I es un grupo abeliano, estructura que hereda de aquella de A, con la operación: $\overline{a} + \overline{b} = \overline{a+b}$. ¿Podemos hacer lo mismo con el producto? Es decir ¿la operación entre clases de equivalencias, $\overline{a} \cdot \overline{b} = \overline{ab}$, está bién definida ? Si la respuesta es positiva, evidentemente que A/I sería un anillo y la proyección canónica, $a \mapsto \overline{a}$, un morfismo; para responder a esto, debemos ver que si $\overline{a} = \overline{\alpha}$ y $\overline{b} = \overline{\beta}$ entonces $\overline{ab} = \overline{\alpha\beta}$. No olvidemos que el cociente de grupos es de la forma $(A,+)\,/\,(I,+)$ y por tanto la notación es aditiva; así las cosas, $\overline{x} = x + I$ y por tanto bajo nuestras hipótesis tenemos $\alpha = a + i$, $\beta = b + j$

con $i, j \in I$. Multiplicando las identidades tenemos $\alpha\beta = ab + aj + ib + ij$; como $aj + ib + ij \in I$ efectivamente se llega a que $\alpha\beta \in ab + I$, es decir, $\overline{\alpha\beta} = \alpha\beta + I = ab + I = \overline{ab}$. Por tanto:

Definición 53 *Si A es un anillo e I un ideal de A, se llama* ***anillo cociente*** *al conjunto de las clases mod(I), A/I provisto de las operaciones, inducidas por la estructura de A:*

$$(a + I) + (b + I) = (a + b) + I y\, (a + I)\,(b + I) = (ab) + I.$$

¿Como se comporta el anillo cociente respecto de algunas propiedades estudiadas hasta ahora? ¿Se traspasan las características que pueda tener un anillo al cociente?

Proposición 54 *Sean A un anillo e I un ideal de A. Entonces si A es principal también lo es A/I. Sin embargo, si A es íntegro, nada se puede afirmar con respecto a A/I.*

Demostración. Consideremos el epimorfismo (morfismo sobreyectivo) canónico $\pi : A \to A/I$, $a \mapsto a + I$. Como se trata de una función sobreyectiva se garantiza que para todo subconjunto $T \subset A/I$ se tiene $\pi(\pi^{-1}(T)) = T$. Pero por el hecho de que sea además un morfismo, si J es un ideal de A/I entonces $\pi^{-1}(J)$ es un ideal de A; como A es principal, existe $x \in A$ tal que $\pi^{-1}(J) = \langle x \rangle$ y por tanto $J = \pi(\pi^{-1}(J)) = \pi(\langle x \rangle) = \langle \pi(x) \rangle$, lo que muestra que A/I es principal. Respecto de la segunda afirmación, tomemos el anillo principal $\mathbb{Z}$ y denotando $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ compruebe que $\mathbb{Z}_2, \mathbb{Z}_3$ y $\mathbb{Z}_5$ son íntegros pero que $\mathbb{Z}_4, \mathbb{Z}_6$ y $\mathbb{Z}_9$ no lo son. ■

Usemos los anillos cocientes para caracterizar ideales primos y maximales:

Proposición 55 *Sean $(A, +, \cdot)$ un anillo y P, M ideales de A. Entonces:*

- *P es un ideal primo si y solo si A/P es un anillo íntegro.*
- *M es un ideal maximal si y solo si A/M es un cuerpo*

Demostración. Se deja como ejercicio. ■

Aunque ya lo sabemos, de este resultado se infiere de manera inmediata y elegante que todo ideal maximal es primo.

Terminamos este capítulo con lo siguiente: cuando estudiamos los grupos vimos como construir el grupo $(\mathbb{Z}, +)$ a partir del monoide $(\mathbb{N}, +)$ (y más generalmente, como a todo monoide conmutativo con cancelación se le asocia un grupo (el menor) que lo contiene como sub-estructura). Veremos ahora como podemos construir el cuerpo $(\mathbb{Q}, +, \cdot)$ a partir del anillo $(\mathbb{Z}, +, \cdot)$ o, más generalmente:

Teorema 56 *Todo anillo íntegro conmutativo puede ser considerado sub-anillo de un cuerpo. El menor de esos cuerpos se denomina el* ***cuerpo de fracciones*** *de A y se denota por $Frac(A)$.*

Demostración. Queda de ejercicio. ■

Para establecer este resultado, desarrolle y demuestre paso a paso las afirmaciones constructivas y deductivas que aquí siguen, basándose en lo realizado en el Teorema 11.

Considere A, un anillo íntegro conmutativo, y sea $A^* = A - \{0\}$:

- Demuestre que la relación $\backsim$ (inspirada de las igualdades de racionales $\frac{n}{m} = \frac{p}{q}$) definida sobre $A \times A^*$ por: $(a, b) \backsim (c, d) \Leftrightarrow ad = bc$, es una relación de equivalencia.
- Denote $Frac(A)$ el conjunto de clases de equivalencia y utilizando la estructura del anillo A, demuestre que las siguientes operaciones en $Frac(A)$: $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$ $\quad y \quad$ $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$ están bien definidas y le brindan a $Frac(A)$ una estructura de cuerpo conmutativo.
- Pruebe que la función (muy natural) $\iota : A \to Frac(A),\ \iota(a) = \overline{(a, 1_A)}$ es un monomorfismo de anillos y haga las identificaciones correspondientes y los cambios de escritura que se imponen.
- Finalmente, demuestre que $Frac(A)$ es el menor de los cuerpos que contienen al anillo A.

Ejercicios

1. Sea $(A, +, \cdot)$ un anillo conmutativo. Denotamos $\tilde{A}$ la estructura que se obtiene definiendo en A las nuevas operaciones de suma "$\oplus$" y producto "$\otimes$"de la manera siguiente: $a \oplus b = a + b + 1$ $\quad$ y $\quad$ $a \otimes b = a + b + ab$.

a) Demuestre que $\tilde{A}$ es un anillo conmutativo.

b) Determine en función de las operaciones " $+$ " y " $\cdot$ " (formula que demostrará por recurrencia) las expresiones de n términos: $a \oplus a \oplus ... \oplus a$ y $a \otimes a \otimes ... \otimes a$.

c) Exprese $a + b$ y ab en función de las operaciones " $\oplus$ " y " $\otimes$ ". ! Cuidado con las apariencias !

2. Sea A un anillo tal que para todo $a \in A$ se tiene $a^2 = a$. Demuestre que A es conmutativo.

3. Sea $(E, +, \cdot)$ una estructura tal que: $(E, +)$ es un grupo abeliano y el producto " $\cdot$ " es asociativo, conmutativo y se distribuye con respecto a la suma. Además, esta estructura cumple con la siguiente propiedad:

   Existe un único $u \in E$ *tal que* $u + x - ux \neq 0$ *para todo* $x \in E$.

   Demuestre que: (a) u es el neutro multiplicativo. (b) para todo $a \neq u$ existe b tal que $(u - a)(u - b) = u$, (c) Concluya que E es un cuerpo.

4. En $\mathbb{Z}$ tenemos que $3 + x - 3x \neq 0$ para todo $x \in \mathbb{Z}$.

   ¿Cual es su comentario respecto del ejercicio anterior?

5. Sean A un anillo y $a, \in A$. Si existe un único $b \in A$ tal que $ab = 1$ demuestre que $ba = 1$.

6. Sean A un anillo no conmutativo y $a, b \in A$ tales que $1-ab$ es invertible, es decir existe $c \in A$ que verifica: $c(1 - ab) = (1 - ab)c = 1$.

   a) Demuestre que $1 - ba$ es invertible, es decir que existe $d \in A$ tal que: $d(1 - ba) = (1 - ba)d = 1$.

   b) Si no logró hacer la pregunta anterior, compruebe que $d = 1 + bca$. ¿A que elemento corresponde $1 + adb$?

7. Consideremos el anillo de matrices cuadradas con coeficientes en el cuerpo $\mathbb{Z}_3$. Sea $A \subset M_2(\mathbb{Z}_3)$ el conjunto formado por todas las matrices del tipo $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Demuestre que A es un sub-cuerpo de $M_2(\mathbb{Z}_3)$ y que $(A^*, \cdot)$ es un grupo cíclico.

8. Demuestre que los anillos A y $\tilde{A}$ del ejercicio 1 son isomorfos.

9. En los siguientes anillos: $\mathbb{Z}_6$, $\mathbb{Z}_3^2$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{16}$ y $\mathbb{Z}_{24}$ encuentre: los elementos invertibles; los endomorfismos; los ideales; los automorfismos.

10. Estudiando casos particulares, enuncie las condiciones que se requieren para que existan morfismos de anillos entre $\mathbb{Z}_n$ y $\mathbb{Z}_m$.

11. Sea A un anillo conmutativo.

    a) Determine los morfismos de $\mathbb{Z}$ en A.

    b) Deduzca que A contiene un sub-anillo tipo $\mathbb{Z}_n$ para algún $n \geq 1$.

12. Determine todas las funciones aditivas y multiplicativas de $\mathbb{R}$ en $\mathbb{R}$, es decir, cuales son las funciones $f(x+y) = f(x)+f(y)$, $f(xy) = f(x)f(y)$ para todo $x, y \in \mathbb{R}$

13. Determine los morfismos de cuerpo, $f : \mathbb{C} \to \mathbb{C}$, que dejan invariante a $\mathbb{R}$ (es decir, $f(\mathbb{R}) \subset \mathbb{R}$).

14. Sea $(A, +, \cdot)$ un anillo conmutativo y I, J ideales de A. Se define el ideal IJ como el engendrado por el conjunto $\{ij;\ i \in I, j \in J\}$; demuestre que $IJ \subset I \cap J$ y que si $A = I + J$ entonces $IJ = I \cap J$.

15. Demuestre que todo cuerpo es un anillo íntegro y que todo anillo íntegro y finito es un cuerpo.

16. En el ejercicio 1 tomar $A = \mathbb{Z}$. Demuestre que $(\tilde{A}, \oplus, \otimes)$ es un anillo íntegro y principal.

17. Sea p un número primo. En $\mathbb{Z}_p$ demuestre que para todo $x \neq 0$ se tiene $x^{p-1} = 1$; concluya que $a^p = a$ para todo $a \in \mathbb{Z}_p$. En $\mathbb{Z}_{2p}$ resuelva la ecuación $x^2 = x$.

18. Demuestre que en un anillo principal toda cadena creciente de ideales,

$$I_0 \subset I_1 \subset I_2 \subset ..... \subset I_n \subset I_{n+1} \subset ....$$

    es estacionaria, es decir que existe $m \in \mathbb{N}$ tal que $I_k \subset I_m$ para todo $k \in \mathbb{N}$. En $\mathbb{Z}$ encuentre una cadena creciente de máxima longitud que comience con $2310\mathbb{Z}$; ¿cuantas de esas cadenas hay?

19. Sea $n \in \mathbb{N}$, $n \neq 0, 1$ y no primo. Demuestre que n se descompone de manera única: $n = p_1^{n_1} p_2^{n_{21}} ... p_k^{n_k}$, donde $p_1 < p_2 < .. < p_k$ son números primos.

20. Sea $n, m \in \mathbb{N}$ y $p \in \mathbb{P}$. Entonces n y m no son múltiplos de p si y solamente si nm tampoco lo es.

21. Demuestre que $\mathbb{Z}_p$ es un cuerpo si y solo si p es primo.

22. Sea k un entero, $n = 2^k$. Consideremos el anillo $\mathbb{Z}_n$.

    a) Caracterice los elementos nilpotentes de $\mathbb{Z}_n$.

    b) Caracterice los elementos invertibles de $\mathbb{Z}_n$.

    c) Demuestre que el conjunto J formado por los elementos no invertibles es un ideal de $\mathbb{Z}_n$.

    d) De un argumento que pruebe que J es maximal.

23. Sea $(A, +, \cdot)$ un anillo conmutativo, J un ideal de A y $\pi : A \to A/J$ la proyección canónica. Demuestre que si I es un ideal de A/J entonces $\pi^{-1}(I)$ es un ideal de A que contiene J.

24. Sea $(A, +, \cdot)$ un anillo conmutativo y J un ideal de A. Demuestre que: (a) J es primo si y solo si A/J es un anillo íntegro. (b) J es maximal si y solo si A/J es un cuerpo. (c) Deduzca que todo ideal maximal es primo.

5. Espacios Vectoriales

En lo que sigue desarrollaremos conceptos, definiciones y propiedades de lo que sin duda constituye una de las estructuras algebraicas más importante. La noción de vector y de espacio de vectores atraviesa varias áreas de la matemática pero también tiene gran incidencia como herramienta conceptual en la física, la astronomía y en las ciencias de la ingeniería.

Sean K un cuerpo y X un conjunto no vacío. Llamamos operación (o acción) **externa** de K sobre X a toda aplicación $\theta : K \times X \to X$; al igual que en las leyes de composición interna estudiadas al comienzo, denotaremos $\theta(\alpha, x)$ por αx.

Definición 57 *Se dice que V es un **espacio vectorial sobre** K (o K-espacio vectorial) si $(V, +)$ es un grupo abeliano y si K opera sobre V con las siguientes propiedades:*

- $1_K v = v$ *y* $\alpha(\beta v) = (\alpha\beta)\, v$, *para todo* $\alpha, \beta \in K$, $v \in V$.
- $(\alpha + \beta)\, v = \alpha v + \beta v$ *y* $\alpha(v + w) = \alpha v + \alpha w$, $\forall \alpha, \beta \in K$, $v, w \in V$.

Los elementos de V, como dijimos, se llaman vectores y a los del cuerpo se les dice escalares. De la definición se deduce, con un poco de escritura, que $0_V = \alpha 0_V = 0_K v$ y que $(-1_K)\, v = -v$ para todo $\alpha \in K, v \in V$.

Como ejemplos de espacios vectoriales, tenemos al cuerpo K y también los conjuntos K^n, con $n \geq 1$, y las operaciones (suma y producto por escalar) evidentes, es decir $(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)_i$ y $\lambda\,(\alpha_1, \ldots, \alpha_n) = (\lambda\alpha_1, \ldots, \lambda\alpha_n)$; más generalmente, si $(V_i)_{i \in I}$ es una familia de K-espacios vectoriales, entonces el producto cartesiano $V = \prod_{i \in I} V_i$, con operaciones definidas por $(u_i)_{i \in I} + (v_i)_{i \in I} = (u_i + v_i)_{i \in I}$ y $\lambda(u_i)_{i \in I} = (\lambda u_i)_{i \in I}$, es un espacio vectorial sobre K. Por último, dado un conjunto X y V un espacio vectorial sobre K, el conjunto $F = \{f;\, f : X \to V\}$ con las operaciones obvias $f + g$ y λf, definidas por $(f + g)(x) = f(x) + g(x)$ y $(\lambda f)\,(x) = \lambda f(x)$, es un K-espacio vectorial.

La noción de morfismo entre espacios vectoriales (sobre un mismo cuerpo evidentemente) exige, como siempre, la compatibilidad con las operaciones en juego, es decir:

Definición 58 *Sean V y W dos K-espacios vectoriales y $f : V \to W$ una función. Entonces se dice que f es una* ***aplicación lineal*** *(o morfismo entre espacios vectoriales) si $f(u+v) = f(u) + f(v)$ y $f(\lambda v) = \lambda f(v)$ para todo $u, v \in V$ y $\lambda \in K$.*

Lema 59 *Sean $f, g : V \to W$, $h : W \to U$ lineales y $\lambda \in K$. Entonces $f+g$, λf y $h \circ f$ son lineales. Además, si f es biyectiva f^{-1} es lineal.*

Demostración. Se deja al lector. ■

Al igual que lo realizado con los grupos y los anillos, a cada aplicación lineal f se le asocia su nucleo $Ker(f) = \{v \in V;\ f(v) = 0_W\} \subset V$ y su imagen $Im(f) = f(V) \subset W$. Es inmediato constatar que tanto el nucleo como la imagen tienen estructuras de K-espacios vectoriales, compatibles con aquellas de los espacios que los contienen, es decir, $0_V \in Ker(f)$ y $0_W \in Im(f)$. Esto nos lleva a:

Definición 60 *Sean V un K-espacio vectorial y H un subconjunto de V. Se dice que H es un* ***subespacio*** *de V si $(H, +)$ es un subgrupo de $(V, +)$ y si $KH \subset H$. Detallando: $0_V \in H$ y para todo $u, v \in H$, $\lambda \in K$ se tiene $u + v \in H$, $-u \in H$ y $\lambda u \in H$.*

Al igual que lo desarrollado con las estructuras estudiadas anteriormente (grupos, anillos) los subespacios triviales son $\{0_V\}$ y V. Tenemos:

Proposición 61 *Sea V un espacio vectorial sobre K. Entonces $H \subset V$ es un subespacio $\Leftrightarrow H \neq \emptyset$ y $\lambda u - v \in H$ para todo $\lambda \in K$, $u, v \in H$. Además, la intersección de cualquier familia de subespacios de V es un subespacio.*

Demostración. Hágamos la primera afirmación; la segunda queda para el lector. El directo es inmediato pues H es un subespacio. En cuanto al recíproco, como H no es vacío, si $h \in H$ se tiene $0_V = 1_K h - h \in H$; además, $-h = 0_K h - h \in H$; por último, si v es otro elemento de H tenemos: $v + u = 1_K v - (-u) \in H$, con lo que se establece que H es un subespacio. ■

Así pues, la intersección de subespacios es una herramienta para construir nuevos subespacios. La **suma** es otra: si H, L son subespacios de V, es inmediato que $H + L = \{h + l;\ h \in H, l \in L\}$ es tambien un subespacio de V y se tiene la cadena de inclusiones: $H \cap L \subset H, L \subset H + L$. La suma de subespacios se dice directa si $H \cap L = \{0_V\}$; si la suma $H + L$ es directa la denotamos

por $H \oplus L$. Si $V = H \oplus L$ se dice que H y L son espacios (mutuamente) suplementarios; más adelante se podrá ver que todo subespacio admite en general muchos (en muchos casos, infinitos) espacios suplementarios.

Lema 62 *Sean H y L subespacios de V. Entonces la suma $W = H + L$ es directa si y sólo si para todo $w \in W$ existen únicos $h \in H$ y $l \in L$ tales que $w = h + l$.*

Demostración. Sea $w \in W$; por definición de $H + L$ existen $h \in H$ y $l \in L$ tales que $w = h + l$; si además se tuviera $w = h' + l'$ se llega a que $h - h' = l' - l$ es decir $h - h', l' - l \in H \cap L = \{0_V\}$ de donde $h' = h$ y $l' = l$ por lo que la escritura $w = h + l$ es única. Recíprocamente, si $v \in H \cap L$ entonces podemos escribir $v \in W = H + L$ de las siguientes maneras: $v = v + 0_V = 0_V + v$, y por la unicidad de la escritura $v = 0_V$, es decir $H \cap L = \{0_V\}$, o sea $W = H \oplus L$. ■

Definición 63 *Sea S un subconjunto del espacio V. El subespacio **engendrado** por S, que denotamos (como siempre) por $\langle S \rangle$, es el resultante de la intersección de todos los subespacios de V que contienen al conjunto S; es, obviamente, el menor subespacio de V que contiene a S.*

Usted puede demostrar que $H + L = \langle H \cup L \rangle$. Ahora bien, como ya es costumbre, no es difícil establecer que $\langle \emptyset \rangle = \{0_V\}$, $\langle v \rangle = Kv$, $\langle u, v \rangle = Ku + Kv$ y más generalmente que $\langle v_1, \ldots, v_n \rangle = Kv_1 + \ldots + Kv_n$.

Los elementos tipo de $Kv_1 + \ldots + Kv_n$ son de la forma $\sum_{1 \le i \le n} \alpha_i v_i$; una expresión de esa forma se llama **combinación lineal** de los vectores $v_1, \ldots, v_n$.

Así las cosas, dado $S \subset V$, finito o infinito, denotamos por

$$CL(S) = \left\{ \sum_{1 \le i \le n} \alpha_i s_i;\ n \ge 1,\ s_i \in S,\ \alpha_i \in K \right\}$$

el conjunto de las combinaciones lineales de elementos de S (sumas finitas).

Proposición 64 *Se tiene $\langle S \rangle = CL(S)$.*

Demostración. Que $CL(S) \subset \langle S \rangle$ sale de comprobar que toda expresión del tipo $\sum_{1 \leq i \leq n} \alpha_i s_i$ está en $\langle S \rangle$, lo que es inmediato. La inclusión recíproca viene de establecer que $CL(S)$ es un subespacio vectorial que contiene a S (lo que requiere un poco de escritura rutinaria pero trivial) y, por tanto, al engendrado por S. ■

Definición 65 *Se dice que $S \subset V$ es un conjunto **generador** si $V = \langle S \rangle$.*

Por lo que hemos visto, la condición de conjunto generador de S nos dice que todo vector del espacio se puede expresar como una combinación lineal de elementos de S; sin embargo nada garantiza que la escritura sea única (es decir, nada impide que se tenga $\sum \alpha_i s_i = \sum \beta_i s_i$ con $s_i \in S$, con algún j tal que $\alpha_j \neq \beta_j$). Este aspecto lo veremos en la sección que sigue.

5.1. Dependencia Lineal, Bases

A partir de ahora trabajaremos con **espacios vectoriales finitamente** generados, es decir aquellos que satisfacen la condición:

$$\textbf{Si } \mathbf{V} = \langle S \rangle \textbf{ entonces existe } \mathbf{T} \subset \mathbf{S}, \mathbf{T} \textbf{ finito, tal que } \mathbf{V} = \langle T \rangle .$$

Es bueno recalcar que una combinación lineal de elementos de un subconjunto S o de una familia $F = (v_i)_{i \in I}$ de vectores, siempre es una suma con un número finito de términos, vectores multiplicados por escalares, mas allá de que S o I sean infinitos; si tal es el caso, esto quiere decir, por ejemplo, que la expresión formal $\sum \alpha_i v_i$ tiene sentido vectorial sólo si, salvo un número finito, los α_i son nulos $(*)$; una familia $(\alpha_i)_{i \in I}$ de escalares que verifique esta condición es llamada **casi nula**. Dicho de otra manera, cada vez que uno encuentra ese tipo de expresiones en el ámbito de los espacios vectoriales, debe asumir la condición $(*)$.

Definición 66 *Se dice que una familia de vectores (o un subconjunto de V) es **linealmente dependiente** (l.d.) o **ligada** si en tal familia (o conjunto) existe al menos un elemento que es combinación lineal de los otros. En caso contrario, decimos que la familia es **linealmente independiente** (l.i.) o **libre**. También se habla de **sistemas** (de vectores) libres o dependientes.*

Dicho de otra manera, un conjunto o familia D es linealmente dependiente si y sólo si existe $d \in D$ tal que $d \in \langle D \setminus \{d\} \rangle$ o, lo que es lo mismo, si y sólo si existe $d \in D$ tal que $\langle D \setminus \{d\} \rangle = \langle D \rangle$.

Del mismo modo, simplemente negando la condición de dependencia lineal, una familia L es libre si y sólo si para todo $l \in L$ tenemos $l \notin \langle L \setminus \{l\} \rangle$ o, lo que es lo mismo, si y sólo si para todo $l \in L$ se tiene que $\langle L \setminus \{l\} \rangle \subsetneq \langle L \rangle$. El lector puede verificar estas equivalencias.

Al respecto de estos conceptos, tenemos los resultados siguientes:

Proposición 67 *Sea $S \subset V$; entonces:*

- *S es un sistema dependiente si y sólo si existe $x \in \langle S \rangle$ que admite al menos dos escrituras distintas como combinación lineal de elementos de S.*
- *S es un sistema libre si y sólo si todo $x \in \langle S \rangle$ se escribe de manera única como combinación lineal de elementos de S.*

Demostración. El directo es evidente pues si S es l.d existe $s \in S$ que es combinación lineal de los otros elementos de S, $s = \sum \alpha_i s_i$, con $s_i \neq s$ para todo i ; como además, $s = s$, tenemos dos escrituras para s en $\langle S \rangle$.

Reciprocamente, si $x = \sum \alpha_i s_i = \sum \beta_i s_i$ con $s_i \in S$, escrituras distintas, entonces existe j tal que $\alpha_j \neq \beta_j$. Esto quiere decir que podemos despejar el s_j ya que $0_V = \sum \alpha_i s_i - \sum \beta_i s_i = \sum (\alpha_i - \beta_i) s_i$ de donde $s_j = \sum_{i \neq j} \lambda_i s_i$ con $\lambda_i = (\beta_j - \alpha_j)^{-1}(\alpha_i - \beta_i)$ para todo $i \neq j$, es decir $s_j \in \langle S \setminus \{s_j\} \rangle$, lo que demuestra que S es l.d.

La segunda equivalencia se deja al lector. ■

Decimos que una combinación lineal es **nula** si $\sum_{i \in I} \alpha_i v_i = 0_V$ y que es **trivialmente** nula si además $\alpha_i = 0_K$ para todo $i \in I$. Tenemos:

Proposición 68 *Sea S familia o subconjunto de V; entonces:*

- *S es un sistema dependiente si y sólo si admite una combinación lineal nula no trivial de sus elementos.*
- *S es un sistema libre si y sólo si toda combinación lineal nula entre sus elementos es trivial*

Demostración. Someramente, pues no difiere de lo hecho en la Proposición anterior: si S es l.d. podemos expresar un elemento de S como combinación lineal de los otros ($s = \sum \alpha_i s_i$, con los $s_i \neq s$), con lo que obtenemos de inmediato una combinación nula no trivial entre elementos de S. Recíprocamente, si existe una combinación nula no trivial entre elementos de S, podemos despejar uno de ellos como combinación lineal de los otros y por tanto S es linealmente dependiente.

La segunda equivalencia es análogamente inmediata. ■

Los resultados expuestos nos dicen que cuando generamos subespacios a partir de sistemas libres obtenemos escrituras únicas para los elementos del engendrado, cuestión que es útil y hace más eficiente los cálculos. Nos dice además que cualquier sistema que contenga al 0_V es dependiente y que cualquier singleton $\{v\}$, con $v \neq 0$, es libre.

Por último, nos entrega un test muy rápido para estudiar si un sistema de vectores es libre: en efecto, esto pasa por darse formalmente una combinación nula de esos vectores y ver si la única posibilidad es que los escalares en juego sean todos nulos y por tanto que toda combinación lineal nula de esos vectores es trivial; así por ejemplo en K^3 sean $u = (1, 1, 0)$, $v = (0, 1, 1)$ y $w = (2, -1, -3)$; para ver si tenemos un sistema libre escribimos $\alpha u + \beta v + \gamma w = 0_V$ y vemos que escalares permiten esto: $\alpha(1, 1, 0) + \beta(0, 1, 1) + \gamma(2, -1, -3) = (0, 0, 0)$ es decir, $(\alpha + 2\gamma, \alpha + \beta - \gamma, \beta + 3\gamma) = (0, 0, 0)$; se infiere que: $\alpha + 2\gamma = 0$, $\alpha + \beta - \gamma = 0$ y $\beta + 3\gamma = 0$; de estas de ecuaciones sale que $\alpha = \beta = \gamma = 0_K$ y por tanto que el sistema u, v, w es libre. Usted puede estudiar el sistema u, v, w, z donde $z = u - 2v + w$.

Es claro entonces que cuando se trabaja con conjuntos que generan al espacio vectorial es más que recomendable optar por aquellos que además constituyan sistemas libres, pues así no sólo cada vector del espacio se expresa como combinación lineal de elementos del sistema sino que además se garantiza una y sólo una escritura para cada vector. Esto nos da:

Definición 69 *Una familia o conjunto B es una* ***base*** *del espacio V si B es a la vez un sistema libre y generador.*

Lo que sigue garantiza que siempre es posible contar con una base en el espacio; recordemos que siempre podemos, en el marco de lo aquí expuesto, extraer de un conjunto generador un subconjunto finito que también engendra al espacio.

Teorema 70 *Sean V un K-espacio vectorial, L un sistema libre y S un sistema generador. Entonces $card(L) \leq card(S)$.*

Demostración. Podemos suponer S finito, $S = \{s_1, \ldots, s_n\}$; recordemos además que por ser L un sistema libre, este no contiene al vector nulo. Sea $l_{k_1} \in L$: dado que S es generador tenemos que $l_{k_1} = \sum_{1 \leq i \leq n} \alpha_i s_i$; como $l_{k_1} \neq 0_V$ existe obligadamente un $\alpha_i s_i \neq 0_V$ y prestos a reenumerar podemos suponer que $\alpha_1 s_1 \neq 0_V$. Podemos así despejar s_1 como combinación lineal de los vectores $l_{k_1}, s_2, \ldots, s_n$ y, por tanto, el conjunto $S_1 = \{l_{k_1}, s_2, \ldots, s_n\}$ también es generador. De la misma manera, tomando l_{k_2}, un segundo elemento de L, este se expresará como combinación lineal de $l_{k_1}, s_2, \ldots, s_n$, es decir $l_{k_2} = \beta_{k_1} l_{k_1} + \sum_{2 \leq i \leq n} \beta_i s_i$; como L es libre, l_{k_2} no puede ser de la forma $\beta_{k_1} l_{k_1}$ por lo que existe un $\beta_i s_i \neq 0_V$; de nuevo, reenumerando si es preciso, podemos suponer que tenemos $\beta_2 s_2 \neq 0_V$ y despejando s_2 construimos un nuevo sistema de generadores, a saber $S_2 = \{l_{k_1}, l_{k_2}, s_3, \ldots, s_n\}$; así sucesivamente, vamos reemplazando elementos de S por aquellos de L y obteniendo nuevos conjuntos generadores del tipo $S_m = \{l_{k_1}, l_{k_2}, \ldots, l_{k_m}, s_{m+1}, \ldots, s_n\}$; notemos que como $l_{k_m} \in \langle S_{m-1} \rangle$, de nuevo por la condición de independencia lineal de L no se puede tener $l_{k_m} \in \langle l_{k_1}, l_{k_1}, \ldots, l_{k_{m-1}} \rangle$, lo que asegura el reemplazo de un elemento de S por l_{k_m} para obtener S_m. Ahora bien, no puede ocurrir que este proceso constructivo de reemplazo de los s por los l se acaben los elementos de S antes que los de L pues en tal caso tendríamos $S_n = \{l_{k_1}, l_{k_2}, \ldots, l_{k_n}\}$ y $l_{k_{n+1}} \in \langle S_n \rangle$ lo que contradice la independencia lineal de L. Esto muestra que $card(L) \leq card(S)$. ■

Corolario 71 *Todas las bases tienen el mismo cardinal.*

Demostración. Si B y B' son bases de V entonces el hecho de que B sea libre y B' generador nos entrega $card(B) \leq card(B')$ y, por las mismas razones, invirtiendo los argumentos, $card(B') \leq card(B)$. ■

El número de elementos de una base es por tanto un invariante de estructura en los espacios vectoriales. Tenemos:

Definición 72 *Sea V un espacio vectorial. Se llama **dimensión** de V sobre K, y se denota por $dim_K(V)$, al cardinal de cualquier base del espacio. Puesto que $\langle \emptyset \rangle = \{0_V\}$ definimos $dim(\{0_V\}) = 0$.*

Como vimos anteriormente, las bases son conjuntos que tienen la información necesaria y suficiente para describir, a partir de combinaciones lineales, todos los elementos del espacio a través de escrituras únicas. Sabemos que si L es un sistema libre, B una base y S un sistema generador entonces $|L| \leq |B| \leq |S|$; esto sugiere una idea simple para construir bases: ya sea agregarle ciertos vectores a L o quitarle algunos vectores a S. Tenemos:

Proposición 73 *(Teorema de la base incompleta) Todo sistema libre está contenido en alguna base.*

Demostración. Sea $L = \{l_1, \ldots, l_m\}$ un sistema libre. Si $\langle L \rangle = V$ entonces L es generador y por tanto base. Si $\langle L \rangle \subsetneq V$ escogemos $s_1 \in V \setminus \langle L \rangle$, lo que nos garantiza que $L_1 = \{l_1, \ldots, l_m, s_1\}$ continúa siendo un sistema libre. Repitiendo esto, vamos construyendo una cadena de sistemas libres $L \subsetneq L_1 \subsetneq \ldots \subsetneq L_j \subsetneq \ldots$ que necesariamente se detiene con L_{n-m} donde $n = dim_K(V)$, pues en caso contrario se contradice la desigualdad estructural expuesta en el Teorema 70. ■

Lo que se nos dice entonces, es que dado un sistema libre de m elementos siempre podemos completarlo, agregando $n - m$ vectores, hasta formar una base. Si $L = \{l_1, \ldots, l_m\}$ y $S = \{s_1, \ldots, s_{n-m}\}$ como la base es $B = L \cup S$, todo $v \in V$ se escribe $v = \sum \alpha_i l_i + \sum \beta_j s_j$ es decir, $v = u + w$ con $u \in \langle L \rangle$ y $w \in \langle S \rangle$; como además no es difícil establecer que $\langle L \rangle \cap \langle S \rangle = \{0_V\}$ concluimos con $V = \langle L \rangle \oplus \langle S \rangle$. Así las cosas, dado cualquier subespacio H de V, para construirle un espacio suplementario basta escoger una base de H, completarla a una base de V con otro sistema libre, el cual engendrará un suplementario de H; así, vemos que habrá tantos suplementarios posibles como posibilidades de escoger bases de H y de completar cada una de ellas a una base de V.

Proposición 74 *(Teorema de la base rebalsada) Todo sistema generador contiene una base.*

Demostración. Sea S un sistema generador: si S no es base entonces no es libre y existe $v_1 \in S$ tal que $v_1 \in \langle S_1 \rangle$ donde $S_1 = S \setminus \{v_1\}$; como es claro, por construcción, que S_1 es también un sistema generador, si este no fuera base se segue aplicando este método escogiendo s_2, etc.. Así sucesivamente, se contruye una cadena de inclusión estrictamente descendente de conjuntos generadores $S \supsetneq S_1 \supsetneq S_2 \supsetneq \ldots \supsetneq S_m \supsetneq \ldots$ que obligadamente converge a una base. El lector puede precisar el término de la demostración. ■

En definitiva, una base es a la vez un sistema libre maximal y un sistema generador minimal.

Por lo anterior, si $dim(V) = n$, un conjunto con más de n vectores no puede ser libre y con menos de n vectores no puede ser generador.

Proposición 75 *Si H y G son subespacios de V se tiene:*

$$dim(H + G) = dim(H) + dim(G) - dim(\{H \cap G).$$

Se infiere que si la suma es directa, $dim(H \oplus G) = dim(H) + dim(G)$.

Demostración. Sea $\{v_1, \ldots, v_r\}$ una base de $H \cap G$. Podemos por tanto completarla a una base de H con $\{h_1, \ldots, h_s, v_1, \ldots, v_r\}$ y también a una base de G con $\{v_1, \ldots, v_r, g_1, \ldots, g_t\}$. Como es inmediato, por construcción, que $\langle\{h_1, \ldots, h_s\}\rangle \cap \langle\{g_1, \ldots, g_t\}\rangle = \{0_V\}$, se infiere que una base de $H + G$ está dada por $\{h_1, \ldots, h_s, v_1, \ldots, v_r, g_1, \ldots, g_t\}$, de lo cual se deduce sin dificultad lo enunciado. ■

Veamos ahora como conectamos estos conceptos con los de aplicación lineal. Primero tenemos un importante resultado:

Teorema 76 *Si V es un espacio vectorial de dimensión n y $f : V \to W$ es una aplicación lineal, entonces $dim(Ker(f)) + dim(Im(f)) = n$.*

Demostración. Sea $\{u_1, \ldots, u_r\}$ una base de $Ker(f)$ y completémosla a una base de V con $\{u_1, \ldots, u_r, v_1, \ldots, v_{n-r}\}$. Es claro, por la estructura de esta base de V, que el sistema $\{f(v_1), \ldots, f(v_{n-r})\}$ engendra a $Im(f)$; basta demostrar entonces que tal sistema es libre, lo que se deja de ejercicio. ■

Proposición 77 *Sea $f : V \to W$ una aplicación lineal. Entonces:*

- *f es inyectiva $\Leftrightarrow$ f transforma sistemas libres en sistemas libres;*
- *f es sobreyectiva $\Leftrightarrow$ f transforma sistemas generadores en sistemas generadores.*

Demostración. Mostremos la primera equivalencia, la segunda queda de ejercicio: sea $\{u_1, \ldots, u_m\}$ un sistema libre de V y demostremos que $\{f(u_1), \ldots, f(u_m)\}$ es uno de W; en efecto, si $\sum \alpha_i f(u_i) = 0_W$, por linealidad de f se tiene $f\left(\sum \alpha_i u_i\right) = 0_W$ es decir $\sum \alpha_i u_i \in Ker(f)$ y, como

f es inyectiva, $\sum \alpha_i u_i = 0_V$; pero la familia $u_1, \ldots, u_m$ es libre por lo que $\alpha_i = 0_K$ para todo i. Recíprocamente, como f es lineal basta demostrar que $Ker(f) = \{0_V\}$ o, lo que es lo mismo, que si $v \neq 0_V$ entonces $f(v) \neq 0_W$: esto último es inmediato pues en tal caso $\{v\}$ es un sistema libre de V y como por hipótesis $\{f(v)\}$ es un sistema libre de W se tiene $f(v) \neq 0_W$. ■

Obviamente que se infiere de la Proposición anterior que f es biyectiva si y sólo si f transforma bases en bases.

Sea ahora V un espacio de dimensión n, $B = \{e_1, \ldots, e_n\}$ una base de V y $f : V \to W$ una aplicación lineal. Como todo elemento de $v \in V$ se escribe de manera única como $v = \sum \alpha_i e_i$, por linealidad se tiene $f\left(\sum \alpha_i e_i\right) = \sum \alpha_i f(e_i)$, lo que significa que f queda absolutamente determinada cuando se conocen las imágenes de los vectores de una base; esto significa, entre otras cosas que si dos aplicaciones lineales coinciden sobre una base (i.e. $f(e_i) = g(e_i)$, $1 \leq i \leq n$) estas son iguales. Todo esto nos dice como construir aplicaciones lineales, cuestión que expresamos con el resultado siguiente:

Teorema 78 *Sean V, W espacios vectoriales sobre K, $B = \{v_1, \ldots, v_n\}$ una base de V y $(w_i)_{1 \leq i \leq n}$ una familia de vectores de W. Entonces existe una y sólo una aplicación lineal $f : V \to W$ tal que $f(v_i) = w_i$, $1 \leq i \leq n$.*

Demostración. Por lo visto preámbularmente, basta definir $f\left(\sum \alpha_i v_i\right) = \sum \alpha_i w_i$. Usted puede terminar la demostración. ■

Corolario 79 *Dos K-espacios vectoriales V y W son isomorfos si y solamente si $dim_K(V) = dim_K(W)$. Además, en tal caso, si $g : V \to W$ es una aplicación lineal, son equivalentes: g inyectiva; g sobreyectiva; g biyectiva.*

Demostración. Si $\{v_1, \ldots, v_n\}$ es una base de V y $f : V \to W$ es un isomorfismo, entonces por la Proposición 76, $\{f(v_1), \ldots, f(v_n)\}$ es una base de W y por tanto $dim_K(V) = dim_K(W)$.

Recíprocamente, si $dim_K(V) = dim_K(W)$ sean $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_n\}$ bases de V y W; por el Teorema 77 y, de nuevo por la Proposición 76, la aplicación lineal definida por $f(v_i) = w_i$, $1 \leq i \leq n$ es un isomorfismo.

La última afirmación sale igualmente de lo anterior pues, por ejemplo, si $g : V \to W$ es inyectiva entonces $B = \{g(v_1), \ldots, g(v_n)\}$ es un sistema libre; como $dim_K(W) = n$, el conjunto B es una base y por tanto g es biyectiva. Los otros casos son igualmente inmediatos. ■

Ejercicios

1. Sean V un espacio vectorial sobre un cuerpo K y $S = \{v_1, \ldots, v_n\} \subset V$. Consideramos los conjuntos de vectores:

$$\begin{aligned} M &= \{v_1 + v_2, v_2 + v_3, \ldots, v_n + v_1\} \\ A &= \{v_1 - v_2, v_2 + v_3, \ldots, v_n + (-1)^n v_1\} \end{aligned}$$

   a) Si S es libre, ¿que se puede decir de M y de A?.

   b) Si S es generador, ¿que se puede decir de M y de A?

2. Sea $L = \{v_1, v_2, \ldots, v_n\}$ un sistema libre no generador. Estudie la independencia lineal de los sistemas:

   a) $\{v_1 + 2v_2, 2v_2 + 3v_3, \ldots, (n-1)v_{n-1} + nv_n, nv_n + v_1\}$.

   b) $L \cup \{u + v_1, u + v_2, \ldots, u + v_n\}$ donde $u \notin \langle L \rangle$.

3. Si $w \in V$ y $\{v_1, \ldots, v_n\} \subset V$ es un sistema libre (resp.: generador; base) ¿es $\{v_1 + w, \ldots, v_n + w\}$ libre (resp. generador; base)?.

4. En $F(\mathbb{R}) = \{f;\ f : \mathbb{R} \to \mathbb{R}\}$, espacio vectorial sobre $\mathbb{R}$, estudie la independencia lineal del sistema $\{f_1, \ldots, f_n\}$ donde $f_k(x) = e^{kx}$, $1 \leq k \leq n$. Estudie también el sistema infinito $\{f_k;\ k \in \mathbb{N}\}$

5. Sean V un espacio vectorial sobre un cuerpo K, S y T subconjuntos de V. Estudie si hay relaciones de inclusión entre:

   (a) $\langle S \cup T \rangle$ y $\langle \langle S \rangle \cup \langle T \rangle \rangle$. (b) $\langle S \cap T \rangle$ y $\langle S \rangle \cap \langle T \rangle$.

6. Sean L y H subespacios vectoriales de V. Muestre que $L \cup H$ es un subespacio vectorial de V si y sólo si $L \subset H$ o $H \subset L$.

7. Sean L, L' y H subespacios de V tales que: $L \subset L'$, $L \cap H = L' \cap H$ y $L + H = L' + H$. Demuestre que $L = L'$.

8. Si $w \in V$ y $\{v_1, \ldots, v_n\} \subset V$ es un sistema libre (respectivamente, generador, base) ¿es $\{v_1 + w, \ldots, v_n + w\}$ libre (resp., generador, base)?.

9. Demuestre que todo espacio vectorial de dimensión n sobre un cuerpo K, es isomorfo (no canónicamente) al espacio vectorial K^n.

10. Demuestre que la dimensión de $\mathbb{R}$ sobre $\mathbb{Q}$ es infinita.

11. Si $f : V \to W$ es lineal, pruebe que: $dim(V) = dim(Imf)+dim(Kerf)$.

12. Sea $f : V \to W$ una aplicación lineal. Si $dim(V) = dim(W)$ demuestre que: f monomorfismo $\Leftrightarrow$ f epimorfismo $\Leftrightarrow$ f isomorfismo.

13. Sean L y H subespacios de V. Demuestre que se tiene:

$$dim(L + H) = dim(L) + dim(H) - dim(L \cap H).$$

14. Muestre que se puede tener $L \oplus H = L \oplus T$, y $H \neq T$.

15. Sean H_i subespacios de V para $1 \leq i \leq m$.

    Muestre que $V = H_1 \oplus \cdots \oplus H_m$ si y sólo si $V = H_1 + \cdots + H_m$ y $H_j \cap \left(\bigoplus_{k \neq j} H_k\right)$ para todo $1 \leq j \leq m$.

16. Si $V = \prod_{1 \leq i \leq m} V_i$ entonces $V = \bigoplus_{1 \leq i \leq m} \pi_i(V)$ donde las π_k son las proyecciones canónicas $\prod_{1 \leq i \leq m} V_i \to V_k$.

17. Sean V un espacio vectorial, U un subespacio no trivial de V, S es un subespacio suplementario de U y $\{s_1, \ldots, s_m\}$ es una base de S. Demuestre que:

    a) Si $u \in U$ el subespacio $S_u = \langle\{u + s_1, \ldots, u + s_m\}\rangle$ también es un suplementario de U.

    b) Si $u, u' \in U$, y $u \neq u'$ entonces $S_u \neq S_{u'}$.

18. Sea V un K-espacio vectorial y H, L subespacios de V. ¿Bajo que condiciones la aplicación $H+L \to H \times L$, $f(h+l) = (h, l)$ está bien definida? Demuestre que en tal caso f es una aplicación lineal biyectiva.

19. Si H es un subespacio de V se define la relación $mod(H)$ basado en la estructura de grupo abeliano de V ($v = w\ mod(H) \Leftrightarrow v - w \in H$).

    Sabemos que las clases son de la forma $v+H$ y que el conjunto de clases, el cociente V/H, es un grupo con $(v + H) + (w + H) = (v + w) + H$.

    Demuestre que V/H es naturalmente un K-espacio vectorial con la operación externa $\lambda(v+H) = \lambda v+H$, para la cual el morfismo canónico $v \mapsto v + H$ es una aplicación lineal (obviamente sobreyectiva).

20. Sean L y H subespacios de V. Demuestre que la relación $mod(L)$ definida sobre H es una relación de equivalencia y que coincide con la relación $mod(L \cap H)$ sobre H.

21. Sean V un espacio vectorial de dimensión finita y H un subespacio. Demuestre que: $dim(V/H) = dim(V) - dim(H)$.

22. Sean L y H subespacios de V. Demuestre que los espacios cocientes $(H + L)/L$ y $H/(H \cap L)$ son isomorfos. Establezca el isomorfismo más natural.

23. Demuestre que un $\mathbb{R}$-espacio vectorial V puede ser considerado como $\mathbb{C}$-espacio vectorial si y sólo si $dim_{\mathbb{R}}(V)$ es par.

24. Sean V un $\mathbb{R}$-espacio vectorial de dimensión par y $f : V \to V$ una aplicación lineal. ¿Puede f operar como una aplicación $\mathbb{C}$-lineal ?. Analizar la situación, estudiar el nucleo y la imágen; etc..

25. Reflexione sobre la posibilidad que exista un espacio vectorial de seis elementos.

26. En relación al problema anterior, sea V un espacio vectorial sobre $\mathbb{Z}_p$, (donde p es un entero primo) de dimensión n.

    a) Calcule el cardinal de V.

    b) Cuántas bases se pueden encontrar en V?

27. Sean K un cuerpo infinito y V un espacio vectorial sobre K. Demuestre que V no puede ser la reunión de un número finito de subespacios propios de V. Reflexione este mismo enunciado cuando el cuerpo es finito.

28. Sea A un anillo íntegro que además es un espacio vectorial de dimensión finita sobre un cuerpo K. Demuestre que A es un cuerpo. ¿Que pasa si la dimensión no es finita?

29. Sea $f : K^2 \to K^2$ una aplicación lineal tal que $f^2 = 0$ .Si $V = K^2$ y $f((\alpha, \beta)) = (1, 1)$, explicite $f((x, y))$ (es decir, calcule $f((x, y))$ en función de α, β, x e y)

30. Sean V un espacio vectorial y $f : V \to V$ una aplicación lineal.

Demuestre que:

a) $f^2 = 0 \Leftrightarrow Im(f) \subset Kerf$.

En tal caso se tiene : $dim(Kerf) \geq \dfrac{dim(V)}{2}$.

b) $f^2 = f \Leftrightarrow$ existe una base B tal que $f(v) = 0$ o v, $\forall v \in B$.
En tal caso se tiene $V = Imf \oplus Kerf$.

c) $f^2 = Id \Leftrightarrow$ existe una base B de V tal que $f(v) = \pm v$, $\forall v \in B$.

d) $f^3 = f \Leftrightarrow$ existe una base B tal que $f(v) = 0$ o $\pm v$, $\forall v \in B$.
En tal caso se tiene $V = Imf \oplus Kerf$.

e) Si $f^m = Id$ y $f^{m-1} \notin \langle Id,\ f, \ldots, f^{m-2} \rangle$, entonces f admite puntos fijos no triviales.

f) Si $f^m = 0$ entonces $m \leq dim(V)$.

31. Sean V un espacio vectorial y $\{ v_1, v_2, \ldots, v_n \}$ una base de V.

Si $x = x_1v_1 + x_2v_2 + \ldots + x_nv_n$ e $y = y_1v_1 + y_2v_2 + \ldots + y_nv_n$, se define el producto escalar: $\langle x, y \rangle = x_1y_1 + x_2y_2 + \ldots + x_ny_n$.

Demuestre que:

a) La aplicación $V \times V \to K$, $(x, y) \longmapsto \langle x, y \rangle$, es bilineal simétrica.

b) Si $S \subset V$ y $S^{\perp} = \{v \in V; \langle v, s \rangle = 0,\ \forall s \in S\}$, entonces $S^{\perp}$ es un subespacio de V.

c) Si W es un subespacio: $(W^{\perp})^{\perp} = W$ y $dimW + dimW^{\perp} = n$.

d) Si H y L son dos subespacios, demuestre que $(H+L)^{\perp} = H^{\perp} \cap L^{\perp}$.

Puede simplificar la escritura apoyándose en el hecho de que todo espacio vectorial de dimensión n sobre K es isomorfo a K^n.

6. El Espacio de Matrices

Si bien las matrices y sus operaciones pueden ser definidas de manera independiente, ellas surgen de manera natural con el estudio de las aplicaciones lineales.

Sean V, W espacios vectoriales sobre K y $f : V \to W$, una aplicación lineal.

Como ya hemos visto, f queda absolutamente determinada si conocemos sus valores en una base; ahora bien, si $B_V = \{v_1, \ldots, v_n\}$ es una base de V y $B_W = \{w_1, \ldots, w_m\}$ es una base de W tenemos $f(v_j) = \sum_{1 \leq i \leq m} \alpha_{ij} w_i$ para todo $1 \leq j \leq n$.

Esto significa que habiendo fijado las bases de los espacios en juego, f queda determinada por la familia de escalares $(\alpha_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, que denotaremos, si no existe confusión, por $(\alpha_{ij})_{ij}$

Definición 80 *Llamamos* ***matriz de tipo*** $m \times n$ *a toda familia de elementos de* K *de la forma* $A = (\alpha_{ij})_{ij}$. *Por convención, debido a criterios operacionales que ya detallaremos, representamos a tal familia por el tablero:*

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \cdots & \alpha_{mn} \end{pmatrix}$$

y hablaremos de una matriz de m ***filas*** *y* n ***columnas***.

Es claro que, **habiendo fijado las bases** B_V y B_W, es equivalente darse una aplicación lineal de V en W y darse una matriz $(\alpha_{ij})_{ij}$ de tipo $m \times n$, pues, como ya vimos, con f obtenemos (sin ambiguedad) los escalares α_{ij} y, recíprocamente, con la matriz $(\alpha_{ij})_{ij}$ podemos definir (de manera única) a la aplicación lineal f a través de $f(v_j) = \sum_{1 \leq i \leq m} \alpha_{ij} w_i$.

En tal caso hablamos de matriz asociada a la aplicación f, que denotamos por $M(f)$ o M_f; en tal matriz, la j-ésima columna está formada por los coeficientes de $f(v_j)$ respecto de la base $B_W = \{w_1, \ldots, w_m\}$.

Esta equivalencia nos permite traspasar a las matrices operaciones que conocemos en las aplicaciones lineales, a saber, la multiplicación por escalar, la suma y la composición. Veamos:

- Sabemos que para todo $\lambda \in K$ la aplicación lineal λf está definida por $(\lambda f)(v) = \lambda f(v)$. Así las cosas, $(\lambda f)(v_j) = \sum_{1 \leq i \leq m} \lambda \alpha_{ij} w_i$.

- De la misma manera, si $h : V \to W$ es lineal con matriz asociada $(\eta_{ij})_{ij}$ respecto de las bases B_V y B_W. Como $(g+h)(v) = g(v) + h(v)$ tenemos

$$(g+h)(v_j) = \sum_{1 \leq i \leq m} \alpha_{ij} w_i + \sum_{1 \leq i \leq m} \eta_{ij} w_i = \sum_{1 \leq i \leq m} (\alpha_{ij} + \eta_{ij}) w_i$$

- Finalmente, si U es otro espacio vectorial y $B_U = \{u_1, \ldots, u_p\}$ es una de sus bases, sea $g : U \to V$ la aplicación definida por $g(u_k) = \sum_{1 \leq j \leq n} \beta_{jk} v_j$.

  Ahora bien, como $f \circ g : U \to W$ sea $(f \circ g)(u_k) = \sum_{1 \leq i \leq m} \gamma_{ik} w_i$. Ya que se tiene $(f \circ g)(u_k) = f(g(u_k))$, entonces se llega a

$$(f \circ g)(u_k) = f\Big(\sum_{1 \leq j \leq n} \beta_{jk} v_j\Big) = \sum_{1 \leq j \leq n} \beta_{jk} f(v_j) = \sum_{1 \leq j \leq n} \beta_{jk} \left(\sum_{1 \leq i \leq m} \alpha_{ij} w_i\right)$$

  y, reordenando, obtenemos

$$\sum_{1 \leq i \leq m} \gamma_{ik} w_i = (h \circ f)(u_j) = \sum_{1 \leq i \leq m} \left(\sum_{1 \leq j \leq n} \alpha_{ij} \beta_{jk}\right) w_i$$

Inspirados en lo anterior, definimos la multiplicación de una matriz por escalar, la suma de dos matrices del mismo tipo y el producto de una matriz de tipo $m \times n$ por una de tipo $n \times p$, de las siguientes maneras:

Definición 81 *Si* $1 \leq i \leq m$, $1 \leq j \leq n$ *y* $1 \leq k \leq p$, *entonces:*

- $\lambda(\alpha_{ij})_{ij} = (\lambda \alpha_{ij})_{ij}$ *y* $(\alpha_{ij})_{ij} + (\eta_{ij})_{ij} = (\alpha_{ij} + \eta_{ij})_{ij}$
- $(\alpha_{ij})_{ij} (\beta_{jk})_{jk} = (\gamma_{ik})_{ik}$ *donde* $\gamma_{ik} = \sum_{1 \leq j \leq n} \alpha_{ij} \beta_{jk}$.

Si denotamos por $M_{m\times n}(K)$ el conjunto de matrices $m\times n$ con coeficientes en K, es inmediato establecer que tenemos aquí un K-espacio vectorial: tanto $0_{m\times n}$ (la matriz nula) como $-A$ (el opuesto de la matriz A) son evidentes.

Cabe remarcar que dadas las restricciones dos matrices son raramente multiplicables: se requiere una de tipo $m \times n$ multiplicada a la derecha por una de tipo $n \times p$ para obtener una de tipo $m \times p$.

Sin embargo, obviamente que en el conjunto de matrices cuadradas de orden n (es decir de tipo $n \times n$), que denotaremos por $M_n(K)$, la multiplicación no tiene condiciones. Así las cosas , $M_n(K)$ tiene una estructura de **K-álgebra**, nombre dado a la mezcla compatible de una estructura de espacio vectorial con la de anillo, compatibilidad brindada por la identidad $\lambda\,(AB) = (\lambda A)\,B = A\,(\lambda B)$. Por lo demás, no es difícil establecer que $M_n(K)$ no es una estructura conmutativa como tampoco íntegra.

Por cierto, es inmediato que la matriz unidad de orden n, está dada por

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & \vdots & & \ddots & 0 \\ 0 & 0 & \cdots & \cdots & 1 \end{pmatrix}$$

Cualquier matriz A asociada a un morfismo entre espacios de dimensión n será cuadrada de orden n y en particular, cualquier matriz asociada a un isomorfismo f será invertible y su matriz inversa A^{-1} será aquella asociada a f^{-1}, es decir, tenemos $AA^{-1} = A^{-1}A = I_n$.

Por otro lado, dada la introducción a este tema, es obvio que matrices y aplicaciones lineales tienen comportamientos estructurales y algebraicos similares; sin embargo no son la misma cosa, salvo cuando elegimos bases de los espacios en juego donde, por cierto, son dos representaciones del mismo concepto. Así las cosas, una aplicación lineal puede tener varias matrices asociadas, dependiendo de la elección de las bases para la escritura de vectores; asimismo, una matriz puede ser la asociada de múltiples aplicaciones lineales.

6.1. Escritura Matricial y Cambio de Base

Manteniendo las notaciones utilizadas hasta ahora, sea $r \in V$; tenemos entonces $r = \sum_{1\leq j\leq n} r_j v_j$ y $f(r) = \sum_{1\leq i\leq m} s_i w_i$. Pero $f(r) = \sum_{1\leq j\leq n} r_j f(v_j)$ y como

$f(v_j) = \sum_{1\leq i\leq m} \alpha_{ij} w_i$ se llega a que

$$\sum_{1\leq i\leq m} s_i w_i = f(r) = \sum_{1\leq j\leq n} r_j \left(\sum_{1\leq i\leq m} \alpha_{ij} w_i \right) = \sum_{1\leq i\leq m} \left(\sum_{1\leq j\leq n} \alpha_{ij} r_j \right) w_i$$

de donde, para todo $1 \leq i \leq m$, se tiene $s_i = \sum_{1\leq j\leq n} \alpha_{ij} r_j$.

Así las cosas, es natural optar por representar un vector matricialmente por una matriz columna. Si $f(r) = s$, con tal convención tenemos:

$$\overset{s}{\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ \vdots \\ s_m \end{pmatrix}} = \overset{f}{\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \cdots & \alpha_{mn} \end{pmatrix}} \overset{r}{\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ \vdots \\ r_n \end{pmatrix}}$$

que resumimos por: $S = MR$.

Es claro que si $m = n$ y f es un isomorfismo de espacios vectoriales, entonces M es una matriz invertible y se tiene, obviamente, $R = M^{-1}S$

Un caso particular de lo anterior es el siguiente: si $\{v_1, \ldots, v_n\}$ y $\{v'_1, \ldots, v'_n\}$ son dos bases de V, tales que $v'_j = \sum_{1\leq i\leq n} \alpha_{ij} v_i$, la matriz $P = (\alpha_{ij})_{ij}$ se llama la **matriz de cambio de base** (o matriz de paso de la base B_V a la base B'_V); esta es claramente invertible pues no es otra que la asociada al isomorfismo definido por $v_j \mapsto v'_j$ para todo $1 \leq j \leq n$. Así las cosas, si $r = \sum_{1\leq i\leq n} r_i v_i = \sum_{1\leq j\leq n} r'_j v'_j$ entonces se tiene:

$$\sum_{1\leq j\leq n} r'_j v'_j = \sum_{1\leq j\leq n} r'_j \Big(\sum_{1\leq i\leq n} \alpha_{ij} v_i \Big) = \sum_{1\leq i\leq n} \left(\sum_{1\leq j\leq n} \alpha_{ij} r'_j \right) v_i$$

y por tanto, $r_i = \sum_{1\leq j\leq n} \alpha_{ij} r'_j$ es decir, $R = PR'$ o $R' = P^{-1}R$.

Con esto tenemos una fórmula rápida para pasar de las coordenadas de un vector respecto de una base a las coordenadas de tal vector respecto de otra base.

Finalmente, sea $\varphi : V \to V$ un endomorfismo: si su matriz respecto de la base B_V es A, ¿cómo es su matriz A' respecto de la base B'_V?. Mostremos que $A' = P^{-1}AP$: sea $r \in V$ con matrices columnas R y R' respectivamente asociadas a las bases B y B' y tal que S y S' sean las matrices asociadas a $\varphi(x)$ respecto de las mismas bases. Por lo ya visto, se tiene $S = AR$ y $S' = A'R'$; como además $R = PR'$ y $S = PS'$, obtenemos: $PS' = S = AR = APR'$ de donde $S' = P^{-1}APR'$, es decir, $S' = A'R' = P^{-1}APR'$; como esto es válido para todo vector columna R' (es decir para todo elemento r de V) deducimos que $A' = P^{-1}AP$.

6.2. Sobre Endomorfismos y Matrices Cuadradas

Como hemos podido darnos cuenta, las matrices cuadradas juegan un rol particular en el ambito de las matrices. Recordemos que $M_n(K)$ posee una rica y compleja estructura de anillo y espacio vectorial (estructura de K-álgebra, por cierto isomorfa a la de $End_K(V)$, con $dim(V) = n$); como ejercicio, el lector puede establecer que $dim(M_n(K)) = n^2$.

En lo que sigue, de manera somera expondremos algunos aspectos que conciernen a matrices cuadradas; el desarrollo de preguntas y/o las demostraciones quedan de ejercicio.

Transpuesta de una Matriz: si $A \in M_n(K)$, $A = (\alpha_{ij})_{ij}$ se define la matriz transpuesta de A como ${}^tA = ({}^t\alpha_{ij})_{ij}$ donde ${}^t\alpha_{ij} = \alpha_{ji}$; es decir, ${}^tA$ se obtiene transformando las filas de A en columnas (y por tanto las columnas en filas). Obviamente que $A = {}^tA$ si y sólo si A es simétrica. Además, es inmediato que ${}^t({}^tA) = A$, ${}^t(A + B) = {}^tA + {}^tB$, ${}^t(\lambda A) = \lambda\, {}^tA$ y, con un poco de escritura se puede establecer que ${}^t(AB) = {}^tB\, {}^tA$, de donde de infiere que si A es invertible entonces ${}^tA$ también lo es y $({}^tA)^{-1} = {}^t(A^{-1})$.

Similitud: dos matrices cuadradas A y B se llaman matrices similares si existe P invertible tal que $B = P^{-1}AP$. Con un poco de escritura se demuestra que en $M_n(K)$ la relación de similitud es una relación de equivalencia; ¿cual es la clase de I_n? ¿es compatible esta relación con la estructura de $M_n(K)$? Al respecto, es claro que si A es invertible, también lo es B y se tiene $B^{-1} = P^{-1}A^{-1}P$; además, si $\Pi : M_n(K) \to M_n(K)$ es una función polinomial definida por $\Pi(X) = \sum \pi_k X^k$ donde $X^0 = I_n$ y $0 \leq k \leq q$, entonces $\Pi(B) = P^{-1}\Pi(A)P$. Por último, si A y B son matrices similares, ¿que se puede decir de ${}^tA$ y ${}^tB$?

Técnicas de Inversión: lo que sigue se realizará trabajando con las filas de las matrices en juego; obviamente que también funciona si se hace con las columnas.

Operar elementalmente sobre una matriz consiste en modificarla de manera reversible con acciones simples tales como permutar sus filas o reemplazar una fila por una combinación lineal del conjunto de filas:

$$\begin{pmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_j \\ \vdots \\ F_n \end{pmatrix} \xrightarrow{T_{ij}} \begin{pmatrix} F_1 \\ \vdots \\ F_j \\ \vdots \\ F_i \\ \vdots \\ F_n \end{pmatrix}; \quad \begin{pmatrix} F_1 \\ \vdots \\ \vdots \\ F_k \\ \vdots \\ \vdots \\ F_n \end{pmatrix} \overset{CL_{k\lambda}}{\to} \begin{pmatrix} F_1 \\ \vdots \\ \vdots \\ \sum \lambda_i F_i \\ \vdots \\ \vdots \\ F_n \end{pmatrix}$$

Obviamente, que la primera acción es involutiva ($T_{ij}^2 = Id$, pues está basada en la trasposición (i, j)) y la segunda requiere, para ser reversible, que el coeficiente λ_k sea no nulo, lo que se deducirá de lo que sigue.

En efecto, si $A \in M_n(K)$ se tiene

$$T_{ij}(A) = T_{ij}(I_n)A \text{ y } CL_{k\lambda}(A) = CL_{k\lambda}(I_n)A \text{ (pruébelo),}$$

es decir que podemos operar con esas transformaciones multiplicando sucesivamente por matrices del tipo:

$$\underset{T_{ij}(I_n)}{\begin{pmatrix} 1 & 0 & \cdots & & & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & \mathbf{0} & \cdots & \mathbf{1}_j & & \\ & & \cdots & & & & \\ & & \mathbf{1}_i & \cdots & \mathbf{0} & & \vdots \\ \vdots & & & & & \ddots & 0 \\ 0 & & & & & & 1 \end{pmatrix}} \text{ y } \underset{CL_{k\lambda}(I_n)}{\begin{pmatrix} 1 & 0 & \cdots & & & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 1 & \cdots & & & \\ \boldsymbol{\lambda}_1 & \boldsymbol{\lambda}_2 & \cdots & \boldsymbol{\lambda}_k & \cdots & \boldsymbol{\lambda}_{n-1} & \boldsymbol{\lambda}_n \\ 0 & & & \cdots & 1 & & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdots & & & \cdots & 0 & 1 \end{pmatrix}}$$

Estas matrices son invertibles, pues es claro que $T_{ij}(I_n)^{-1} = T_{ij}(I_n)$ y, por otro lado, no es difícil comprobar que la inversa de $CL_{k\lambda}(I_n)$, con $\lambda_k \neq 0$, es $CL_{k\theta}(I_n)$ donde $\theta_k = \lambda_k^{-1}$ y $\theta_i = \lambda_i \lambda_k^{-1}$ para todo $i \neq k$.

Si A es invertible, sabemos por el método del pivot de Gauss que podemos transformarla en la matriz unidad a partir de operaciones elementales sucesivas, es decir, después de un proceso de r multiplicaciones matriciales tendremos $\Omega_r \Omega_{r-1} \cdots \Omega_2 \Omega_1 A = I_n$, donde Ω_l denota una matriz del tipo $T_{ij}(I_n)$ o $CL_{k\lambda}(I_n)$: esto significa que $A^{-1} = \Omega_r \Omega_{r-1} \cdots \Omega_2 \Omega_1$. Ahora bien, si efectuamos las mismas transformaciones sobre I_n obtendremos $\Omega_r \Omega_{r-1} \cdots \Omega_2 \Omega_1 I_n$ que no es otra cosa que A^{-1}; esto nos dice que las operaciones que trasforman A en I_n llevan a I_n hasta A^{-1}.

Así por ejemplo, realizando sobre A las modificaciones:

$$F_2 \to F_2 - F_3 \ , \quad F_1 \to F_1 + F_3 \ , \quad F_1 \to F_1 - F_2,$$

$$F_1 \to \frac{1}{2} F_1 \ , \quad F_2 \leftrightarrows F_3 \quad \text{y} \quad F_2 \to F_2 - F_1 \quad \text{tenemos}$$

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

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

Ahora, las mismas operaciones sobre I_n :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\to \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 1 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} \to \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 1 & -1 \end{pmatrix} = A^{-1}$$

Ejercicios

1. Encuentre la base canónica de $M_{m\times n}(K)$. Si $m = n$, establezca la tabla de multiplicación entre los elementos de la base canónica.

2. Para $n = 2, 3$, de un ejemplo de $A, B \in M_n(K)$, no nulas, tales que $AB = 0$. Trate de dar ejemplos para todo n.

3. Si $A, B \in M_n(K)$, no nulas, tales que $AB = 0$, ¿se tiene $BA = 0$?

4. Sea $A \in M_2(K)$. Demuestre que $A^n \in \langle I_2, A\rangle$ para todo $n \in \mathbb{N}$.

   Puede usted establecer un resultado análogo para $B \in M_3(K)$.

5. Sean $A \in M_2(K)$ y $B \in M_3(K)$ tal que $A^3 = B^4 = 0$. Demuestre que $A^2 = B^3 = 0$ (ojo: los anillos de matrices no son íntegros). Generalice.

6. Caracterise las matrices $A \in M_2(K)$ tales que:

$$A^2 = 0;\ A^2 = Id;\quad A^2 = A.$$

7. Sea $A \in M_2(K)$. Determine las matrices B tales que $AB = BA$.

8. Determine $Z(M_n(K))$, el centro de $(M_n(K), \cdot)$.

9. Una matriz $A = (\alpha_{ij})_{ij} \in M_n(K)$ se dice antisimétrica si $\alpha_{ji} = -\alpha_{ij}$. Demuestre que A es antisimétrica si y sólo si ${}^tA = -A$. Caracterice la diagonal principal (los α_{ii} $1 \leq i \leq n$) de una matriz antisimétrica. ¿Como son las matrices de orden n que son simétricas y antisimétricas a la vez?

10. Demuestre que toda matriz cuadrada se puede expresar como suma de una matriz simétrica y una antisimétrica.

7. El Anillo de Polinomios

Abordamos ahora el estudio de otra de las estructuras más importantes, herramienta formal múltiple que se utiliza en diversos ámbitos.

En variadas situaciones encontramos expresiones del tipo x^5-2x^3+3x+2, $1-3x-5x^3$, etc., donde x puede representar un número racional, un número complejo, una aplicación lineal, una matriz, etc.. En lo que sigue le daremos un ámbito formal a este tipo de escritura y a sus propiedades algebraicas. La construcción que haremos puede realizarse con cualquier anillo unitario y muchas de las propiedades que exhibiremos se obtienen con un anillo íntegro; nosotros la haremos con un cuerpo.

7.1. Construcción y primeras propiedades de K[X]

Sea K un cuerpo y consideremos el conjunto de todas las familias numerables (o sucesiones) de elementos del cuerpo: $K^{\mathbb{N}} = \left\{(a_k)_{k\in\mathbb{N}} \ ; \ a_k \in K\right\}$. Si no se produce confusión, escribiremos $(a_k)_k$ en vez de $(a_k)_{k\in\mathbb{N}}$.

Se dice que una familia $(a_k)_k$ es **casi nula** si existe $m \in \mathbb{N}$ tal que $a_k = 0$ para todo $k \geq m$. Denotamos por $K^{(\mathbb{N})}$ el conjunto de las familias casi nulas de $K^{\mathbb{N}}$.

Ahora bien, brindada por la estructura de K y el producto cartesiano, el conjunto $K^{\mathbb{N}}$ posee una estructura natural de K-espacio vectorial de dimensión infinita, del cual $K^{(\mathbb{N})}$ es trivialmente un subespacio, con las operaciones a nivel de coordenadas:

- la estructura de grupo abeliano dada por $(a_k)_k + (b_k)_k = (a_k + b_k)_k$;
- la ley externa o multiplicación por escalar dada por $\lambda\,(a_k)_k = (\lambda a_k)_k$.

Agreguemos ahora una tercera operación para proveer a $K^{\mathbb{N}}$ de una estructura de anillo conmutativo, compatible con la estructura de espacio vectorial, y que hará de $K^{(\mathbb{N})}$ un sub-anillo:

$$(a_k)_k \cdot (b_k)_k = (c_k)_k \,;\ \text{donde } c_k = \sum_{i+j=k} a_i b_j \quad \left(\text{o, lo que es igual, } \sum_{i=0}^{k} a_i b_{k-i}\right).$$

Demostrar que este producto es conmutativo, asociativo, distribuitivo con respecto a la suma, como asimismo que dispone de un elemento neutro es

una rutina de escritura que se deja al lector; la única dificultad de escritura se encontrará en la asociatividad, y se establece por las igualdades:

$$\sum_{p+s=k} a_p \left(\sum_{q+r=s} b_q c_r \right) = \sum_{p+q+r=k} a_p b_q c_r = \sum_{r+s=k} \left(\sum_{p+q=s} a_p b_q \right) c_r.$$

También se podrá observar que tal producto es compatible con la ley externa, es decir que se tiene: $\lambda \left[(a_k)_k \cdot (b_k)_k \right] = (\lambda a_k)_k \cdot (b_k)_k = (a_k)_k \cdot (\lambda b_k)_k$.

Apoyándonos en esto podemos introducir la escritura **suma formal,** dada por : $(a_k)_k = a_0(1,0,\ldots)+a_1(0,1,0,\ldots)+a_2(0,0,1,0,\ldots)+\cdots\cdots$ y colocando $U_k = (0,0,\ldots,0,\overset{k}{1},0,0,\ldots)$, podemos escribir $(a_k)_k = \sum_{k=0}^{+\infty} a_k U_k$.

Es claro que $\{U_0, U_1, U_2, \ldots\}$ es un sistema libre de $K^{\mathbb{N}}$ pero no es generador ya que, por ejemplo, el elemento $(1,1,1,\ldots)$ no puede obtenerse con una combinación lineal finita de los U_n; no debe confundirse la "suma formal" (que es una escritura) con la "suma" (que es una operación que actúa sobre un número finito de elementos). Ahora bien, el subespacio engendrado por $\{U_0, U_1, U_2, \ldots\}$ está formado por los elementos de la forma $\sum_{k=m}^{n} a_k U_k$, que no son otra cosa que el conjunto de las familias casi nulas de $K^{\mathbb{N}}$, es decir, $\{U_0, U_1, U_2, \ldots\}$ es base de $K^{(\mathbb{N})}$.

Hacemos notar, por último, que el producto definido sobre $K^{\mathbb{N}}$ nos entrega que $U_i \cdot U_j = U_{i+j}$; es claro que U_0 es el neutro.

Con todo esto, la aplicación $K \to K^{\mathbb{N}}$, $\lambda \mapsto \lambda U_0$ es trivialmente un morfismo no nulo de anillos, por tanto inyectivo; podemos así identificar el cuerpo K con su imagen, es decir hacer $\lambda \simeq \lambda U_0$, y así, simplemente considerar a K como una sub-estructura de $K^{\mathbb{N}}$.

Ahora bien, si denotamos $X = U_1$ y definimos $X^0 = 1$, podemos sin dificultad constatar que se tiene: $X^n = U_n$ para todo $n \in \mathbb{N}$; así, un elemento tipo de $K^{\mathbb{N}}$ podemos representarlo como la suma formal dada por $\sum_{k=0}^{+\infty} a_k X^k$ y, análogamente, los elementos no nulos de $K^{(\mathbb{N})}$ por la suma $\sum_{k=0}^{n} a_k X^k$, donde se tiene: $n = \text{máx}(k;\ a_k \neq 0)$. Usualmente, X es llamada la **indeterminada**.

Procedamos ahora a bautizar las estructuras que surgen de los conjuntos $K^{\mathbb{N}}$ y $K^{(\mathbb{N})}$, enriquecidos por las operaciones algebraicas que hemos introducido:

- A $K^{\mathbb{N}}$ lo llamamos **el anillo de las series formales**, y lo denotamos por $K\left[[X]\right]$.
- A $K^{(\mathbb{N})}$ lo llamamos **el anillo de polinomios**, denotado por $K\left[X\right]$.

Algunas consideraciones, convenciones de escritura y definiciones:

Un polinomio será denotado por $P(X)$ o simplemente P; la indeterminada X no es pues una variable ni tampoco una incognita. La situación polinomial $\sum_k \gamma_k X^k = 0$ no es una ecuación; significa solamente que $\gamma_k = 0$, para todo índice k.

Sea $P(X)$ un polinomio no nulo, $P = \sum_{k=0}^{n} \alpha_k X^k$ con $\alpha_n \neq 0$ (escritura que reservaremos, en general, para polinomios no nulos; el polinomio nulo es simplemente el 0):

Definición 82 *El índice n se llama **el grado** de P y se denota $gr(P)$. Los polinomios de grado 0 son elementos no nulos de K y se llaman **constantes**.*

Si $\lambda \neq 0$, como $\lambda P(X) = \sum_{i=0}^{n} \lambda\alpha_i X^i$, entonces $gr(\lambda P) = gr(P)$. Además, si $Q \in K\left[X\right]$ se define $(P+Q)(X) = P(X)+Q(X)$ y $(PQ)(X) = P(X)Q(X)$ que escribiremos simplemente $P+Q$ y PQ. Al respecto tenemos:

Proposición 83 *$gr(PQ) = gr(P)+gr(Q)$ y $gr(P+Q) \leq \max(gr(P), gr(Q))$.*

Demostración. Sean $P = \sum_{i=0}^{n} \alpha_i X^i$ y $Q = \sum_{i=0}^{m} \beta_i X^i$ dos polinomios no nulos. Como $\alpha_n, \beta_m \neq 0$ el grado de PQ lo entrega el término $\alpha_n\beta_m X^{n+m}$ lo que demuestra la primera afirmación. En cuanto a la segunda, supongamos $n \geq m$: si $n > m$, el grado de $P+Q$ lo entrega el término $\alpha_n X^n$; si $n = m$ éste es entregado por $(\alpha_n + \beta_n)X^n$ por lo que $gr(P+Q) \leq n$. ■

Si quisieramos "otorgarle" un grado al polinomio nulo, de manera de tener coherencia con lo que plantea la Proposición 83, este sería $-\infty$, con la convención: $-\infty + n = (-\infty) + (-\infty) = -\infty$, para todo entero natural n.

Corolario 84 *$K[X]$ es un anillo íntegro.*

Demostración. Si $P, Q \neq 0$, $gr(PQ) = gr(P) + gr(Q) \geq 0$. Luego $PQ \neq 0$. ■

El cuerpo de fracciones de $K[X]$ se denota $K(X)$ y sus elementos son los P/Q con $Q \neq 0$. Sabemos que podemos considerar a $K[X]$ como un sub-anillo de $K(X)$; más aún, recordamos que el cuerpo de fracciones es el menor cuerpo que contiene al anillo íntegro y en este caso además se tiene la cadena de sub-estructuras: $K \subset K[X] \subset K(X)$.

7.2. Resultados estructurales en K[X]

Dejamos al lector demostrar que si $P \in K[X]$ entonces P es invertible si y sólo si P es una constante no nula. Respecto de divisibilidades tenemos el importante resultado llamado **división euclidiana**, con un espíritu semejante a lo que sabemos de los enteros:

Teorema 85 *Sea $D \in K[X]$, $D \neq 0$. Entonces para todo $P \in K[X]$ existen $Q, R \in K[X]$, únicos, tales que $P = QD + R$ y $gr(R) < gr(D)$.*

Demostración. Veamos primero la unicidad: si $P = QD + R = SD + T$, con $gr(R), gr(T) < gr(D)$, reordenando tenemos: $(*)$ $(Q - S)D = T - R$. Ahora bien, como $gr((Q - S)D) = gr(Q - S) + gr(D) > gr(D)$ y además $gr(T - R) \leq \text{máx}(gr(T), gr(R)) < gr(D)$, la igualdad $(*)$ es posible sólo si es nula. Puesto que $K[X]$ es íntegro y $D \neq 0$, obtenemos $Q = S$ y $R = T$.

Respecto de la existencia, sean $D = \sum_{i=0}^{d} \delta_i X^i$ y $P = \sum_{i=0}^{n} \alpha_i X^i$. Es claro que si $n < d$ la afirmación es trivial. Supongamos por tanto que $n \geq d$ y que la propiedad se cumple para todo polinomio de grado menor que n : como δ_d es no nulo, se tiene que $gr(P - \alpha_n \delta_d^{-1} X^{n-d} D) < n$. Se infiere, por hipótesis inductiva, que existen Q y $R \in K[X]$, $gr(R) < gr(D)$, tales que $P - \alpha_n \delta_d^{-1} X^{n-d} D = QD + R$, de donde $P = (\alpha_n \delta_d^{-1} X^{n-d} + Q)D + R$ como queríamos demostrar. ■

Dado lo recién expuesto, introducimos lo siguiente:

Definición 86 *Sean $P, D \in K[X]$, $D \neq 0$. Se dice que D **divide** a P, lo que se denota por $D \mid P$, si el resto de la división euclidiana de P por D es 0. Es equivalente decir que P es **múltiplo** de D, o sea que se tiene $P = QD$.*

Es evidente que la noción de división polinomial se trivializa con las constantes (no nulas). En general, nos referiremos e interesaremos a divisores de grado ≥ 1. Tenemos el resultado inmediato:

Lema 87 *Sean $P, Q \in K[X]$, $gr(P),\ gr(Q) \geq 1$. Entonces $P \mid Q$ y $Q \mid P$ sí y solamente sí existe $\lambda \in K$, $\lambda \neq 0$, tal que $P = \lambda Q$.*

Demostración. Si tenemos $P = AQ$ y $Q = BP$ se llega a $P = ABP$, es decir $P(AB - 1) = 0$; como $K[X]$ es íntegro, $AB = 1$, es decir $A, B \in K$. El recíproco es trivial. ■

Definición 88 *Dos polinomios son **primos entre si** cuando no tienen divisores comunes de grados ≥ 1 (noción que se extiende sin dificultad a tres, cuatro, etc.. polinomios).*

*Un polinomio es **irreducible** si no tiene divisores no triviales (o sea, si sólo es divisible por él mismo y por las constantes no nulas).*

Es claro que cualquier polinomio de grado 1 es irreducible. Por otro lado, un polinomio no es irreducible si puede expresarse como un producto polinomial no trivial; al respecto tenemos:

Teorema 89 *Todo polinomio de grado ≥ 1 es irreducible o es producto de polinomios irreducibles; en tal caso, la descomposición es única salvo el orden de los factores.*

Demostración. Se establece sin problemas por inducción, pues sabemos que el enunciado se cumple si el grado es 1 y por tanto supongamos que el enunciado es válido para todo polinomio de grado $< n$. Si $P \in K[X]$ y $gr(P) = n$ tenemos dos posibilidades: (a) P es irreducible y no hay más que hacer; (b) P no es irreducible, entonces $P = ST$ con $0 < gr(S), gr(T) < n$ y la hipótesis se aplica a los polinomios S y T. ■

Así las cosas, para un polinomio P, $gr(P) \geq 1$, se tendrá $P = Q_1^{s_1} \cdots Q_m^{s_m}$ donde los $Q_i \in K[X]$ son irreducibles.

Recordemos ahora que la notación $\langle S \rangle = \{QS;\ Q \in K[X]\}$ expresa el ideal engendrado por S.

Tenemos un poderoso resultado de estructura:

Teorema 90 *$K[X]$ es un anillo principal.*

Demostración. Sea I un ideal de $K[X]$. Si I es un ideal trivial es inmediato pues se tiene $I = \langle 0 \rangle$ o $I = \langle 1 \rangle$. Supongamos entonces que I no es trivial y sea $D \in I$ de grado mínimo (es claro que podemos escoger tal polinomio basados en el axioma del buen orden: *todo conjunto de enteros naturales tiene un elemento mínimo*). Si $P \in I$, por el teorema de la división euclidiana existen (únicos) Q y R, $gr(R) < gr(D)$, tales que $P = QD + R$; luego $R = P - QD$ y por tanto $R \in I$. Dada la condición de minimalidad en el grado exigida a D, necesariamente $R = 0$, de lo cual se infiere que $P = QD$ de donde $I = \langle D \rangle$. ■

Un polinomio $\alpha_0 X^i + \alpha_1 X + \cdots + \alpha_n X^n$ se llama **mónico** si $\alpha_n = 1$. Es útil y simplificador de cálculo y escritura considerar siempre (salvo obligadas excepciones) generadores mónicos para los ideales de $K[X]$; esto es posibilitado por lo siguiente:

Lema 91 *Sean $P \in K[X]$ y $\lambda \in K,\ \lambda \neq 0$. Entonces $\langle P \rangle = \langle \lambda P \rangle$ por lo que si I es un ideal de $K[X]$ existe un y sólo un polinomio mónico M tal que $I = \langle M \rangle$.*

Demostración. No presenta dificultad ver que $P \in \langle \lambda P \rangle$ y $\lambda P \in \langle P \rangle$. Para lo que sigue, si $\langle M \rangle = \langle N \rangle$ con $M, N \neq 0$, se infiere que $M \mid N$ y $N \mid M$ por lo que existe $\mu \in K$ tal que $N = \mu M$; si además M y N son mónicos obligadamente $\mu = 1$. ■

Ahora le vamos a sacar partido al hecho que sea un anillo principal:

Definición 92 *Sean $P, Q \in K[X]$ de grados ≥ 1. Se dice que:*

- *$M \in K[X]$, múltiplo a la vez de P y de Q, es **mínimo común múltiplo** de P y Q si es mónico y si divide a todo otro múltiplo común de P y Q.*
- *$D \in K[X]$, divisor a la vez de P y de Q, es **máximo común divisor** de P y Q si es mónico y si es múltiplo de todo otro divisor común de P y Q.*

Teorema 93 *Dados $P, Q \in K[X]$, $gr(P), gr(Q) \geq 1$, siempre existen y son únicos un mínimo común múltiplo de P y Q, que denotamos por **mcm(P,Q)**, y un máximo común divisor de P y Q, que denotamos por **mcd(P,Q)**.*

Demostración. Este resultado es consecuencia directa del Teorema 90 y del Lema 91.

Para lo primero: como $\langle P\rangle \cap \langle Q\rangle$ es un ideal, sea M mónico tal que $\langle M\rangle = \langle P\rangle \cap \langle Q\rangle$; es claro que M es el polinomio de menor grado que es múltiplo común de P y Q. Además, si N es otro múltiplo común, $N \in \langle P\rangle \cap \langle Q\rangle = \langle M\rangle$ y por tanto $N = AM$, que es lo que se nos pedía establecer.

Para lo segundo, sea $D \in K[X]$ mónico tal que $\langle P\rangle + \langle Q\rangle = \langle D\rangle$; como $P, Q \in \langle P\rangle + \langle Q\rangle = \langle D\rangle$ se infiere que $P = AD$ y $Q = BD$ y por tanto D es un divisor común de P y Q. Sea ahora T otro divisor común de estos polinomios, es decir que se tiene $P = RT$ y $Q = ST$ para ciertos $R, S \in K[X]$. Por otro lado, como tenemos $D \in \langle D\rangle = \langle P\rangle + \langle Q\rangle$ podemos escribir $D = EP + FQ$ con $E, F \in K[X]$; luego, $D = ERT + FST = (ER + FS)T$ que es lo que queríamos demostrar. ■

Corolario 94 *P y Q son primos entre si $\Leftrightarrow$ $\langle P\rangle + \langle Q\rangle = K[X]$. Además, $M \in K[X]$ es irreducible $\Leftrightarrow$ $\langle M\rangle$ es un ideal maximal.*

Demostración. La primera equivalencia es inmediata pues si P y Q son primos entre si entonces $mcd(P, Q) = 1$.

En cuanto a la segunda afirmación, mostremos que si $\langle M\rangle \subsetneq \langle S\rangle$ entonces $\langle S\rangle = K[X]$: en efecto, de $\langle M\rangle \subsetneq \langle S\rangle$ se tiene $S \notin \langle M\rangle$ y como M es irreducible, M y S son primos entre si; luego, por la primera afirmación, $\langle M\rangle + \langle S\rangle = K[X]$; pero $\langle M\rangle + \langle S\rangle = \langle S\rangle$ ya que $\langle M\rangle \subset \langle S\rangle$. Recíprocamente, si M no fuera irreducible entonces se tendría $M = AB$, con $1 \leq gr(A), gr(B) < gr(M)$, por lo que $A, B \notin \langle M\rangle$ y por tanto $\langle M\rangle$ no sería un ideal primo y menos aún maximal, lo que contradice la hipótesis. ■

Otra manera de enunciar la segunda parte del Corolario anterior es decir que $M \in K[X]$ es irreducible si y sólo si $K[X]/\langle M\rangle$ es un cuerpo. Este resultado es muy fuerte y nos va abrir paso al tema que sigue.

Corolario 95 *Si $P \mid QS$ y P es primo con Q entonces $P \mid S$.*

Demostración. Si P es primo con Q entonces $\langle P\rangle + \langle Q\rangle = K[X]$, es decir, existen $A, B \in K[X]$ tales que $1 = AP + BQ$. Luego $S = APS + BQS$; como $P \mid QS$ se deduce que $P \mid S$. ■

El teorema que cierra este capítulo requiere de los resultados estructurales que siguen:

Proposición 96 *Para todo $P \in K[X]$ podemos considerar a K como sub-cuerpo del anillo cociente. $K[X]/\langle P\rangle$.*

Demostración. Esto lo brinda la proyección $\pi : K[X] \to K[X]/\langle P\rangle$, $S \mapsto \overline{S}$, el epimorfismo (morfismo sobreyectivo) canónico (natural), cuya restricción a K es trivialmente inyectiva (pues $\alpha \in \ker(\pi) \Leftrightarrow \pi(\alpha) = \overline{\alpha} = \overline{0}$ $\Leftrightarrow \alpha \in \langle P\rangle \Leftrightarrow \alpha = 0$) por lo que $\pi(K)$ es una copia isomórfica de K y por tanto sub-cuerpo de $K[X]/\langle P\rangle$. ■

Desde ahora asumimos que K es un sub-cuerpo de $K[X]/\langle P\rangle$ y por tanto que $K[X]/\langle P\rangle$ tiene una estructura natural de espacio vectorial sobre K. Más aún, tal estructura de K-espacio es además compatible con la estructura de anillo de $K[X]/\langle P\rangle$, pues es inmediato que se tiene $\left(\lambda\overline{S}\right)\overline{T} = \overline{\lambda S}\,\overline{T} = \overline{\lambda ST} = \lambda\overline{ST} = \lambda\left(\overline{S}\;\overline{T}\right)$.

Al respecto tenemos:

Proposición 97 *$K[X]/\langle P\rangle$ es un K-espacio vectorial de dimensión $gr(P)$.*

Demostración. Veamos primero que si $T \in K[X]$ entonces $\overline{T} = \overline{T(X)} = T(\overline{X})$, es decir que si $T = \sum \tau_i X^i$ entonces $\overline{T} = \sum \tau_i \overline{X}^i$. Por otro lado, dividiendo T por P tenemos $T = QP + R$ con $gr(R) < gr(P)$; se llega a que $\overline{T} = \overline{QP} + \overline{R} = \overline{R}$ pues $\overline{P} = \overline{0}$ (sabemos que $\overline{S} = \overline{0}$ si y sólo si $S \in \langle P\rangle$).

Así las cosas, si $gr(P) = n$, como $\overline{T} = \overline{R}$ y $gr(R) < n$, vemos que $\overline{T}$ es combinación lineal de $1, \overline{X}, \ldots, \overline{X}^{n-1}$ y por tanto $K[X]/\langle P\rangle$ es un K-espacio vectorial de dimensión finita; que esta familia también es libre viene del hecho siguiente: si $\overline{0} = \sum_{i=0}^{n-1} \alpha_i \overline{X}^i = \overline{\sum_{i=0}^{n-1} \alpha_i X^i}$ entonces $\sum_{i=0}^{n-1} \alpha_i X^i \in \langle P\rangle$, lo que es posible (por los grados polinomiales en juego) solamente si $\sum_{i=0}^{n-1} \alpha_i X^i = 0$, es decir si $\alpha_i = 0$ para todos los índices i. ■

Lo anterior nos dice que si $P = \pi_0 + \pi_0 X + \cdots + \pi_{n-1}X^{n-1} + X^n$ (es bueno, como indicamos, trabajar con polinomios mónicos) en el cociente se opera con escrituras únicas del tipo $\sum_{i=0}^{n-1} \alpha_i \overline{X}^i$, aplicando para los productos la regla de cálculo que emana de $\overline{P} = 0 : \overline{X}^n = -\pi_0 - \pi_0\overline{X} - \cdots - \pi_{n-1}\overline{X}^{n-1}$.

Así por ejemplo los elementos del anillo $\mathbb{R}[X]/\langle X^2+1\rangle$ son de la forma $\alpha+\beta\overline{X}$ con $\overline{X}^2=-1$; más aún, como como X^2+1 es irreducible en $\mathbb{R}$, el anillo cociente $\mathbb{R}[X]/\langle X^2+1\rangle$ es un cuerpo isomorfo a $\mathbb{C}$ y por tanto algebraicamente indistinguible de $\mathbb{C}$ (esta es una de las maneras de construir el cuerpo de los números complejos).

Agregamos ahora otros conceptos: retomando lo que motiva la construcción del anillo de polinomios, dado $P(X)\in K[X]$, podemos reemplazar la indeterminada X por cualquier elemento de un anillo (es decir, una estructura que tenga suma y producto), acción que llamamos **sustitución**; así por ejemplo, si A es una matriz cuadrada de orden n, $P(A)$ es la expresión $\sum \alpha_i A^i$, que es calculable en $M_n(K)$.

En particular, cuando las sustituciones las hacemos con elementos del cuerpo K, hablamos de **función polinomio**: $f_P : K\to K$; denotaremos, más simplemente, $P(\lambda)$ en vez de $f_P(\lambda)$. La función polinomio opera, por tanto, evaluando el polinomio en una constante; es claro que si P es un polinomio constante β, la función asociada coincide con P, es decir, $P(\lambda)=\beta$ para todo $\lambda\in K$. Ahora bien, pese a las apariencias, no hay que confundir polinomio y función polinomio; por ejemplo, en $\mathbb{Z}_2[X]$ el polinomio no nulo X^2-X posee una función polinomio nula. Cabe por tanto la pregunta: ¿bajo que condiciones polinomios y funciones polinomios tienen comportamientos "equivalentes"? (ver ejercicio 10, al final de este capítulo).

Definición 98 *Se dice que $\lambda\in K$ es **una raíz** de $P\in K[X]$ si $P(\lambda)=0$.*

Teorema 99 *Sean $P\in K[X]$ y $\lambda\in K$: entonces λ es raíz de P sí y solamente sí $X-\lambda$ divide P.*

Demostración. Supongamos que λ es raíz de P y escribamos la división euclidiana de P por $X-\lambda$: $P=(X-\lambda)Q+R$ donde $gr(R)<gr(X-\lambda)=1$ y por tanto $R\in K$. Evaluando P en λ se tiene $0=P(\lambda)=R(\lambda)=R$, luego, $P=(X-\lambda)Q$. El recíproco es inmediato. ■

Es claro que si un polinomio admite una raíz $\lambda\in K$, no puede ser irreducible; asimismo, un polinomio irreducible de grado ≥ 2 no puede admitir una raíz en K. Sin embargo, el recíproco de esto no es válido pues si P y Q son irreducibles de grado ≥ 2, el producto de ellos no es irreducible y sin embargo no tiene raíces en K (pues si ese fuera el caso tendríamos $X-\lambda \mid PQ$, siendo $X-\lambda$ primo con P y Q lo que es imposible).

Corolario 100 *Un polinomio de grado n admite a lo más n raíces, no necesariamente distintas.*

Demostración. Esta afirmación se infiere recursivamente de lo siguiente: si λ es raíz de P entonces $P = (X - \lambda)Q$ y $gr(Q) = gr(P) - 1$.

Por otro lado, hacemos notar que cualquier raíz de Q será también raíz de P y nada obliga que sea distinta de λ. ■

Finalizamos esta parte con resultados que nos llevan al tópico siguiente, la extensión de cuerpos.

Teorema 101 *Sea $P \in K[X]$. Siempre existe un cuerpo L del cual K es sub-cuerpo y $\lambda \in L$ tal que λ es raíz de P.*

Demostración. Si P tiene raíz en K no hay nada que demostrar; supongamos pues que no tiene raíces en K. Podemos considerar a P irreducible, pues en caso contrario si $P = QT$ con Q irreducible, si encontramos una raíz λ de Q, esta también será raíz de P.

Habiendo precisado lo anterior, recordemos que $P \in K[X]$ es irreducible si y sólo si $K[X]/\langle P\rangle$ es un cuerpo y que en el cociente se tiene $P(\overline{X}) = 0$, por lo que la respuesta se logra tomando $L = K[X]/\langle P\rangle$ y $\lambda = \overline{X}$. ■

Corolario 102 *Dado $P \in K[X]$ existe un cuerpo L, del cual K es sub-cuerpo, que contiene todas las raíces de P. Un cuerpo mínimo que verifica esta propiedad se denomina* ***cuerpo de descomposición*** *del polinomio P.*

Demostración. Es consecuencia recursiva del teorema anterior. ■

Ejercicios

1. Sean $B_n(X) \in K[X],\ n \in \mathbb{N}$, tal que $gr(B_n(X)) = n$. Demuestre que la familia $(B_n(X))_{n\in\mathbb{N}}$ es una base del K-espacio vectorial $K[X]$ y con un ejemplo, constate que no toda familia libre infinita de $K[X]$ es una base.

2. Sea $S \in K[X]$ y $f_S : K[X] \to K[X]$ definida por $f_S(P(X)) = P(S)$. Demuestre que : (a) f_S es un morfismo (llamado morfismo de sustitución); (b) f_S inyectivo $\Leftrightarrow gr(S) \geq 1$; (c) f_S biyectivo $\Leftrightarrow gr(S) = 1$.

3. Sean $A(X), B(X) \in K[X]$. Demuestre las equivalencias:

   $B(X)$ divide a $A(X) \Leftrightarrow$ para todo S, $gr(S) \geq 1$, $B(S)$ divide a $A(S)$ $\Leftrightarrow$ existe S, $gr(S) \geq 1$ tal que $B(S)$ divide a $A(S)$.

4. Sea $\lambda \in K^*$. Para $n \geq 1$ construya polinomios $Q_n(X)$ tales que se tenga

$$Q_n(\lambda + \frac{1}{\lambda}) = \lambda^n + \frac{1}{\lambda^n}.$$

5. Sean K un cuerpo, $2 \neq 0$ y $Q(X) \in K[X]$.

   a) Demuestre que existen únicos $Q_p(X)$ y $Q_i(X)$, parte par e impar de $Q(X)$, tales que: $Q_p(-X) = Q_p(X)$, $Q_i(-X) = -Q_i(X)$ y que verifican: $Q(X) = Q_p(X) + Q_i(X)$.

   b) Demuestre que existe un único $T(X) \in K[X]$ de manera que:

$$Q(X) = \frac{1}{2}\left[T(X+1) + T(X-1)\right].$$

6. Para todo $n \geq 1$ factorice en elementos simples (de primer grado) a

$$P_n(X) = \sum_{k=0}^{n} \frac{X(X+1)\ldots(X+k-1)}{k!}$$

7. En $\mathbb{Z}_{15}[X]$ encuentre las raíces de $X^2 - 1$. ¿Comentarios?

8. Dados $a_1, \ldots, a_n$ elementos distintos de un cuerpo K, construya polinomios P_i, $i = 1, 2, \ldots, n$, tales que $P_i(a_j) = \delta_{ij}$ (el delta de Kronecker).

   Utilice lo anterior para demostrar que si $(b_1, \ldots, b_n) \in K^n$ existe un único polinomio P tal que $P(a_i) = b_i$, $i = 1, 2, \ldots, n$ (esto se conoce como el teorema de interpolación de Lagrange).

9. Sean K un cuerpo y P, $Q \in K[X]$ tales que $PQ = X^n - 1$:

   a) Si $P = \sum_{k=0}^{p} a_k X^k$ y $Q = \sum_{k=0}^{q} b_k X^k$ entonces $\sum_{k=0}^{p+q} \left(\sum_{i+j=k} a_i b_j \right) = 0$.

   b) Si $R = \sum_{k=0}^{p} a_k X^{p-k}$ y $S = \sum_{k=0}^{q} b_k X^{q-k}$ entonces $PQ + RS = 0$.

10. Dado un cuerpo K sea $K^K = \{f;\ f : K \to K\}$.

    Con las operaciones:

    $$(f+g)(\alpha) = f(\alpha) + g(\alpha), (f \cdot g)(\alpha) = f(\alpha)g(\alpha) \text{ y } (\lambda f)(\alpha) = \lambda f(\alpha)$$

    el conjunto K^K es una K-álgebra (estructuras de anillo y espacio vectorial compatibles).

    Denotemos por K^K_{Pol} la subálgebra de las funciones polinomios:

    $$K^K_{Pol} = \{f_P : K[X] \to K[X] \ /\ P \in K[X],\ f_P(\lambda) = P(\lambda)\}.$$

    Demuestre que:

    a) Si K es finito, $K^K_{Pol} = K^K$.

    b) Si K es infinito, $K^K_{Pol} \cong K[X]$.

11. Sean K un cuerpo y $\Omega : K[X] \to K[X]$ la función definida por:

    $$\text{si } \ A(X) = \sum_{k=0}^{n} a_k X^k,\ gr(A) = n, \ \text{ entonces } \ \Omega(A(X)) = \sum_{k=0}^{n} a_{n-k} X^k.$$

    Estudie si Ω es aditiva y/o multiplicativa (para esto busque escrituras eficientes para operar con Ω). Vea además si Ω es inyectiva y/o sobreyectiva y encuentre enteros i, j, mínimales, $i < j$, tales que $\Omega^i = \Omega^j$.

    Además demuestre que:

    a) $gr(\Omega(A(X))) \leq gr(A(X))$ y que se tienen las equivalencias:

    $$gr(A(X)) = gr(\Omega(A(X))) \Leftrightarrow A(0) \neq 0 \Leftrightarrow A(X) = \Omega^2(A(X)).$$

    b) Si $gr(A(X)) \leq gr(B(X))$ y $\Omega(A(X)) = \Omega(B(X))$ entonces $A(X)$ divide a $B(X)$; encuentre la forma del polinomio $Q(X) \in K[X]$ tal que $B(X) = Q(X)A(X)$.

    c) Caracterice en función de $A(X)$ y de Ω al conjunto $\Omega^{-1}(A(X))$

    d) Muestre que si $A(X)$ es irreducible también lo es $\Omega(A(X))$. ¿Bajo que condiciones el réciproco es válido?

e) Sea ahora $P(X)$ un punto fijo de Ω (se dice, también, polinomio palindrómico). Muestre que 0 no es raíz de $P(X)$ y que:

• Si $gr(P(X))$ es par y 1 es raíz de $P(X)$, entonces es raíz doble.

• Si $gr(P(X))$ es impar entonces -1 es raíz de $P(X)$ y el polinomio $Q(X) = P(X)/(X+1)$ también es palindrómico.

12. Si $P \in \mathbb{R}[X]$ y $z \in \mathbb{C}$ demuestre que $P(z) = 0 \Leftrightarrow P(\overline{z}) = 0$.

    Admitiendo que "$(*)$*...los únicos polinomios irreducibles de* $\mathbb{C}[X]$ *son los de primer grado...*", infiera que los irreducibles de $\mathbb{R}[X]$ son los de primer grado y aquellos de segundo grado, $\alpha X^2 + \beta X + \gamma$, que verifican $\beta^2 - 4\alpha\gamma < 0$.

    Para una demostración de $(*)$ ver Análisis Complejo de Rudin o, una manera puramente algebraica en Algebra de Lentin y Rivaud.

13. Sea $P \in \mathbb{Z}[X]$ tal que $P(0)$ y $P(1)$ son impares. Demuestre que P no admite raíces enteras.

14. Sea $A(X) = \sum_{k=0}^{n} a_k X^k,\ a_k \in \mathbb{Z}$. Si $\frac{r}{s} \in \mathbb{Q}$ (r y s primos entre si) es raíz de A entonces:

    a) $r \mid a_0$ y $s \mid a_n$;

    b) $r - s \mid A(1)$ y $r + s \mid A(-1)$.

    Utilice estos resultados para encontrar las raíces de los polinomios: $2X^3 + 12X^2 + 13X + 15$ y $6X^4 - 11X^3 - X^2 - 415$

15. Sean $P(X) \in \mathbb{Z}[X]$ y $a \in \mathbb{Z}$. Si $b = P(a)$ demuestre que para todo $c \in \mathbb{Z}$ el entero $P(a + bc)$ es divisible por b.

    Utilice lo anterior para demostrar que no existe polinomio entero no constante $Q(X)$ tal que $Q(n)$ sea un número primo para todo entero n.

16. Si $P \in K[X]$, $P(X) = \sum_{k=0}^{n} \gamma_k X^k$, se define el polinomio derivado de P, de la siguiente manera: $P'(X) = \sum_{k=1}^{n} k\gamma_k X^{k-1}$.

Demuestre que:

a) $P - Q \in K \iff P' = Q'$.

b) $\alpha' = 0$ y $(\alpha P)' = \alpha P'$, $\forall \alpha \in K,$.

c) $(P + Q)' = P' + Q'$;

d) $(PQ)' = P'Q + PQ'$.

17. Sea $\lambda \in K$. Entonces λ es raíz múltiple de $P \Leftrightarrow P(\lambda) = P'(\lambda) = 0$.

18. $P\,'$ divide a P si y sólo si $P = \alpha(X - \beta)^n$ con $\alpha, \beta \in K$ (considere $car(K) = 0$).

19. Consideramos el anillo $K[X]$ donde $car(K) = 2$. Demuestre que si $n \in \mathbb{N}^*$ se tiene: $X^{2n} + 1 = (X + 1)^2(X^{n-1} + X^{n-2} + \ldots + 1)^2$.

20. En el anillo $\mathbb{Z}[X]$ demuestre que:

a) El ideal (X) es primo pero no es un ideal maximal.

b) El ideal $(3, X)$ es maximal.

c) $\{P(X)\ ;\ P(0)$ par$\}$ es un ideal no maximal.,

21. En $\mathbb{Q}[X]$ estudie si $\langle X^2 - 1, X - X^2\rangle$ y $\langle 2X^2 - 6\rangle$ son maximales.

22. Sea $P \in K[X]$. Demuestre que no siempre el anillo $K[X]/\langle P\rangle$ es íntegro pero que todo ideal de $K[X]/\langle P\rangle$ es principal.

8. Sobre Extensiones de Cuerpos

Como hemos visto, las situaciones "un cuerpo contenido en otro" como también, "dado un cuerpo, construir otro que lo contenga" aparece de manera natural. En lo que sigue formalizamos y conceptualizamos estas ideas.

8.1. Extensiones Finitas

Sean K y L cuerpos, $K \subset L$. Tenemos:

Definición 103 *Si K es un subcuerpo de L decimos que L es una **extensión** de K, cuestión que denotamos por $K < L$. En tal caso L es un espacio vectorial sobre K y su dimensión como K-espacio la denotaremos por $[L : K]$; si además $[L : K] < +\infty$, diremos que L es una **extensión finita** sobre K, de **grado** $[L : K]$.*

En el capítulo anterior encontramos una manera de construir extensiones (cocientando el anillo $K[X]$ por polinomios irreducibles). Ahora bien, obviamente un cuerpo puede o no contener sub-cuerpos (por ejemplo, es evidente que el menor sub-cuerpo de un cuerpo no puede tener sub-cuerpos): si no contiene, diremos que el cuerpo es **primo** (por ejemplo $\mathbb{Q}$ o $\mathbb{Z}_p$ con p primo no poseen sub-cuerpos; !demuéstrelo!); pero, en caso contrario, si contiene sub-cuerpos, obligadamente contendrá a $\mathbb{Q}$ o a un $\mathbb{Z}_p$ (y por tanto estos son los únicos cuerpos primos). Todo esto se infiere de lo que sigue.

Si K es un cuerpo consideremos la aplicación $\kappa : \mathbb{Z} \to K,\ \kappa(m) = m1_K$. La función κ es trivialmente un morfismo de anillos y por tanto su núcleo es un ideal de $\mathbb{Z}$; recordemos que $\mathbb{Z}$ es un anillo principal, por lo que cada uno de sus ideales es monógeno. Tenemos:

Definición 104 *Se define la **característica** de K y se denota por $car(K)$ al entero natural p tal que $ker(\kappa) = p\mathbb{Z}$.*

Es claro que si $car(K) = p \neq 0$ entonces p es el menor entero no nulo para el cual $p1_K = 0_K$. No es difícil establecer que la característica de un cuerpo es cero o un número primo: en efecto, si $car(K) = p \neq 0$, la situación $p = rs$ nos lleva a $0_K = p1_K = rs1_K = (r1_K)(s1_K)$ por lo que $r1_K$ o $s1_K$ es nulo, lo que contradice la minimalidad de p. Por último, del isomorfismo canónico $\mathbb{Z}/ker(\kappa) \simeq Im(\kappa) < K$, inferimos lo siguiente:

- si $car(K) = 0$ entonces κ es inyectiva y $\mathbb{Z} \simeq Im(\kappa) < K$; luego, por identificación isomórfica, $\mathbb{Z} < K$ y por tanto $\mathbb{Q} < K$.
- si $car(K) = p \neq 0$ entonces $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \simeq Im(\kappa) < K$ y, de nuevo por identificación isomórfica, $\mathbb{Z}_p < K$.

Pasemos ahora a estudiar más de cerca esto de las extensiones de cuerpos:

Proposición 105 *Consideremos la torre de extensiones $F < K < L$. Entonces las extensiones $F < K$ y $K < L$ son finitas, si y sólo si $F < L$ también lo es.*

En esta situación se tiene que: $[L : F] = [L : K]\,[K : F]$.

Demostración. Supongamos que $[L : K] = m$ y $[K : F] = n$ y consideremos los conjuntos $\{l_1, \ldots, l_m\}$ una base de L sobre K y $\{k_1, \ldots, k_n\}$ una base de K sobre F. Si $u \in L$ se tiene $u = \sum_{i=0}^{m} \alpha_i l_i$ con $\alpha_i \in K$ para todo i. Pero como $\alpha_i = \sum_{j=0}^{n} \beta_{ij} k_j$ donde $\beta_{ij} \in F$ para todo j, se llega a que $u = \sum_{i=0}^{m} \left(\sum_{j=0}^{n} \beta_{ij} k_j \right) l_i$ que reescribimos $u = \sum_{i=0}^{m} \sum_{j=0}^{n} \beta_{ij} k_j l_i$, lo que muestra que el conjunto $\{k_j l_i;\ \ 1 \leq j \leq n,\ \ 1 \leq i \leq m\}$ es un sistema generador de L en tanto F- espacio vectorial.

Demostrar que esta familia es además libre, es en cierta manera desandar lo caminado, es decir, si $\sum_{i=0}^{m} \sum_{j=0}^{n} \gamma_{ij} k_j l_i = 0$, con $\gamma_{ij} \in F$, entonces $\sum_{i=0}^{m} \left(\sum_{j=0}^{n} \gamma_{ij} k_j \right) l_i = 0$ y como los coeficientes $\sum_{j=0}^{n} \gamma_{ij} k_j$ son elementos de K y $\{l_1, \ldots, l_m\}$ es una base de L sobre K se infiere que $\sum_{j=0}^{n} \gamma_{ij} k_j = 0$; por último, como cada γ_{ij} es un elemento de F y $\{k_1, \ldots, k_n\}$ es base de K sobre F se llega finalmente a que $\gamma_{ij} = 0$, o sea que el conjunto $\{k_j l_i;\ \ 1 \leq j \leq n,\ 1 \leq i \leq m\}$ es libre sobre F.

Hasta aquí hemos demostrado el directo y la última afirmación. Veamos el recíproco: puesto que $K < L$, el F-espacio K es un subespacio del F-espacio L y por tanto $[K : F] \leq [L : F]$. Por otro lado, tomando a L como K-espacio vectorial, toda familia de L que sea libre lo será también en tanto

F-espacio pues $F < K$; como $[L : F]$ es finito, esto significa que no puede haber una familia libre de L, en tanto K-espacio vectorial, que sea infinita; obligadamente, $[L : K] < +\infty$. ■

8.2. Elementos Algebraicos

Dada una extensión $K < L$ y $\lambda \in L$ podemos construir al menor cuerpo que contenga K y λ, es decir, al cuerpo engendrado por K y λ, que por ahora denotamos $\langle K, \lambda \rangle$. Es claro que se tiene $K < \langle K, \lambda \rangle < L$. ¿Como es $\langle K, \lambda \rangle$? Decir que es la intersección de todos los sub-cuerpos de L que contienen $K \cup \{\lambda\}$ no nos entrega precisiones finas. Es inmediato que tal cuerpo contiene a todos los elementos de la forma $\alpha_0 + \alpha_1\lambda + \cdots + \alpha_n\lambda^n$ con $\alpha_i \in K$, es decir a todos los $P(\lambda)$ con $P \in K[X]$ o sea al conjunto $K[\lambda] = \{P(\lambda)\,;\, P \in K[X]\}$. Ahora bien, $K[\lambda]$ es ni más ni menos que la imagen de la aplicación $f_\lambda : K[X] \to L$ definida por $f_\lambda(P) = P(\lambda)$; como $f_\lambda(P + Q) = P(\lambda) + Q(\lambda)$ y $f_\lambda(PQ) = P(\lambda)Q(\lambda)$, esta aplicación es un morfismo por lo que $\mathrm{Im}(f_\lambda) = K[\lambda]$ es un sub-anillo de L y, como L es un cuerpo, $K[\lambda]$ es íntegro. Finalmente, como sabemos que todo anillo íntegro posee un cuerpo de fracciones (que es el menor cuerpo que contiene al anillo en cuestión) concluimos que $\langle K, \lambda \rangle$ no es otra cosa que $Frac(K[\lambda])$, que denotaremos naturalmente por $K(\lambda)$.

Ahora bien, teniendo $K < K(\lambda) < L$ podemos escoger otro elemento de $\mu \in L$ y construir $K(\lambda)(\mu)$; este cuerpo es en definitiva el menor sub-cuerpo de L que contiene K, λ y μ, por lo que cabe denotarlo por $K(\lambda, \mu)$.

Definición 106 *Sean $K < L$ y $\lambda \in L$. Decimos que $K < K(\lambda)$ es una **extensión simple** y que λ es un **elemento primitivo** de $K(\lambda)$. Más generalmente, decimos que $K(\lambda_1, \ldots, \lambda_m)$ es el cuerpo que se obtiene de K a través de una torre de extensiones simples sucesivas por adjunción de los elementos $\lambda_1, \ldots, \lambda_m \in L$.*

¿Cuando una extensión simple es finita?. Lo que sigue responde a esto:

Definición 107 *Sea $K < L$ una extensión y $\lambda \in L$. Entonces diremos que:*

- *λ es **algebraico sobre** K si existe $P \in K[X]$ tal que $P(\lambda) = 0$; en caso contrario diremos que λ es un elemento **trascendente**.*
- *L es una **extensión algebraica** de K si todo elemento de L es algebraico sobre K.*

Agreguemos que se llama **número algebraico** a todo número complejo que sea algebraico sobre el cuerpo $\mathbb{Q}$ de los racionales; entre ellos tenemos evidentemente las raíces de racionales positivos como $\sqrt{2}$, a " i " la unidad imaginaria, etc..

Entre los números trascendentes importantes tenemos a e (resultado logrado por Hermite en 1873) y a π (aún mucho más difícil de probar, establecido por Lindemann en 1882).

Proposición 108 *Toda extensión finita es algebraica.*

Demostración. Sean $K < L$ una extensión finita de grado n y $\lambda \in L$. Como en tanto K-espacio vectorial la dimensión de L es n, obligadamente la familia de $n+1$ elementos $1, \lambda, \lambda^2, \ldots, \lambda^n$ es dependiente, es decir, existe una combinación lineal nula no trivial: $\alpha_0+\alpha_1\lambda+\alpha_2\lambda^2+\cdots+\alpha_n\lambda^n = 0$. Tomando $P \in K[X]$, $P = \sum \alpha_i X^i$ se tiene $P(\lambda) = 0$ y por tanto λ es algebraico. ■

No es cierto, en cambio, que toda extensión algebraica sea finita; le invitamos a buscar un ejemplo.

Si λ es algebraico sobre K, obviamente existe una infinidad polinomios no nulos de $K[X]$ que se anulan en λ (tome por ejemplo los múltiplos de uno de ellos). Sin embargo, existe sólo uno que sea mónico y de grado mínimo, pues $\{P \in K[X];\ P(\lambda) = 0\}$ no es otra cosa que el núcleo del morfismo $f_\lambda : K[X] \to L$, $P \mapsto P(\lambda)$, y por tanto es un ideal de $K[X]$; luego existe $M_\lambda \in K[X]$, mónico, tal que $\langle M_\lambda \rangle = \{P \in K[X];\ P(\lambda) = 0\}$.

Definición 109 *Dada la extensión $K < L$, si $\lambda \in L$ es algebraico se llama* ***polinomio mínimo*** *de λ sobre K al polinomio M_λ. Si $gr(M_\lambda) = n$ decimos que λ es algebraico* ***de grado*** *n.*

Proposición 110 *El polinomio mínimo de un elemento algebraico es irreducible.*

Demostración. Si se tuviera $M_\lambda = SR$, con $R, S \in K[X]$ no constantes, entonces para todo $\alpha \in L$ se tendría $M_\lambda(\alpha) = S(\alpha)R(\alpha) \in L$ y, en particular, $0 = M_\lambda(\lambda) = S(\lambda)R(\lambda)$. Esto implicaría que S o R se anularía en λ lo que contradice la minimalidad del grado de M_λ. ■

Teorema 111 *λ es algebraico sobre K si y sólo si $K[\lambda] = K(\lambda)$. En caso que λ sea algebraico de polinomio mínimo M_λ se tiene $[K(\lambda) : K] = gr(M_\lambda)$.*

Demostración. Sea λ algebraico; sabemos que su polinomio mínimo M_λ es irreducible por lo que $K[X]/\langle M_\lambda\rangle$ es un cuerpo; pero $\langle M_\lambda\rangle$ no es otra cosa que $\ker(f_\lambda)$; ahora bien, $K[X]/\ker(f_\lambda)$ es isomorfo a $\mathrm{Im}(f_\lambda) = K[\lambda]$ y por tanto $K[\lambda]$ es también un cuerpo, por lo que $K[\lambda] = K(\lambda)$.

El recíproco utiliza el mismo tipo de herramientas: si $K[\lambda] = K(\lambda)$ entonces $K[\lambda]$ es un cuerpo y como $K[\lambda] \simeq K[X]/\ker(f_\lambda)$ esto significa que $\ker(f_\lambda) \neq \{0\}$ y por tanto que existe al menos un polinomio no nulo que se anula en λ.

La última aserción sale del isomorfismo $K[\lambda] \simeq K[X]/\langle M_\lambda\rangle$ pues sabemos que $K[X]/\langle M_\lambda\rangle$ es un K-espacio vectorial de dimensión $gr(M_\lambda)$. ■

Conviene aquí detenerse en lo siguiente: si λ y μ son algebraicos sobre K, ¿podemos de cierta manera determinar $[K(\lambda,\mu) : K]$?. Al respecto tenemos:

Proposición 112 *Sean $\lambda_1, \lambda_2, \ldots, \lambda_m \in L$ algebraicos sobre K, de grados $n_1, n_2, \ldots, n_m$. Entonces $K < K(\lambda_1, \lambda_2, \ldots, \lambda_m)$ es una extensión finita y $[K(\lambda_1, \lambda_2, \ldots, \lambda_m) : K] \leq n_1 n_2 \cdots n_m$. Reciprocamente, toda extensión finita de K es producto de una torre finita de extensiones simples algebraicas sucesivas*

Demostración. Basta hacer la demostración con dos elementos algebraicos, pues como $K(\lambda_1, \ldots, \lambda_m) = K(\lambda_1, \ldots, \lambda_{m-1})(\lambda_m)$ la recursividad funciona sin problemas. Sean pues λ y μ algebraicos sobre K, de grados r y s respectivamente; sabemos que r es el grado del polinomio mínimo $M_\lambda \in K[X]$. Ahora bien, como $K < K(\mu)$ nada asegura que M_λ siga siendo minimal tomado como polinomio de $K(\mu)[X]$; esto quiere decir que λ será de grado a lo más r sobre $K(\mu)$. Con esto claro, tenemos: $[K(\lambda,\mu) : K(\mu)] \leq r$ y por tanto $[K(\lambda,\mu) : K] = [K(\lambda,\mu) : K(\mu)][K(\mu) : K] \leq rs$.

Para el recíproco, si $K < L$ es una extensión finita de grado n, escogiendo elementos de L convenientemente, vamos construyendo la torre de extensiones simples $K < K(\lambda_1) < K(\lambda_1, \lambda_2) < \cdots < L$ y, por la finitud de las dimensiones de los espacios en juego, obligadamente se llegará a tener $K(\lambda_1, \lambda_2, \ldots, \lambda_m) = L$, en a lo más n etapas. ■

Comentario 113 *Es claro que $K = K(\lambda_1, \ldots, \lambda_m) \Leftrightarrow$ sí $\lambda_1, \ldots, \lambda_m \in K$. Por otro lado, si $P \in K[X]$, sabemos por el Corolario 102 que existe una extensión L de K que contiene a todas sus raíces; si $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ son esas raíces, es inmediato que $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ es un cuerpo mínimo que*

contiene a todas las raíces de $P \in K[X]$, *es decir* $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *es cuerpo de descomposición del polinomio* P. *Como la construcción de tal extensión solo puede variar en función del orden en que se van adjuntando las raíces, podemos concluir que dos cuerpos de descomposición de un polinomio dado son isomorfos o, dicho de otra manera, que el cuerpo de descomposición de un polinomio* ***es único salvo isomorfismo.***

Ahora bien, existen cuerpos que son autosuficientes en cuanto a proveer de todas sus raíces a los polinomios construidos sobre él. Tenemos:

Definición 114 *Un cuerpo* K *es* ***algebraicamente cerrado*** *si toda extensión algebraica de* K *es trivial.*

Por trivial queremos decir que si $K < L$ es algebraica entonces $K = L$. Un importante ejemplo de cuerpo algebraicamente cerrado es $\mathbb{C}$, resultado establecido por Gauss en 1799. Tenemos los resultados siguientes:

Teorema 115 *Sea* $K < L$ *una extensión. Entonces son equivalentes:*

1. K *es algebraicamente cerrado.*
2. *Toda extensión finita de* K *es trivial.*
3. *Todo polinomio de* $K[X]$ *tiene todas sus raíces en* K.

Demostración. Es claro que (1) $\Rightarrow$ (2) es inmediato pues toda extensión finita es algebraica. En cuanto a (2) $\Rightarrow$ (3), como todo polinomio se descompone en producto de polinomios irreducibles, basta demostrar que los únicos irreducibles de $K[X]$ son los de primer grado: si $P \in K[X]$ es irreducible, por el Teorema 20, el cuerpo $K[X]/\langle P\rangle$ le entrega al menos una raíz a P (sabemos que $\lambda = \overline{X}$ es raíz de P); pero $K < K[X]/\langle P\rangle$ es una extensión finita de grado $gr(P)$ y por tanto $K = K[X]/\langle P\rangle$, lo que significa que $gr(P) = 1$. Por último, (3) $\Rightarrow$ (1) : sea $K < L$ es una extensión algebraica y $\lambda \in L$; como λ es algebraico, tiene un polinomio mínimo $M_\lambda \in K[X]$; por definición de M_λ sabemos que λ es raíz de M_λ y, luego, por la hipótesis (3), se infiere que $\lambda \in K$, lo que prueba que $L = K$. ■

Otra manera de demostrar la implicación (2) $\Rightarrow$ (3) es utilizando el Corolario 102, el cual nos garantiza que existe un cuerpo, extensión de K, que contiene todas las raíces de P. Ahora bien, si $\alpha_1, \alpha_2, \ldots, \alpha_n$ fueran sus raíces, la extensión $K < K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ es finita, luego por la hipótesis (2), $K = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$; se infiere entonces que $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$.

Proposición 116 *Todo cuerpo algebraicamente cerrado es infinito.*

Demostración. Si K fuera finito y $\alpha_1, \alpha_2, \ldots, \alpha_n$ sus elementos, entonces el polinomio $(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)+1$ no tendría raíces. ■

¿Que pasa si operamos con elementos algebraicos? Si tenemos $K < L$ denotemos por $A_K(L)$ el conjunto de los elementos de L que son algebraicos sobre K. Es claro que se tiene $K \subset A_K(L) \subset L$, pero la estructura es aún mucho más rica.

Teorema 117 *Se tiene $K < A_K(L) < L$. Además $A_K(L)$ es un cuerpo algebraicamente cerrado.*

Demostración. La Proposición 108 se utiliza varias veces en lo que sigue.

Sean $\alpha, \beta \in A_K(L)$. Sabemos que $[K(\alpha,\beta) : K]$ es una extensión finita y por tanto algebraica, es decir, todos los elementos de $K(\alpha,\beta)$ son algebraicos sobre K, o sea $K(\alpha,\beta) \subset A_K(L)$. Se infiere de todo esto que $\alpha \pm \beta$, $\alpha\beta$ y $\alpha\beta^{-1}$ (cuando $\beta \neq 0$) son elementos de $A_K(L)$, lo que demuestra que $A_K(L)$ es un cuerpo.

Con respecto a la segunda afirmación, sea η un elemento de alguna extensión algebraica de $A_K(L)$, de polinomio mínimo $M \in A_K(L)[X]$, $gr(M) = m$; si los coeficientes de M son $\gamma_0, .., \gamma_m$, es claro que η es algebraico sobre el cuerpo $K(\gamma_0, .., \gamma_m)$ y que la extensión $K(\gamma_0, .., \gamma_m) < K(\gamma_0, .., \gamma_m, \eta)$ es finita. Pero los coeficientes de M pertenecen a $A_K(L)$ y por tanto son algebraicos sobre K, por lo que la extensión $K < K(\gamma_0, .., \gamma_m)$ es finita. Concluimos que $K(\gamma_0, .., \gamma_m, \eta)$ es una extensión finita - y por tanto algebraica - de K. O sea η es algebraico sobre K, es decir $\eta \in A_K(L)$. ■

8.3. Contructibilidad con Regla y Compás

Lo que sigue es un regalo estético, que relaciona de manera insospechada a dos temas: en efecto, veremos como la teoría de cuerpos puede entregar respuestas a problemas que vienen de la geometría clásica, principalmente del mundo y de la cultura de los griegos. No referimos a problemas que surgen de construcciones geométricas que se realizan con una regla (no en tanto instrumento de medida sino que trazadora de rectas) y un compás.

¿Quién no ha escuchado la frase "estar buscando la cuadratura del círculo" para señalar que alguien pierde el tiempo o que busca lo imposible?. ¿Que tanto de cierto hay en ello?

Entre los problemas que se mantuvieron tenazmente irresolutos durante siglos están:

1. La cuadratura del círculo: construir un cuadrado con una superficie o un perímetro igual a la de una circunferencia dada. De lo que se trata es de construir con regla y compás el lado de tal cuadrado, teniendo como dato el radio de la circunferencia.

2. La duplicación del cubo: construir un cubo que tenga el doble del volumen o de la superficie de un cubo dado. Aquí la tarea es construir el lado de tal cubo, teniendo como dato el lado del cubo original.

3. La trisección de un ángulo dado.

Definamos ahora el contexto en donde vamos a operar: primero, necesitamos darnos una longitud (o medida) definida como unidad (el uno) y trabajaremos en el plano $\mathbb{R} \times \mathbb{R}$. Teniendo una figura en el plano, utilizando regla y compás, es decir trazando rectas y circunferencias, iremos obteniendo nuevos puntos a partir de las intersecciones que se produzcan:

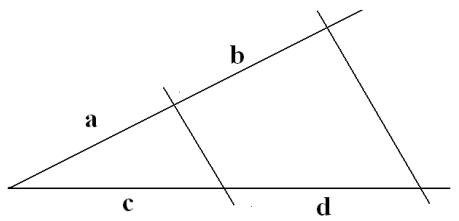
Definición 118 *Diremos que un punto de* $\mathbb{R}\times\mathbb{R}$ *es* ***constructible*** *si podemos obtenerlo con regla y compás a partir de una figura construida. Diremos además que un número real* α *es constructible si podemos construir un segmento de longitud* $|\alpha|$.

Como tenemos la longitud unidad (el uno: 1), tenemos como comenzar a operar; además, es claro que en la definición va implícito que el número de utilizaciones de regla y compás es finito. Por último, como la longitud de un segmento se calcula a partir de las coordenadas de los extremos del segmento, hay una suerte de equivalencia entre constructibilidad de puntos y de números.

Teorema 119 *El conjunto de los números constructibles es un cuerpo, extensión de* $\mathbb{Q}$.

Demostración. Tenemos el 1 y obviamente la longitud nula es constructible. Por otro lado, si λ y μ son longitudes constructibles, con el compás copiamos sobre una recta la longitud λ y después concatenamos la longitud μ : obtenemos la longitud $\lambda + \mu$; como por definición si μ es constructible también lo es $-\mu$ se obtiene que $\lambda + (-\mu) = \lambda - \mu$ es constructible (en todo caso, es evidente como se obtiene $\lambda - \mu$ con regla y compás).

Con respecto al producto y a los inversos, nos apoyamos en Thales, cuyo teorema nos dice que dada la figura:



constructible con regla y compás con los datos a, b y c, tenemos la proporción $\frac{a}{b} = \frac{c}{d}$. Tomando $a = 1$, $b = \mu$ y $c = \lambda$ obtenemos $d = \lambda\mu$; asimismo, con $a = \mu$, $b = 1$ y $c = \lambda$ se llega a $d = \lambda/\mu$.

Hemos establecido así que el conjunto de los números constructibles es un cuerpo; que este contiene a $\mathbb{Q}$ es inmediato pues su característica es obviamente nula. ■

¿Que tipo de extensión de $\mathbb{Q}$ es este cuerpo?; dicho de otra manera, ¿todo número real es constructible? Por lo pronto tenemos lo siguiente:

Proposición 120 *Si $\alpha \in \mathbb{R}$ es constructible entonces $\sqrt{\alpha}$ también.*

Demostración. Seguimos apoyándonos en los resultados de la geometría clásica, y no podía ser de otra manera. Dándonos las longitudes p y q construimos el segmento de longitud $p + q$ y con ayuda de regla y compás trazamos la perpendicular a este segmento en el punto de unión entre el segmento de longitud p y el de longitud q. Acto seguido, de nuevo con regla y compás, buscamos el punto medio del segmento de longitud $p+q$ y en ese centro trazamos la circunferencia de radio $(p + q)/2$. La intersección de esta circunferencia con la perpendicular nos determina la altura del triángulo, de longitud h.Ahora bien, sabiendo que todo ángulo inscrito en una semi-circunferencia es recto,

el teorema de Euclides nos dice que $h^2 = pq$. Así las cosas, tomando $p = \alpha$ y $q = 1$ se obtiene $h = \sqrt{\alpha}$. ■

Indaguemos un poco más para ver que condicionantes se imponen en la constructibilidad de puntos del plano o de longitudes. Como trabajamos con regla y compás, la construcción de tales puntos estará determinada por sistemas que surjan, según cada caso, de intersecciones entre rectas, entre una recta y una circunferencia o entre circunferencias (que, dicho sea de paso se puede reducir al caso de una recta con una circunferencia). Como sabemos que la ecuación general de una recta está dada por $ax + by + c = 0$ y la de una circunferencia por $x^2 + y^2 + ax + by + c = 0$ (con $a^2 + b^2 - 4c > 0$), estas intersecciones dan nacimiento a sistemas de ecuaciones de primer o de segundo grado, por lo que las longitudes constructibles serán raíces de polinomios de grados 1 o 2.

Con lo anterior, podemos enunciar el hermoso resultado:

Teorema 121 *El conjunto de los números constructibles es una extensión algebraica de* $\mathbb{Q}$. *Además, si* $\lambda \in \mathbb{R}$ *es constructible entonces* $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2^n$ *para cierto entero* n.

Demostración. Por la discusión recién realizada en torno a las ecuaciones en juego en las construcciones con regla y compás se deduce que todo número constructible es algebraico.

Por otro lado, hemos visto que si construimos α a partir de $\mathbb{Q}$ entonces obligadamente $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$ o 2. Análogamente, si construimos β a partir de α y $\mathbb{Q}$ tendremos la torre de extensiones $\mathbb{Q} < \mathbb{Q}(\alpha) < \mathbb{Q}(\alpha, \beta)$ donde se tiene $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 1$ o 2 por lo que $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 1, 2$ o 4 y por tanto el orden de β sobre $\mathbb{Q}$ (o sea $[\mathbb{Q}(\beta) : \mathbb{Q}]$) es $1, 2$ o 4. La idea se extiende recursivamente sin problema alguno, por lo que si hemos construido $\lambda \in \mathbb{R}$ después de m etapas, entonces $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2^n$ para $n \leq m$. ■

Ya estamos en situación de responder a los problemas clásicos señalados al comienzo. Veamos los dos primeros, el tercero queda para el lector:

- la cuadratura del círculo de radio r, en sus dos versiones, es imposible ya que está involucrado el número π, que sabemos es trascendente: respecto del perímetro la ecuación es $2x - \pi r = 0$ y respecto de la superficie, $x^2 - \pi r^2 = 0$.

- La duplicación del cubo de lado a es realizable respecto de la superficie (la ecuación es $x^2 - 2a^2 = 0$), pero no en lo que respecta al volumen, donde la ecuación es $x^3 - 2a^3 = 0$ y sabemos que $\sqrt[3]{2}$ no es constructible.

8.3.1. Algo sobre Cuerpos Finitos

Sabemos que todo cuerpo de característica nula contiene al cuerpo $\mathbb{Q}$; esto significa que si un cuerpo es finito obligadamente es extensión de $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, con p entero primo. Sin embargo, el recíproco no es válido: podemos tener cuerpos infinitos de característica p; el cuerpo de fracciones $\mathbb{Z}_p(X)$ es un ejemplo de ello.

Por otro lado, es inmediato que si $K < L$ entonces $car(K) = car(L)$.

Proposición 122 *Sea L un cuerpo finito, extensión de K tal que $[L : K] = n$. Si $|K| = q$, entonces $|L| = q^n$. Se infiere de esto que todo cuerpo finito tiene p^m elementos, donde p es un número primo.*

Demostración. Como L es un espacio vectorial de dimensión n sobre K es vectorialmente isomorfo a K^n; como K es finito, $|L| = |K|^n$. La segunda afirmación es inmediata por el comentario que antecede la proposición. ■

Reciprocamente, tenemos:

Proposición 123 *Para todo p, $n \in \mathbb{N}^*$, con p primo, existe un cuerpo L tal que $|L| = p^n$.*

Demostración. Consideremos en $\mathbb{Z}_p[X]$ el polinomio $P = X^q - X$, donde $q = p^n$; sabemos que para todo $\alpha \in \mathbb{Z}_p$ se tiene $\alpha^p = \alpha$ de donde se deduce que $\alpha^q = \alpha$ y por tanto que todo elemento de $\mathbb{Z}_p$ es raíz de P. Más aún, como $q = 0$ en $\mathbb{Z}_p$ (pues $p = 0$), se tiene se tiene $P' = -1$ y por tanto P no tiene raíces múltiples (2.3, ejercicio 17). Luego, P admite q raíces distintas que encontramos en alguna extensión de $\mathbb{Z}_p$. Sea R el conjunto de las raíces de P : como para todo $\rho \in R$, se tiene $P(\rho) = 0$, o sea $\rho^q = \rho$, si $\lambda, \mu \in R$ se tiene $(\lambda\mu)^q = \lambda\mu$ y, cuando $\mu \neq 0$, $(\lambda/\mu)^q = \lambda/\mu$; pero además, como $q = 0$, en los cálculos al interior de $\mathbb{Z}_p$ los coeficiente binomiales $\binom{q}{k}$ son nulos para $0 < k < q$, por lo que también se tiene que $(\lambda \pm \mu)^q = \lambda \pm \mu$. Todo esto permite establecer que R es un cuerpo de q elementos. ■

Dada la forma en que fue definido, el cuerpo R no es otro que el cuerpo de descomposición de $X^q - X$.

Para terminar, tenemos un importante teorema, cuya demostración requiere de rudimentos de la teoría de grupos.

Si K es un cuerpo y $K^* = K - \{0_K\}$, entonces $(K^*, \cdot)$ es un grupo, y se llama **el grupo multiplicativo** del cuerpo K:

Teorema 124 *El grupo multiplicativo de un cuerpo finito es cíclico.*

Necesitamos las tres proposiciones que siguen. Recordamos que el orden de un elemento g de un grupo G, que denotamos por $o(g)$, es el menor entero n tal que $g^n = 1_G$; para todo $g \in G$ se tiene $o(g) \mid |G|$.

Proposición 125 *Sean $(G, \cdot)$ un grupo, $g \in G$ y $h = g^k$. Si $o(g) = n$ y $d = mcd(n, k)$ entonces $o(h) = \dfrac{n}{d}$.*

Demostración. Es claro que los enteros $\dfrac{k}{d}$ y $\dfrac{n}{d}$ son primos entre si.

Pongamos $o(h) = m$. De $1_G = h^m = g^{km}$ se infiere que $n \mid km$ y por tanto que $\dfrac{n}{d} \mid \dfrac{k}{d}m$; ahora bien como $\dfrac{k}{d}$ y $\dfrac{n}{d}$ son primos entre si deducimos que $\dfrac{n}{d} \mid m$. Por otro lado, tenemos que $h^{\frac{n}{d}} = (g^k)^{\frac{n}{d}} = (g^n)^{\frac{k}{d}} = 1_G$ de donde resulta que $m \mid \dfrac{n}{d}$. Hemos establecido así que $m = \dfrac{n}{d}$. ■

Proposición 126 *Sean G un grupo y g, h elementos de G tales que $gh = hg$, $o(g) = n, o(h) = m$ y $mcd(n, m) = 1$. Entonces se tiene que $o(gh) = nm$.*

Demostración. Como $(gh)^{nm} = (g^n)^m (h^m)^n = 1$ entonces $o(gh) \mid nm$. Por otro lado, dado que $mcd(n, m) = 1$ existen $r, s \in \mathbb{Z}$ tales que $rn + sm = 1$; así las cosas, $g = gh^{sm} = g^{rn+sm}h^{sm} = (gh)^{sm}$ de donde $g \in \langle gh \rangle$ y por tanto $n \mid o(gh)$; de la misma manera, $h \in \langle gh \rangle$ y $m \mid o(gh)$. Como n y m son primos entre si, $nm \mid o(gh)$; luego $o(gh) = nm$. ■

Proposición 127 *Sean $(G, \cdot)$ un grupo abeliano finito y $g \in G$ un elemento de orden máximo. Entonces para todo $h \in G$ se tiene que $o(h) \mid o(g)$.*

Demostración. Pongamos $o(g) = n$ y $o(h) = m$. Supongamos que m no divide a n : en tal caso existe una potencia de un primo p en la descomposición de m que no aparece o aparece con un exponente menor en la descomposición de n : escribamos $n = us$ y $m = vr$ con $u = p^j,\ v = p^k$ donde $0 \leq j < k$.

Por las proposiciones anteriores se tiene: $o(g^u) = s$ y $o(h^r) = v$ y, como además $mcd(s, v) = 1$, el orden de $g^u h^r$ es sv lo que es superior a n, contradiciendo así la maximalidad del orden de g. ■

Podemos ahora demostrar el Teorema inicial:

Demostración. Sean K un cuerpo finito y $\alpha \in (K^*, \cdot)$ un elemento de orden máximo. Es claro que $o(\alpha) \leq |K^*|$ (mas aún, sabemos que $o(\alpha)$ divide a $|K^*|$); ahora bien, por el resultado anterior se infiere que todo elemento de K^* es raíz del polinomio $X^{o(\alpha)} - 1$; esto obliga a que $|K^*| \leq o(\alpha)$. Se establece así que $|K^*| = o(\alpha)$ y por tanto que $K^* = \langle \alpha \rangle$. ■

Ejercicios

1. Establezca los isomorfismos siguientes:
   (a) $K[X]/\langle X + 1\rangle \cong K$. (b) $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$.

2. Sea K un cuerpo, $car(K) \neq 2, 3$. Demuestre los siguientes isomorfismos:

   a) $K[X]/\langle X^2 - 1\rangle \simeq K[X]/\langle X^2 - 4\rangle \simeq K[X]/\langle X^2 - 9\rangle$.
   b) $K[X]/\langle X^2 + 1\rangle \simeq K[X]/\langle X^2 + 2X + 2\rangle \simeq K[X]/\langle X^2 + 6X + 10\rangle$.

3. Construya dos cuerpos infinitos de característica p (p un entero primo).

4. Compruebe que $X^2 + 4X + 5$ es irreducible sobre $\mathbb{R}$ y estudie si los cuerpos $\mathbb{Q}(i)$ y $\mathbb{Q}[X]/\langle X^2 + 4X + 5\rangle$ son isomorfos.

   Si no es el caso, argumente con claridad la imposibilidad; si lo fuese, precise los isomorfismos posibles.

5. Sea K un cuerpo de caracteristica 0. Establezca condiciones necesarias y suficientes para que se tenga el $K-$isomorfismo de anillos cocientes: $K[X]/\langle X^2 + \alpha X + \beta\rangle \simeq K[X]/\langle X^2 + \gamma X + \delta\rangle$.

   (un K-isomorfismo deja las constantes fijas)

6. Sean $K < L$ extensión de cuerpos, P y $Q \in K[X]$. Demuestre que:

   a) Si Q divide a P en $L[X]$ entonces también lo divide en $K[X]$.
   b) Si P y Q son primos entre si en $K[X]$ también lo son en $L[X]$.

c) Si P es irreducible sobre K y $\lambda \in L$ es raíz de P entonces es raíz simple.

7. En el cuerpo $\mathbb{C}$, demuestrese que los siguientes números son algebraicos: $\sqrt{2}+\sqrt{3}$, $\sqrt{7}+\sqrt{12}$, $2+i\sqrt{3}$ y $cos(\frac{2\pi}{k})+isen(\frac{2\pi}{k})$ con k entero positivo.

8. Determine el grado sobre $\mathbb{Q}$ de:
$\sqrt{2}+\sqrt{3}$, $2+i\sqrt{3}$, $cos(\frac{2\pi}{3})+isen(\frac{2\pi}{3})$ y $cos(\frac{2\pi}{8})+isen(\frac{2\pi}{8})$.

9. Sean K un subcuerpo de L y $\lambda \in L$. Demuestre que: λ^2 es algebraico sobre $K \Leftrightarrow$ también lo es λ. Más generalmente, sea $P \in K[X]$, P no constante: entonces $P(\lambda)$ es algebraico sobre $K \Leftrightarrow$ también lo es λ.

10. Exhiba dos cuerpos, $K < L$, de manera que L sea una extensión algebraica no finita de K.

11. Sean α y β algebraicos sobre K, de grados n y m respectivamente. Si n y m son primos entre si, demuestre que $[K(\alpha,\beta):K]=nm$.

12. De un ejemplo de números algebraicos α y β, de grados respectivos 2 y 3 sobre $\mathbb{Q}$, de manera que $\alpha\beta$ tenga sobre $\mathbb{Q}$, un grado menor que 6.

13. Sea K un subcuerpo de L. Si $[L:K]=p$ es un número primo, demuestre que para todo $\lambda \in L$ se tiene $K(\lambda)=K$ o $K(\lambda)=L$. Concluya que $K<L$ es una extensión simple.

14. Sean $F<K<L$. Si $[L:F]=2^n$, entonces $[K:F]=2^m$ para un entero $m \leq n$.

15. Sean $P \in K[X]$ un polinomio irreducible de grado n y D su cuerpo de descomposición Demuestre que $[D:K] \leq n!$.

16. Consideremos la extensión simple finita $K<K(\lambda)$ y la función $g_\lambda : K(\lambda) \to K(\lambda)$ definida por $g_\lambda(x)=\lambda x$, la cual es trivialmente lineal. Demuestre que el polinomio característico de g_λ es el polinomio mínimo asociado al elemento algebraico λ.

17. Sean L una extensión de K y $\tau \in L$. Demuestre que:

    a) τ es trascendente si y sólo si $P(\tau)$ lo es para todo $P \in K[X]$.

b) si τ es trascendente, $\sqrt[n]{\tau}$ también lo es para todo $n \in \mathbb{N}^*$.

c) si τ es trascendente, entonces $K(\tau)$ no es algebraicamente cerrado.

18. Lo que sigue es el punteo de la demostración de Cantor para establecer que $Alg_{\mathbb{Q}}(\mathbb{C})$, el conjunto de los números algebraicos, es numerable y deducir además la existencia en $\mathbb{R}$ de elementos trascendentes.

    a) Sea $P \in \mathbb{Z}[X]$, $P = \sum \alpha_i X^i$. Se define la altura del polinomio P como $h(P) = gr(P) + \sum |\alpha_i|$.

    Demuestre que existe un número finito de polinomios enteros para una altura dada ($\forall n \in \mathbb{N}$ se tiene: $|\{P \in \mathbb{Z}[X];\ h(P) = n\}| < \infty$).

    b) Demuestre que si $\alpha \in Alg_{\mathbb{Q}}(\mathbb{C})$ existe $P \in \mathbb{Z}[X]$ tal que $P(\alpha) = 0$.

    c) De (a) y (b) concluya que $Alg_{\mathbb{Q}}(\mathbb{C})$ es numerable y, por tanto, también $Alg_{\mathbb{Q}}(\mathbb{C}) \cap \mathbb{R}$, lo que asegura la existencia de una infinidad (tipo $\aleph_1$) de trascendentes reales.

19. Demuestre que si la cantidad α es constructible, también lo es $\sqrt[2^n]{\alpha}$.

20. Demuestre que es imposible trisectar un ángulo de 60^o utilizando regla y compás.

21. Demuestre que el número real δ es constructible si y sólo si $\sqrt{\delta + \sqrt{\delta}}$ también lo es.

22. En $\mathbb{Z}_2[X]$ encuentre todos los polinomios irreductibles de grado ≤ 9. Encuentre las descomposiciones de $X^n - 1$ para $n \leq 10$.

23. En $\mathbb{Z}_3[X]$ encuentre todos los polinomios irreductibles de grado ≤ 5. Encuentre las descomposiciones de $X^n - 1$ para $n \leq 6$.

24. En $\mathbb{Z}_5[X]$ encuentre todos los polinomios irreductibles de grado ≤ 3. Encuentre las descomposiciones de $X^n - 1$ para $n \leq 4$.

25. Sea K un cuerpo finito, $|K| = q$. Demuestre que:

    a) El polinomio $\alpha X^q + \beta X$, $\beta \neq 0$, no tiene raíces múltiples.

    b) Si n es primo con q, $\alpha X^n + \beta$, $\beta \neq 0$, no tiene raíces múltiples.

26. Construya dos cuerpos con 9 elementos y verifique que son isomorfos.

27. Construya cuerpos con 25, 27, 49, 81 y 125 elementos.

28. Para todo cuerpo finito K, donde $|K| = q$, se tiene $\prod_{a \in K^*} a = (-1)^q$.

29. Si p es primo, encuentre el resto de la división de $(p-1)!$ por p.

30. Demuestre que dos cuerpos finitos con el mismo número de elementos son isomorfos (esto quiere decir que, salvo isomorfismo, existe un único cuerpo de una cardinalidad dada)

9. Determinantes y Diagonalización

En este último capítulo desarrollamos la noción de determinante (de un sistema de vectores, de una matriz, etc.) y estudiamos sus propiedades; terminaremos con el concepto de diagonalización de un endomorfismo, de una matríz cuadrada, etc. En lo que se pueda, reemplazaremos escrituras más bien densas por argumentos lógicos más digeribles.

Sean K un cuerpo en el cual $2 \neq 0$ (es decir, un cuerpo de *característica* distinta de 2), V un espacio vectorial sobre K y $\varphi : V^n \to K$ una aplicación:

Definición 128 *φ se llama **forma multilineal** si para todo $\alpha, \beta \in K$ se tiene:*

$$\varphi(v_1, \ldots, \alpha v_i + \beta u_i, \ldots, v_n) = \alpha\varphi(v_1, \ldots, v_i, \ldots, v_n) + \beta\varphi(v_1, \ldots, u_i, \ldots, v_n).$$

*Además, se dice que φ es **alternada**, si para todo $1 \leq i < j \leq n$ se tiene:*

$$\varphi(\ldots, v_i, \ldots, v_j, \ldots) = -\varphi(\ldots, v_j, \ldots, v_i, \ldots).$$

Nota 129 *Algunos comentarios que surgen de la definición:*

1. *En general, es costumbre denominar **forma** a las aplicaciones lineales o multilineales cuyo espacio de llegada es el cuerpo de base.*

2. *Dada la multilinealidad de φ, es claro que si alguno de los v_k es el vector nulo entonces $\varphi(v_1, \ldots, v_n) = 0_K$. Además, como en el cuerpo K se tiene $2 \neq 0$, no es difícil mostrar que φ es alternada si y sólo si para todo $i \neq j$, si $v_i = v_j$ se tiene $\varphi(v_1, \ldots, v_n) = 0_K$.*

3. *Lo anterior nos dice que si φ es multilineal alternada y $\{v_1, \ldots, v_n\}$ es un sistema linealmente dependiente, es decir si uno de los v_k es combinación lineal de los otros, entonces $\varphi(v_1, \ldots, v_n) = 0_K$. En efecto:*

$$\varphi(v_1, \ldots, \overbrace{\sum_{i \neq k} \alpha_i v_i}^{k}, \ldots, v_n) \underset{multilineal}{=} \sum_{i \neq k} \alpha_i \varphi(v_1, \ldots, \overset{k}{\widehat{v_i}}, \ldots, v_n) \underset{alternada}{=} 0_K$$

4. *Finalmente, deducimos inmediatamente de (3) que para $1 \leq k \leq n$:*

$$\varphi(v_1, \ldots, v_k, \ldots, v_n) = \varphi(v_1, \ldots, v_k + \sum_{i \neq k} \alpha_i v_i, \ldots, v_n)$$

Supongamos ahora que la dimensión del espacio V es n y sea $\{e_1, \ldots, e_n\}$ una base de V. Expresemos $\varphi(v_1, \ldots, v_n)$ en función de $\varphi(e_1, e_2, \ldots, e_n)$: si para todo $1 \leq i \leq n$ tenemos $v_i = \sum_{k_i=1}^{n} \alpha_{ik_i} e_{k_i}$, entonces:

$$\varphi(v_1, v_2, \ldots, v_n) = \varphi\left(\sum_{k_1=1}^{n} \alpha_{1k_1} e_{k_1}, \sum_{k_2=1}^{n} \alpha_{2k_2} e_{k_2}, \ldots, \sum_{k_n=1}^{n} \alpha_{nk_n} e_{k_n}\right)$$

lo que por multilinealidad de φ nos da:

$$\sum_{k_1,\ldots,k_n=1}^{n} \alpha_{1k_1}\alpha_{2k_2}\cdots\alpha_{nk_n}\varphi(e_{k_1}, e_{k_2}, \ldots, e_{k_n}).$$

Ahora bien, la condición "forma alternada" de φ nos dice que en la expresión anterior se anulan todos los términos $\varphi(e_{k_1}, e_{k_2}, \ldots, e_{k_n})$ en los que hay alguna repetición. Por tanto, quedan solamente aquellos en que $(e_{k_1}, e_{k_2}, \ldots, e_{k_n})$ es una permutación de $(e_1, e_2, \ldots, e_n)$, es decir,

$$(e_{k_1}, e_{k_2}, \ldots, e_{k_n}) = \left(e_{\sigma(1)}, e_{\sigma(2)}, \ldots, e_{\sigma(n)}\right), \text{ donde } \sigma \in S_n.$$

Ahora bien, podemos pasar de $\varphi\left(e_{\sigma(1)}, e_{\sigma(2)}, \ldots, e_{\sigma(n)}\right)$ a $\varphi(e_1, e_2, \ldots, e_n)$ utilizando las transposiciones de la descomposición de σ, multiplicando por -1 por cada transposición, es decir, en definitiva obtenemos:

$$\varphi\left(e_{\sigma(1)}, \ldots, e_{\sigma(n)}\right) = sg(\sigma)\varphi(e_1, \ldots, e_n), \text{ donde } sg(\sigma) \text{ es el signo de } \sigma.$$

Con estas cosas aclaradas, podemos escribir:

$$\varphi(v_1, v_2, \ldots, v_n) = \left(\sum_{\sigma\in S_n} sg(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\cdots\alpha_{n\sigma(n)}\right)\varphi(e_1, e_2, \ldots, e_n) \qquad (*)$$

Nota 130 *De todo esto emanan varios importantes resultados:*

1. *De $(*)$ se infiere que dadas dos formas multilineales alternadas φ y ψ, estas son proporcionales; es decir existe $\lambda \in K$ tal que $\psi = \lambda\varphi$. Otra manera de expresar esto es decir que el espacio de formas multilineales alternadas definidas sobre V^n es de dimensión 1.*

2. *También de la identidad $(*)$ son inmediatas las equivalencias siguientes: φ es una forma no nula $\Leftrightarrow$ existe una base $\{e_1, \ldots, e_n\}$ tal que $\varphi(e_1, e_2, \ldots, e_n) \neq 0_K \Leftrightarrow$ para toda base se tiene $\varphi(e_1, e_2, \ldots, e_n) \neq 0_K$.*

3. *Si* $\varphi(e_1, e_2, \ldots, e_n) = \lambda \neq 0$ *entonces* $\varphi\left(\lambda^{-1}e_1, e_2, \ldots, e_n\right) = 1$, *por lo que podemos siempre escoger una base tal que* $\varphi(e_1, e_2, \ldots, e_n) = 1$; *por lo dicho en (1), para esa base* φ *es la única forma que verifica eso. Más aún, de* $(*)$ *podemos establecer que para toda otra base* $\{\varepsilon_1, \ldots, \varepsilon_n\}$ *tal que* $\varphi(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = 1$, *si* $v_i = \sum_{k=1}^{n} \gamma_{ik}\varepsilon_k$, $1 \leq i \leq n$, *entonces*

$$\sum_{\sigma \in S_n} sg(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)} \cdots \alpha_{n\sigma(n)} = \sum_{\sigma \in S_n} sg(\sigma)\gamma_{1\sigma(1)}\gamma_{2\sigma(2)} \cdots \gamma_{n\sigma(n)}$$

4. *Por último, dados los índices* i, j *el coeficiente* α_{ij} *aparece una y sólo una vez en la expresión* $\sum_{\sigma \in S_n} sg(\sigma)\alpha_{1\sigma(1)} \cdots \alpha_{n\sigma(n)}$; *puesto que además* $(\sigma(k), k) = (l, \sigma^{-1}(l))$ *con* $l = \sigma(k)$, *y* $sg(\sigma^{-1}) = sg(\sigma)$, *tenemos:*

$$\sum_{\sigma \in S_n} sg(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)} \cdots \alpha_{n\sigma(n)} = \sum_{\sigma \in S_n} sg(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2} \cdots \alpha_{\sigma(n)n}$$

Luego si $(w_1, w_2, \ldots, w_n) \in V^n$ *donde* $w_i = \sum_{j=1}^{n} \beta_{ij}e_j$ *con* $\beta_{ij} = \alpha_{ji}$ *entonces:* $\varphi(w_1, w_2, \ldots, w_n) = \varphi(v_1, v_2, \ldots, v_n)$.

9.1. Determinante de una Matriz

Definición 131 *Sean* $\{e_1, \ldots, e_n\}$ *una base tal que* $\varphi(e_1, e_2, \ldots, e_n) = 1$, *una familia* $(v_1, v_2, \ldots, v_n) \in V^n$ *tal que* $v_i = \sum_{k=1}^{n} \alpha_{ik}e_k$, *para todo* $1 \leq i \leq n$, *y* $A = (\alpha_{ij})_{1 \leq i,j \leq n}$, *una matriz cuadrada de orden* n :

- *El* ***determinante del sistema de vectores*** $(v_1, v_2, \ldots, v_n)$ *es el escalar:* $det(v_1, v_2, \ldots, v_n) = \sum_{\sigma \in S_n} sg(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)} \cdots \alpha_{n\sigma(n)}$
- *El* ***determinante de la matriz*** A *está dado por:* $|A| = det(F_1, \ldots, F_n)$ *donde los* F_i *son los "vectores fila (o línea)" de la matriz.*

  Obviamente, que se obtiene $\sum_{\sigma \in S_n} sg(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)} \cdots \alpha_{n\sigma(n)}$ *y, por el punto 3 de la Nota 130, tambien es igual a* $det(C_1, \ldots, C_n)$ *donde los* C_i *son los "vectores columna" de* A.

En lo que sigue trasladaremos al lenguaje matricial lo que se ha ido desarrollando en los puntos anteriores con respecto a los sistemas de n vectores.

Sea $A = (\alpha_{ij})_{1\leq i,j\leq n}$, una matriz cuadrada de orden n. De las definiciones y diversos comentarios hasta ahora presentados, se infiere de inmediato que:

1. Si $\lambda \in K$ y $A = (F_1, \ldots, F_n)$ entonces $|(F_1, \ldots, \lambda F_i, \ldots, F_n)| = \lambda\,|A|$; por tanto, $|\lambda A| = \lambda^n\,|A|$.

2. Si permutamos dos filas de A el determinante de la matriz resultante es $-\,|A|$.

3. Si A tiene dos filas iguales, o si una fila es combinación lineal de las otras filas, entonces $|A| = 0$.

4. Si a una fila se le agrega una combinación lineal de las otras filas, el determinante de la matriz resultante es el mismo que el de A.

5. Lo mismo que en (1,), (2), (3) y (4), cambiando la palabra "fila" por "columna".

6. Por último, si ${}^tA = (\alpha_{ji})_{1\leq i,j\leq n}$, es la matriz transpuesta de A, entonces $|{}^tA| = |A|$.

Terminamos esta parte introduciendo los elementos de estructura y de escritura para establecer un resultado que permite el cálculo explícito del determinante de una matriz.

Si A es una matriz de orden n denotemos por A_{ij} la matriz de orden $n-1$ que se obtiene de A al borrarle su i-ésima fila y su j-ésima columna. Sabemos que:

$$|A| = \sum_{\sigma\in S_n} sg(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\cdots\alpha_{n\sigma(n)}.$$

Si en esta sumatoria buscamos los términos en donde aparece el coeficiente α_{11} y factorizamos por él, vamos a encontrar:

$$\alpha_{11}\sum_{\substack{\sigma\in S_n\\ \sigma(1)=1}} sg(\sigma)\alpha_{2\sigma(2)}\cdots\alpha_{n\sigma(n)}$$

Ahora bien, es inmediato que $\{\sigma \in S_n; \sigma(1) = 1\}$ es isomorfo a S_{n-1} y por tanto lo que tenemos no es otra cosa que $\alpha_{11}\,|A_{11}|$ donde, como sabemos, A_{11} es la matriz de orden $n-1$ que se obtiene de A al borrarle su primera fila y su primera columna.

Utilicemos lo anterior para determinar el factor de α_{ij} en la sumatoria que corresponde a $|A|$: lo que haremos es hacer ciertas tranformaciones sobre la matriz A para dejar el coeficiente α_{ij} en el lugar de α_{11}. Para eso, permutemos la fila F_i con F_{i-1}, después con F_{i-2} y asi sucesivamente hasta permutarla con F_1; con estas $i-1$ transposiciones hemos obtenido así una matriz A' que verifica $|A'| = (-1)^{i-1}|A|$. Ahora tranformemos la matriz A' permutando su columna C_j sucesivamente con las $j-1$ columnas precedentes $(C_{j-1}, C_{j-2}, \ldots, C_1)$; la matriz A'' que se obtiene verifica $|A''| = (-1)^{j-1}|A'| = (-1)^{i+j}|A|$ y que $A''_{11} = A_{ij}$. Concluimos entonces que el factor de α_{ij} en la sumatoria está dado por $(-1)^{i+j}|A_{ij}|$.

Podemos ahora enunciar lo que se denomina "**el desarrollo del determinante por la i-ésima fila**" (o por la j-ésima columna):

Proposición 132 *Tenemos:* $|A| = \sum_{j=1}^{n}(-1)^{i+j}\alpha_{ij}|A_{ij}|$ *(o,* $\sum_{i=1}^{n}(-1)^{i+j}\alpha_{ij}|A_{ij}|$*)*

Demostración. Puesto que tomamos los coeficientes de una fila, y dada la estructura del determinante en donde los términos $\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\cdots\alpha_{n\sigma(n)}$ tomán un solo elemento por fila, en $\sum_{j=1}^{n}(-1)^{i+j}\alpha_{ij}|A_{ij}|$ están todos los términos de $\sum_{\sigma\in S_n} sg(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\cdots\alpha_{n\sigma(n)}$. ■

Para lo que viene, basta reflexionar recursivamente sobre n, desarrollando el determinante por la primera fila.

Proposición 133 *Sean A una matriz cuadrada de orden n y B una de orden m. Entonces: si* $P = \begin{pmatrix} A & 0s \\ 0s & B \end{pmatrix}$ *se tiene* $|P| = |A||B|$.

Demostración. Es claro que si $n = 1$ es trivial.

Tenemos: $|P| = \sum_{k=1}^{n}(-1)^{1+k}\alpha_{1k}|P_{1k}|$. Pero las matrices P_{1k} tienen la misma estructura que P y por tanto, recursivamente, $|P_{1k}| = |A_{1k}||B|$. Luego, $|P| = \sum_{k=1}^{n}(-1)^{1+k}\alpha_{ik}|A_{1k}||B| = \left(\sum_{k=1}^{n}(-1)^{1+k}\alpha_{ik}|A_{1k}|\right)|B| = |A||B|$ ■

Proposición 134 *Si $n = m$ se tiene:* $\begin{vmatrix} A & 0s \\ \lambda I & B \end{vmatrix} = |A||B|$, *donde I es la matriz unidad de orden n y $\lambda \in K$.*

Demostración. Si $Q = \begin{pmatrix} A & 0s \\ \lambda I & B \end{pmatrix}$, no hay dificultad en ver que, al igual que el caso anterior, las matrices menores Q_{1k} tienen la misma forma que Q, lo que posibilita la recurrencia. ■

Teorema 135 *Sean $A, B \in M_n(K)$. Entonces se tiene $|AB| = |A|\,|B|$.*

Demostración. Utilizaremos los resultados de las proposiciones anteriores y propiedades conocidas de los determinantes. Tomemos la matriz Q de la Proposición 87 con $\lambda = -1$; sabemos que $|Q| = |A|\,|B|$.

$$Q = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} & 0 & \cdots & & 0 \\ \alpha_{21} & \cdots & & \vdots & \vdots & \cdots & & \vdots \\ \vdots & \cdots & & \vdots & & & \cdots & \\ \alpha_{n1} & \cdots & \cdots & \alpha_{nn} & 0 & \cdots & \cdots & 0 \\ -1 & 0 & \cdots & 0 & \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ 0 & -1 & \ddots & \vdots & \beta_{21} & \cdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \cdots & & \vdots \\ 0 & \cdots & 0 & -1 & \beta_{n1} & \cdots & \cdots & \beta_{nn} \end{pmatrix}$$

Sabemos que si permutamos dos filas (o dos columnas) el determinante cambia de signo. Además, recordemos que el determinante de una matriz no cambia si a una fila (o a una columna) le sumamos una combinación lineal de otras filas (otras columnas). Estas operaciones las denotaremos por $F_k \to F_k + \sum_{j \neq k} \delta_j F_j$ o $C_k \to C_k + \sum_{j \neq k} \delta_j C_j$ donde F_k (respectivamente, C_k) es la k-ésima fila (respectivamente, columna).

Teniendo claro lo anterior, transformemos la matriz Q con las siguientes operaciones, que dejan invariante al determinante:

$$C_{n+k} \to C_{n+k} + \sum_{i=1}^{n} \beta_{ik} C_i \; ; \quad k = 1, 2, \ldots, n$$

Se puede verificar que las modificaciones llevadas a cabo lo que hacen es transformar la matriz Q en la matriz $R = \begin{pmatrix} A & D \\ -I & 0s \end{pmatrix}$. Si denotamos los coeficientes de D por δ_{ij} (que ocupa el lugar $(i, n+j)$ en la matriz R) tenemos $\delta_{ij} = \sum_{k=1}^{n} \alpha_{ik}\beta_{kj}$, es decir D no es otra cosa que la matriz AB $(*)$.

La segunda etapa de transformaciones, ahora modificando la matriz R, viene con las operaciones siguientes:

$$F_k \to F_k + \sum_{i=1}^{n} \alpha_{ki} F_{n+i} \; ; \quad k = 1, 2, \ldots, n$$

De esta manera, habiendo mantenido invariantes a los determinantes, llegamos a la matriz:

$$S = \begin{pmatrix} 0s & D \\ -I & 0s \end{pmatrix}, \text{ con } \; |S| = |R|$$

Por último, en esta nueva matriz, permutando las filas F_k y F_{n+k}, $k = 1, 2, \ldots, n$, obtenemos la matriz:

$$T = \begin{pmatrix} -I & 0s \\ 0s & D \end{pmatrix}, \quad \text{con} \quad |T| = (-1)^n |S| .$$

Ahora bien, con todo lo realizado tenemos:

$$|Q| = |R| = |S| = (-1)^n |T| \overset{Prop.\ 86}{=} (-1)^n |-I| \, |D| = (-1)^{2n} |D| = |D| .$$

Como $|Q| \overset{Prop.\ 87}{=} |A| \, |B|$ y $|D| \overset{(*)}{=} |AB|$, se establece el resultado. ■

Corolario 136 *A es invertible $\Leftrightarrow |A| \neq 0$. En tal caso tiene $|A^{-1}| = |A|^{-1}$.*

Demostración. La implicación directa sale inmediatamente de aplicar el resultado anterior a la identidad $AA^{-1} = I_n$.

El recíproco viene de lo siguiente: si fijamos una base $e_1, e_2, \ldots, e_n$, hay equivalencia entre matrices y endomorfismos; sea por tanto f el endomorfismo cuya matriz es A : se tiene $f(e_i) = C_i$, la i-ésima columna de A.

Por tanto, si A no es invertible entonces f no es biyectiva y esto significa que $dim(Im(f)) < n$, es decir que $f(e_1), f(e_2), \ldots, f(e_n)$ no es libre, lo que en el lenguaje matricial se traduce en que las columnas de A son linealmente dependientes.

Concluimos que $|A| = 0_K$. ■

9.2. Diagonalización de un Endomorfismo

Dados un espacio vectorial y un endomorfismo f, desde el punto de vista de la escritura y del cálculo, es muy agradable poder trabajar con aquellos vectores v para los cuales $f(v)$ es un elemento del subespacio engendrado por v (es decir Kv), o sea, tener $f(v) = \lambda v$ para un cierto $\lambda \in K$. Si podemos contar con una base del espacio formada por este tipo de elementos, por ejemplo v_1, v_2, v_3, con $f(v_k) = \lambda_k v_k$, $k = 1, 2, 3$, la representación matricial de f con respecto a esta base será la matriz diagonal:

$$\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$$

lo que evidentemente simplifica bastante todo lo que se refiere a operatoria algebraica matricial. Introduzcamos pues:

Definición 137 *Sean K un cuerpo, V un espacio vectorial de dimensión n sobre K y $f : V \to V$ una aplicación lineal.*

- *Se llama **vector propio** asociado al endomorfismo f a todo vector **no nulo** $v \in V$ tal que $f(v) \in Kv$.*
- *Si $f(v) = \lambda v$, el escalar λ se llama **valor propio** de f asociado al vector v.*
- *Si λ es un valor propio de f, el conjunto $U_\lambda = \{v \in V;\ f(v) = \lambda v\}$ se denomina el **subespacio propio** asociado al valor λ.*

Ahora bien, es evidente que el vector nulo 0_V cumple la definición para cualquier valor propio y por ello debe ser excluido. Por otro lado, de la definición se infiere que la existencia de vectores propios no depende de las opciones de bases para expresar la aplicación; por lo demás, tal existencia no está garantizada; para convencerse estudie el caso de $f \in End_K(K^2)$ definida por $f(a, b) = (2b - a, b - a)$ cuando $K = \mathbb{R}$ y $\mathbb{C}$. Finalmente, es inmediato verificar que los conjuntos U_λ son realmente subespacios vectoriales de V.

Proposición 138 *Si $\lambda_1, \ldots, \lambda_m$ son valores propios distintos de f entonces para todo $k = 1, 2, 3, \ldots, m$ se tiene $U_{\lambda_k} \cap \sum_{k \neq i} U_{\lambda_i} = \{0_V\}$.*

El enunciado de esta proposición es equivalente a decir que **la suma de los subespacios propios es directa**, lo que -dicho de otra manera- significa que si se toma una familia libre por subespacio propio, la reunión de estas es una familia libre del espacio. De ahora en adelante, si no hay confusión posible, escribiremos U_k en vez de U_{λ_k}.

Demostración. Para $m = 2$ es inmediato pues si $u \in U_1 \cap U_2$ se tiene $\lambda_1 u = f(u) = \lambda_2 u$ y como $\lambda_1 \neq \lambda_2$ se infiere que $u = 0_V$. Supongamos pues que para toda colección de $m-1$ subespacios propios el enunciado se verifica y sea $u \in U_k \cap \sum_{k \neq i} U_i$ con $k = 1, 2, 3, \ldots, m$.

Reenumerando si es necesario, consideremos que $k = m$; se tiene entonces $u = u_1 + u_2 + \cdots + u_{m-1}$ con $u_i \in U_i$ y por tanto, aplicando f, se llega a $\lambda_m u = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_{m-1} u_{m-1}$, lo que se traduce en la combinación lineal $(\lambda_1 - \lambda_m)u_1 + (\lambda_2 - \lambda_m)u_2 + \cdots + (\lambda_{m-1} - \lambda_m)u_{m-1} = 0_V$. Como, por hipótesis de inducción, la suma de los subespacios U_i, con $1 \leq i \leq m-1$, es directa y los valores propios son distintos obligadamente los u_i son nulos y por tanto $u = 0_V$. ■

Definición 139 *Se dice que f es diagonalizable si V admite una base formada por vectores propios de f o, dicho de manera equivalente, si $V = \bigoplus_{i=1}^{m} U_i$.*

Es claro entonces que f es diagonalizable si y sólo si $dim_K(V) = \sum_{i=1}^{m} dim_K(U_i)$ y que la matriz diagonal asociada a f respecto de tal base es de la forma:

$$\begin{pmatrix}
\lambda_1 & 0 & \cdots & & \cdots & & \cdots & & 0 \\
0 & \ddots & \ddots & 0 & \cdots & & \cdots & & 0 \\
 & \ddots & \lambda_1 & \ddots & \cdots & & \cdots & & \vdots \\
\vdots & & 0 & \lambda_2 & 0 & \cdots & & \cdots & \\
 & & & \ddots & \ddots & \ddots & & & \vdots \\
\vdots & & & & 0 & \lambda_2 & \ddots & & \\
 & & & & & \ddots & \ddots & \ddots & \vdots \\
\vdots & \cdots & & \cdots & & \cdots & 0 & \ddots & 0 \\
0 & & \cdots & & \cdots & & \cdots & 0 & \lambda_m
\end{pmatrix}$$

donde el valor propio λ_i aparece $dim_K(U_i)$ veces.

So pena de ser repetitivo, insistamos en que las bases que diagonalizan a f son aquellas formadas por reuniones $\cup B_k$, donde B_k es cualquier base del subespacio propio U_k.

El problema que se plantea ahora es como hacer para encontrar los valores y vectores propios de un endomorfismo, de manera general. Veamos primero que si escogemos una base B para la escritura vectorial y si M es la matriz de f con respecto a B (de partida y de llegada), con respecto a otra base B' será de la forma $M' = CMC^{-1}$, donde C es la matriz de cambio de base; por la propiedad multiplicativa de los determinantes se tiene $|M'| = |CMC^{-1}| = |C|\,|M|\,|C|^{-1} = |M|$. Esto nos lleva a:

Definición 140 *El* ***determinante de*** f, *que denotamos por* $det(f)$, *se define como el determinante de su matriz asociada, en cualquier opción de base.*

Vamos ahora a lo siguiente: si λ es valor propio de f significa, como sabemos, que existe un vector no nulo v tal que $f(v) = \lambda v$, lo que reescrito como $(\lambda Id - f)(v) = 0_V$ nos dice que la aplicación lineal $\lambda Id - f$ no es inyectiva. Por lo demás, tenemos las equivalencias inmediatas:

$$\lambda \text{ es valor propio de } f \;\Leftrightarrow\; \lambda Id - f \text{ no es inyectiva} \;\Leftrightarrow\; det(\lambda Id - f) = 0$$

Asi las cosas, para encontrar los valores propios debemos buscar las raíces del polinomio $det(xId - f) \in K[x]$. Ahora bien, sabemos que la existencia de raíces está muy ligada al cuerpo de base, pero ya hemos visto que siempre podemos encontrar un cuerpo que contenga todas las raíces de un polinomio dado; además, en caso extremo, podemos operar con cuerpos algebraicamente cerrados, en los cualles cualquier polinomio se descompone en producto de polinomios de primer grado (el cuerpo $\mathbb{C}$ tiene esta propiedad y no asi $\mathbb{R}$).

Observemos además que si $g : V \to V$ es un automorfismo se tiene $xId - (g \circ f \circ g^{-1}) = g \circ (xId - f) \circ g^{-1}$. Inferimos, como era esperable, que el polinomio $det(xId - f)$ no depende de la opción de bases en el espacio vectorial, pues $det\,(g \circ (xId - f) \circ g^{-1}) = det(g)det(xId - f)det(g)^{-1} = det(xId - f)$.

Definición 141 *El polinomio* $det(xId - f)$ *se llama* ***el polinomio característico*** *del endomorfismo* f.

Las definiciones que hemos introducido hasta ahora no dependen, como hemos visto, de las bases que están en juego para la escritura.

Podemos por tanto fijar una, sin consecuencia estructural alguna y trabajar propiamente en el ámbito matricial, dado que en tal caso hay equivalencia entre endomorfismos y matrices cuadradas. Precisemos solamente el "diccionario"; si $dim(V) = n$ entonces :

$$\begin{aligned} vectores &\leftrightarrow matrices\ columna\ de\ largo\ n \\ endomorfismos &\leftrightarrow matrices\ cuadradas\ de\ orden\ n \end{aligned}$$

$$f(w) \leftrightarrow \begin{pmatrix} a_{11} & \cdots & \\ \vdots & \ddots & \\ & & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

Reescribamos para las matrices lo realizado para los endomorfismos; sea A una matriz cuadrada:

- *A es diagonalizable si existe una matriz invertible C tal que $D = CAC^{-1}$ sea diagonal. La matriz D se llama la diagonalizada de A.*
- *El polinomio característico de A está dado por $|xI - A|$, donde I es la matriz unidad de orden n. Estudiar la diagonalización de A consiste en buscar las raíces de su polinomio característico*

Es claro, por lo visto anteriormente, que si A es diagonalizable su polinomio característico es el mismo que el de la matriz D; por tanto, si

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & & \cdots & & \cdots & & 0 \\ 0 & \ddots & \ddots & 0 & \cdots & & \cdots & & 0 \\ & \ddots & \lambda_1 & \ddots & \cdots & & \cdots & & \vdots \\ \vdots & & 0 & \lambda_2 & 0 & \cdots & & \cdots & \\ & & & \ddots & \ddots & \ddots & & & \vdots \\ \vdots & & & & 0 & \lambda_2 & \ddots & & \\ & & & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & \cdots & & \cdots & & \cdots & 0 & \ddots & 0 \\ 0 & & \cdots & & \cdots & & \cdots & 0 & \lambda_m \end{pmatrix}$$

entonces $|xI - D| = (x - \lambda_1)^{n_1}(x - \lambda_2)^{n_2} \cdots (x - \lambda_m)^{n_m}$.

Vemos que la multiplicidad de cada raíz no es otra cosa que la dimensión de su respectivo subespacio propio; o sea, entonces, para que una matriz sea diagonalisable se debe tener $n_1 + n_2 + \cdots + n_m = n$.

Si tal condición no se verifica, habiendo sin embargo valores propios, la matriz A será equivalente a una matriz del tipo:

$$\begin{pmatrix} \Delta & 0s \\ 0s & B \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 & \cdots & & \cdots & & \cdots & & 0 \\ 0 & \ddots & \ddots & 0 & \cdots & & \cdots & & 0 \\ & \ddots & \lambda_k & \ddots & \cdots & & \cdots & & \vdots \\ \vdots & & 0 & \ddots & 0 & \cdots & & \cdots & \\ & & & \ddots & \lambda_m & \ddots & & & \vdots \\ \vdots & & & & 0 & b_{11} & \cdots & \cdots & b_{1p} \\ & & & & & \vdots & \ddots & & \vdots \\ \vdots & \cdots & & \cdots & & \vdots & & \ddots & \vdots \\ 0 & & \cdots & & \cdots & b_{p1} & \cdots & \cdots & b_{pp} \end{pmatrix}$$

y su polinomio característico tendrá la forma $(x - \lambda_1)^{n_1} \cdots (x - \lambda_m)^{n_m} P(x)$, donde $P(x) = |xI - B|$ es un polinomio irreductible de grado p y obviamente se tiene $n = p + n_1 + \cdots + n_m$.

Sin embargo, tal cual lo hemos visto, siempre podemos extender el cuerpo de manera de contar con todas las raíces de un polinomio. Más aún, no está demás decir que habitualmente se trabaja con el cuerpo $\mathbb{C}$ de los números complejos que, como sabemos, es algebraicamente cerrado, lo que garantiza la existencia de todas las raíces.

Bueno, para terminar, nos queda indagar como se construyen los vectores propios. La cosa es simple de plantear: si λ es un valor propio de A basta resolver el sistema lineal que resulta de la ecuación matricial $AX = \lambda X$:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

También podemos operar de la sigiente manera: si la diagonalizada de A es D y conocemos la matriz C tal que $A = C^{-1}DC$ entonces, tomando $Y = CX$, se trata de resolver el sistema lineal $DY = \lambda Y$.

9.3. Algunos Ejemplos

1. Tomemos el ejercicio propuesto al comienzo: tenemos $f \in End_K(K^2)$ definida por $f(a,b) = (2b-a, b-a)$ cuando $K = \mathbb{R}$ y $\mathbb{C}$. La matriz de f con respecto a la base canónica y su polinomio característico son dados por:

$$\begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}; \quad \begin{vmatrix} x+1 & -2 \\ 1 & x-1 \end{vmatrix} = x^2 + 1$$

   Los valores propios son por tanto complejos; concluimos que en $\mathbb{R}$ el endomorfismo no tiene valores propios, y cuando el cuerpo de base es $\mathbb{C}$, la aplicación f es diagonalizable y su matriz diagonal asociada es:

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix};$$ y una base de valores propios es: $\{(1-i,1); (1+i,1)\}$

2. Sean V un K-espacio vectorial y $f, g \in End_K(V)$ tales que: $f^2 = f$ y $g^2 = Id$. Estudiemos si estas aplicaciones son diagonalizables (de la primera se dice que es un proyector; de la segunda que es una involución). Veamos:

   a) Para la primera los casos extremos son $f = Id$ y $f = 0$ que son trivialmente diagonales. Fuera de esos casos, de $f(v) = \lambda v$ se infiere que $\lambda^2 = \lambda$ por lo que los valores propios posibles son 0 y 1. Ahora bien, es claro que $U_0 = Ker(f)$ y no es difícil ver que $U_1 = Im(f)$. Como además $dim(Ker(f)) + dim(Im(f)) = dim(V)$ se deduce que $V = Ker(f) \oplus Im(f)$, es decir que f es diagonalizable. En conclusión, todo proyector puede referirse a una base respecto de la cual tendrá una matriz diagonal formada por $0s$ (tantos como la dimensión del nucleo) y $1s$ (tantos como la dimensión de la imagen).

   b) Para la segunda los casos extremos son $g = \pm Id$, que son trivialmente diagonales. Fuera de esos casos, de $g(v) = \lambda v$ se infiere que $\lambda^2 = 1$ por lo que los valores propios posibles son 1 y -1. Como además, para todo $v \in V$ se tiene $v + g(v) \in U_1$ y $v - g(v) \in U_{-1}$ entonces $v = \frac{1}{2}(v + g(v)) + \frac{1}{2}(v - g(v))$ (pues $K \neq \mathbb{Z}_2$)), se deduce que $V = U_1 \oplus U_{-1}$, es decir g es diagonalizable y su matriz asociada diagonal está formada por $1s$ y $-1s$.

Ejercicios

1. Estudiar la diagonalización y la determinación de vectores propios asociados de $h, k, l \in End_{\mathbb{C}}(V)$ tales que $h^3 = h$, $k^3 = k^2$ y $l^3 = Id$.

2. Sea v un vector propio de f asociado al valor propio λ. Demuestre que v es un vector propio de f^n correspondiente al valor propio λ^n y que si P es un polinomio, v es vector propio de $P(f)$ asociado al valor $P(\lambda)$.

3. Muestre que una matriz A no nula y nilpotente (es decir $A^n = 0$ para algún entero positivo) no es diagonalizable.

4. Considere las matrices reales: $M(a,c,b,d) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ d & c & a & b \\ c & d & b & a \end{pmatrix}$

   a) Muestre que este conjunto de matrices es un espacio vectorial sobre $\mathbb{R}$ y encuentre una base (la "más natural").

   b) Muestre que M es diagonalizable y deduzca su determinante.

5. Estudie, sobre $\mathbb{C}$, la diagonalización de las matrices $n \times n$ tales que:

   a) Todos los coeficientes son $1s$.

   b) La primera y la última línea asi como la primera y la última columna estan formadas de $1s$.

   Hágalo para $n = 2, 3, 4$ y formule (y demuestre si le es posible) una hipótesis para cualquier n.

6. Dados $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$ encuentre el polinomio característico de la matriz:

$$A = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 & -\alpha_0 \\ 1 & \ddots & & \cdots & 0 & -\alpha_1 \\ 0 & \ddots & 0 & & \vdots & \vdots \\ \vdots & \ddots & 1 & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & \cdots & 0 & 1 & -\alpha_n \end{pmatrix}$$

7. Según los valores de $\alpha \in [0, 2\pi[$, estudie la diagonalización en $\mathbb{R}$ de las siguientes matrices.

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \quad B = \begin{pmatrix} \cos\alpha & 0 & -\sin\alpha \\ -\sin\alpha & 1 & \cos\alpha \\ \cos\alpha & 0 & -\sin\alpha \end{pmatrix}$$

8. Sea $a \in \mathbb{R}$ y considere la matriz $A \in M_3(\mathbb{R})$:

$$A = \begin{pmatrix} 3 & -2 & 2a-6 \\ a & 1-a & a^2-3a \\ 1 & -1 & a-2 \end{pmatrix}$$

   a) Calcule A^2 y a partir de ello deduzca los valores propios de A (sugerencia: reflexione sobre lo que ha escrito...). Diagonalice la matriz A.

9. Sea $\omega \in \mathbb{C}$ una raíz cúbica de la unidad, $(\omega^3 = 1)$ distinta de 1.

   a) Demuestre la identidad $\omega^2 = -(\omega + 1)$ (que utilizará en lo que viene)

   b) Considere la matriz compleja:

$$B = \begin{pmatrix} \omega & 0 & 3-3\omega \\ 0 & \omega^2 & 1-\omega^2 \\ 0 & 0 & 1 \end{pmatrix}$$

   Estudie la diagonalización de la matriz B. ¿Que puede concluir?

10. Muestre que una matriz no nula y nilpotente no es diagonalizable.

11. Sea V un K-espacio vectorial de dimensión finita y $f : V \to V$ lineal, distinta de la identidad. Si $f^3 = Id$, encuentre condiciones para que f sea diagonalizable.

.

10. Una Aplicación: la Teoría de Códigos

En lo que sigue, como una aplicación importante de nociones algebraicas que hemos desarrollado hasta ahora (conjuntos, combinatoria, espacios vectoriales, matrices, cuerpos finitos, polinomios,etc.), presentaremos aspectos de la teoría de códigos de longitud constante, también llamados códigos en bloque.

La comunicación es un paradigma de la humanidad. Desde sus albores las comunidades humanas buscaron maneras de comunicar más allá del alcance de la palabra; era necesario, a la distancia, señalar la ubicación de una presa, el advenimiento de un peligro, la visita de alguien importante, el festejo de un rito o simplemente el anuncio de una buena nueva.

Surgen así silbidos, ruidos de tambores, el trinar de pitos y trompetas, señales de humo, que según su cadencia de emisión y su duración trasmitían mensajes descifrables por alguien del entorno y de cultura símil.

Estos primeros ejemplos de transmisión de mensajes tenían limitaciones obvias. El desarrollo de los primeros tipos de escritura y de los transportes elementales, con la invención de la rueda, la domesticación del caballo y el dominio de las aguas, permitió la trasmisión de textos de una manera más amplia, menos ambigua y más segura, aunque de insalvable lentitud.

Con la revolución industrial y el descubrimiento de la electricidad surge el telégrafo, invención de Samuel Morse en 1832. Es recién en 1838 que Morse propone codificar las señales eléctricas con tres símbolos: el punto ($\cdot$), el guión ($-$) y el espacio ( ).

El telégrafo y el código Morse provocan una verdadera revolución en las comunicaciones. Mas bien adaptado a textos cortos (por razones de eficiencia y de costos), con este sistema se llega a la era de los mensajes "instantáneos". En este procedimiento, por razones obvias, el número de símbolos que codifica una letra del abecedario está en relación inversa a su utilización en el idioma, en este caso el inglés; así por ejemplo tenemos:

$$A = \cdot-,\ B = -\cdot\cdot\cdot,\ E = \cdot,\ I = \cdot\cdot,\ J = \cdot---,\ M = --,\ X = -\cdot\cdot-$$

El telégrafo fué perfeccionado por Thomas A. Edison unos cuarenta años después, en 1874, logrando hacer transitar, simultaneamente, dos mensajes por un mismo circuito.

10.1. Códigos de Longitud Constante

En la era moderna los mensajes son trasmitidos a través de ondas electromagnéticas. Los códigos que surgen requieren de estructuras que permitan recuperar palabras que llegan cambiadas a la recepción; estos siguen siendo listas de símbolos en donde parte de ellos codifican la palabra y los otros detectan y permiten corregir errores propios de la trasmisión.

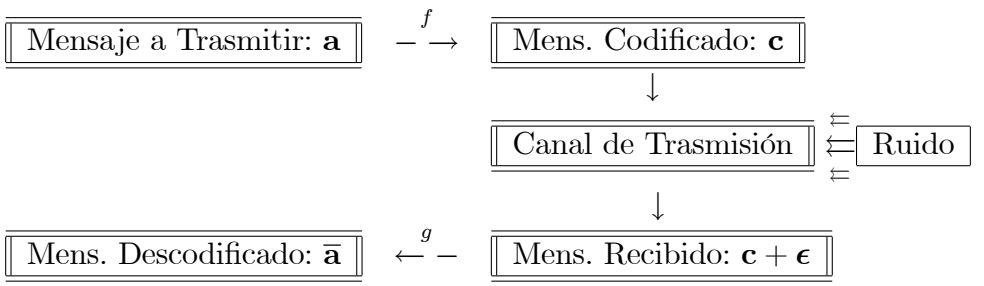
Más precisamente, en lo que respecta a códigos en bloque (de longitud constante), si $a_1 \dots a_k$ es una palabra de un mensaje, codificar esta palabra consiste en insertarla (de una u otra manera, previamente estipulada) en una palabra $c_1 \dots c_n$ con $k < n$.

Así por ejemplo posibles codificaciones de la palabra $a_1a_2a_3$ son :

$a_1a_2a_3a_1,\ a_1a_2a_3a_1a_2,\ a_1a_1a_2a_2a_3a_3,\ a_1c_1a_2c_2a_3c_3,\ a_1a_2c_1a_3c_1c_2,$ etc.

Como vemos se trata de variar la longitud de la palabre del mensaje ocupando ciertos lugares de manera sistemática y utilizando símbolos, los cuales no son necesariamente distintos entre ellos como tampoco a aquellos utilizados en la palabra original. Estas $n - k$ nuevas componentes se llaman los símbolos de control y sirven para estimar la diferencia (errores de la trasmisión) entre la palabra enviada y aquella recepcionada, como así mismo para descodificar y recuperar el texto original.

En un esquema de codificación simplificado, lo que ocurre es lo siguiente:



Necesitamos pues **un alfabeto**, **el lenguaje** (o conjunto de palabras que tal alfabeto produce) y **el código** (dado por algunas palabras del lenguaje).

Sea $A \neq \emptyset$ un conjunto finito y $n \in \mathbb{N}^*$. Llamaremos palabra a todo elemento de A^n; éstas serán denotadas indistintivamente (según contexto y el uso común en la literatura ah-hoc) por $a = (a_1, \dots, a_n)$ o por $a = a_1 \dots a_n$.

A es el alfabeto y A^n, las palabras de largo n, el lenguaje.

Definición 142 *Se llama* ***código de longitud*** *n sobre el alfabeto A cualquier subconjunto no vacío C de A^n.*

Así, por ejemplo: $C = \{(\lambda, \lambda, \theta, \lambda), (\theta, \lambda, \theta, \lambda), (\lambda, \theta, \theta, \lambda)\}$ es un código de longitud 4 sobre el alfabeto $A = \{\lambda, \theta\}$.

Si $\sigma \in S_n$ es una permutación, sea $\overline{\sigma} : A^n \to A^n$ la biyección inducida naturalmente y definida por: $\overline{\sigma}((a_1, \ldots, a_n)) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$. Tenemos:

Definición 143 *Dos códigos C y $\overline{C}$ de longitud n* ***son equivalentes*** *si existe una permutación $\sigma \in S_n$ tal que $\overline{\sigma}(C) = \overline{C}$. Es claro que esto define una relación de equivalencia en el conjunto de códigos sobre un alfabeto A.*

Dos códigos equivalentes tendrán las mismas propiedades estructurales (propiedades que serán desarrolladas en lo que sigue), por lo que, salvo mención de lo contrario, trabajaremos con un tipo de código por clase.

Como vimos anteriormente, los errores de trasmisión son medidos por las diferencias entre las palabras emitidas y aquellas recepcionadas; por ejemplo, se envía la palabra $xyxxyx$ y se recibe $xyyxyx$. Necesitamos formalizar la noción de "lejanía" entre tales palabras:

Definición 144 *Si $a, b \in A^n$ se llama* ***distancia de Hamming*** *entre a y b el número de componentes distintas que poseen dichas palabras, es decir, si $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ entonces:*

$$d(a, b) = |\{ k ;\ a_k \neq b_k \}| .$$

La distancia de Hamming nos permitirá definir y precisar aspectos estructurales referentes a los códigos. La denominación de "distancia" no es gratuita; en efecto:

Proposición 145 *(A^n, d) es un espacio métrico discreto.*

Demostración. Se deja de ejercicio. ■

Queda claro que d no presenta interés desde el punto de vista topológico, pues todo se trivializa. Sin embargo, la distancia de Hamming presenta otras bondades; es evidente que estamos frente a un espacio métrico de una homogeneidad sin sorpresas, que podemos imaginar como una malla multidimensional uniforme. Es inmediato que todas las distancias y radios en juego son números enteros.

Si $k \leq n$ y $a \in A^n$, definimos la esfera de centro a y radio k; de la manera siguiente: $E(a, k) = \{ x \in A^n ;\ d(a, x) = k \}$. Tenemos:

Proposición 146 $|\,E(a,k)\,| = \binom{n}{k}(|A|-1)^k$.

Demostración. Es claro que si cambiamos k componentes de a obtenemos una palabra b tal que $d(a,b) = k$. Ahora bien, si por ejemplo remplazamos la componente a_i debemos hacerlo por un elemento de $A - \{a_i\}$; es decir tenemos $|A| - 1$ opciones por componente cambiada; esto significa que para una elección de k componentes tenemos $(|A| - 1)^k$ posibilidades de reemplazo. El resultado pedido se establece entendiendo que tenemos $\binom{n}{k}$ opciones de escoger k componentes. ■

Lo anterior nos lleva a establecer una importante propiedad que confirma la homogeneidad estructural de la cual hicimos mención más arriba:

Teorema 147 *Todas las bolas de radio r tienen* $\sum_{k=0}^{r}\binom{n}{k}(|A|-1)^k$ *elementos.*

Demostración. Se deduce inmediatamente de la proposición 146 pues $B(a,r)$ es la unión disjunta de las esferas $E(a,k)$, $0 \leq k \leq r$. ■

No es difícil entender que la eficiencia de un código tiene directa relación con la uniformidad que exista en las distancias entre cada palabra emitida y su respectiva recepcionada. Necesitamos el concepto siguiente:

Definición 148 *Sea $e \in \mathbb{N}$ y C un código de longitud n. Diremos que C es un* ***código e-corrector*** *(o que verifica la condición de descodificación e) si para todo $x \in A^n$ existe a lo más un elemento $c \in C$ tal que $d(x,c) \leq e$.*

El siguiente punto de vista es muy útil:

Proposición 149 *Decir que C es un código e-corrector es equivalente a decir que las bolas cerradas de radio e, centradas en los elementos de C, son disjuntas dos a dos.*

En lo que sigue, incorporamos nuevos conceptos:

Definición 150 *Se llama* ***radio de recubrimiento*** *de un código C, el cual denotamos ρ_C, al menor entero r tal que las bolas de radio r, centradas en los elementos de C, recubren A^n.*

Definición 151 *Llamamos* ***distancia mínima*** *de un código C, la cual denotamos δ_C, el número dado por :*

$$\delta_C = \text{mín}\{d(x,y);\ x,y \in C,\ x \neq y\}.$$

Estamos en condiciones de establecer precisiones estructurales:

Teorema 152 *Sean C un código y $e \in \mathbb{N}$. Si $2e+1 \leq \delta_C$ entonces C es un código e-corrector.*

Demostración. Basta demostrar que la condición $2e+1 \leq \delta_C$ implica que las bolas $B(a,e)$ con $a \in C$ son disjuntas dos a dos (ver ejercicio 149). Se deja como entretención para el lector. ■

Es claro que el número e más grande que verifique la condición del teorema está dado por

$$e_C = \left\lfloor \frac{\delta_C - 1}{2} \right\rfloor$$

donde $\lfloor x \rfloor$ es **la parte entera** de un número real x (por ejemplo, $\lfloor \pi \rfloor = 3$). Con esto tenemos:

Definición 153 *La cantidad e_C se llama **capacidad de corrección** del código C. Decimos que un código es **e-corrector** si $e \leq e_C$; decimos que es **perfecto** si $e_C = \rho_C$.*

Las nociones que hemos desarrollado nos permiten formular preguntas sensatas. Dados e y ρ :

¿Cuál es el máximo de elementos que puede tener un código para que sea e-corrector?

¿Cuál es el mínimo de elementos que debe tener un código para que su radio de recubrimiento sea ρ?

Respondemos a esto con el siguiente resultado:

Teorema 154 *(Cotas de Hamming) Sea C un código de longitud n sobre el alfabeto A. Tenemos las siguientes desigualdades:*

1. *Si C es e-corrector, entonces:*

$$|C| \sum_{k=0}^{e} \binom{n}{k} (|A|-1)^k \leq |A|^n .$$

2. *Si ρ_C es el radio de recubrimiento de C, entonces:*

$$|C| \sum_{k=0}^{\rho_C} \binom{n}{k} (|A|-1)^k \geq |A|^n .$$

Demostración. Constatando que se tienen las inclusiones inmediatas

$$\bigcup_{a\in C} B(a,e) \subset A^n \quad \text{y} \quad \bigcup_{a\in C} B(a,\rho_C) = A^n$$

y sabiendo además que la primera es una reunión disjunta y que la segunda no necesariamente lo es, basta aplicar el teorema 147 para establecer al resultado pedido. ■

Este teorema nos brinda cotas para la construcción de códigos en donde exijamos cierta capacidad de corrección y/o cierto radio de recubrimiento.

10.2. Códigos Lineales: Primeros Conceptos

Comenzamos aquí el estudio de códigos en bloque de longitud n, cuyo alfabeto es un cuerpo finito $\mathbb{K}$ de q elementos; el lenguaje o conjunto de palabras es por tanto el espacio vectorial $\mathbb{K}^n$; precisamos que salvo mención contraria, las bases utilizadas serán siempre las **canónicas**.

Como contamos con el 0_K podemos introducir el concepto de peso de un elemento. Sea $a = (a_1, \ldots, a_n)$ un elemento de $\mathbb{K}^n$:

Definición 155 *El **peso de Hamming** de a, denotado $w(a)$, está dado por $w(a) = |\{\, k\,;\ a_k \neq 0\,\}|$. Es claro que w es una función de $\mathbb{K}^n$ en $\mathbb{N}$ y que $w(a) = d(a,0)$.*

Proposición 156 *La función w es par y $w(a-b) = d(a,b)$, $\forall a, b \in \mathbb{K}^n$.*

Demostración. No presenta mayor dificultad. ■

Sabemos que un código es un subconjunto de $\mathbb{K}^n$; sin embargo tomar cualquier subconjunto no tiene mayor interés pues $\mathbb{K}^n$ es un espacio vectorial de dimensión n sobre $\mathbb{K}$, y no sería sensato perder la riqueza algebraica que ello nos brinda. La estructura vectorial de $\mathbb{K}^n$ nos va a permitir crear herramientas útiles y poderosas en cuanto a la construcción de códigos. Por estas razones es conveniente introducir:

Definición 157 *Llamamos codigo lineal de tipo (n,k) todo subespacio vectorial de $\mathbb{K}^n$ de dimensión k.*

Es claro que si C es un código lineal (n,k) entonces $|C| = q^k$. Tenemos:

Proposición 158 *Sea C un código lineal; entonces:*

$$\{d(x,y);\, x,y \in C\} = \{w(x);\, x \in C\}\,.$$

Demostración. Se infiere sin problemas del hecho que $w(x-y) = d(x,y)$ y de que en particular se tiene $w(x) = d(x,0)$. ■

Por tanto, en un código lineal toda "distancia" es un "peso" y todo "peso" es una "distancia". En particular, la distancia mínima δ_C de C corresponde al peso mímimo: $min\,\{w(x);\, x \in C,\, x \neq 0\}$.

Definición 159 *Se llama peso de C, denotado w_C, al peso mínimo.*

Sean $C < \mathbb{K}^n$ un código lineal (n,k) y $\{v_1,\ldots,v_k\}$ una base de C. No olvidemos que cada v_i es una n-upla $(\alpha_{1i},\ldots,\alpha_{ni})$; así mismo recordemos que todo elemento x de C se escribe de manera única como

$$x = \mu_1 v_1 + \ldots + \mu_k v_k = \left(\sum_{i=1}^{k} \mu_i \alpha_{1i},\ \sum_{i=1}^{k} \mu_i \alpha_{2i}, \ldots\ldots, \sum_{i=1}^{k} \mu_i \alpha_{ni} \right).$$

Consideremos G, la matriz $k \times n$ cuyas líneas están respectivamente formadas por las componentes de cada v_i y denotemos por $c_1,\, c_2,\, \ldots,\, c_n$ las respectivas matrices columnas de G.

Ahora bien, si tomamos $\mu = (\mu_1,\ldots,\mu_k) \in \mathbb{K}^k$ como matriz línea y si "$\bullet$" denota el producto escalar, se tiene:

$$\mu G = (\mu_1,\ldots,\mu_k) \begin{pmatrix} \alpha_{11} \ldots \alpha_{n1} \\ \alpha_{12} \ldots \alpha_{n2} \\ \vdots \qquad \vdots \\ \alpha_{1k} \ldots \alpha_{nk} \end{pmatrix} = \left(\ \mu \bullet c_1,\ \mu \bullet c_2, \cdots, \mu \bullet c_n \ \right) = x.$$

Es decir, la aplicación lineal $\mathbb{K}^k \to C$, $\mu \to \mu G$ es un isomorfismo de espacios vectoriales. Todo esto nos lleva a estipular:

Definición 160 *Dado C un código lineal (n,k), se llama matriz generadora de C a toda matriz cuyas lineas constituyen una base de C.*

Comentario 161 *Es claro que una matriz generadora de un código (n,k) es de rango k; también es inmediato que un código admite muchas matrices generadoras. Ahora bien, operando si es necesario con códigos equivalentes,*

podemos siempre suponer que éstas son de la forma $G = (M, A)$ *donde* M *es una matriz invertible de orden* k *y* A *es una matriz* $k \times (n-k)$*; recíprocamente toda matriz de tipo* (M, A) *es generadora de algún código lineal. Por último, con un póco de álgebra lineal, no es difícil establecer que el número de columnas nulas de una matriz generadora es un invariante de estructura del código (hágalo).*

Ejemplo 162 *Sean* $\mathbb{K}$ *un cuerpo de característica* 7, C *un código lineal* $(5, 3)$ *sobre* $\mathbb{K}$ *y* G *una matriz generadora de* C*:*

$$Si\ G = \begin{pmatrix} 1 & 4 & 6 & 2 & 5 \\ 3 & 2 & 1 & 3 & 6 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}\ entonces\ M = \begin{pmatrix} 1 & 4 & 6 \\ 3 & 2 & 1 \\ 4 & 5 & 3 \end{pmatrix}\ y\ A = \begin{pmatrix} 2 & 5 \\ 3 & 6 \\ 2 & 1 \end{pmatrix}.$$

Teorema 163 *Sea* C *un código lineal* (n, k) *cuyas matrices generadoras tienen* r *columnas nulas. Entonces se tiene:*

$$\sum_{x \in C} w(x) = (n-r)(q-1)q^{k-1}.$$

Demostración. Constatemos primero que se tiene:

$$\sum_{x \in K^n} w(x) = n(q-1)q^{n-1} \qquad (*)$$

cuya demostración se deja al lector (esto no requiere de más "estructura" que aquella brindada por las nociones conjuntistas).

La reflexión que sigue nos llevará a establecer $\sum_{x \in C} w(x)$; para esto necesitaremos apoyarnos en la estructura algebraica de C.

Describamos C como un tablero de $q^k \times n$ cuyas lineas están dadas por los vectores del subespacio C. Sea Col una columna no nula de tal lista y tomemos cualquier coordenada no nula de Col (por ejemplo, la primera que encontremos leyendo de arriba a abajo) y llamémosla μ. Sea ahora Lin la linea del tablero que contiene a μ; es claro que podemos utilizar el vector Lin (no nulo) para construir una base de C.

Si es necesario, permutando líneas y/o columnas (operaciones que preservan el peso de las líneas o columnas involucradas) podemos establecer una matriz generadora $G = (M, A)$ de manera que μ sea un coeficiente de M.

Obviamente que a estas alturas podemos no estar trabajando con la lista asociada a C sino que con una asociada a un código equivalente, es decir no sólo isomorfo sino que además con el mismo peso.

El tablero T que se obtiene es del tipo siguiente:

$$\begin{array}{c} \overbrace{\qquad\qquad\qquad}^{k} \overbrace{\qquad\qquad\qquad}^{n-k} \\ k\left\{\begin{array}{cccccccc} \mu_{11} & \mu_{12} & \cdots & \mu_{1k} & \cdots & \cdots & \mu_{1n} \\ \mu_{21} & \mu_{22} & \cdots & \mu_{2k} & \cdots & \cdots & \mu_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mu_{k1} & \mu_{k2} & \cdots & \mu_{kk} & \cdots & \cdots & \mu_{kn} \end{array}\right\} G = (M, A) \\ \left.\begin{array}{cccccc} \mu_{k+11} & \cdots & \mu_{k+1k} & \cdots & \cdots & \mu_{k+1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mu_{q^k1} & \cdots & \mu_{q^kk} & \cdots & \cdots & \mu_{q^kn} \end{array}\right\} \text{Resto del código} \end{array}$$

Como la matriz cuadrada de orden k :

$$M = \begin{pmatrix} \mu_{11} & \mu_{12} & \cdots & \mu_{1k} \\ \mu_{21} & \mu_{22} & \cdots & \mu_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ \mu_{k1} & \mu_{k2} & \cdots & \mu_{kk} \end{pmatrix}$$

es invertible por construcción, si nos restringimos a las k primeras columnas del tablero T lo que obtenemos es un nuevo tablero, en donde los últimos $q^k - k$ vectores son combinación lineal de los k primeros:

$$\begin{array}{c} \overbrace{\qquad\qquad}^{k} \\ k\left\{\begin{array}{cccc} \mu_{11} & \mu_{12} & \cdots & \mu_{1k} \\ \mu_{21} & \mu_{22} & \cdots & \mu_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ \mu_{k1} & \mu_{k2} & \cdots & \mu_{kk} \end{array}\right. \\ q^k - k\left\{\begin{array}{ccc} \mu_{k+11} & \cdots & \mu_{k+1k} \\ \vdots & \vdots & \vdots \\ \mu_{q^k1} & \cdots & \mu_{q^kk} \end{array}\right. \end{array}$$

Dicho de otra manera, tenemos allí la lista de los vectores de K^k.

Por homogeneidad, utilizando $(*)$, se infiere que cada columna de este segundo tablero pesa $(q-1)q^{k-1}$ y por tanto, dadas las condiciones para escoger Col, que toda columna no nula de C pesa lo mismo. Podemos establecer entonces que:

$$w(C) = (n-r)(q-1)q^{k-1}$$

donde r es el número de columnas nulas de cualquier base de C. ■

Por razones de estética y cálculo lo ideal es poder encontrar para un código una matriz generadora $G = (I_k, A)$; en tal caso nos referiremos a una matriz generadora normalizada.

Ahora bien, sabemos que cualquier matriz invertible puede ser transformada en la matriz unidad aplicando operaciones elementales bien conocidas; podemos por tanto aplicar tales operaciones a la matriz G :

$$G = (M, A) \overset{Operaciones.\,Elementales}{\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows} (I_k, A') = G'$$

Si en las operaciones elementales no se realizan permutaciones de columnas, G' continúa siendo una matríz generadora de C. En caso contrario, G' es matriz generadora de un código $C' \cong C$.

Desde el punto de vista de los resultados estructurales, todo lo anterior significa que podemos siempre considerar códigos con matrices generadoras normalizadas. Introduzcamos entonces:

Definición 164 *Un código lineal es sistemático si posee una matriz generadora normalizada.*

Para resumir la discusión preambular a esta definición enunciemos:

Proposición 165 *Se tienen las siguientes propiedades:*

1. *Todo código lineal es equivalente a un código lineal sistemático.*
2. *Un código sistemático posee una sola matriz generadora normalizada.*
3. *Dado un código lineal sistemático C de tipo (n,k) entonces para cada elemento $(\mu_1, \ldots, \mu_k) \in \mathbb{K}^k$ existe una y sólo una palabra de C de la forma $(\mu_1, \ldots, \mu_k, x_{k+1}, \ldots, x_n)$.*

Demostración. Está casi todo dicho. El lector puede formalizar. ■

Como lo precisamos en los preliminares, respecto de las clases de códigos equivalentes basta trabajar con un código por clase, pués los parámetros que se obtienen para uno (dimensión, distancia mínima, radio de recubrimiento, peso mímimo, capacidad de corrección, cotas, etc) se transfieren a todos los de su clase de equivalencia. Veremos ahora nuevas cotas, propias de los códigos lineales, utilizando la distancia mínima δ_C:

Teorema 166 *Sea C un codigo lineal (n, k) sobre $\mathbb{K}$, con $|\mathbb{K}| = q$. Se tiene:*

1. $\delta_C \leq n - k + 1$ *(Cota de Singleton).*
2. $\delta_C \leq \dfrac{n(q-1)q^{k-1}}{q^k - 1}$ *(Cota de Plotkin).*

Demostración. Recordemos que en un código lineal se tiene $\delta_C = w_C$.

La primera afirmación no presenta dificultad teniendo en cuenta que basta demostrarla para un código sistemático: en efecto, es claro que si v es un vector de la base normalizada, entonces $\delta_C = w_C \leq w(v) \leq n - k + 1$.

En cuanto a la segunda afirmación, por el teorema 163 sabemos que se tiene:

$$\sum_{x \in C} w(x) \leq n(q-1)q^{k-1}$$

El resultado demandado se establece teniendo en cuenta que w_C no puede ser mayor al promedio de la suma de los pesos de los $q^k - 1$ vectores no nulos del código C. ■

A partir de ahora trabajaremos, en general, con códigos lineales sistemáticos; veremos que la escritura y los cálculos se facilitan y permiten una mejor visión del proceso. Según el esquema de codificación exhibido al comienzo, la primera etapa (implícita) consiste en asociar a una palabra m una cadena de k símbolos: $m \to (\mu_1, \ldots, \mu_k)$; si bien en definitiva esto es una codificación, ella no es correctora.

Evidentemente que es deseable limitar al máximo la cantidad de símbolos que se van a utilizar y ello depende del número de palabras que tiene el mensaje que se va a trasmitir. Si tal número es N entonces k es el menor entero tal que $N \leq q^k$ donde $q = |\mathbb{K}|$; de esta manera el código en construcción se ajusta a las restricciones sobre distancias, necesarias a la corrección de errores.

La segunda etapa consiste en "insertar" la palabra m en una palabra codificada. Si utilizamos una matriz generadora normalizada se obtiene:

$$(\mu_1, \ldots, \mu_k) \to (\mu_1, \ldots, \mu_k)(I_k, A) = (\mu_1, \ldots, \mu_k, x_{k+1}, \ldots, x_n).$$

Aquí ya estamos en un código corrector de errores.

Las primeras k componentes son los símbolos de información; las $n - k$ siguientes son los símbolos de control (también se les llama símbolos de redundancia).

10.3. Matriz de Control, Descodificación

El ejemplo que sigue introduce bien el sentido de esta sección:

Ejemplo 167 *Consideremos la palabra $a = a_1a_2a_3a_4$ que codificamos en la palabra de largo 7 de la siguiente manera: $c = a_1a_2a_3a_4c_1c_2c_3$. Tomemos una matriz H de 3×7 y de rango 3; por ejemplo:*

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \text{ donde el cuerpo tiene característica 2.}$$

Consideremos ahora la ecuación matricial: $H \cdot {}^tc = 0$ (donde ${}^tc$ es la transpuesta de la línea c); obtenemos el siguiente sistema:

$$\begin{array}{lll} a_1 + a_2 + a_4 + c_1 + c_2 + c_3 = 0 & & c_1 = a_2 + a_3 + a_4 \\ a_1 + a_3 + c_2 + c_3 = 0 & \text{de donde:} & c_2 = a_1 + a_3 + a_4 \\ a_2 + a_3 + c_1 + c_3 = 0 & & c_3 = a_4 \end{array}$$

Es decir, podemos determinar los símbolos de control a partir de los símbolos de información que conforman la palabra original.

Si $S_H : \mathbb{K}^7 \to \mathbb{K}^3$ es la aplicación lineal asociada a la matriz H, los elementos del código C estarán dados por los $x \in \mathbb{K}^7$ tales que $S_H(x) = 0$, es decir $C = ker(S_H)$.

Formalicemos por tanto la idea expresada en el ejemplo recien expuesto:

Como un código lineal C es un subespacio vectorial, podemos asociarle su ortogonal $C^\perp$, es decir: $\{\, x \in \mathbb{K}^n;\ x \bullet a = 0, \text{ para todo } a \in C \,\}$.

También se dice que $C^\perp$ es el código dual de C.

Si C es de tipo (n, k) entonces $C^\perp$ será de tipo $(n, n-k)$. Si H es una matriz generadora del código $C^\perp$ es claro que para todo $a \in C$ se tiene $H \cdot {}^t a = 0$; más aún, si $b \in \mathbb{K}^n$ verifica $H \cdot {}^t b = 0$ entonces $b \in C$ ya que se tiene $(C^\perp)^\perp = C$.

Todo lo anterior nos permite introducir el siguiente concepto:

Definición 168 *Llamamos matriz de control de un código lineal C a toda matriz generadora del código $C^\perp$.*

Obviamente que las matrices de control del código dual $C^\perp$ son las matrices generadoras de C.

Nota 169 *Si G una matriz generadora del código C no presenta dificultad establecer que:*

1. *Si H es una matriz de control de C, entonces $G \cdot {}^t H = 0$.*
2. *Si H es una matriz de rango máximo tal que $G \cdot {}^t H = 0$, entonces es una matriz de control de C.*

El resultado que sigue nos permite construir con poca dificultad una matriz de control:

Proposición 170 *Sea C un código lineal sistemático de matriz generadora $G = (I_k, A)$. Entonces $H = (-{}^t A, I_{n-k})$ es una matriz de control de C.*

Demostración. Esquemáticamente, hay que verificar que se tiene:

$$\begin{array}{c|c} G & {}^t H \\ \hline \begin{array}{|c|c|}\hline I_k & A \\ \hline \end{array} & \begin{array}{|c|}\hline -A \\ \hline I_{n-k} \\ \hline \end{array} \end{array} = O_{k\times(n-k)}.$$

La escritura formal (por lo demás inmediata) queda como ejercicio. ■

Nota 171 *Sea C un código lineal y consideremos el mensaje $a = (a_1, \ldots, a_k)$ que codificamos en $c = (a_1, \ldots, a_k, b_{k+1}, \ldots, b_n) \in C$. Si $H = (-{}^tA, I_{n-k})$ es una matriz de control de C y denotamos por L_i las lineas de ${}^tA$, como $H \cdot {}^tc = 0$ se infiere que: $(b_{k+i}) = L_i \cdot {}^ta$, $1 \leq i \leq k$.*

Recordamos que los b_{k+i} se llaman símbolos de control. Operar con una matriz de control normalizada nos permite facilmente determinar los símbolos de control utilizados para codificar una palabra en función de los símbolos de la palabra misma.

Por último hacemos ver que $({}^tA, -I_{n-k})$ es también una matriz de control del código lineal C.

Ejemplo 172 *Consideremos la matriz normalizada G con coeficientes en $\mathbb{Z}_{11}$:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 2 & -3 \\ 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 1 & -4 & 5 \end{pmatrix}; \quad \textit{entonces} \quad M = \begin{pmatrix} 2 & -3 \\ 1 & -1 \\ -4 & 5 \end{pmatrix}.$$

Luego se obtiene: $H = \begin{pmatrix} -2 & -1 & 4 & 1 & 0 \\ 3 & 1 & -5 & 0 & 1 \end{pmatrix}$.

Se sugiere, por lo demás, comprobar que $G \cdot {}^tH = 0$.

Supongamos ahora que codificamos la palabra $(1, 2, 3)$; tendríamos pues que $c = (1, 2, 3, x, y) \in C$.

Haciendo nulo el producto $H \cdot {}^tc$ se obtiene:

$$0 = \begin{pmatrix} -2 & -1 & 4 & 1 & 0 \\ 3 & 1 & -5 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ x \\ y \end{pmatrix} = \begin{pmatrix} 8 + x \\ -10 + y \end{pmatrix}.$$

Luego $x = 3$ e $y = 10$; es decir, $c = (1, 2, 3, 3, 10)$.

Proposición 173 *Sean C un código lineal con una matriz de control H y r un entero no nulo. Entonces existe un elemento $x \in C$ de peso r si y solamente si existen r columnas de H linealmente dependientes. Es claro que el peso mínimo w_C está dado por el menor de esos enteros r.*

Demostración. Denotemos por $c_1, c_2, \ldots, c_n$ las columnas de H y sea $x = (x_1, x_2, \ldots, x_n) \neq (0, 0, \ldots, 0)$. Se tiene entonces:

$$H \cdot {}^t x = H \cdot {}^t(x_1, x_2, \ldots, x_n) = x_1 c_1 + x_2 c_2 + \ldots + x_n c_n.$$

Ahora bien, el peso de x está dado por el número de x_i no nulos. Por otro lado sabemos que $x \in C$ si y sólo si $H \cdot {}^t x = 0$, es decir:

$$H \cdot {}^t x = x_1 c_1 + x_2 c_2 + \ldots + x_n c_n = 0.$$

Obtenemos por tanto una combinación nula no trivial de las columnas de H.

Recíprocamente, si se tiene $x_{i_1} c_{i_1} + x_{i_2} c_{i_2} + \ldots + x_{i_r} c_{i_r} = 0$, donde todos los x_{i_j} son diferentes de cero, entonces el elemento x con componentes x_{i_j} en los lugares i_j y todas las otras componentes nulas, es un elemento de C de peso r. ■

Ahora vamos a introducir ciertas nociones de descodificación para los códigos lineales.

Si escogemos bases para los espacios vectoriales $\mathbb{K}^n$ y $\mathbb{K}^{n-k}$ (en principio serán las bases canónicas) entonces a cada aplicación lineal $\mathbb{K}^n \to \mathbb{K}^{n-k}$ le corresponde una y sólo una matriz de $\mathbb{K}_{n\times(n-k)}$ y recíprocamente a cada matriz de $\mathbb{K}_{n\times(n-k)}$ le corresponde una y sólo una aplicación $\mathbb{K}^n \to \mathbb{K}^{n-k}$.

Teniendo esto claro, sea C un código lineal sistemático de tipo (n, k). Si H es la matriz de control de C, sea $S_H : \mathbb{K}^n \to \mathbb{K}^{n-k}$ su aplicación lineal asociada.

Definición 174 *Llamamos síndrome de $x \in \mathbb{K}^n$ el elemento $S_H(x)$ de $\mathbb{K}^{n-k}$.*

Por las propiedades de H sabemos que $S_H(x) = 0$ si y solamente si $x \in C$; dicho de otra manera, $C = ker(S_H)$, o si se quiere, los elementos de C son aquellos de síndrome nulo.

Supongamos ahora que queremos enviar la palabra $a = (a_1, \ldots, a_k)$ codificada en $c \in C$ (donde $c_i = a_i$ para $1 \leq i \leq k$) y que la palabra recibida, a través de un canal de trasmisión con ruido, sea $b \in \mathbb{K}^n$. La diferencia $\epsilon = b - c$ se llama error (o palabra error) y $r = w(\epsilon)$ evidentemente indica el número de errores cometidos en la trasmisión. Tenemos entonces $b = c + \epsilon$; como $c \in C = ker(S_H)$ se infiere entonces que $S_H(\epsilon) = S_H(b)$, es decir que b (la palabra recibida) y ϵ (el error) tienen el mismo síndrome; es claro que esto es equivalente a tener $\epsilon \equiv b \, mod(C)$.

Ahora bien, dadas las dimensiones de los espacios en juego, se tiene que $dim(\mathbb{K}^n/C) = n - k$ y por tanto la aplicación lineal $\overline{S_H} : \mathbb{K}^n/C \to \mathbb{K}^{n-k}$, $\overline{S_H}(x + C) = S_H(x)$, es un isomorfismo. Todo esto nos dice que para conocer el conjunto de posibilidades de recepción de palabras trasmitidas es suficiente (y necesario) trabajar a nivel de las clases de equivalencia $x + C$, $x \in \mathbb{K}^n$.

Sabemos que cualquier elemento de una clase puede ser escogido como un representante de ésta. Sin embargo, en nuestro caso tenemos una buena manera de discriminar: el peso de los elementos. Por tanto tomaremos como representante de una clase a un elemento que tenga el menor peso, el que llamaremos un líder de la clase. Es claro que si una palabra se ha trasmitido con el mínimo de errores posibles, el error ϵ es un líder de su clase.

Habiendo establecido todo lo anterior, introducimos el siguiente método elemental de descodificación:

Algoritmo 175 *Suponiendo que en la trasmisión $c \to b$ hubo r errores:*

1. *Cálcular el síndrome de la palabra recibida b.*
2. *Determinar la clase de equivalencia asociada.*
3. *Buscar, en tal clase, el error ϵ, es decir las palabras de peso r.*
4. *Cálcular $c = b - \epsilon$ según los posibles ϵ encontrados*
5. *Encontrar los posibles mensajes originales a.*

Así, por ejemplo, sea $C < \mathbb{Z}_2^4$ un código de tipo $(4, 2)$ determinado por

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \text{ y } H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Tenemos el siguiente cuadro de descodificación:

Palabras a codificar	00	10	01	11	Síndrome
Palabras codificadas : C	0000	1010	0111	1101	00
	0001	1011	0110	1100	01
Palabras con error : $x + C$	1000	0010	1111	0101	10
	0100	1110	0011	1001	11
	líder				

Nos proponemos hacer la descodificación de ciertos casos, para $r = 3$.

Si la palabra recibida es $b = 0111$, su síndrome es $S_H(b) = 00$, la clase asociada es C y por tanto no sabemos si hubo errores. Si suponemos que los hubo, necesariamente $r = 2, 3$. Si suponemos que hubo dos errores, entonces $\epsilon = 1010$; luego $c = 1101$ y el mensaje original es 11; por último, en caso de tener tres errores, entonces $\epsilon = 1101$, $a = 1010$ y el mensaje original es 10.

Si $b = 1110$, entonces $S_H(b) = 11$ y la clase asociada es la del líder 0100, por lo que en la trasmisión hubo errores. Si hubo un error concluimos que $\epsilon = 0100$, $c = 1010$ y el mensaje original es 10; si asumimos que hubo dos errores, entonces $\epsilon = 0011$ o 1001, $c = 0111$ o 1101 y el mensaje original es 01 o 11; para terminar, con tres errores se tiene $\epsilon = 1110$, $c = 0000$ y el mensaje original es 00

Se deja al lector estudiar la descodificación cuando $b = 0011$.

Finalmente, dejamos como pregunta: ¿cuál es la capacidad de corrección de este código?

Nota 176 *Para los que todavía tengan algunas lagunas en álgebra lineal, considerando b como matriz linea su síndrome está dado por:*

$$b \cdot {}^tH, \quad o, \text{ lo que es igual, } \ {}^t(H \cdot {}^tb).$$

Se sugiere dar una demostración formal a esta afirmación.

Definición 177 *Sea $C < \mathbb{K}^n$. Se dice que C es un código de repetición si es de tipo $(n, 1)$ y si sus elementos son de la forma $c = (c_1, \ldots, c_n)$ donde se tiene $c_j = c_1$ para todo $1 \leq j \leq n$.*

En algunos ejemplos así como varios ejercicios hemos trabajado sobre códigos en donde el cuerpo de base es $\mathbb{Z}_2$. Ahora bien, cualquier código en donde el alfabeto contenga dos símbolos se denomina binario; los casos a los que nos estamos refiriendo se llaman códigos lineales binarios; entre los códigos de esa familia tenemos:

Definición 178 *Sea $C < \mathbb{Z}_2^n$ un código lineal. Se dice que C es un código de chequeo de paridad si C es de tipo $(n, n-1)$ y si sus elementos son de la forma $c = (c_1, \ldots, c_n)$ donde se tiene $c_n = c_1 + \ldots + c_{n-1}$.*

Para esta clase de códigos la palabra recibida $b \in C$ tiene un número de errores par si $b_n = 0$ e impar si $b_n = 1$.

Introduzcamos la próxima definición con lo siguiente:

Sean $k \geq 2$ y $n = 2^k - 1$; consideremos la matriz $D_k \in M_{\mathbb{Z}_2}(\ k \times n)$ cuyas columnas están formadas por los coeficientes de la representación en base 2 de los enteros $1,\ 2, \cdots,\ 2^k - 1$.

Vamos a convenir que la i-ésima línea corresponde a los coeficientes de 2^{i-1}; así por ejemplo, si $k = 3$ tenemos:

$$D_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Definición 179 *Sea $C < \mathbb{Z}_2^n$ un código lineal donde $n = 2^k - 1$. Si la matriz de control H es igual o equivalente (permutaciones de líneas y/o columnas) a D_k se dice que C es un código de Hamming.*

Si en cambio D_k es igual o equivalente a la matriz generadora G, entonces se dice que C es un código lineal simpléctico.

En cuanto a las propiedades de estos códigos, tenemos:

Proposición 180 *Un codigo de Hamming C de longitud $n = 2^k - 1$ es de dimensión $2^k - k - 1$ y tiene una capacidad de corrección $e_C = 1$.*

Un código simpléctico C de longitud $n = 2^k - 1$ es de dimensión k y tiene una capacidad de corrección $e_C = 2^{k-2} - 1$.

Demostración. Demostremos lo que respecta a un código de Hamming.

Como lo de la dimensión es inmediato, analicemos su capacidad de corrección: veamos primero que tal código no puede tener un elemento de peso 1 pues por la proposición 173 se deduce que H tendría una columna nula, lo que es imposible ; por la misma proposición el código no puede tener un elemento de peso 2, pues en tal caso H tendría dos columnas iguales. Ahora bien, es claro que la suma de dos columnas de H es también una columna de H. Se infiere entonces, utilizando una vez más la proposición 173, que el peso mínimo de C es $w_C = 3$ y por tanto $e_C = 1$ (teorema 152).

La demostración afirmación que concierne los códigos simplécticos queda como ejercicio. ■

10.4. Introducción a los Códigos Cíclicos

En esta sección, estudiaremos algunos aspectos de una clase importante de códigos lineales.

En lo que viene, por razones de comodidad de la lectura (y por tanto, de la escritura), un elemento $\alpha \in \mathbb{K}^n$ lo denotaremos por $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$. Igualmente, como vamos a trabajar con polinomios, por estética coherente de escritura que ya veremos, tanto la indeterminada X como los polinomios $P(X)$ los denotaremos con minúsculas.

Sean $\psi : \mathbb{K}^n \to \mathbb{K}[x]$, definida por $(\alpha_0, \ldots, \alpha_{n-1}) \longmapsto \alpha_0 + \ldots + \alpha_{n-1}x^{n-1}$ y $\mathbb{K}_n[x] = \{p(x) \in \mathbb{K}[x]\,;\, gr(p) < n\}$.

Es inmediato que ψ es una aplicación lineal inyectiva y por tanto se tiene el isomorfismo de espacios vectoriales $\mathbb{K}^n \simeq \mathbb{K}_n[x]$.

Esto quiere decir que todo código lineal puede ser concebido como un subespacio de $\mathbb{K}_n[x]$. Evidentemente esta representación polinomial no tiene sentido en la medida que tratemos tales códigos sin otras exigencias estructurales.

Definición 181 *Se llama código cíclico a todo código lineal $C < \mathbb{K}^n$ que verifique la propiedad: si $(c_0, \ldots, c_{n-1}) \in C$ entonces $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.*

Dependiendo de la literatura, se dice que la palabra $(c_{n-1}, c_0, \ldots, c_{n-2})$ es el "shift" de $(c_0, \ldots, c_{n-1})$.

Un ejemplo de código cíclico está dado por $C < \mathbb{K}^9$ de matriz generadora:

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

Si denotamos por u, v y w los vectores línea de G (tales vectores conforman una base de C) y si $c = \alpha u + \beta v + \gamma w$ con α, β, $\gamma \in \mathbb{K}$, entonces el shift de c es $\gamma u + \alpha v + \beta w$, que evidentemente es una palabra de C.

Para representar C polinomialmente, asociamos a u, v y w los polinomios:

$$p_u = 1 + x^3 + x^6,\ p_v = x + x^4 + x^7,\ p_w = x^2 + x^5 + x^8.$$

El código C estaría representado por el subespacio vectorial de $\mathbb{K}[x]$ engendrado por los polinomios p_u, p_v, y p_w.

Sin embargo, no reflejamos en tal representación la riqueza estructural de la circularidad que entrega el shift. Ahora bien, si $C < \mathbb{K}^n$ es un código cíclico y $c = (c_0, \ldots, c_{n-1})$ un elemento de C, considerando su polinomio asociado $c_0 + c_1x +, \ldots + c_{n-1}x^{n-1}$ podemos observar que:

$$x(c_0 + c_1x +, \ldots + c_{n-1}x^{n-1}) = c_{n-1}x^n + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1}.$$

Vemos que la multiplicación por x tiene un efecto cuasi-shift; el problema lo da el término $c_{n-1}x^n$. Nos interesa, por tanto, convertir x^n en 1; es decir debemos operar en el anillo cociente $\mathbb{K}[x] / \langle x^n - 1 \rangle$.

Recordemos que los elementos de este anillo cociente $\mathbb{K}[x] / \langle x^n - 1 \rangle$ son de la forma $\alpha_0 + \alpha_1\overline{x} +, \ldots + \alpha_{n-1}\overline{x}^{n-1}$ y los cálculos se realizan teniendo en cuenta que $\overline{x}^n = 1$.

La escritura $\alpha_0 + \alpha_1\overline{x} +, \ldots + \alpha_{n-1}\overline{x}^{n-1} \in \mathbb{K}[x] / \langle x^n - 1 \rangle$ es única ya que si se tiene $\alpha_0 + \alpha_1\overline{x} +, \ldots + \alpha_{n-1}\overline{x}^{n-1} = 0$, ello significa que en el anillo $\mathbb{K}[x]$ el polinomio $\alpha_0 + \alpha_1x + \ldots + \alpha_{n-1}x^{n-1}$ es múltiplo de $x^n - 1$; ello es posible si y solamente si $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 0$.

Todo esto nos permite inferir que si $\pi : \mathbb{K}[x] \to \mathbb{K}[x] / \langle x^n - 1 \rangle$ es la proyección canónica, la aplicación $\pi \circ \psi : \mathbb{K}^n \to \mathbb{K}[x] / \langle x^n - 1 \rangle$ es un isomorfismo de espacios vectoriales.

De aquí para adelante indistintivamente hablaremos de códigos lineales como subespacios de $\mathbb{K}^n$ o de $\mathbb{K}[x] / \langle x^n - 1 \rangle$ y si $c \in C$ tendremos en mente que $c = (c_0, \ldots, c_{n-1})$ o que $c = c_0 + c_1\overline{x} + \ldots + c_{n-1}\overline{x}^{n-1}$ dependiendo del contexto en que se trabaja.

Estamos ciertos de que la convenciones de escritura que acabamos de imponer no se prestarán a confusión alguna. Tenemos:

Teorema 182 *Un código lineal C es cíclico si y solamente si es un ideal de $\mathbb{K}[x] / \langle x^n - 1 \rangle$.*

Demostración. Como C es lineal, es claro que $(C, +)$ es un subgrupo del anillo cociente; como además C es cíclico entonces para todo $c \in C$ se tiene $\overline{x}c \in C$ (propiedad del shift) y por tanto $\overline{x}^i c \in C$ para todo entero i. Por último, como los elementos $\overline{x}^i$, con $0 \leq i \leq n-1$, engendran $\mathbb{K}[x] / \langle x^n - 1 \rangle$, entonces para todo $p(\overline{x}) \in \mathbb{K}[x] / \langle x^n - 1 \rangle$ se tiene $p(\overline{x})C \subset C$; esto demuestra que C es un ideal. El recíproco es inmediato (ejercicio). ■

En definitiva, este teorema nos dice que conocer los códigos cíclicos de longitud n es equivalente a conocer los ideales no triviales del anillo cociente $\mathbb{K}[x]/\langle x^n-1\rangle$. Al respecto, recordamos un resultado ya conocido:

Proposición 183 *Todo ideal J no trivial de $\mathbb{K}[x]/\langle x^n-1\rangle$ es principal. Más precisamente J es el engendrado por la clase de un polinomio $g(x)$, divisor de x^n-1.*

Demostración. En efecto, si J es un ideal no trivial de $\mathbb{K}[x]/\langle x^n-1\rangle$ entonces $I=\pi^{-1}(J)$ es un ideal no trivial de $\mathbb{K}[x]$ que contiene x^n-1. Como $\mathbb{K}[x]$ es un anillo principal, existe $g(x)\in\mathbb{K}[x]$ de grado mínimo tal que $I=\langle g(x)\rangle$; como $x^n-1\in\langle g(x)\rangle$ existe $h(x)\in\mathbb{K}[x]$ tal que $g(x)h(x)=x^n-1$. Se infiere que $gr(g(x))<n$ y es claro que $J=\langle g(\overline{x})\rangle$. ■

Definición 184 *Decimos que el polinomio $g(x)$ es un generador de C. Si tal polinomio es mónico, entonces $g(x)$ se llama el generador de C.*

La clasificación de los códigos cíclicos de longitud n está dada por sus generadores, es decir, por las clases de los por los divisores de x^n-1. Como nos manejamos con polinomios de grados menores a n, sin provocar confusión podemos escribir x en vez de $\overline{x}$; sin embargo, cuando sea necesario señalaremos por $\overline{g}(x)$ la clase de $g(x)$ en el anillo cociente.

Ejemplo 185 *La descomposición de x^7-1 sobre el cuerpo $\mathbb{Z}_2$ es:*

$$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1).$$

Los códigos cíclicos no triviales de largo 7, según sus generadores, son :

1. $x-1$.
2. x^3+x+1.
3. x^3+x^2+1
4. $(x-1)(x^3+x+1)=x^4+x^2+x^3+1$.
5. $(x-1)(x^3+x^2+1)=x^4+x^2+x+1$.
6. $(x^3+x+1)(x^3+x^2+1)=x^6+x^5+x^4+x^3+x^2+x+1$.

Sean ahora $g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{n-k}$ y $h(x) = h_0 + h_1 x + \ldots + h_k x^k$, donde $0 < k < n$, polinomios que verifican $g(x)h(x) = x^n - 1$ (como los que aparecen en la demostración de la proposición 183).

Como $gr(g(x)) < n$, $\overline{g}(x)$ tiene la misma escritura que $g(x)$; lo mismo se aplica a $h(x)$. Obviamente que en $\mathbb{K}[x] / \langle x^n - 1 \rangle$ se tiene $\overline{g}(x)\overline{h}(x) = 0$

Ahora bien, los elementos de $C = \langle \overline{g}(x) \rangle$ son de la forma $\overline{a}(x)\overline{g}(x)$ donde $a(x) = a_0 + \ldots + a_t x^t$ con $t < n$, no olvidando la regla de cálculo $x^n = 1$.

De la igualdad $\overline{a}(x)\overline{g}(x) = a_0\overline{g}(x) + \ldots + a_t x^t \overline{g}(x)$ se infiere que el conjunto $\{ x^j \overline{g}(x);\ 0 \leq j < n \}$ genera, en tanto subespacio vectorial, al código $\langle \overline{g}(x) \rangle$.

Para extraer una base de este conjunto veamos lo siguiente: en $\mathbb{K}[x]$, si efectuamos la división euclidiana $a(x) = q(x)h(x) + r(x)$ donde $gr(r(x)) < k$, hacemos aparecer $h(x)$ en el producto $a(x)g(x)$ y podemos utilizar el fuerte dato entregado por: $g(x)h(x) = x^n - 1$.

De esta manera, se tiene:

$$a(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)\left(x^n - 1\right) + r(x)g(x)$$

Se establece así que en el cociente, $\overline{a}(x)\overline{g}(x) = \overline{r}(x)\overline{g}(x)$ por lo que el conjunto $\{ x^j \overline{g}(x);\ 0 \leq j < k \}$ también es un sistema vectorial generador de $\langle \overline{g}(x) \rangle$ en $\mathbb{K}[x] / \langle x^n - 1 \rangle$.

Que además es un sistema libre queda de ejercicio.

Con todo lo anterior hemos establecido el importante resultado:

Teorema 186 *Un código cíclico C de longitud n y de polinomio generador de grado $n-k$ es de dimensión k. Mas aún, si $g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{n-k}$ es el generador del ideal C, una matriz generadora asociada es:*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & \cdots & \cdots & g_{n-k} & 0 & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & \cdots & g_{n-k} & 0 & 0 & \cdots & \vdots \\ \vdots & 0 & \ddots & \ddots & \cdots & \cdots & \cdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \cdots & \cdots & \ddots & \ddots & 0 \\ 0 & \vdots & \vdots & 0 & g_0 & g_1 & \cdots & \cdots & \cdots & g_{n-k} & 0 \\ 0 & 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & \cdots & g_{n-k} \end{pmatrix}.$$

Comentario 187 *Es claro que la matriz G es de rango k; basta considerar la matriz cuadrada formada por las últimas k columnas: su determinante es $g_{n-k}^k \neq 0$.*

Por otro lado, como $g(x)h(x) = x^n - 1$ y 0 no es raíz de $x^n - 1$ deducimos que $g_0\, h_0 = -1$. Esto significa que la matriz cuadrada formada por las k primeras columnas tambien es invertible.

Ahora bien, el polinomio $m(x) = g_0^{-1} g(x)$ es también un generador de C, por lo que la matriz $M = g_0^{-1} G$ es otra matriz generadora de C y su primera diagonal está compuesta de 1s.

Por último, sabemos que fabricar las palabras de C es obtener todos los elementos aG donde $a = (a_0, \ldots, a_{k-1})$, o (en el lenguaje de teoría de anillos), es obtener todos los elementos $a(x)g(x)$ donde $a(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}$.

Vemos que en definitiva, la codificación "cíclica" de tipo (n, k) consiste en multiplicar divisores de $x^n - 1$ por polinomios de grado inferior a k.

Si $a(x)g(x)$ es la palabra enviada y $b(x)$ es la palabra recibida, como se tiene $b(x) = g(x)q(x) + r(x)$ (división euclidiana), el error está dado por el resto. Si $r(x) \neq 0$, sabremos que han ocurrido errores en la trasmisión.

10.5. Polinomio y Matriz de Control

Sean $C < \mathbb{K}[x] / \langle x^n - 1 \rangle$ un código cíclico de tipo (n, k) y $g(x)$ un polinomio generador de C. Sabemos que $g(x)$ es un polinomio de grado $n - k$ y que en $\mathbb{K}[x]$ divide a $x^n - 1$.

Definición 188 *Llamamos polinomio de control de C al todo polinomio $h(x)$ tal que $g(x)h(x) = x^n - 1$. Si $g(x)$ es mónico, entonces $h(x)$también lo es y entonces se llama el polinomio de control de C.*

Escribamos $h(x) = h_0 + h_1 x + \ldots + h_k x^k$, donde $0 < k < n$.

Si $c \in C$ y $c(x)$ es su polinomio asociado (de grado menor que n) entonces existe $a(x)$ de grado inferior a k tal que $c(x) = a(x)g(x)$ (ver última parte del comentario 187); en $\mathbb{K}[x] / \langle x^n - 1 \rangle$ se tiene $c(x)h(x) = 0$.

Ahora bien, es claro que $\langle h(x) \rangle$ es un código cíclico de tipo $(n, n-k)$. Sin embargo, no es difícil constatar que su matriz generadora no es una matriz de control del código $C = \langle g(x) \rangle$.

Basados en todo lo anterior, tenemos:

Lema 189 *La matriz* $(n-k)\times n$:

$$H=\begin{pmatrix} h_k & h_{k-1} & \cdots & \cdots & h_1 & h_0 & 0 & 0 & \cdots & \cdots \\ 0 & h_k & h_{k-1} & \cdots & \cdots & h_1 & h_0 & 0 & 0 & \cdots \\ \vdots & 0 & \ddots & \ddots & \cdots & \cdots & \ddots & \ddots & \ddots & \ddots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \cdots & \ddots & \ddots & \ddots \\ 0 & \vdots & \vdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_1 & h_0 \end{pmatrix}$$

es un matriz de control del código C.

Demostración. Como el determinante de la matriz formada por las primeras k columnas es $h_k^{n-k}\neq 0$ la matriz H es de rango $n-k$.

Sea G_i la i-ésima línea de la matriz G (ver teorema 186); es claro que i representa el número de ceros comenzantes de la línea $G_i=(\overbrace{0\ \ldots\ 0}^{i}\, g_0\, g_1\ \ldots)$.

Asimismo, sea $H_j=(\overbrace{0\ \ldots 0}^{j}\, h_k\, h_{k-1}\, k_{k-2}\ \ldots)$ la j-ésima línea de H.

Sin pérdida de generalidad, supongamos que $j\leq i$ y que la posición $i+1$ de H_j lo ocupe h_r.

Ahora bien, en el producto $G\cdot {}^tH$ el coeficiente (i,j) está dado por el producto escalar $G_i\bullet H_j$. Así, tenemos:

$$(0\ \ldots\ 0\, g_0\, g_1\ \ldots)\bullet(0\ \ldots 0\, h_k\, h_{k-1}\ \ldots h_r\ \ldots)=g_0h_r+g_1h_{r-1}+g_2h_{r-2}+\cdots$$

Lo obtenido no es otra cosa que el coeficiente de x^r en el producto $g(x)h(x)$; como r fluctúa entre 0 y k, tal coeficiente es nulo. ■

Sabemos que H no es la matriz generadora de $\langle h(x)\rangle$; ella es la generadora de un código equivalente (basta observar la permutación de columnas).

Más precisamente, H es la matriz generadora del código cíclico $\langle \underline{h}(x)\rangle$ donde $\underline{h}(x)$ es el polinomio recíproco de $h(x)$ y cuyos coeficientes están dados por : $\underline{h}_i=h_{k-i}$, $0\leq i\leq k$. Como $h_0\neq 0$, el polinomio $\underline{h}(x)$ también es de grado k.

Corolario 190 *El código ortogonal al código cíclico* C *es* $C^{\perp}=\langle \underline{h}(x)\rangle$.

Obviamente que $C^{\perp}$ es un código cíclico de tipo $(n,n-k)$.

Es claro que si $g(x)h(x) = x^n - 1$ podemos tomar a ambos polinomios como mónicos. En tal caso diremos que g es el polinomio generador de C y que $h(x)$ es el polinomio de control de C.

Hacemos notar que con esta convención, el generador de $C^\perp$ es el polinomio $h_0^{-1}\underline{h}(x)$.

Ejercicios

1. Analice si los siguientes códigos sobre A son e-correctores:

   a) Sean $A = \{\lambda, \theta\}$, $n = 3$, $e = 1$ y los códigos:

   $C = \{(\lambda, \lambda, \lambda),\ (\theta, \lambda, \theta)\}$ y $C' = \{(\lambda, \theta, \lambda), (\lambda, \lambda, \theta), (\theta, \theta, \theta)\}$.

   b) Sean $A = \{\lambda, \theta, \mu\}$, $n = 5$, $e = 2$ y el código:

   $$C = \{(\lambda, \theta, \mu, \theta, \lambda),\ (\mu, \lambda, \theta, \lambda, \theta),\ (\theta, \theta, \lambda, \theta, \mu)\}.$$

   c) Sean $A = \{\lambda, \theta, \mu, \nu\}$, $n = 6$, $e = 3$ y los códigos :

   $C = \{(\lambda, \theta, \theta, \nu, \lambda, \mu),\ (\nu, \theta, \lambda, \mu, \lambda, \theta),\ (\mu, \theta, \lambda, \nu, \theta, \lambda),\ (\theta, \theta, \lambda, \nu, \lambda, \mu)\}$,

   $C' = \{(\lambda, \theta, \theta, \mu, \mu, \nu),\ (\theta, \lambda, \nu, \theta, \lambda, \mu),\ (\mu, \theta, \lambda, \theta, \lambda, \nu),\ (\nu, \lambda, \theta, \theta, \mu, \theta)\}$.

2. Analice si existen códigos e-correctores cuando:
   (a) $|A| = 2$, $n = 5$ y $e = 1$. (b) $|A| = 4$, $n = 4$ y $e = 2$.
   (c) $|A| = 5$, $n = 4$ y $e = 3$. (d) $|A| = 7$, $n = 3$ y $e = 4$.

3. Estudie si existen códigos de radio ρ_C cuando:
   (a) $|A| = 2$, $n = 5$ y $\rho_C = 1$. (b) $|A| = 5$, $n = 4$ y $\rho_C = 2$.
   (c) $|A| = 6$, $n = 4$ y $\rho_C = 3$. (d) $|A| = 7$, $n = 3$ y $\rho_C = 4$.

4. Construya un código perfecto. Estudie si en los ejemplos tratados en los ejercicios hay códigos perfectos.

5. Sobre la función peso, si $x, y \in \mathbb{K}^n$ demuestre las propiedades siguientes:
   (a) $w(x) = d(x + y, y)$. (b) $w(x) = 0$ si y solamente si $x = 0_{\mathbb{K}^n}$. (c) $w(\lambda x) = w(x)$ para todo $\lambda \in \mathbb{K}^*$. (d) $w(x + y) \leq w(x) + w(y)$.

6. Sea $\mathbb{K}$ un cuerpo de q elementos y $n \in \mathbb{N}^*$. Calcule $\sum_{x \in \mathbb{K}^n} w(x)$.

7. Sean $u = (u_1, \ldots, u_n)$ y $v = (v_1, \ldots, v_n)$ elementos de $\mathbb{Z}_2^n$.

   a) Demuestre que $w(u + v) = w(u) + w(v) - 2w(u * v)$, donde la operación denotada " $*$ " se define por: $u * v = (u_1 v_1, \ldots, u_n v_n)$.

   b) Deduzca la paridad de $w(u + v)$ en función de las paridades de $w(u)$ y $w(v)$.

8. Sea C un código lineal sobre $\mathbb{Z}_2$. Demuestre que todas o la mitad de las palabras de C son de peso par.

9. Demuestre que un codigo lineal C tiene capacidad de corrección e_C si su peso w_C es igual a $2e_C + 1$ o a $2e_C + 2$.

10. Si todos los $x \in C^*$ tienen el mismo peso w, entonces existe un entero positivo m tal que se tiene:

$$w = mq^{k-1} \quad \text{y} \quad n - r = m\frac{q^k - 1}{q - 1}.$$

11. Considere un código lineal de tipo $(8, 5)$ sobre $\mathbb{Z}_{11}$, de matriz generadora:

$$G = \begin{pmatrix} 3 & 5 & 1 & 0 & 2 & 0 & 3 & 0 \\ 4 & 8 & 4 & 1 & 4 & 3 & 0 & 4 \\ 2 & 5 & 0 & 2 & 3 & 1 & 1 & 3 \\ 1 & 1 & 3 & 7 & 0 & 2 & 4 & 9 \\ 2 & 9 & 8 & 3 & 7 & 2 & 6 & 5 \end{pmatrix}.$$

   a) Normalice G (puede que obtenga un código sistemático equivalente) y entonces construya H, la matriz de control asociada al código resultante.

   b) Codifique en el código lineal sistemático las palabras:

   $(1, 2, 3, 2, 1), (4, 7, 3, 0, 5), (6, 4, 6, 2, 8), (9, 1, 8, 2, 7)$ y (5,5, 0, 7, 7).

12. Sea C un código lineal con una matriz de control H y $s \in \mathbb{N}$. Entonces $\delta_C \geq s+1$ si y solamente si toda familia de s columnas de H es linealmente independiente.

13. Sea C un código lineal sistemático de tipo $(5,2)$ sobre $\mathbb{Z}_2$ con respectivas matrices generadora y de control:

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix} \text{ y } H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

    Configure para este código el cuadro de descodificación y, para $r = 1, 2, 3$, estudie las posibilidades de mensaje original cuando las palabras recibidas son 11011, 11010 y 10111. Determine la capacidad de corrección e_C del código C.

14. Determine la estructura de las matrices generadora y de control de un código de repetición.

15. Construya sobre el cuerpo $\mathbb{Z}_2$ un código lineal sistemático con capacidad de correción $e_C = 1$.

16. Demuestre que si el cuerpo de base es $\mathbb{Z}_2$, un código R es de repetición si y solamente si su dual $R^\perp$ es un código de chequeo de paridad.

17. Demuestre que el dual de un código de Hamming (resp. de un código simpléctico) es un código simpléctico (resp. de Hamming).

18. Demuestre que en un código simpléctico de tipo $(2^k-1, k)$ toda palabra no nula pesa 2^{k-1}. ¿Puede establecerse un resultado análogo para un código de Hamming?

19. Determine las matrices sistemáticas para los códigos (binarios) de repetición y de chequeo paridad introducidos en las definiciones 177 y 178.

20. Demuestre que el código dual de un código de repetición $(1, n)$ sobre $\mathbb{Z}_2$ es el codigo de chequeo de paridad. Estudie el recíproco.

21. Clasifique los códigos lineales que admiten sólo una matriz generadora.

22. Demuestre que un código lineal puede detectar a lo más s errores si y sólo si $\delta_C \geq s+1$.

23. Sea H la matriz de control de un código lineal C. Demuestre que $\delta_C = m$ si y sólo si toda familia de $m-1$ columnas de H es libre y existe una familia de m columnas dependiente.

24. Sean C_1 y C_2 dos códigos lineales de tipo (n_1, k) y (n_2, k), con matrices generadoras G_1 y G_2.

    A partir de estos códigos, construimos los códigos lineales C_3 y C_4 definiendo como respectivas matrices generadoras:

$$G_3 = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix} \text{ y } G_4 = \begin{pmatrix} G_1 & G_2 \end{pmatrix}.$$

    Demuestre que C_3 y C_4 son respectivamente de tipo $(n_1+n_2, 2k)$ y (n_1+n_2, k) y que además se tiene $\delta_{C_1} = \text{mín}(\delta_{C_1}, \delta_{C_2})$, $\delta_{C_2} \geq \delta_{C_1} + \delta_{C_2}$.

25. Construya un código lineal auto dual de dimensión k, sobre $\mathbb{K}$, $|\mathbb{K}| = q$.

26. Construya el cuadro de descodificación de un código de Hamming de longitud 7.

27. Demuestre que los códigos de Hamming son perfectos.

28. Clasifique los códigos cíclicos de longitud 4 y 7 sobre $\mathbb{Z}_2$; así mismo, aquellos de longitud 3 y 5 sobre $\mathbb{Z}_3$.

29. Construya las matrices generadoras de los códigos cíclicos dados en el ejemplo 185 y de aquellos que aparezcan en el ejercicio anterior.

30. Demuestre que en $\mathbb{K}[x]$ se tiene $\underline{g}(x)\underline{h}(x) = 1 - x^n$.

31. Determine las matrices de control de los códigos cíclicos dados en el ejemplo 185 y de aquellos que aparezcan en el ejercicio 27. Para cada uno de esos códigos construya un código sistemático equivalente. Para cada uno de esos códigos sistemáticos, encuentre los polinomios generador y de control asociados.

32. Entregue la descomposición de $x^7 - 1$ sobre $\mathbb{Z}_2$ y demuestre que los códigos cíclicos binarios de tipo (7,4) son de Hamming.

11. Ejercicios Resueltos

Rudimentos Conjuntistas

1. Sea U un conjunto y definamos los conjuntos: $\{n \in \mathbb{N} \ / \ n^2 < 0\}$, $\{A \subset U \ / \ A = \complement A\}$, $\{u \in U \ / \ u \neq u\}$ y $\{x \in \mathbb{R} \ / \ x^3 \leq 125\}$. Dé razones y argumentos que prueben que los tres primeros son iguales y que están contenidos estrictamente en el último.

   Solución. Los primeros tres conjuntos son conjuntos vacíos; el último no lo es ya que contiene al número 5. Lo que hay que demostrar aquí es que un conjunto vacío está contenido en todo otro conjunto y deducir de ello que existe un único conjunto vacío por lo que podemos denotarlo sin ambiguedad por $\emptyset$. En efecto, si V es un conjunto vacío y A cualquier conjunto, postular que $V \nsubseteq A$ obliga, por la definición de subconjunto, a suponer que existe $x \in V$ tal que $x \notin A$, lo que contradice la definición de V. Por otro lado si V y V' son vacíos, dado lo que acabamos de ver se tiene $V \subset V'$ y $V' \subset V$, es decir $V = V'$.

2. Sean $A, B \subset U$. Demuestre las leyes de De Morgan: $\complement(A \cup B) = \complement A \cap \complement B$ y $\complement(A \cap B) = \complement A \cup \complement B$.

   Solución. Se tiene: $x \in \complement(A \cup B) \iff x \notin A \cup B \iff x \notin A$ y $x \notin B$ $\iff x \in \complement A$ y $x \in \complement B \iff x \in \complement A \cap \complement B$. La segunda igualdad se deduce aplicando la primera sobre los subconjuntos $\complement A$ y $\complement B$.

3. Sean $A, B \subset E$ y $f : E \to F$ una función.

   a) $f(A \cap B) \subset f(A) \cap f(B)$;

   b) Pruebe que f es inyectiva si y sólo si $f(A \cap B) = f(A) \cap f(B)$ para todo $A, B \subset E$.

   c) Además demuestre que:

      1) f es inyectiva si y sólo si $f(\complement A) \subset \complement f(A)$ para todo $A \subset E$.

      2) f es sobreyectiva si y sólo si $\complement f(A) \subset f(\complement A)$ para todo $A \subset E$.

   Solución. Se tiene:

   (a): Como $A \cap B \subset A$ se tiene $f(A \cap B) \subset f(A)$ y, de manera análoga, $f(A \cap B) \subset f(B)$; de todo ello se infiere que $f(A \cap B) \subset f(A) \cap f(B)$.

Lo siguiente nos muestra que la igualdad no se establece siempre: si $A = \{a\}$, $B = \{b\}$, con $a \neq b$ y $f(a) = f(b) = x$, se tiene $f(A \cap B) = \emptyset$ y $f(A) \cap f(B) = \{x\}$.

(b): ($\Rightarrow$) Por (a), basta demostrar que $f(A) \cap f(B) \subset f(A \cap B)$: si $x \in f(A) \cap f(B)$, existen $a \in A$ y $b \in B$ tales que $y = f(a) = f(b)$; como f es injectiva, $a = b$ y por tanto $x \in f(A \cap B)$.

($\Leftarrow$) Si $a \neq b$, $\emptyset = f(\{a\} \cap \{b\}) = f(\{a\}) \cap f(\{b\}) = \{f(a)\} \cap \{f(b)\}$, es decir $f(a) \neq f(b)$.

(c (i)): ($\Rightarrow$) Como f es inyectiva, aplicando (b) se tiene $f(A) \cap f(\complement A) = \emptyset$ y, por ende $f(\complement A) \subset \complement f(A)$.

($\Leftarrow$) Si $a \neq b$ entonces $b \in \complement\{a\}$ donde, por hipótesis:

$$f(b) \in f(\complement\{a\}) \subset \complement f(\{a\}) = \complement\{f(a)\}$$

es decir $f(a) \neq f(b)$, luego f es inyectiva.

(c (ii)): ($\Rightarrow$) Sabemos que siempre se tiene $f(A \cup \complement A) = f(A) \cup f(\complement A)$; como f es sobreyectiva $f(A) \cup f(\complement A) = F$ de donde se infiere que $\complement f(A) \subset f(\complement A)$.

($\Leftarrow$) Como $f(\emptyset) = \emptyset$, $F = \complement f(\emptyset)$; ahora bien, por hipótesis tenemos $\complement f(\emptyset) \subset f(\complement\emptyset) = f(E)$ por tanto f es sobreyectiva.

4. Sean $f : E \to F$ y $h : F \to H$ funciones. Demuestre que se tiene:

   a) Si $h \circ f$ es inyectiva entonces f es inyectiva.

   b) Si $h \circ f$ es sobreyectiva entonces h es sobreyectiva.

   Solución. Si $f(a) = f(b)$ entonces $h(f(a)) = h(f(b))$ y como $h \circ f$ es inyectiva se tiene $a = b$. En cuanto a la segunda afirmación, si $h \circ f$ es sobreyectiva se tiene $h(f(E)) = H$ y como $f(E) \subset F$, a fortiori $h(F) = H$.

5. Sean $f : E \to F$ y $h, k : E \to F$ funciones tales que $h \circ f = Id_E$ y $f \circ k = Id_F$. Demuestre que f es biyectiva y $h = k$.

   Solución. Como Id_E y Id_F por el ejercicio precedente se infiere que f es inyectiva y sobreyectiva, es decir biyectiva. Se tiene además que: $h = h \circ Id_F = h \circ f \circ k = Id_E \circ k = k$.

6. Sea $f : E \to F$ una función. Demuestre que se tiene:

   a) Si f es inyectiva entonces existe $g : F \to E$ sobreyectiva tal que $g \circ f = Id_E$.

   b) Si f es sobreyectiva entonces existe $g : F \to E$ inyectiva tal que $f \circ g = Id_F$.

   Solución. Veamos la primera afirmación: como f es inyectiva, todo $x \in F$ tiene a lo más una pre-imagen; fijemos $b \in E$ y definamos $g : F \to E$ de la manera siguiente:

$$g(x) = \begin{cases} a \text{ si } f^{-1}(\{x\}) = \{a\} \\ b \text{ si } f^{-1}(\{x\}) = \emptyset \end{cases}.$$

   La función g es sobreyectiva por construcción.

   En cuanto a la segunda, como para todo $y \in F$, $f^{-1}(\{x\}) \neq \emptyset$, escogemos $a_x \in f^{-1}(\{x\})$ y definimos $g : F \to E$ de la manera siguiente: $g(x) = a_x$. Esta función es inyectiva por construcción ya que si $x \neq y$ se tiene $f^{-1}(\{x\}) \neq f^{-1}(\{y\})$.

7. Sean F un conjunto finito totalmente ordenado y $f : F \to F$ una función. Demuestre que:

   a) Si f es creciente, entonces existe $a \in F$, tal que $f(a) = a$ (es decir, f tiene un punto fijo).

   b) Si f es decreciente, entonces tiene un punto fijo o existen $a, b \in F$, tales que $f(a) = b$ y $f(b) = a$ (es decir, un ciclo de orden 2).

   Solución. Sin pérdida de generalidad, podemos considerar que F es el conjunto $\{1, 2, ..., n\}$. Como $1 \leq f(1)$ y f es una función creciente se tiene $1 \leq f(1) \leq f^2(1) \leq \cdots \leq f^n(1)$; esta cadena no puede estar constituida sólo por desigualdades estrictas (pues hay $n+1$ elementos) por tanto para algún k, $0 \leq k \leq n-1$, se tiene $f^{k+1}(1) = f^k(1)$, es decir $f^k(1)$ es un punto fijo.

   Otra demostración es la siguiente: es claro que $f(n) \leq n$, luego si n no es punto fijo, entonces $f(n) \leq n-1$. Luego, como f es creciente, $f(n-1) \leq n-1$; si suponemos que $n-1$ tampoco es punto fijo

llegaremos a que $f(n-2) \leq n-2$. Por tanto, sucesivamente, en el peor de los casos llegaremos a que $f(1) \leq 1$; en tal situación, obligadamente $f(1) = 1$.

Para la segunda afirmación utilizamos la primera: en efecto, si f es decreciente entonces f^2 es creciente y por tanto tiene un punto fijo k; esto significa que f tiene al menos un ciclo de largo 2:

$$k \to f(k) \to f^2(k) = k$$

8. Demuestre que no existe una función sobreyectiva de E en $\wp(E)$.

   Solución. Supongamos lo contrario y sea $\varphi : E \to \wp(E)$ sobreyectiva.

   En tal caso existen $a, b \in E$ tales que $\varphi(a) = \emptyset$ y $\varphi(b) = E$.

   Esto quiere decir que podemos particionar E con los conjuntos:

$$S = \{x \in E \,/\, x \in \varphi(x)\} \quad \text{y} \quad N = \{x \in E \,/\, x \notin \varphi(x)\}$$

   Por hipótesis existe $c \in E$ tal que $\varphi(c) = N$; ahora bien las dos alternativas posibles llevan a contradicción:

$$c \in N \Longrightarrow c \notin N \quad \text{y} \quad c \notin N \Longrightarrow c \in N$$

   Luego no podemos suponer una sobreyección de E en $\wp(E)$.

9. Sea F un conjunto finito. Si $|F| = n$ demuestre que $|\wp(F)| = 2^n$.

   Solución. Si $A_k = \{a_1, a_2, ..., a_k\}$ es inmediato que:

$$\wp(A_{n+1}) = \wp(A_n) \cup \{S \cup \{a_{n+1}\} \quad / \quad S \in \wp(A_n)\}$$

   De esto se infiere que $|\wp(A_{n+1})|$ es el doble de $|\wp(A_n)|$; como $|\wp(\emptyset)| = 1$ se deduce que $|\wp(A_n)| = 2^n$.

10. Sean E un conjunto y $\varphi : \wp(E) \to \wp(E)$ creciente (según el orden dado por la inclusión). Demuestre que φ admite un punto fijo.

    Solución. Obviamente se tiene $\emptyset \subset \varphi(\emptyset)$, cuestión que cumple cualquier función $\wp(E) \to \wp(E)$. Esto nos permite asegurar que el conjunto $F = \{M \subset E) \,/\, M \subset \varphi(M)\}$ no es vacío.

Sea $A = \bigcup_{M \in F} M$; es claro que para todo $M \in F$ se tiene $M \subset A$. Como φ es creciente para el orden de la inclusión, $\varphi(M) \subset \varphi(A)$; así tenemos:

$$A = \bigcup_{M \in F} M \subset \bigcup_{M \in F} \varphi(M) \subset \varphi(A), \quad \text{es decir,} \quad A \in F.$$

Pero de $A \subset \varphi(A)$ viene que $\varphi(A) \subset \varphi(\varphi(A))$ o sea $\varphi(A) \in F$ y, en tal caso, $\varphi(A) \subset A$. Se concluye que $\varphi(A) = A$.

11. Demuestre que:

    a) Dados dos conjuntos, existe una función inyectiva o una sobreyectiva de uno en el otro (primera parte del teorema de Cantor-Schröder-Bernstein).

    b) Si dados dos conjuntos existen funciones inyectivas de uno en el otro, entonces existe una biyección entre ellos (segunda parte del teorema de Cantor-Schröder-Bernstein).

Solución.

(a) (Bosquejo de demostración) Sean E y F tales conjuntos y supongamos que no existe inyeccion de F en E; sabemos que esto es equivalente a decir que no existe sobreyección de E en F (ejercicio 6). Luego, sea cual sea la manera de llevar, por una función, los elementos de E en F, esté último conjunto nunca podrá ser copado por la imagen del primero. Así las cosas, desde los elementos de E podemos ir tirando flechas paralelas hacia F, pues si en algún momento no pudieramos hacerlo ello significaría que habríamos copado F con tales flechas, cuestión que por hipótesis es imposible. Tenemos así (la idea de) una función inyectiva de E en F, que es lo que se quería.

(b) Sean $f : E \to F$ y $g : F \to E$ funciones inyectivas. El problema queda resuelto si encontramos $A \subset E$ que $g(\complement f(A)) = \complement A$, pues en tal caso definiríamos $h : E \to F$ biyectiva, de la manera siguiente:

$$h(x) = \begin{cases} f(x) & \text{si } x \in A \\ z \text{ si } x \notin A \text{ y } g(z) = x \end{cases}$$

Ahora bien, tal subconjunto verificaría $A = \complement(g(\complement f(A)))$; como es inmediato establecer que la aplicación:

$$\wp(E) \to \wp(E), X \to \complement(g(\complement f(X)))$$

es creciente para el orden de la inclusión y que por tanto admite un punto fijo, la existencia de A está garantizada.

12. Si A es finito o numerable y B es numerable, demuestre que $A \cup B$ es numerable.

    Solución. Sin pérdida de generalidad podemos suponer A y B disjuntos, ya que en caso contrario trabajaríamos con A y $B-A$, manteniendo las condiciones de la hipótesis. Sea $B = \{b_0, b_1, b_2, ...\}$; si A es finito, $A = \{a_0, a_1, ..., a_n\}$, la función $f : A \cup B \to \mathbb{N}$ definida por:

    $$f(x) = \begin{cases} k \text{ si } x = a_k \\ n + k + 1 \text{ si } x = b_k \end{cases} \quad \text{es biyectiva.}$$

    Si A es infinito, $A = \{a_0, a_1, a_2, ...\}$ la función $g : A \cup B \to \mathbb{N}$ definida por:

    $$g(x) = \begin{cases} 2k \text{ si } x = a_k \\ 2k + 1 \text{ si } x = b_k \end{cases} \quad \text{es biyectiva.}$$

13. Si $A \subset \mathbb{R}$ y $card(A) \leq \aleph_0$, demuestre que $card(\mathbb{R} - A) = \aleph_1$ (esto demuestra en particular que el cardinal conjunto de los irracionales es infinitamente mas "grande" que aquel de los racionales).

    Solución. Es claro que $card(\mathbb{R} - A) \leq \aleph_1$. Si $card(\mathbb{R} - A) \leq \aleph_0$, como $card(A) \leq \aleph_0$ se inferiría que $\mathbb{R} = A \cup (\mathbb{R} - A)$ tendría a lo sumo $\aleph_0$ como cardinal, lo que es imposible.

14. Demuestre que $card(\mathbb{N} \cup \wp(\mathbb{N})) = \aleph_1$.

    Solución. Del ejercicio anterior se infiere que si A es finito o numerable, entonces $card(A \cup \mathbb{R}) = \aleph_1$. En el caso que nos ocupa, esto se aplica de inmediato ya que $\wp(\mathbb{N})$ es equipotente a $\mathbb{R}$.

15. Demuestre que si A es numerable, entonces A^2 es numerable.

    Solución. Como A es equipotente a $\mathbb{N}$ basta demostrar que $\mathbb{N}^2$ es numerable. Como es inmediato que $card(\mathbb{N}) \leq card(\mathbb{N}^2)$, ya que la función $n \to (n, 0)$ es inyectiva, basta demostrar que $card(\mathbb{N}^2) \leq card(\mathbb{N})$ lo que se establece con la función inyectiva $\mathbb{N}^2 \to \mathbb{N}$, $(n, m) \to 2^n 3^m$.

16. Demuestre que la reunión de una familia numerable de conjuntos finitos o numerables es numerable.

Solución. Sin pérdida de generalidad podemos suponer que tenemos una familia disjunta de conjuntos numerables $A_n = \{a_{n0}, a_{n1}, a_{n2}, ...\}$. La función $\bigcup_{n\in\mathbb{N}} A_n \to \mathbb{N}^2$, $a_{nm} \to (n, m)$, es biyectiva.

17. Dados $a, b \in \mathbb{R}$, $a < b$, demuestre que se tiene

$$card(]a, b[) = card([a, b[) = card(]a, b]) = card([a, b]) = \aleph_1$$

Solución. Pruebe que la función $\mathbb{R} \to]0, 1[$, $y \mapsto \dfrac{y}{1 + |y|}$ es biyectiva.

Por otro lado, es claro que la función $f(x) = \dfrac{x - a}{b - a}$ establece una biyección entre los intervalos $]a, b[$ y $]0, 1[$.

De lo anteriormente expuesto deducimos que todo intervalo abierto tiene cardinalidad $\aleph_1$.

El resultado demandado se establece por la cadena de inclusiones:

$$]a, b[\subset [a, b[, \ ]a, b] \subset [a, b] \subset]a - 1, b + 1[.$$

Sobre Inducción y Conteo

18. Demuestre que:

- $1 + 2 + \cdots + n = \frac{1}{2}n(n + 1)$
- $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n + 1)(2n + 1)$.
- $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.

Encuentre una expresión en función de n para $1^4 + 2^4 + 3^4 + \cdots + n^4$

Solución. Hagamos por recurrencia la suma de cubos: como sabemos que se tiene $1+2+3+\cdots+n = \frac{1}{2}n(n+1)$ lo que debemos demostrar por inducción es $1^3+2^3+3^3+\cdots+n^3 = \frac{1}{4}n^2(n+1)^2$, lo que es trivialmente válido para $n = 1$.

Supongamos válida la afirmación para n y utilicemos esta hipótesis para probar el nivel $n+1$. Tenemos:

$$\left(1^3+2^3+3^3+\cdots+n^3\right)+(n+1)^3=\frac{1}{4}n^2(n+1)^2+(n+1)^3.$$

Ahora bien, factorizando el segundo miembro por $\frac{1}{4}(n+1)^2$ se obtiene $1^3+2^3+3^3+\cdots+n^3+(n+1)^3=\frac{1}{4}(n+1)^2(n+2)^2$, como queríamos.

Veamos la última pregunta: de $(k+1)^5=k^5+5k^4+10k^3+10k^2+5k+1$, tenemos de inmediato:

$$\sum_0^n(k+1)^5=\sum_0^n k^5+5\sum_0^n k^4+10\sum_0^n k^3+10\sum_0^n k^2+5\sum_0^n k+\sum_0^n 1$$

y, por tanto, $5\sum_0^n k^4=(n+1)^5-10\sum_0^n k^3-10\sum_0^n k^2-5\sum_0^n k-\sum_0^n 1.$

Reemplazando las sumas (de cubos, cuadrados, etc.) por las expresiones que ya conocemos y despejando la suma de potencias cuartas obtenemos:

$$\sum_0^n k^4=\frac{1}{5}(n+1)^5-\frac{1}{2}n^2(n+1)^2-\frac{1}{3}n(n+1)(2n+1)-\frac{1}{2}n(n+1)-\frac{1}{5}(n+1)$$

y, factorizando, finalmente, $\sum_0^n k^4=\frac{1}{30}n\left(2n+1\right)\left(n+1\right)\left(3n+3n^2-1\right).$

19. Sean A y B dos conjuntos finitos, $|A|=n$ y $|B|=m$. Encuentre el número de funciones de A en B. Si $n\leq m$ ¿cuantas de estas funciones son inyectivas?

Solución. Recordemos que la única restricción para definir una función de A en B es que cada elemento tenga una y sólo una imagen. Así las cosas, para cada elemento de A tenemos m posibilidades de asociarle un elemento de B y como tenemos n elementos de A obtenemos m^n funciones posibles.

Si $n\leq m$, para las funciones inyectivas se suma la restricción de no tener imagenes repetidas por lo que tenemos m posibilidades de caida en B para un primer elemento de A, $m-1$ para un segundo, $m-2$ para un tercero, etc., lo que nos entrega $m(m-1)(m-2)\cdots(m-n+1)=m!/(m-n)!$ inyecciones de A en B.

20. Sea A un conjunto, $|A| = n$ y k tal que $1 \leq k \leq n$. Si $x_1, \ldots, x_k,$ son elementos distintos de A, cuente el número de subconjuntos de A que no contienen ningun x_i, $1 \leq i \leq k$.

Solución. Si $X = \{x_1, x_2, \ldots, x_k\}$, obviamente lo que se pide está dado por $|\wp(A - X)| = 2^{n-k}$.

21. Sean $|A| = n \geq 2$ y $a, b \in A$. Cuente el número de subconjuntos de A que contienen a lo más uno de los elementos a o b. La misma situación anterior, pero cambiando la frase "a lo más uno" por la frase "al menos uno".

Solución. Primero, un poco de escritura....

Definamos $X = A \setminus \{a, b\}$, $P = \{Y;\ Y \subset X\}$, $P_a = \{Y \cup \{a\};\ Y \subset X\}$, $P_b = \{Y \cup \{b\};\ Y \subset X\}$ y $P_{ab} = \{Y \cup \{a, b\};\ Y \subset X\}$.

No es difícil establecer que $|P| = |P_a| = |P_b| = |P_{ab}| = 2^{n-2}$. Tambien es inmediato ver que los conjuntos que verifican lo primero están dados por $P \cup P_a \cup P_b$ y lo segundo por $P_a \cup P_b \cup P_{ab}$; como estas reuniones son trivialmente disjuntas el número pedido en ambos casos es $3 \cdot 2^{n-2}$.

22. Sea A un conjunto finito, $|A| = n \geq 1$. Demuestre que

$$|\{P \ / \ P \subset A,\ |P| \text{ par}\}| = |\{I \ / \ I \subset A,\ |I| \text{ impar}\}| = 2^{n-1} \quad (*)$$

Solución. Es claro que si tomamos conjuntos de 0,1,2 y 3 elementos lo que se propone se verifica sin problemas (es cosa de escribir y contar). Esto nos lleva a proponer la hipótesis de inducción: si $|A| = n$ entonces $|\{P \ / \ P \subset A,\ |P| \text{ par}\}| = |\{I \ / \ I \subset A,\ |I| \text{ impar}\}| = 2^{n-1}$ Demostremos la propiedad para $n + 1$:

Sea $b \notin A$ y $B = A \cup \{b\}$. Es inmediato que $|\{P \ / \ P \subset B,\ |P| \text{ par}\}|$ es igual a $|\{P \ / \ P \subset A,\ |P| \text{ par}\}| + |\{I \cup \{b\} \ / \ I \subset A,\ |I| \text{ impar}\}|$ o sea $2^{n-1} + 2^{n-1} = 2^n$. Analogamente, $|\{I \ / \ I \subset B,\ |I| \text{ impar}\}|$ es igual a $|\{I \ / \ I \subset A,\ |I| \text{ impar}\}| + |\{I \cup \{b\} \ / \ I \subset A,\ |I| \text{ impar}\}| = 2^n$.

23. Calcule en función de n las sumas $\sum_{k=0}^{n} \binom{n}{k}$, $\sum_{k=0}^{n} \binom{n}{2k}$ y $\sum_{k=0}^{n} \binom{n}{2k+1}$.

Solución. Recordemos que $\binom{n}{k} = C_n^k$, es decir el número de subconjuntos de k elementos de un conjunto A con n elementos. Por tanto

la primera suma da,el número de subconjuntos de A, o sea 2^n. Por las mismas razones, y dado el ejercicio anterior, las otras sumas dan 2^{n-1}.

Estructuras Algebraicas, Grupos

24. Sea F una estructura asociativa finita. Demuestre que F tiene un elemento idempotente (es decir, existe x tal que $x^2 = x$).

    Solución. Sea $y \in F$; como F es finito, obligadamente la sucesión de potencias de y tiene repeticiones, por lo que existen enteros $0 < m < n$ tales $y^m = y^n$.

    Hay tres situaciones: $2m = n$, $2m < n$, y $2m > n$. Para el primer caso, $x = y^m$ es un idempotente; para el segundo, se tiene: $x = y^{n-m} = y^{n-2m}y^m = (y^{n-m})^2$. En cuanto a la última situación, notemos que $y^n = y^{n-m}y^m = y^{2n-m} = y^{2n-2m}y^m = y^{3n-2m} = ... = y^{kn-(k-1)m}$. Como $p = kn - (k-1)m$ puede ser tan grande como lo necesitemos, basta tomar $p \geq 2m$ para resituarnos en las dos primeras condiciones.

    Otra forma de hacer este ejercicio es considerar la estructura circular de $n-m$ elementos : $y^m, y^{m+1}, ..., y^{m+r}, ..., y^{m+(n-m)} = y^n$. Esto significa que, respecto de los exponentes, operamos en $\mathbb{Z}_{n-m}$. Suponer que $y^{m+r} = (y^{m+r})^2$ nos lleva a una ecuación $mod(n-m)$ de cuya solución sale que r es de la forma $kn - (k+1)m$ (¡hágalo!).

25. Sea E una estructura asociativa que verifica las propiedades siguientes: existe e tal que para todo $a \in E$ se tiene $ea = a$ (neutro izquierdo) y para todo $a \in E$ existe b tal que $ba = e$ (inverso izquierdo). Demuestre que E es un grupo.

    Solución. Hay que establecer que el neutro y los inversos a la izquierda lo son también a la derecha. Demostremos primero que si $ba = e$ entonces $ab = e$: en efecto, si c es el inverso izquierdo de b se tiene $ab = e(ab) = (cb)(ab) = c((ba)b) = c(eb) = cb = e$. Apoyándonos en esto, tenemos: $ae = a(ba) = (ab)a = ea = a$.

26. Sea F una estructura asociativa finita que verifica las cancelaciones a la izquierda y a la derecha, $(xy = xz \Longrightarrow y = z;\ yx = zx \Longrightarrow y = z)$. Muestre que F es un grupo. De un ejemplo en el cual, teniendo las propiedades de cancelación, no tengamos un grupo.

Solución. Por el primer ejercicio sabemos que tal estructura tiene un idempotente e y es inmediato que e es un neutro a la izquierda; por otro lado, la función $r_x : F \to F$, $r_x(z) = zx$, es biyectiva (¿porqué?), lo que nos lleva a establecer que x tiene inverso izquierdo. Por el ejercicio anterior, F es un grupo.

27. Encontrar todos los grupos con dos, tres, cuatro elementos.

Solución. Sabemos que la tabla de composición de un grupo no admite repeticiones ni en sus filas ni en sus columnas (¿porqué?). Teniendo claro esto, si $\{e, a, b, c\}$ es un grupo con neutro e, las únicas tablas posibles son:

$\diamond$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

y

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(demuéstrelo).

Estos grupos corresponden respectivamente a $(\mathbb{Z}_4, +)$ y a $(\mathbb{Z}_2^2, +)$.

28. Muestre que un grupo es conmutativo si y sólo si para todo a, b se tiene una de las condiciones siguientes:

(a) $(ab)^{-1} = a^{-1}b^{-1}$. (b) $(ab)^2 = a^2b^2$. (c) $(ab)^n = a^nb^n$, para tres enteros consecutivos.

Solución. Hagamos el tercero. Se tiene:

$$(ab)^n = a^nb^n, (ab)^{n+1} = a^{n+1}b^{n+1} \text{ y } (ab)^{n+2} = a^{n+2}b^{n+2}$$

De $(ab)^n = a^nb^n$ y $(ab)^{n+2} = a^{n+2}b^{n+2}$ obtenemos: $b^naba = a^2b^{n+1}$ (*). Ahora bien, como de $(ab)^n = a^nb^n$ y $(ab)^{n+1} = a^{n+1}b^{n+1}$ se desprende que $b^na = ab^n$, aplicando esto a (*) tenemos: $b^naba = a^2b^{n+1} = b^na^2b$. Sale de inmediato que $ba = ab$.

29. Si G es un grupo finito tal que $x^2 = 1_G$ para todo $x \in G$, entonces es isomorfo a $\mathbb{Z}_2^n$ para cierto $n \in \mathbb{N}$.

Solución. Por el ejercicio precedente, G es conmutativo.

Si G tuviese más de dos elementos, entonces tendría al menos cuatro: en efecto, en tales condiciones es claro que G tiene un subgrupo de

dos elementos, $D = \{1_G, x_1\}$, por lo que si $x_2 \in G$, es immediato que $x_3 = x_1x_2 \neq 1_G,\ x_1,\ x_2$.

Supongamos ahora que G tiene un subgrupo propio H, isomorfo a $\mathbb{Z}_2^k$; entonces G contiene un subgrupo isomorfo a $\mathbb{Z}_2^{k+1}$: en efecto, sea entonces $x_{m+1} \in G - H$; como $x_i x_{m+1} = y \Leftrightarrow x_{m+1} = x_i y$, se tiene $x_{m+i} = x_i x_{m+1} \neq 1_G,\ x_1, x_2, .., x_m,\ x_{m+1}$, para todo $1 \leq i \leq m$, obteniéndose así 2^k nuevos elementos autoinversos.

Como G es finito, hemos establecido recursivamente que G es isomorfo a $\mathbb{Z}_2^n$ para cierto $n \in \mathbb{N}$.

30. Sea $n \geq 1$ un entero dado y E una estructura asociativa que verifica la siguiente identidad : $yxy = x^n$ para todo $x, y \in E$. Demuestre que:

    a) Si $n = 1$, E es un grupo conmutativo.

    b) E tiene un idempotente ($a^2 = a$) que se precisará.

    c) Si E es un grupo no trivial, n es impar.

    d) Si E tiene cancelación (izquierda o derecha) entonces es un grupo conmutativo.

    Solución. Si $n = 1$, la relación que define la estructura de E queda $yxy = x$; es claro que tenemos $x^3 = x$ para todo $x \in E$. Por otro lado, de $x(yxy) = (xyx)y$ resulta que $x^2 = y^2$ para todo $x, y \in E$; esto significa que $f(z) = z^2$ es una función constante. Pongamos $f(z) = e \in E$; como $x = x^2x = xx^2$, se establece que e es el neutro y que $x^{-1} = x$ para todo $x \in E$. En tales condiciones, E es un grupo conmutativo.

    En cuanto a (b), es claro que para todo $x \in E$, $x^3 = x^n$, luego la relación se reescribe como: $yxy = x^3$. De manera análoga a lo realizado en el primer punto, concluimos que $f(z) = z^4$ es una función constante.

    Pongamos $f(z) = \epsilon$; puesto que $\epsilon \in E$, se tiene $\epsilon^4 = \epsilon$ y una rápida verificación muestra que $a = \epsilon^3$ es un idempotente.

    Para responder a la pregunta (c) supongamos que E es un grupo; si n fuera par, entonces dado cualquier $x \in E$, tendríamos $x^{n+1} = x^n$ (¿porqué?) de donde se concluye que $x = 1_E$.

    Pasando a la pregunta (d), como para todo $x \in E$ se tiene $x^2xx^2 = x^3$, con la cancelación deducimos que $x^3 = x$. Así la relación que define la estructura toma la forma de $yxy = x$ para todo $x, y \in E$.

31. Muestre que si un grupo G tiene un número par de elementos, entonces existe por lo menos un elemento $a \neq 1_G$ que verifica $a = a^{-1}$.

Solución. Supongamos que para todo $a \neq 1_G$ se tenga $a \neq a^{-1}$. Entonces $G = \{1_G, a, a^{-1}, b, b^{-1}, ...\}$ y, a fortiori, $|G|$ es impar.

32. Sean G un grupo finito y H un subconjunto no vacio tal que $H^2 \subset H$. Demuestre que H es un subgrupo de G.

Solución. La hipótesis nos dice que H es una estructura finita, asociativa y con cancelación derecha e izquierda (¿porqué?).

33. Sea $G = \{a_1, ..., a_n\}$ un grupo abeliano. Si $g = a_1 \cdot a_2 \cdot ... \cdot a_n$, demuestre que $g^2 = 1_G$ y, si n es impar, que $g = 1_G$. Establezca además que:

    a) Si existe un único $x \neq 1_G$, tal que $x^2 = 1_G$, entonces $x = g$.

    b) Si existe mas de un elemento $x \in G$, $x \neq 1_G$, tal que $x^2 = 1_G$ entonces $g = 1_G$.

Solución. Notemos que g es el producto de todos los $x \in G$ tales que $x = x^{-1}$ (o, lo que es lo mismo, $x^2 = 1_G$); ahora bien, el conjunto D formado por esos elementos es trivialmente no vacío y forma un subgrupo (demuéstrelo) que por añadidura contiene a g (¿porqué?).

Este preámbulo permite responder a todas las afirmaciones del ejercicio.

34. Sean G un grupo y $g, h \in G$ tales que $gh = hg$, $o(g), o(h) < \infty$ y $\langle g \rangle \cap \langle h \rangle = \{1_G\}$. Demuestre que $o(gh) = mcm(o(g), o(h))$.

Solución. Sean $o(g) = p$, $o(h) = q$, $o(gh) = r$ y $mcm(p, q) = m$.

Es claro que $(gh)^m = 1_G$ (¿porqué), luego $r \mid m$ (¿porqué?).

Por otro lado, tenemos que $g^r h^r = 1_G$ (¿porqué?); con esto, la condición $\langle g \rangle \cap \langle h \rangle = \{1_G\}$ obliga a que $p \mid r$ y $q \mid r$, de donde se infiere que $m \mid r$. Luego $m = r$.

35. Demuestre que si la reunion de dos subgrupos (de un grupo G) es un subgrupo, entonces uno de los subgrupos en cuestión contiene al otro.

Solución. Sean H, $K < G$ tales que $H \cup K = L < G$. Supongamos que ningún subgrupo contiene al otro; sean $h \in H - K$ y $k \in K - H$. Como $L = H \cup K$, se tiene que $hk \in H$ o $hk \in K$; esto implica que $k \in H$ o $h \in K$, lo que es imposible.

36. Sean H, $K < G$. Entonces $HK < G$ si y solamente si $HK = KH$.

Solución. Recordemos que $XY = \{xy;\ x \in X,\ y \in Y\}$, por lo que la igualdad $HK = KH$ no es término a término: esto significa que dados $h \in H$ y $k \in K$, existen $h' \in H$ y $k' \in K$ tales que $hk = k'h'$.

Si HK es un subgrupo de G, entonces para todo $h \in H$ y $k \in K$ se tiene $kh = (h^{-1}k^{-1})^{-1} \in HK$, por tanto $KH \subset HK$; análogamente, $HK \subset KH$. Recíprocamente, si $L = HK = KH$ se tiene: $(hk)^{-1} = k^{-1}h^{-1} \in L$ y $hkh_1k_1 = hh'k'l_1 \in L$, lo que demuestra que L es un subgrupo de G.

37. Sea G un grupo; recordamos que $Z(G) = \{x \in G \ /\ gx = xg \ \ \forall g \in G\}$. Si S el subconjunto mas grande de G tal que $xy = yx$ para todo $x, y \in S$, demuestre que:

    a) S es un subgrupo de G y contiene a $Z(G)$.

    b) Si $card(G - S) < card(S)$ entonces $S = G$ (o sea, G es abeliano).

Solución. Lo primero es trivial. En cuanto a la segunda, supongamos que $G \neq S$. Si $g \in G - S$ entonces $gS \subset G - S$ (¿porqué?). Como l_g es biyectiva, $card(S) < card(G - S)$, lo que contradice la hipótesis.

Subgrupos normales

38. Sean G un grupo y H un subgrupo. Demuestre que:

    a) Para todo $x, y \in G$ se tiene $card(xH) = card(Hy) = card(H)$.

    b) $card(G/H) = card(G\backslash H)$.

    c) Si G es finito, $|G| = |G/H|\,|H|$.

Solución. La primera afirmación resulta de que las funciones, multiplicación a la derecha y a la izquierda, r_z, $l_z : G \to G$, con $z \in G$, definidas por $r_z(t) = tz$ y $l_z(t) = zt$, son biyectivas. La segunda del hecho que la aplicación $G/H \to G\backslash H$, $xH \to Hx^{-1}$, es también biyectiva. La tercera se infiere de que las clases $modH$ tienen el mismo cardinal y forman una partición de G.

39. Sea G un grupo. Demuestre que si H y L son dos subgrupos normales de G, también lo son los subgrupos $H \cap L$ y HL.

Solución. El primero no presenta dificultad. En cuanto al segundo, que HL es un subgrupo sale de que para todo $h \in H$ se tiene $Lh = hL$ (¿porqué). Por último, para establecer que HL es un subgrupo normal, basta ver que $x^{-1}HLx = (x^{-1}Hx)(x^{-1}Lx)$ para todo $x \in G$.

40. Sean G un grupo y H un subgrupo de G tal que $xHx \subset H$, $\forall x \in G$.

    a) Demuestre que $x^{2k} \in H$ para todo $x \in G$. Deduzca que si $y \in G$ tiene orden impar entonces $y \in H$.

    b) Demuestre que el subgrupo H es normal

    c) Utilizando (a) y (b), demuestre que el grupo cociente G/H es conmutativo.

    d) De un ejemplo que muestre que el reciproco de (b) no es válido (es decir, H normal no implica $xHx \subset H$ para todo $x \in G$).

Solución. Que para todo $k \in \mathbb{Z}$, $x \in G$ se tiene $x^{2k} \in H$ es inmediato; luego, si $y \in G$ es de orden $2n+1$, se deduce que $y = y^{-2n} \in H$. La segunda pregunta sale de: $x^{-1}Hx = x^{-2}(xHx)$. La tercera resulta de: $(xH)^2 = H$.

41. Sean G un grupo, $n \in \mathbb{N}$ y H un subgrupo de G tal que $x^nHx \subset H$ para todo $x \in G$. Demuestre que H es un subgrupo normal.

Solución. Es inmediato que $x^{n+1} \in H$ para todo $x \in G$. Lo pedido sale de: $x^{-1} = (x^{-1})^{n+1}x^n$.

42. Sean G un grupo y S un conjunto generador de G (es decir, se tiene $S \subset G$ y $\langle S \rangle = G$). Muestre que un subgrupo H es normal si y solo si $s^{-1}Hs = H$ para todo $s \in S$.

Solución. Se tiene $s^{-k}Hs^k = H$ para todo $s \in S$ y $k \in \mathbb{Z}$ (¿porqué?). La demostración sale del hecho de que todo $x \in G$ es un producto $y_1^{m_1}y_2^{m_2}...\ y_n^{m_n}$, donde y_i o $y_i^{-1} \in S$ para $1 \leq i \leq n$.

43. Sea H un subgrupo de un grupo G. Si $x \in G$, demuestre que xHx^{-1}es un subgrupo de G (llamado el conjugado de H por x). Pruebe además que $N(H) = \bigcap\limits_{x \in G} x^{-1}Hx$ es un subgrupo normal contenido en H.

Solución. Que los conjuntos xHx^{-1} y $N(H)$ sean subgrupos no presenta dificultad, como también que se tenga $N(H) < H$. Por otro lado, se tiene: $y^{-1}\left(\bigcap_{x\in G} x^{-1}Hx\right)y = \bigcap_{x\in G}(xy)^{-1}Hxy = N(H)$ (¿porqué?).

44. Si H y L son dos subgrupos normales de G tales que $H \cap L = \{1_G\}$, muestre que $hl = lh$ para todo $h \in H$ y $l \in L$.

Solución. Por ser H y L subgrupos normales, para todo $h \in H$ y $l \in L$ se tiene $hlh^{-1}l^{-1} \in H \cap L$.

Basta aplicar el resto de la hipótesis para concluir.

45. Sean G un grupo y H un subgrupo. Demuestre que si $|G/H| = 2$ entonces H es normal.

Solución. Como $|G/H| = |G\backslash H|$, luego, si $x \notin H$ el grupo G es particionado por cada una de las familias de clases: $\{H,\, xH\}$ y $\{H,\, Hx\}$.

46. Se define el conmutador (o derivado) de G, de la manera siguiente: $G' = \langle\{x^{-1}y^{-1}xy :\ x, y \in G\}\rangle$. Demuestre que:

    a) G es abeliano si y solo si $G' = \{1_G\}$.

    b) G' es un subgrupo normal de G.

    c) El grupo cociente G/G' es conmutativo.

    d) G' está contenido en todo subgrupo normal H tal que G/H sea abeliano.

Solución. Hagamos (b), (c) y (d): sean $x \in G$ y $g \in G'$; por definición $x^{-1}gxg^{-1} \in G'$ por tanto G' es normal.

Por otro lado, para todo $x, y \in G$, $x^{-1}y^{-1}xy \in G'$ por lo que se tiene: $\overline{x}^{-1}\,\overline{y}^{-1}\,\overline{x}\,\overline{y} = G' = \overline{1_G}$, es decir $\overline{x}\,\overline{y} = \overline{y}\,\overline{x}$.

Por último, G/H si es abeliano, $\overline{x}^{-1}\,\overline{y}^{-1}\,\overline{x}\,\overline{y} = H$ o, dicho de otra manera $x^{-1}y^{-1}xy \in H$ para todo $x, y \in G$.

Por tanto, el subgrupo H contiene al conjunto que engendra a G'.

47. Sean G un grupo no necesariamente finito y H un subgrupo de G, tal que G/H es finito.

a) Demuestre que todo $x \in G$ tiene una potencia en H

b) Consideremos ahora que $|G/H| = 3$. Si existe $x \in G$, $x^2 \notin H$, tal que $xH = Hx$, demuestre que H es un subgrupo normal. De un ejemplo en donde $|G/H| = 3$ y H no sea normal.

Solución. Lo primero sale del hecho que el conjunto formado por las clases H, xH, x^2H, $x^3H, ...$ es finito. En cuanto a la segunda pregunta, es claro $x \notin H$ (¿porqué?) y por ende $xH \neq x^2H$ (¿porqué?), de manera que $G/H = \{H, xH, x^2H\}$; ahora bién, de $x^2H = xHx = Hx^2$ concluimos que $G/H = G\backslash H$. El ejemplo pedido se deja al lector.

48. Consideremos el grupo cociente aditivo $\mathbb{Q}/\mathbb{Z}$. Sean p, q dos enteros positivos primos entre si; demuestre que:

$$\text{si } \frac{a}{p} = \frac{b}{q} \; mod(\mathbb{Z}) \text{ entonces } \frac{a}{p} \;\; y \;\; \frac{b}{q} \;\; \text{son enteros.}$$

Deduzca que $\mathbb{Q}/\mathbb{Z}$ es un grupo infinito.

Solución. Tal situación es equivalente a: $aq - bp = pqk$, para algún $k \in \mathbb{Z}$; de esto se infiere que a es múltiplo de p y b lo es de p. Finalmente, si p y q son números primos distintos, por lo anterior $\frac{1}{p} \neq \frac{1}{q} \; mod(\mathbb{Z})$ y como hay infinitos números primos, $\mathbb{Q}/\mathbb{Z}$ es infinito.

49. Sea G un grupo. Si $g \in G$ se define el centralizador de g en G de la manera siguiente: $C(g) = \{x \in G : gx = xg\}$. Demuestre que:

a) $C(g)$ que es un subgrupo de G.

b) $Z(G) = \bigcap_{g \in G} C(g)$.

Solución. La primera parte es rutina. Para la segunda, notemos que $Z(G) \subset C(g)$ para todo $g \in G$, luego $Z(G) \subset \bigcap_{g \in G} C(g)$.

La inclusión recíproca es inmediata.

50. Sean G un grupo y $g \in G$. El normalizador de g es el conjunto de los conjugados de g: $N(g) = \{x^{-1}gx, \; x \in G\}$. Demuestre que:

a) Los conjuntos $N(g)$, $g \in G$ forman una partición de G.

b) $x^{-1}gx = y^{-1}gy$ si y sólo si $x = y\ mod C(g)$.

c) Si G es finito, establezca que : $|N(g)| = (G : C(g))$.

d) Tomando un elemento g por clase de conjugación (es decir, un representante por cada normalizador $N(g)$), deduzca las identidades: (que se denominan ecuaciones de clases)

$$|G| = \sum_g |N(g)|\,,\ \sum_g \frac{1}{|C(g)|} = 1 \ \text{ y } \ |G| \ = \ |Z(G)| \ + \sum_{g \in G - Z(G)} \frac{|G|}{|C(g)|}$$

Solución. Es claro que $G = \bigcup N(g)$; queda por demostrar que dos de tales conjuntos son iguales o son disjuntos: si $x^{-1}gx = z^{-1}hz$, entonces $g = (zx^{-1})^{-1}hzx^{-1}$ y por tanto $g \in N(h)$. La segunda pregunta no presenta mayor problema; sin embargo, si G es finito, de ella se deduce que hay tantos elementos en $N(g)$ como clases $mod C(g)$, lo que es la respuesta a la tercera pregunta. En cuanto a la última, como la reunión $G = \bigcup_g N(g)$ es disjunta, tomando un representante g por clase de conjugación se tiene: $|G| = \sum_g |N(g)|$; basta aplicar (c) para establecer la segunda identidad. Por último, como $g \in Z(G)$ si y solamente si $\{g\} = N(g)$, tenemos $|G| \ = \ |Z(G)| \ + \sum_{g \in G - Z(G)} |N(g)|$.

51. Sean p un entero primo y G un grupo de orden p^n. Entonces $|Z(G)| \geq p$.

Solución. Sea $m = |Z(G)| \geq 1$; se tiene:

$$|G| \ = \ m \ + \sum_{g \in G - Z(G)} \frac{|G|}{|C(g)|} \quad (\bullet)$$

Ahora bien, por otro lado sabemos que los subgrupos $C(g)$ tienen un orden de tipo p^{n_h} con $1 \leq n_h < n$ (¿porqué?), por lo que la igualdad $(\bullet)$ se reescribe como sigue:

$$p^n \ = \ m \ + \sum_{g \in G - Z(G)} p^{n - n_h}$$

De esto se infiere que p divide a m.

52. Sea p un entero primo. Demuestre que todo grupo de orden p^2 es abeliano.

Solución. Sabemos que $|Z(G)| \geq p$. Sea $g \in Z(G)$; si $o(g) = p^2$ entonces G es cíclico. Si $o(g) = p$, sea $h \notin \langle g \rangle$, $o(h) = p$; como p es primo, necesariamente $\langle g \rangle \cap \langle h \rangle = \{1_G\}$. De todo ello se infiere que $G = \langle g \rangle \langle h \rangle$ (¿porqué?), luego G es abeliano.

Otra demostración de esto, la encuentra en el libro Algebra Abstracta de Herstein.

53. Sean $(G, \cdot)$ un grupo, $g \in G$ y $h = g^k$. Si $o(g) = n$ y $d = mcd(n, k)$ entonces $o(h) = \dfrac{n}{d}$.

Es claro que los enteros $\dfrac{k}{d}$ y $\dfrac{n}{d}$ son primos entre sí.

Solución. Pongamos $o(h) = m$. De $1_G = h^m = g^{km}$ se infiere que $n \mid km$ y por tanto que $\dfrac{n}{d} \mid \dfrac{k}{d}m$; ahora bien como $\dfrac{k}{d}$ y $\dfrac{n}{d}$ son primos entre sí deducimos que $\dfrac{n}{d} \mid m$. Por otro lado, tenemos que $h^{\frac{n}{d}} = (g^k)^{\frac{n}{d}} = (g^n)^{\frac{k}{d}} = 1_G$ de donde resulta que $m \mid \dfrac{n}{d}$. Hemos establecido que $m = \dfrac{n}{d}$.

54. Sean G un grupo y g, h elementos de G tales que $gh = hg$, $o(g) = n, o(h) = m$ y $mcd(n, m) = 1$. Entonces se tiene que $o(gh) = nm$.

Solución. Como $(gh)^{nm} = (g^n)^m (h^m)^n = 1$ entonces $o(gh) \mid nm$. Por otro lado, dado que $mcd(n, m) = 1$ existen $r, s \in \mathbb{Z}$ tales que $rn + sm = 1$; así las cosas, $g = gh^{sm} = g^{rn+sm}h^{sm} = (gh)^{sm}$ de donde $g \in \langle gh \rangle$ y por tanto $n \mid o(gh)$; de la misma manera, $h \in \langle gh \rangle$ y $m \mid o(gh)$.

Como n y m son primos entre sí, $nm \mid o(gh)$; luego $o(gh) = nm$.

55. Sean $(G, \cdot)$ un grupo abeliano finito y $g \in G$ un elemento de orden máximo. Entonces para todo $h \in G$ se tiene que $o(h) \mid o(g)$.

Solución. Pongamos $o(g) = n$ y $o(h) = m$. Supongamos que m no divide a n : en tal caso existe una potencia de un primo p en la descomposición de m que no aparece o aparece con un exponente menor en la

descomposición de n : escribamos $n = us$ y $m = vr$ con $u = p^j,\ v = p^k$ donde $0 \leq j < k$.

Por las proposiciones anteriores se tiene: $o(g^u) = s$ y $o(h^r) = v$ y, como además $mcd(s, v) = 1$, el orden de $g^u h^r$ es sv lo que es superior a n, contradiciendo así la maximalidad del orden de g.

Morfismos

56. Sean G, H dos grupos y $f : G \to H$ una función. Demuestre que si para todo $x, y \in G$ se tiene $f(xy) = f(x)f(y)$ entonces f es un morfismo.

    Solución. De $f(x^2) = f(x)^2$ se infiere que $f(1_G) = 1_H$.

57. Establezca todos los morfismos entre: $(\mathbb{Z}, +)$ y $(\mathbb{Z}, +)$; $(\mathbb{Z}, +)$ y $(\mathbb{Z}_5, +)$; $(\mathbb{Z}_3, +)$ y $(\mathbb{Z}_6, +)$; $(\mathbb{Z}_3, +)$ y $(\mathbb{Z}_5, +)$; $(\mathbb{Z}_8, +)$ y $(\mathbb{Z}_4, +)$; $(\mathbb{Z}_4, +)$ y $(\mathbb{Z}_8, +)$.

    Solución. Como en todos estos casos $f(m) = mf(1)$, se trata de definir $f(1)$ de manera de no producir contradicciones (por ejemplo, no puede resultar que $f(0) \neq 0$); denotamos f_n: $f_n(1) = n$. Sin dificultad se establece que $End(\mathbb{Z}) = \{f_n\ ;\ n \in \mathbb{Z}\}$, grupo que es trivialmente isomorfo a $(\mathbb{Z}, +)$. Fácil es establecer que $Hom(\mathbb{Z}, \mathbb{Z}_n) = \{f_n\ ;\ n \in \mathbb{N}\}$. Sin embargo, usted puede constatar que $Hom(\mathbb{Z}_3, \mathbb{Z}_5) = \{f_0\}$, como también que $Hom(\mathbb{Z}_3, \mathbb{Z}_6) = \{f_n\ ;\ n = 0, 2, 4\}$.

58. Establezca los automorfismos de los grupos siguientes:

$$(\mathbb{Z}, +); (\mathbb{Z}_4, +); (\mathbb{Z}_5, +); (\mathbb{Z}_6, +); (\mathbb{Z}_2^2, +); (\mathbb{Z}_2 \times \mathbb{Z}_4, +).$$

    Solución. De lo que se trata aquí es de determinar en cada caso los conjuntos generadores de estos grupos monógenos y enviar el 1 sobre un generador (¿porqué?).

    Así las cosas, $Aut(\mathbb{Z}) = \{f_n\ ;\ n = 1, -1\}$, $Aut(\mathbb{Z}_4) = \{f_n\ ;\ n = 1, 3\}$, $Aut(\mathbb{Z}_6) = \{f_n\ ;\ n = 1, 5\}$. ¿Puede usted generalizar, es decir, determinar el grupo de automorfismos de $\mathbb{Z}_m$?

59. Sabemos que los conjuntos $\mathbb{Z}$ y $\mathbb{Z} \times \mathbb{Z}$ son equipotentes (es decir, que existe una biyección entre ellos). ¿ Cree usted que los grupos aditivos $\mathbb{Z}$ y $\mathbb{Z} \times \mathbb{Z}$ son isomorfos? Argumente su respuesta.

Solución. Los grupos $(\mathbb{Z},+)$ y $(\mathbb{Z}\times\mathbb{Z},+)$ no son isomorfos, pues el primero es monógeno y en cambio el segundo es engendrado por dos elementos (por ejemplo: $(1,0)$ y $(0,1)$ entre otros).

60. Si p y q son primos entre si, demuestre que los grupos aditivos $\mathbb{Z}_{pq}$ y $\mathbb{Z}_p\times\mathbb{Z}_q$ son isomorfos.

    Solución. Sabemos que dado un grupo G y $g,h\in G$ tales que $gh=hg$, $o(g),o(h)<\infty$ y $\langle g\rangle\cap\langle h\rangle=\{1_G\}$, entonces $o(gh)=mcm(o(g),o(h))$. Aplicando esto a $(1,1)=(1,0)+(0,1)$ y teniendo en cuenta de la hipótesis se concluye que $o((1,1))=pq$, luego $\mathbb{Z}_p\times\mathbb{Z}_q$ es cíclico.

61. Sea G un grupo. Para todo $x\in G$ se define la aplicación $i_x:G\to G$ de la manera siguiente: $i_x(g)=x^{-1}gx$.

    a) Demuestre que para todo $x\in G$, $i_x\in Aut(G)$ (estas aplicaciones se llaman automorfismos interiores de G; usted puede demostrar que un subgrupo es normal si y solo si es invariante para todo automorfismo interior).

    b) Sea $Int(G)=\{i_x : x\in G\}$. Demuestre que $Int(G)$ es un subgrupo normal de $Aut(G)$.

    c) Demuestre que los grupos $Int(G)$ y $G/Z(G)$ son isomorfos. El isomorfismo que debe establecerse entre estos grupos es canónico, es decir, el mas natural.

    Solución. De $x^{-1}ghx=x^{-1}gxx^{-1}hx$ sale la multiplicatividad de i_x, lo que establece (a). En cuanto a (b), es inmediato que $i_{1_G}=Id_G$ y que $i_x\circ i_x=i_{xy}$; además, si $f\in Aut(G)$, se tiene $f\circ i_x\circ f^{-1}=i_{f(x)}$ y por tanto $Int(G)$ es un subgrupo normal de $Aut(G)$. Para terminar, la aplicación $\varphi:Int(G)\to G/Z(G)$, $\varphi(i_x)=xZ(G)$ es por construción un morfismo sobreyectivo de grupos; la inyectividad de φ sale de lo siguiente: si $i_x\in Ker(\varphi)$ entonces $x\in Z(G)$ por lo que para todo $g\in G$ se tiene $gx=xg$, es decir $i_x=Id_G$.

62. Sea G un grupo finito.

    Demuestre que $Aut(G)=\{Id_G\}$ si y sólo si $|G|=1,2$.

    Solución. Bajo tal hipótesis, G es conmutativo pues en caso contrario si existiesen $x,y\in G$ tales que $xy\neq yx$, el automorfismo interior asociado a x, definido por $i_x(g)=xgx^{-1}$, sería distinto de Id.

Como G es conmutativo, la función $f(x) = x^{-1}$ es un automorfismo; luego, dada la hipótesis, $f = Id$, y por tanto $x^2 = 1_G$ para todo $x \in G$.

En tal situación, sabemos que G es isomorfo a $\mathbb{Z}_2^n$ para cierto $n \in \mathbb{N}$.

Ahora bien, necesariamente $n \leq 1$: en efecto, en caso contrario la aplicación $G \to G$, definida por $(x_1, x_2, .., x_n) \to (x_2, x_1, .., x_n)$, nos brinda un automorfismo distinto de la identidad.

63. Sea G un grupo tal que $Z(G) = \{1_G\}$.

Demuestre que entonces se tiene $Z(Aut(G)) = \{Id_G\}$.

Solución. La aplicación $\iota : (G, \cdot) \to (Int(G), \circ)$, $\iota(x) = i_x$ es un morfismo sobreyectivo (por construcción) de grupos y $Ker(\iota) = Z(G)$. Bajo la hipótesis propuesta, tal aplicación es biyectiva (*).

Sea $f \in Z(Aut(G)$: entonces, para todo $x \in G$ se tiene : $f \circ i_x = i_x \circ f$.

Luego, si $g \in G$, entonces $f(x)f(g)f(x)^{-1} = xf(g)x^{-1}$, esto significa que los automorfismos interiores $i_{f(x)}$ y i_x coinciden sobre $f(g)$ para todo $g \in G$.

Como f es biyectiva, $i_{f(x)} = i_x$, de donde, por (*), $f(x) = x$.

64. Sea G un grupo finito y $f \in Aut(G)$, una involución con un único punto fijo (es decir, $f^2 = Id$ y $|Fix(f)| = 1$).

Demuestre que $f(x) = x^{-1}$ y deduzca que G es abeliano.

Solución. No es difícil establecer que $f(x^{-1}f(x)) = (x^{-1}f(x))^{-1}$; luego, si demostramos que $\psi(x) = x^{-1}f(x)$ es biyectiva, el ejercicio queda resuelto (¿porqué?).

Ahora bien, como G es finito basta demostrar que tal función es inyectiva: si se tiene $\psi(x) = \psi(y)$ se infiere sin dificultad que xy^{-1} es un punto fijo de f. Luego, necesariamente, $xy^{-1} = 1_G$.

El Grupo Simétrico

65. Demuestre que si $n \geq 3$ entonces $Z(S_n) = \{Id\}$.

Solución. Para todo $1 \leq k \leq n$, sea θ_k una permutación tal que $Fix(\theta_k) = \{k\}$ (la existencia de θ_k está asegurada por la condición de que $n \geq 3$ ¿porqué?). Si $\sigma \in Z(S_n)$ se tiene: $(\theta_k \circ \sigma)(k) = (\sigma \circ \theta_k)(k)$ de donde se obtiene que $\theta_k(\sigma(k)) = \sigma(k)$.

66. La aplicación $sg : S_n \to \{1, -1\}$, $\sigma \mapsto sg(\sigma)$, es un morfismo de grupos.

Solución. Sean σ y θ dos permutaciones con descomposiciones en producto de transposiciones: $\sigma = \tau_1\tau_2\cdots\tau_s$ y $\theta = \rho_1\rho_2\cdots\rho_r$.

Entonces $\sigma\theta = \tau_1\tau_2\cdots\tau_s\rho_1\rho_2\cdots\rho_r$; ahora bien, esta escritura puede ser modificada en la medida que haya simplificación en el centro del producto, es decir, en el caso que $\tau_s = \rho_1$ y, si ello ocurre, la simplificación podrá continuar si $\tau_{s-1} = \rho_2$ y así sucesivamente.

Sea cual sea la situación, el proceso de simplificación elimina pares de transposiciones por lo que el número final de transposiciones que expliciten el producto $\sigma\theta$ será del tipo $s + r - 2q$, que obviamente tiene la misma paridad que $s + r$.

Luego $sg(\sigma)sg(\theta) = (-1)^{s+r} = (-1)^{s+r-2q} = sg(\sigma\theta)$, lo que establece el enunciado.

67. Determine los grupos simétricos y alternos que son abelianos.

Solución. Por lo anterior, S_n es abeliano si $n \leq 2$. En cuanto a los grupos A_n, se requiere que $n \leq 3$ ya que $|A_3| = 3$ y si $n \geq 4$, siempre se puede construir dos permutaciones pares que no conmutan (hágalo).

68. Determine la paridad de una permutación de orden 14 sobre 10 letras.

Solución. Sea σ esa permutación. Sabemos que σ se descompone de manera única en producto de ciclos disjuntos c_i (por tanto conmutables) y que $o(\sigma) = mcm(o(c_i))$. Esto nos dice que los ordenes posibles de los ciclos en cuestión son 2 y 7 (¿porqué se excluye 14?); de esta manera σ sólo puede ser producto de un ciclo de orden 7 y un ciclo de orden 2, por lo que la permutación es impar.

69. Estudie la existencia de una permutación σ tal que:

(a) $\sigma(1,2)\sigma^{-1} = (1,3)$. (b) $\sigma(1,2)\sigma^{-1} = (1,2,3)$.

(c) $\sigma(1,2,3)\sigma^{-1} = (4,5,6)$. (d) $\sigma(1,2,3)\sigma^{-1} = (1,2,4)(5,6,7)$.

(e) $\sigma(1,2) = (1,2,3,4)\sigma$. (f) $(1,2)\sigma = \sigma(1,3)(2,4)$.

Solución. Nótese primero, que si $\alpha \in S_n$, en general se tiene:

$$sg(\sigma\alpha\sigma^{-1}) = sg(\alpha) \quad y \quad \left|Fix(\sigma\alpha\sigma^{-1})\right| = |Fix(\alpha)| \quad (\text{¿porqué?}).$$

Con esto podemos decir que las ecuaciones propuestas en (b), (d), (e) y (f) no tienen solución. En cuanto al resto, las soluciones de (a) son todas las permutaciones que dejen fijo al 1 e intercambien 2 y 3.

70. Si α, β y γ son transposiciones, pruebe que $\alpha\beta\gamma \neq Id$.

Solución. $\alpha\beta\gamma$ es una permutación impar.

71. Demuestre que toda permutación par puede expresarse como composición de ciclos de largo 3.

Solución. Basta demostrar el enunciado para el producto de dos transposiciones (¿porqué). En tal caso se tienen dos posibilidades:

$(a,b)(b,c) = (a,b,c)$ y $(a,b)(c,d) = (a,b,c)(b,c,d)$.

72. Demuestre que los siguientes conjuntos de permutaciones generan S_n :

a) $\{(1,2,3,...,n-1),\ (n-1,n)\}$.

b) $\{(1,2),\ (2,3),\ (3,4),...,\ (n-1,n)\}$.

Solución. Como $(1,2)(2,3)(3,4)...(n-2,n-1) = (1,2,3,...,n-1)$, basta demostrar la pregunta (a).

Para lo que sigue, recordemos que: $(1,2,..,n-1)^{-1} = (n-1,..,2,1)$. Por otro lado, para todo $1 \leq k \leq n-1$ no es difícil verificar que se tiene $(n-1-k,n) = (n-1,n-2,...,2,1)^k(n-1,n)(1,2,3,...,n-1)^k$. Esto quiere decir que podemos construir todas las transposiciones del tipo (m,n) con $m < n$. Finalmente, un rápido cómputo nos brinda que $(p,q) = (p,n)(q,n)(p,n)$. De esta manera obtenemos todas las transposiciones posibles.

73. Demuestre que todo elemento de A_n puede expresarse como producto de ciclos de orden n.

Solución. Se tiene:

$(a,b,c) = (a,c,b,x_4,...,x_{n-1},x_n)(x_n,x_{n-1},..,x_4,b,a,c)$. Por otro lado, sabemos que toda permutación par es producto de ciclos de largo 3.

74. Encuentre representaciones eficientes de los grupos:

(a) grupo de Klein (b) $\mathbb{Z}_6$ (c) $\mathbb{Z}_2 \times \mathbb{Z}_4$ (d) $\mathbb{Z}_4 \times \mathbb{Z}_6$.

(e) el grupo de transformaciones del cuadrado.

Solución. La aplicación $\mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$. $1 \to (1,2)$, es un isomorfismo. Por otro lado, si $\tau, \gamma \in S_5$, son disjuntos y de órdenes respectivos 2 y 3, la aplicación $\mathbb{Z}_2 \times \mathbb{Z}_3 \to S_5$, $(1,2) \to \tau\gamma$, es un monomorfismo. Luego, se concluye que $\mathbb{Z}_6 \cong \langle \tau, \gamma \rangle \subset S_5$.

Anillos y Cuerpos

75. Sea $n \in \mathbb{N} - \mathbb{P}$, $n \neq 0, 1$. Demuestre que n se descompone de manera única: $n = p_1^{n_1} p_2^{n_{21}} ... p_k^{n_k}$, donde $p_1 < p_2 < .. < p_k$ son números primos.

Solución. Supongamos la proposición válida para los enteros menores que n y sea p_1 el menor número primo que divide a n; en tal caso tenemos $n = p_1^{n_1} q$ donde q no es múltiplo p_1. Como $q < n$, por hipótesis de recurrencia se tiene $q = p_2^{n_{21}} ... p_k^{n_k}$.

76. Sea $n, m \in \mathbb{N}$ y $p \in \mathbb{P}$. Entonces n y m no son múltiplos de p si y solamente si nm tampoco lo es.

Solución. Es claro que en la descomposición en números primos de estos enteros no aparece el primo p; esto es equivalente a decir que p no aparece en la descomposición del producto nm.

77. Demuestre que todo cuerpo es un anillo íntegro y que todo anillo íntegro y finito es un cuerpo.

Solución. Lo primero es inmediato. En cuanto a la última parte como A es íntegro y finito, para todo $a \in A^*$, la aplicación l_a es biyectiva, lo que nos garantiza la existencia de un inverso derecho para a.

78. Demuestre que $\mathbb{Z}_p$ es un cuerpo si y solo si p es primo.

Solución. La primera implicación no presenta mayor dificultad. Recíprocamente, si p es primo y $0 < r, s < p$, es claro que rs no es múltiplo de p. Pasando al cociente, se infiere de esto que $\mathbb{Z}_p$ es íntegro.

79. Sea p un número primo. En $\mathbb{Z}_p$ demuestre que para todo $x \neq 0$ se tiene $x^{p-1} = 1$; concluya que $a^p = a$ para todo $a \in \mathbb{Z}_p$. En $\mathbb{Z}_{2p}$ resuelva la ecuación $x^2 = x$.

Solución. Es claro que la identidad se cumple si $x = 0$; por otro lado, como $\mathbb{Z}_p^*$ es un grupo multiplicativo de orden $p-1$, para todo $x \neq 0$ se tiene $x^{p-1} = 1$.

En cuanto a la segunda pregunta, 0 y 1 son soluciones triviales sea cual sea el número primo p.

Antes de entrar al caso general, estamos obligados de estudiar la situación cuando $p = 2$, es decir en $\mathbb{Z}_4$: aquí también las únicas soluciones son las triviales.

Sea ahora $p > 2$; suponiendo que no se presta a confusión, denotaremos por el mismo símbolo al entero y a su clase en el anillo cociente y escojamos el representante de la clase de manera conveniente, es decir, $0 \leq x \leq 2p-1$. En $\mathbb{Z}$ la identidad implica que $x(x-1)$ es un múltiplo de $2p$. Como $x(x-1)$ es un número par, concluimos que $x(x-1)$ es divisible por p. Como p es primo, deducimos que x o $x-1$ son múltiplos de p; ahora bien, dada la elección de x no queda otra posibilidad que tengamos $x = p$ o $x - 1 = p$.

Concluimos que las soluciones generales de la ecuación $x^2 = x$ en $\mathbb{Z}_{2p}$ son 0, 1, p y $p+1$.

80. Sea A un anillo. Un elemento $a \in A$ es nilpòtente si existe $n \in \mathbb{N}$ tal que $a^n = 0$.

   a) Determine los nilpotentes de A si este es un anillo íntegro.

   b) Demostrar que si a es nilpotente, entonces para todo y $k \in \mathbb{N}^*$, $1 \pm a^k$.es invertible.

   c) Sean $a, b \in A$. Demuestre que si ab es nilpotente también lo es ba.

   d) Sean $a, b \in A$ tales que $ab = ba$. Demuestre que si a y b son nilpotentes, también lo son $a + b$ y ab.

   e) De dos ejemplos, conceptualmente distintos, de anillos con nilpotentes no triviales.

Solución. Si a es nilpotente es claro que $-a$ y a^k tambien lo son. Basta entonces demostrar que $1-a$ es invertible; ello se deduce de la igualdad $1 - a^m = (1-a)(1 + a + a^2 + ... + a^{m-1})$, $m \in \mathbb{N}^*$. En cuanto a (c), basta notar que $(ba)^{n+1} = b(ab)^n a$. Respecto de la segunda parte de la

pregunta (d), constate que si $a^n = b^m = 0$ entonces $(a+b)^{n+m} = 0$. Finalmente, entre los ejemplos de anillos con nilpotentes no triviales podemos exhibir $\mathbb{Z}_m$ con $m \notin \mathbb{P}$ y $M_n(\mathbb{R})$ con $n > 1$.

81. Sea A un anillo tal que para todo $a \in A$ se tiene $a^2 = a$. Demuestre que A es conmutativo. Caracterice el anillo A cuando este es íntegro.

Solución. Es inmediato que $x = -x$ para todo $x \in A$. Además, de $(a+b)^2 = a+b$ se infiere que $ab = -ba$.

82. Determine todas las funciones aditivas y multiplicativas de $\mathbb{R}$ en $\mathbb{R}$, es decir, cuales son las funciones $f : \mathbb{R} \to \mathbb{R}$ tales que:

$$f(x+y) = f(x) + f(y), f(xy) = f(x)f(y) \text{ para todo } x, y \in \mathbb{R}.$$

Solución. Dado que la aplicación nula cumple con las condiciones demandadas, suponemos por tanto que f no es nula.

Como f es aditiva, de $f(0) = f(0+0)$ deducimos que $f(0) = 0$; por otro lado, como f es multiplicativa, se tiene $f(1) = f(1^2) = f(1)^2$ de donde inferimos que $f(1) = 0, 1$; ahora bien, como $f(x) = f(1 \cdot x) = f(1) \cdot f(x)$, obligadamente $f(1) = 1$ ya que si no la aplicación sería nula. Por otro lado, dado que $f(n+1) = f(n) + f(1) = f(n) + 1$, recursivamente se establece que $f(n) = n$ para todo $n \in \mathbb{N}$.

Además, de $0 = f(1 + (-1))$ deducimos que $f(-1) = -1$ y por tanto podemos extender sobre $\mathbb{Z}$ la acción de f como aplicación identidad ya que $f(-n) = f((-1) \cdot n) = -n$.

En cuanto a la acción de f sobre $\mathbb{Q}$, de $1 = f(n \cdot \frac{1}{n})$ sale que $f(\frac{1}{n}) = \frac{1}{n}$; aplicando esto logramos: $f(\frac{m}{n}) = f(m \cdot \frac{1}{n}) = \frac{m}{n}$.

Hasta aquí hemos demostrado que la restricción de f a $\mathbb{Q}$ es la identidad.

Queda por tanto demostrar que ocurre lo mismo sobre el conjunto de los irracionales.

Veamos primero que f es creciente: se trata de demostrar que si $y \leq w$ entonces $f(y) \leq f(w)$; sin embargo, como f es aditiva, esto se puede reescribir como sigue: si $0 \leq w - y$ entonces $0 \leq f(w-y)$ lo que en definitiva nos dice que f será creciente si cada vez que $0 \leq x$ entonces

$0 \leq f(x)$. Ahora bien, como x es no negativo, se tiene $x = (\sqrt{x})^2$, luego $f(x) = f((\sqrt{x})^2) = f((\sqrt{x}))^2 \geq 0$.

Estamos en condiciones de estudiar la acción de f sobre los irracionales: sea u un irracional y supongamos que $u \neq f(u)$. Sin perdida de generalidad, podemos suponer que $u < f(u)$; sabemos que dados dos reales distintos, siempre podemos encontrar un racional entre ellos: sea por tanto $r \in \mathbb{Q}$ tal que $u < r < f(u)$; como f es creciente tenemos $f(u) < f(r) = r$ lo que es una contradicción (es claro que el caso $f(u) < u$ produce la misma contradicción). Obligadamente $f(u) = u$ y por tanto $f = Id$.

83. Determine los morfismos de cuerpo, $f : \mathbb{C} \to \mathbb{C}$, que dejan invariante a $\mathbb{R}$ (es decir, $f(\mathbb{R}) \subset \mathbb{R}$).

Solución. Por lo anterior y dada la hipótesis, si $z = a + bi$ es un número complejo, $f(z) = a + bf(i)$ con $f(i)^2 = -1$. Puesto que esta última identidad compleja nos lleva a que $f(i) = \pm i$, concluimos que $f(z) = z$ o $f(z) = \overline{z}$. es decir que f es la identidad o la conjugación.

84. En $\mathbb{Z}$ se define: (suma) $a \oplus b = a+b+1$ y (producto) $a \otimes b = a+b+ab$. Demuestre que $(\mathbb{Z}, \oplus, \otimes)$ es un anillo conmutativo, íntegro y principal.

Solución. No presenta dificultad establecer que $0_{\oplus} = -1$ y $1_{\otimes} = 0$. La función más simple y evidente que preserva los neutros en cuestión es $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}, \oplus, \otimes)$ definida por $f(a) = a - 1$, la cual es trivialmente biyectiva. Ahora bien, se tiene :

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

$$f(a) \otimes f(b) = (a-1) + (b-1) + (a-1)(b-1) = ab - 1 = f(ab)$$

Luego esta aplicación es un transporte biyectivo de estructura entre $(\mathbb{Z}, +, \cdot)$ y $(\mathbb{Z}, \oplus, \otimes)$; concluimos que $(\mathbb{Z}, \oplus, \otimes)$ es indistinguible de $(\mathbb{Z}, +, \cdot)$ y por tanto es un anillo conmutativo, íntegro y principal

Que duda cabe que observar y reflexionar es mejor (y más provechoso en cuanto a modelar el espíritu) que el método aburrido y carretero de testear propiedades.

85. Sea $(E, +, \cdot)$ una estructura tal que: $(E, +)$ es un grupo abeliano y el producto " $\cdot$ " es asociativo, conmutativo y se distribuye con respecto a la suma.

86. Además, esta estructura cumple con la siguiente propiedad:

Existe un único $u \in E$ *tal que* $u + x - ux \neq 0$ *para todo* $x \in E$.

Demuestre que:

a) El elemento u es el neutro multiplicativo.

b) Para todo $a \neq u$ existe b tal que $(u - a)(u - b) = u$.

c) Concluya que E es un cuerpo.

d) En $\mathbb{Z}$ tenemos que $3 + x - 3x \neq 0$ para todo $x \in \mathbb{Z}$. ¿Cual es su comentario?

Solución. Supongamos que u no es el neutro multiplicativo, es decir que existe un elemento $x \in E$ tal que $x \neq ux$ Esta suposición nos debe llevar a una contradicción; ahora bien, sólo podemos contradecir la propiedad axiomática dada en el enunciado y de ella no es cuestión la existencia de u (puesto que la damos por hecho al escribir $x \neq ux$): contradeciremos por tanto la unicidad. Para ello debemos construir un elemento diferente de u que cumpla con la misma propiedad algebraica; tal construcción sólo podemos hacerla a partir de nuestra suposición, es decir que se tiene $x \neq ux$.

De $x - ux \neq 0$ obtenemos $u+ x - ux \neq u$ (tenemos pues un elemento distinto de u); sea $v = u+ x - ux$ y veamos si este elemento satisface la propiedad en cuestión, es decir que para cualquier $y \in A$, se verifique que $v + y - vy \neq 0$. Para lograr esto, debemos establecer esta última identidad a través del axioma que distingue al elemento u : $v+y-vy = u+x-ux+y-(u+x-ux)y = u+(x+y+xy)-u(x+y+xy) \neq 0$. Luego v cumpliría la propiedad, lo que contradice la unicidad exigida.

Se establece, por tanto que u es el neutro multiplicativo.

Sea ahora $a \neq u$ y supongamos que lo demandado no se cumple, es decir que para todo $b \in E$ se tiene $(u - a)(u - b) \neq u$; si desarrollamos la multiplicación (sabiendo que u es el neutro multiplicativo) logramos $a+b-ab \neq 0$. Así, el elemento $a \neq u$ también cumpliría con la propiedad axiomática de u, lo que es una contradicción.

Existe pues $b \in E$ tal que $(u - a)(u - b) = u$.

La tercera afirmación sale sin problemas puesto que si $x \neq 0$ basta tomar $a = u - x$ (que esun elemento distinto de u) y aplicar el resultado anterior: $(u-a)(u-b) = x(u-b) = u$, por lo que x tiene inverso.

Por último, es inmediato que para todo $x \in \mathbb{Z}$ tenemos: $n + x - nx \neq 0$ para todo $n > 2$. Es decir, en este caso la unicidad no se cumple.

87. Sean A un anillo y $a, \in A$. Si existe un único $b \in A$ tal que $ab = 1$ demuestre que $ba = 1$.

Solución. Como $ab = 1$ se tiene $aba = a$; luego $a(b + ba - 1) = 1$, de donde, por hipótesis, $b = b + ba - 1$.

88. Sean A un anillo no conmutativo y $a, b \in A$ tales que $1-ab$ es invertible, es decir existe $c \in A$ que verifica: $c(1-ab) = (1-ab)c = 1$.

    a) Demuestre que $1 - ba$ es invertible, es decir que existe $d \in A$ tal que: $d(1-ba) = (1-ba)d = 1$.

    b) Si no logró hacer la pregunta anterior, compruebe que $d = 1 + bca$. ¿A que elemento corresponde $1 + adb$?

Solución Como se tiene $c(1-ab) = 1$, hacemos aparecer el término "ba" multiplicando por b (a la izquierda) y por a (a la derecha); luego debemos recuperar el "1", lo que hacemos sumándolo a ambos lados de la igualdad. Así obtenemos $1 - ba + bca - bcaba = 1$, de donde $(1 + bca)(1 - ba) = 1$.

Para establecer que $(1-ba)(1+bca) = 1$ basta realizar el mismo proceso a partir de la otra igualdad, es decir de $(1-ab)c = 1$.

Con respecto a la pregunta (b), hacemos notar que de la hipótesis se infiere que $abc = cab = c - 1$, con lo que la primera parte sale sin problemas a partir de un pequeño cálculo.

En cuanto a la segunda, se tiene:

$$1 + adb = 1 + a(1 + bca)b = 1 + ab + abcab =$$

$$1 + ab + (c-1)ab = 1 + cab = c$$

89. Consideremos el anillo de matrices cuadradas con coeficientes en el cuerpo $\mathbb{Z}_3$. Sea $A \subset M_2(\mathbb{Z}_3)$ el conjunto formado por todas las matrices del tipo $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

a) Demuestre que A es un sub-cuerpo de $M_2(\mathbb{Z}_3)$.

b) Demuestre que $(A^*, \cdot)$ es un grupo cíclico.

Solución. Como sabemos que $M_2(\mathbb{Z}_3)$ es un anillo, y A contiene por definición a los neutros (aditivo y multiplicativo), respecto de la estructura de anillo de A basta por tanto comprobar que tal conjnunto es estable para las operaciones de suma y producto. Esto es casi inmediato; en efecto si definimos:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

notemos que $J^2 = -I$.

Como todo elemento de A es de la forma $aI + bJ$, tenemos:

$$\begin{aligned} (aI + bJ) + (cI + dJ) &= (a + c)I + (b + d)J \\ (aI + bJ)(cI + dJ) &= (ac - bd)I + (ad + bc)J \end{aligned}$$

Ahora bien, como A es finito, basta demostrar que es íntegro para establecer que es un cuerpo. Para ello hay que resolver el sistema:

$$\begin{cases} ax - by = 0 \\ bx + ay = 0 \end{cases}$$

bajo la condición de que a y/o b sean no nulos.

Como operamos con elementos de $\mathbb{Z}_3$ (es decir, $3 = 0$ y $\forall\, x \neq 0$, $x^2 = 1$) se tiene:

$$det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 = \begin{cases} 1 & \text{si} \quad ab = 0 \\ 2 & \text{si} \quad ab \neq 0 \end{cases}$$

El sistema es por tanto de Cramer, con solución única $x = y = 0$, lo que demuestra que A es íntegro.

Antes de entrar en la segunda pregunta de este ejercicio, observemos que la aplicación definida por:

$$f : \mathbb{Z}_3^2 \to A, \quad f((a,b)) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

es una biyección (compruébelo) por lo que el conjunto A tiene 9 elementos.

El grupo multiplicativo $(A^*, \cdot)$ tiene por tanto 8 elementos, por lo que el orden de cualquier elemento es un divisor de 8.

Si, consideramos el elemento $T = aI + bJ$ con $a, b \in \mathbb{Z}_3^*$, dada la forma de la multiplicación arriba explicitada se tiene $T^2 = 2abJ$, luego $T^4 = -I$ y por último $T^8 = I$, lo que muetra que $(A^*, \cdot)$ es un grupo cíclico.

90. Sea $(A, +, \cdot)$ un anillo conmutativo y I, J ideales de A. Demuestre que:

    a) $I \cap J$ y $I + J$ son ideales de A.

    b) Si $IJ = \langle \{ij;\ i \in I,\ j \in J\} \rangle$ demuestre que $IJ \subset I \cap J$ y que si $A = I + J$ entonces $IJ = I \cap J$.

    Solución. Hagamos (b): que $IJ \subset I \cap J$ no presenta dificultad. Si suponemos que $A = I + J$, entonces existen $i \in I$ y $j \in J$ tales que $1_A = i + j$; luego, si $x \in I \cap J$ se tiene: $x = ix + xj \in IJ$.

91. Sea $(A, +, \cdot)$ un anillo conmutativo, J un ideal de A y $\pi : A \to A/J$ la proyección canónica. Demuestre que si I es un ideal de A/J entonces $\pi^{-1}(I)$ es un ideal de A que contiene J.

    Solución. En general, la imagen recíproca de un ideal por un morfismo es un ideal (demuéstrelo) y en particular, el núcleo de tal morfismo. Respecto del ejercicio, la primera afirmación dice que $\pi^{-1}(I)$ es un ideal de A y la segunda que $J \subset \pi^{-1}(I)$.

92. Sea $(A, +, \cdot)$ un anillo conmutativo y P, M ideales de A. Demuestre que:

    a) P es primo si y solo si A/P es un anillo íntegro.

    b) M es maximal si y solo si A/M es un cuerpo. Deduzca que todo ideal maximal es primo.

Solución. Se tienen las equivalencias siguientes:

P es primo $\Leftrightarrow$ si $xy \in P$ entonces $x \in P$ o $y \in P \Leftrightarrow$ si $\overline{xy} = \overline{x}\,\overline{y} = \overline{0}$ entonces $\overline{x} = \overline{0}$ o $\overline{y} = \overline{0} \Leftrightarrow A/P$ es íntegro. Esto prueba la primera afirmación.

M es maximal $\Leftrightarrow$ si $u \in A - M$ entonces existen $a \in A$ y $m \in M$, $1_A = au + m \Leftrightarrow$ si $\overline{u} \neq \overline{0}$, entonces existe $a \in A$, $\overline{1_A} = \overline{a}\,\overline{u} \Leftrightarrow A/M$ es un cuerpo. Esto prueba la segunda afirmación.

Por último, como todo cuerpo es un anillo íntegro, se infiere que todo ideal maximal es primo.

93. Determine los ideales del anillo $\mathbb{Z}$. Caracterize los ideales primos y maximales.

Solución. Es inmediato que para todo $n \in N$ los conjuntos $n\mathbb{Z}$ son ideales de $\mathbb{Z}$. Vamos a demostrar que todos los ideales tienen esa forma; dicho de otra manera, que $\mathbb{Z}$ es un anillo principal.

Sea I un ideal de $\mathbb{Z}$; si I es el ideal nulo no nada que demostrar.

Si $I \neq \{0\}$, sean $n = min(I^+)$ y $x \in I$; sabemos que podemos escribir $x = qn + r$ con $0 \leq r < n$. De esto resulta que $r = x - qn \in I$ (¿porqué?); luego, dada la condición de minimalidad de la elección de n, necesariamente $r = 0$. Hemos establecido así que $I = n\mathbb{Z}$.

Para terminar, concluimos que en $\mathbb{Z}$ los ideales primos son maximales, pues sabemos que $\mathbb{Z}/n\mathbb{Z}$ es íntegro (equivalente a cuerpo dado que es finito) si y solamente si n es primo.

94. Sean $p, q \in \mathbb{N}$; demuestre que:

   a) $p\mathbb{Z} \cap q\mathbb{Z} = mcm(p,q)\mathbb{Z}$ y $p\mathbb{Z} + q\mathbb{Z} = mcd(p,q)\mathbb{Z}$.

   b) Si p y y q son primos entre sí, existen $r, s \in \mathbb{Z}$ tales que $pr + qs = 1$.

   c) Utilice lo anterior para demostrar que si p es primo:

      1) Si $p \mid qt$ y $p \nmid q$ entonces $p \mid t$.
      2) $\mathbb{Z}_p$ es un cuerpo.

Solución. Es claro que $p\mathbb{Z} \cap q\mathbb{Z}$ es un ideal y está formado por los múltiplos comunes de p y q; sabemos además que existe $n \in \mathbb{N}$ tal

que $p\mathbb{Z} \cap q\mathbb{Z} = n\mathbb{Z}$, donde n es el menor positivo del ideal: luego, $n = mcm(p, q)$.

Por otro lado, sea $m \in \mathbb{N}$ tal que $p\mathbb{Z} + q\mathbb{Z} = m\mathbb{Z}$ (a); de ello se infiere que $p, q \in m\mathbb{Z}$: luego existen $l, k \in \mathbb{N}$ tales que $p = lm$ y $q = km$, es decir, m es un divisor común de p y q. Pero de (a) tambien sale que $m \in p\mathbb{Z} + q\mathbb{Z}$: luego existen $r, s \in \mathbb{Z}$, $m = rp + sq$ (b). Sea $d \in \mathbb{Z}$ otro divisor de p y q : existen, entonces $t, u \in \mathbb{Z}$ tales que $p = td$ y $q = ud$; reemplazando esto en (b) se obtiene $m = (rt + su)d$, es decir, que m es múltiplo de d. Luego, $m = mcd(p, q)$.

La segunda pregunta es inmediata: en efecto, si p y y q son primos entre sí, entonces $mcd(p, q) = 1$, es decir $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$.

Respecto de la tercera pregunta, esta ya fue desarrollada en ejercicios anteriores; aquí lo hacemos con nuevas técnicas, más estéticas y eficientes: sabemos que si p es primo, para todo $q \in \mathbb{Z}$, q no múltiplo de p, existen $r, s \in \mathbb{Z}$ tales que $1 = rp + sq$: por un lado esto significa que se tiene $t = rtp + sqt$, por lo que $p \mid t$; por el otro, pasando al cociente, resulta que $\overline{s}\,\overline{q} = \overline{1}$ en $\mathbb{Z}_p$, luego $\mathbb{Z}_p$ es un cuerpo.

95. Sea k un entero, $n = 2^k$. Consideremos el anillo $\mathbb{Z}_n$.

   a) Caracterice los elementos nilpotentes de $\mathbb{Z}_n$.

   b) Caracterice los elementos invertibles de $\mathbb{Z}_n$.

   c) Demuestre que el conjunto J formado por los elementos no invertibles es un ideal de $\mathbb{Z}_n$.

   d) De un argumento que pruebe que J es maximal.

Solución. Al igual que en el primer ejercicio, utilizaremos el mismo símbolo para un entero y su clase módulo n. Si $x \in \mathbb{Z}_n$ es nilpotente, entonces existe $m \in \mathbb{N}$ tal que $x^m = 0$. Esto quire decir que el entero x^m es múltiplo de $n = 2^k$ por lo que necesariamente $x = a2^b$ con $a \in \mathbb{Z}$ y $b \in \mathbb{N}^*$. Pasando al cociente se establece que los nilpotentes de $\mathbb{Z}_n$ son los elementos de la forma $a2^b$ con $a \in \{0, 1, ..., n-1\}$ y $b \in \mathbb{N}^*$.

En lo que se refiere a los invertibles, $u \in \mathbb{Z}_n$ tiene inverso si existe $v \in \mathbb{Z}_n$ tal que $uv = 1$. Si remontamos a $\mathbb{Z}$ esto quiere decir que $1 - uv$ es múltiplo de 2^k por lo que obligadamente u (y también v) es un número impar. Ahora bien, la descomposición tipo de un impar es

$u = a2^b + 1$ donde a no es divisible por 2. Esto quiere decir que los invertibles de $\mathbb{Z}_n$ son aquellos de la forma $1 - x$ con x nilpotente de $\mathbb{Z}_n$.

Los dos resultados anteriores pueden resumirse diciendo que las clases módulo n de los números pares nos dan todos los nilpotentes de $\mathbb{Z}_n$ y las clases de los números impares, los invertibles.

Si $J = \{x \in \mathbb{Z}_n \ / \ x \text{ nilpotente}\}$, dada la caracterización que acabamos de hacer, es inmediato que J es un ideal maximal.

96. Demuestre que en un anillo principal toda cadena creciente de ideales,

$$I_0 \subset I_1 \subset I_2 \subset ..... \subset I_n \subset I_{n+1} \subset ....$$

es estacionaria, es decir que existe $m \in \mathbb{N}$ tal que $I_k \subset I_m$ para todo $k \in \mathbb{N}$. En $\mathbb{Z}$ encuentre una cadena creciente de máxima longitud que comience con $2310\mathbb{Z}$; ¿cuantas de esas cadenas hay?

Solución. Es inmediato que $I = \bigcup_{n\in\mathbb{N}} I_n$ es un ideal del anillo.

Como este es principal, existe $x \in A$ tal que $(x) = I$. Como $x \in I$, existe un índice $k \in \mathbb{N}$ tal que $x \in I_k$; de esta manera, se infiere que $I = (x) \subset I_k$.

Reflexionemos sobre que nos brinda este resultado:

Si $I_k = a_k A$, las relaciones de inclusión de la cadena nos dicen que $a_0 = b_1 a_1,\ a_1 = b_2 a_2$ y así sucesivamente hasta $a_{n-1} = b_n a_n$; todo esto nos lleva a que $a_0 = b_1 b_2 \cdots b_n a_n$.

Luego, si nos ubicamos en el anillo $\mathbb{Z}$, busquemos la descomposicion en primos de 2310 (cuestión rápida pues al ojo se ve que entre sus divisores están 2, 3, 5 y 11 ¿porqué?); así las cosas, obtenemos que $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

Respondemos a la pregunta diciendo que una cadena máximal posible es $2310\ \mathbb{Z} \subset\ 2 \cdot 3 \cdot 5 \cdot 7\ \mathbb{Z} \subset\ 2 \cdot 3 \cdot 5\ \mathbb{Z} \subset\ 2 \cdot 3\ \mathbb{Z} \subset\ 2\ \mathbb{Z}$.

Obviamente que hay 5! de estas cadenas.

Definición. Sean $(A, +, \cdot)$ un anillo conmutativo y $a, b, \pi \in A^*$:

- Se dice que b divide a, y se denota $b \mid a$ si existe $c \in A$ tal que $a = bc$.

- Un elemento d es un máximo común divisor de a y b (lo que se denota un "$mcd(a,b)$") si $d \mid a$ y $d \mid b$, y si cada vez que $e \mid a$ y $e \mid b$ entonces se tiene que $e \mid d$.
- Si 1_A es un máximo común divisor de a y b se dice que a y b son primos entre sí.
- Se dice que π es un elemento primo (o irreducible) si no es invertible y si $ab = \pi$ entonces a o b es invertible.

97. Sea A un anillo íntegro. Demuestre que si d y d' son $mcd(a,b)$ entonces $d' = ud$, con u invertible.

    Solución. Por ser d y d' máximos comunes divisores de a y b se tiene $d \mid d'$ y $d' \mid d$, luego $d' = ud'$ y $d = vd$ para ciertos $u, v \in A$. Se infiere que $d = vud$ es decir $(1 - vu)d = 0$; como $d \neq 0$ y A es íntegro $vu = 1$.

98. Sea A un anillo principal (es decir A es íntegro y todo ideal de A es monógeno). Demuestre que:

    a) Existe $d = mcd(a,b)$. Si d es invertible, entonces a y b son primos entre sí.

    b) Si $a \mid bc$ y $mcd(a,b) = 1$ entonces $a \mid c$.

    c) Si π es primo y $\pi \nmid a$ entonces π y a son primos entre sí.

    d) Si π es primo y $\pi \mid ab$ entonces $\pi \mid a$ o $\pi \mid b$.

    e) El elemento π es primo si y solamente si el ideal $\langle \pi \rangle$ es primo.

    f) Todo ideal primo es máximal.

    Solución.

    a) Como el anillo A es principal, existe $d \in A$ tal que $\langle a \rangle + \langle b \rangle = \langle d \rangle$, Como en tal caso $a, b \in \langle d \rangle$ se tiene $a = ud$ y $b = vb$ con $u, v \in A$. Por otro lado, como $d \in \langle a \rangle + \langle b \rangle$ entonces existen $k, l \in A$ tales que $d = ka + lb$; luego si $e \mid a$ y $e \mid b$ es inmediato que $e \mid d$. La segunda afirmación es inmediata pues si d es invertible, $\langle d \rangle = A = \langle 1 \rangle$.

    b) Tenemos $bc = as$. Si $mcd(a,b) = 1$ entonces $1 = ka + lb$ y luego $c = (kc + ls)\, a$ lo que demuestra el enunciado.

c) Sabemos que $\pi = mcd(a,\pi)s$ y $a = mcd(a,\pi)t$. Como π es primo $mcd(a,\pi)$ o s es un invertible; si s lo fuera tendríamos $a = \pi t s^{-1}$ contradiciendo que $\pi \nmid a$. Luego $mcd(a,\pi)$ es invertible y por tanto 1 es un $mcd(a,\pi)$, es decir, a y π son primos entre sí.

d) Supongamos que $\pi \nmid a$: luego estos elementos son primos entre si y existen $k, l \in A$ tales que $1 = ka + l\pi$; se infiere que $b = kab + l\pi b$ por lo que $\pi \mid b$.

e) Demostremos que $\langle \pi \rangle$ es un ideal maximal (con lo que la afirmación (f) también quedará establecida). Sea $a \notin \langle \pi \rangle$; luego a no es múltiplo de π (es decir, $\pi \nmid a$) y existen $k, l \in A$ tales que $1 = ka + l\pi$; se infiere que $\langle \langle \pi \rangle \cup \{a\} \rangle = \langle \pi \rangle + \langle a \rangle = A$. Recíprocamente, supongamos que $\langle \pi \rangle$ es un ideal primo y que se tiene $\pi = ab$; luego a o b pertenece a $\langle \pi \rangle$. Supongamos que $a = \lambda\pi$; se tiene $\pi = \lambda\pi b$ y, como A es íntegro, se deduce que $\lambda b = 1$ y por tanto que b es invertible, lo que demuestra que π es primo.

Espacios Vectoriales

99. Sean V un espacio vectorial sobre K y $T = \{v_1, \ldots, v_n\} \subset V$.

Consideramos los conjuntos de vectores:

$$\begin{aligned} S &= \{v_1 + v_2, v_2 + v_3, \ldots, v_n + v_1\} \\ R &= \{v_1 - v_2, v_2 + v_3, \ldots, v_n + (-1)^n v_1\} \end{aligned}$$

Si T es libre (resp. generador), ¿que se puede decir de S y de R?.

Solución. Supongamos T libre y sea

$\alpha_1(v_1 + v_2) + \alpha_2(v_2 + v_3) + \cdots + \alpha_{n-1}(v_{n-1} + v_n) + \alpha_n(v_n + v_1) = 0$ una combinación lineal nula de los elementos de S.

Reacomodando la escritura se tiene:

$$(\alpha_1 + \alpha_n)\, v_1 + (\alpha_1 + \alpha_2)\, v_2 + (\alpha_2 + \alpha_3)\, v_3 + \cdots + (\alpha_{n-1} + \alpha_n)\, v_n = 0.$$

Como T es libre, obtenemos la relación $\alpha_n = -\alpha_1$ y el sistema de ecuaciones sistemático:

$$\begin{cases} \alpha_1 + \alpha_2 = 0 \\ \alpha_2 + \alpha_3 = 0 \\ \vdots \\ \alpha_{n-1} + \alpha_n = 0 \end{cases}$$

del cual se deduce que $\alpha_k = (-1)^{k+1}\alpha_1$.

Se infiere que S es libre si y sólo si n es impar. El estudio de R se deja al lector.

100. Sean V un espacio vectorial y $f : V \to V$ una aplicación lineal. Demuestre que:

a) Si $f^2 = 0$ entonces $dim(Kerf) \geq \frac{dim(V)}{2}$.

b) Si $f^2 = f$ entonces $V = Imf \oplus Kerf$.

c) Si $f^2 = Id$ entonces existe una base B de V tal que $f(v) = \pm v$ para todo $v \in B$.

d) Si $f^m = 0$ entonces $m \leq dim(V)$.

OJO: En (a) y (c) car(K) $\neq$2; ¿que pasa en tal caso contrario?

Solución. En lo que sigue hay que tener presente la hermosa relación $dim(V) = dim(Imf) + dim(Kerf)$ que se obtiene construyendo una base de V por la vía de completar una base de $Kerf$; el mismo procedimiento sirve para establecer que si H y L son subespacios de V, entonces: $dim(H + L) = dim(H) + dim(L) - dim(H \cap L)$.

a) Es claro que $f^2 = 0$ es equivalente a $Imf \subset Kerf$ y por tanto $dim(Imf) \leq dim(Kerf)$.

b) Asimismo, $f^2 = f$ es equivalente a $Im(Id - f) \subset Kerf$; el resultado se establece notando que para todo $x \in V$ se tiene $x = (x - f(x)) + f(x)$.

c) Si $Fixf_+ = \{u \in V;\ f(u) = u\}$ y $Fixf_- = \{w \in V;\ f(w) = -w\}$, es inmediato demostrar que $Fixf_+$ y $Fixf_-$ son subespacios vectoriales de V y que $Fixf_+ \cap Fixf_- = \{0\}$.

Por otro lado, para todo $x \in V$, se tiene $x = \frac{1}{2}(x_+ + x_-)$, donde $x_+ = x + f(x)$ y $x_- = x - f(x)$. Se infiere que $V = Fixf_+ \oplus Fixf_-$.

d) Suponemos que m es el menor entero tal que $f^m = 0$. Esto significa que $f^{m-1} \neq 0$ por lo que existe $x \in V$ tal que $f^{m-1}(x) \neq 0$; es inmediato que $f^k(x) \neq 0$ para $0 \leq k \leq m-1$, (conviniendo que $f^0 = Id$).

Si $\sum_{k=0}^{m-1} \alpha_k f^k(x) = 0$ es una combinación lineal nula de esta familia, aplicando f^{m-1} se obtiene $\alpha_1 f^{m-1}(x) = 0$ por lo que $\alpha_1 = 0$.

Recursivamente, supongamos que $\alpha_j = 0$ para $j < i \leq m-1$; la combinación lineal nula se escribe entonces $\sum_{k=i}^{m-1} \alpha_k f^k(x) = 0$ y aplicando f^{m-1-i} se llega a que $\alpha_i = 0$. Concluimos que la familia de m vectores, x, $f(x)$, $f^2(x)$, ..., $f^{m-1}(x)$, es libre y por tanto $m \leq dim(V)$.

101. Sean V un espacio vectorial de dimensión n y $f : V \to V$ una aplicación lineal. Demuestre que f es inyectiva si y sólo si f es sobreyectiva.

Solución. Sea B una base de V. Sabemos que si f es inyectiva transforma sistemas libres en sistemas libres; luego $f(B)$ es un sistema libre de n elementos y por tanto $f(B)$ es una base: se infiere que f es biyectiva. El recíproco es análogo, cambiando "inyectiva" por "sobreyectiva" y "libre" por "generador".

Nota: Esto tambien se puede demostrar facilmentre utilizando la conocida relación: $dimV = dimKer(f) + dinIm(f)$.

102. Sea A un anillo íntegro que además es un espacio vectorial de dimensión finita sobre un cuerpo K. Demuestre que A es un cuerpo.

Solución. Sea $a \in A,\ a \neq 0_A$. La función $L_a : A \to A$, $x \to ax$ es trivialmente lineal; como A es íntegro, L_a es además inyectiva. Dado que $dim_K(A) < \infty$, concluimos que L_a es biyectiva, por lo que existe $b \in A$ tal que $ab = 1_A$. Se establece así que A es un cuerpo.

103. Sean V un espacio vectorial de dimensión finita, B una base de V, $f : V \to V$ una aplicación lineal no nula y F su matriz asociada respecto de la base B. Demuestre que:

a) Si F es diagonalizable y su matriz diagonal asociada es D entonces F^k también es diagonalizable y su diagonalizada es D^k (utilice la relación matricial que existe entre F y D).

b) Si $f^m = 0$, $m \geq 2$, entonces F no es diagonalizable.

c) Si $f^2 = f$ entonces F es diagonalizable.

Solución. Sea P la matriz de pasaje, es decir se tiene $D = PFP^{-1}$. Sin dificultad se deduce que $D^k = PF^kP^{-1}$ lo que responde a la primera afirmación.

En cuanto a la segunda, sea λ un valor propio de f asociado a un vector propio $v : f(v) = \lambda v$. Iterando se tiene que $f^m(v) = \lambda^m v = 0$, de donde $\lambda = 0$. Como F no es la matriz nula, F no puede ser diagonalizable.

Por último, si $f(v) = \lambda v$ y $f^2 = f$, se llega a que $\lambda^2 = \lambda$, por lo que los valores propios posibles son 0 y 1. Es claro que el subespacio propio asociado a 0 es $Ker(f)$ y el asociado al valor propio 1 es $Im(f)$; como $dimKer(f) + dimIm(f) = dimV$, F es diagonalizable.

104. Considere las matrices reales $M(x, y, z, t)$ definidas como sigue:

$$M(x, y, z, t) = \begin{pmatrix} x & z & y & t \\ z & x & t & y \\ t & y & x & z \\ y & t & z & x \end{pmatrix}$$

Muestre que este conjunto de matrices es un espacio vectorial; encuentre una base (la "más natural.º canónica; por lo demás, para lo que viene le sugerimos estudiar posibles relaciones multiplicativas entre los elementos de tal base.). Pruebe que M es diagonalizable (los valores propios pueden ser complejos).

Solución. Este conjunto de matrices es el subespacio engendrado por las matrices $I = M(1, 0, 0, 0)$, $A = M(0, 1, 0, 0)$, $B = M(0, 0, 1, 0)$ y $C = M(0, 0, 0, 1)$, que además constituyen un sistema libre (compruébelo); es decir, se tiene $M(x, y, z, t) = xI + yA + zB + tC$.

Un pequeño cálculo nos muestra que $A^2 = B$ y $A^3 = C$, por lo que si A es diagonalizable, con matriz diagonal D_A, B y C también lo serán con $D_B = D_A^2$ y $D_C = D_A^3$. Así las cosas, si P es la matriz de

pasaje, se tendría $PM(x,y,z,t)P^{-1} = P\left(xI + yA + zB + tC\right)P^{-1} = xI + yPAP^{-1} + zPBP^{-1} + tPCP^{-1} = xI + yD_A + zD_B + tD_C$ y por tanto $M(x,y,z,t)$ sería diagonalizable.

Basta estonces demostrar que A es diagonalizable: el polinomio característico esta dado por $det(M(-\lambda,1,0,0)) = \lambda^4 - 1$ y sus raices son $1, -1,\ i, -i$. Como tenemos cuatro valores propios, A es diagonalizable.

105. Sean V un espacio vectorial y $\{\, v_1, v_2, \ \ldots\ , v_n \,\}$ una base de V.

Si $x = x_1v_1 + x_2v_2 + \ \ldots\ + x_nv_n$ e $y = y_1v_1 + y_2v_2 + \cdots + y_nv_n$, el producto escalar de x e y está dado por:

$$x \bullet y = x_1y_1 + x_2y_2 + \ \ldots\ + x_ny_n.$$

Con esto, para todo $S \subset V$, se define $S^{\perp} = \{v \in V;\ v \bullet s = 0,\ \forall s \in S\}$.

Si U, W son subespacios vectoriales de V demuestre que:

a) $(U+W)^{\perp} = U^{\perp} \cap W^{\perp}$

b) $dimU + dimU^{\perp} = n$.

c) $\left(U^{\perp}\right)^{\perp} = U$.

Solución.

a) Es inmediato pues $U, W \subset U + W$; luego $x \bullet (U+W) = \{0\}$ si y sólo si $x \bullet U = x \bullet W = \{0\}$.

b) Sean $\left\{ u_i = \sum_{k=1}^{n} u_{ik}v_k\,;\ 1 \le i \le m \right\}$ una base de U y $x = \sum_{k=1}^{n} x_kv_k$ un elemento cualquiera de $U^{\perp}$.

Como $x \bullet u_i = 0$ para todo $1 \le i \le m$, el ortogonal de U es el subespacio definido por las m relaciones lineales sobre las componentes de x: $U^{\perp} = \left\{ x = \sum_{k=1}^{n} x_kv_k\,;\ \sum_{k=1}^{n} u_{ik}x_k\ = 0,\ 1 \le i \le m \right\}$.

Estas relaciones de restricción son independientes (¿porqué?) y cada una se traduce en la pérdida de un grado de dimensión (¿porqué?).

Como hay m relaciones, obtenemos que $dimU^{\perp} = n - m$.

c) Aplicando (b) es inmediato, pués de $U \bullet U^{\perp} = \{0\}$ se infiere que $U \subset \left(U^{\perp}\right)^{\perp}$.

El Anillo de Polinomios

106. Sea $S \in K[X]$ y $f_S : K[X] \to K[X]$ definida por $f_S(P(X)) = P(S)$. Es inmediato que f_S es un morfismo (aditivo y multiplicativo), llamado morfismo de sustitución (hágalo). Demuestre que : f_S inyectivo $\Leftrightarrow$ $gr(S) \geq 1$;además, f_S biyectivo $\Leftrightarrow$ $gr(S) = 1$.

Solución. Si $S = \sigma \in K$ se tiene $f_S(X - \sigma) = 0$, por lo que f_S no es inyectiva. Reciprocamente, como es claro que $gr(P(S)) = gr(P)gr(S)$ pues $f_S(\sum a_k X^k) = \sum a_k S^k$, si $gr(S) \geq 1$ entonces $f_S(\sum a_k X^k) = 0$ implica de inmediato que todos los a_k son nulos, es decir $ker() = \{0\}$, o sea que f_S es inyectiva. Lo último se deja al lector.

107. Sean $A(X), B(X) \in K[X]$. Demuestre las equivalencias:

$B(X)$ divide a $A(X)$ $\Leftrightarrow$ para todo S, $gr(S) \geq 1$, $B(S)$ divide a $A(S)$ $\Leftrightarrow$ existe S, $gr(S) \geq 1$ tal que $B(S)$ divide a $A(S)$.

Solución. Sale inmediatamente del ejercicio anterior, pues, por ejemplo, si $A = BQ$ entonces

$$A(S) = f_S(A) = f_S(BQ) = f_S(B)f_S(Q) = B(S)Q(S)$$

es decir, $B(S)$ divide a $A(S)$; el recíproco es inmediato y la otra equivalencia se deja al lector.

108. Sean K un cuerpo y P, $Q \in K[X]$ tales que $PQ = X^n - 1$.

Demuestre que:

a) Si $P = \sum_{k=0}^{p} a_k X^k$ y $Q = \sum_{k=0}^{q} b_k X^k$ entonces $\sum_{k=0}^{p+q} \left(\sum_{i+j=k} a_i b_j \right) = 0$.

b) Si $R = \sum_{k=0}^{p} a_k X^{p-k}$ y $S = \sum_{k=0}^{q} b_k X^{q-k}$ entonces $PQ + RS = 0$.

Solución. Lo primero es inmediato cuando se desarrolla formalmente el producto PQ.

En cuanto a lo segundo, trabajemos en el cuerpo de fracciones racionales $K(X)$: como del enunciado se deduce que $a_0, a_p, b_0, b_q \neq 0$ y por tanto que $gr(R) = gr(P) = p$ y $gr(S) = gr(Q) = q$, de donde podemos inferir que $R = X^p P(\frac{1}{X})$ y $S = X^q Q(\frac{1}{X})$, con $p + q = n$.

Luego, tenemos:

$$RS = X^p P(\frac{1}{X}) X^q Q(\frac{1}{X}) = X^n \, (PQ) \, (\frac{1}{X}) = X^n \left(\frac{1}{X^n} - 1 \right) = 1 - X^n$$

.

109. Sea $L \in \mathbb{Z}[X]$. Demuestre que si la función polinomio f_L no se anula en $\mathbb{Z}$ pero se anula en $\mathbb{Q}$ entonces el polinomio L no es mónico.

Solución.

En efecto, pongamos $L(X) = \lambda_0 + \lambda_1 X + \cdots + \lambda_{n-1} X^{n-1} + \lambda_n X^n$, $\lambda_k \in \mathbb{Z}$ y sea $\alpha = \dfrac{r}{s}$, con r y s primos entre si $(*)$, tal que $f_L(\alpha) = L(\alpha) = 0$.

Se tiene entonces:

$$s^n L(\frac{r}{s}) = \lambda_0 s^n + \lambda_1 r s^{n-1} + \cdots + \lambda_{n-1} r^{n-1} s + \lambda_n r^n = 0$$

de donde se deduce que s divide a $\lambda_n r^n$. Ahora bien, es claro por $(*)$ y un resultado del curso que s divide a λ_n; como además, también por las exigencias de $(*)$, obligadamente $s \neq \pm 1$, se infiere que $\lambda_n \neq 1$.

110. Dados $a_1, \ldots, a_n$ elementos distintos de un cuerpo K, construya polinomios P_i, $i = 1, 2, \ldots, n$, tales que $P_i(a_j) = \delta_{ij}$ (el delta de Kronecker).

Utilice lo anterior para demostrar que si $(b_1, \ldots, b_n) \in K^n$ existe un único polinomio de grado mínimo P tal que $P(a_i) = b_i$, $i = 1, 2, \ldots, n$ (esto se conoce como el teorema de interpolación de Lagrange).

Solución. Con un poco de tanteo se llega rápidamente a que

$$P_i(X) = \frac{(X - a_1)(X - a_2) \cdots (X - a_{i-1})(X - a_{i+1}) \cdots (X - a_n)}{(a_i - a_1)(a_i - a_2) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)}.$$

Con esto, lo segundo lo entrega

$$P(X) = \sum_{i=1}^{n} b_i P_i(X)$$

111. Dado un cuerpo K sea $K^K = \{f;\ f : K \to K\}$. Con las operaciones:

$$(f+g)(\alpha) = f(\alpha) + g(\alpha), (f \cdot g)(\alpha) = f(\alpha)g(\alpha) \text{ y } (\lambda f)(\alpha) = \lambda f(\alpha)$$

el conjunto K^K es una K-álgebra (estructuras de anillo y espacio vectorial compatibles).

Denotamos por K^K_{Pol} la subálgebra de las funciones polinomios:

$$K^K_{Pol} = \{f_P : K[X] \to K[X] \ / \ P \in K[X],\ f_P(\lambda) = P(\lambda)\}.$$

Demuestre que:

a) Si K es finito, $K^K_{Pol} = K^K$.

b) Si K es infinito, $K^K_{Pol} \cong K[X]$.

Solución. Supongamos K finito, $K = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Basta demostrar entonces que $K^K \subset K^K_{Pol}$: si $g \in K^K$ por el ejercicio anterior existe al menos un polinomio $P \in K[X]$ tal que $P(\alpha_i) = g(\alpha_i)$ para $i = 1, 2, \ldots, n$; esto significa que $g = f_P$, lo que demuestra la primera afirmación.

Por otro lado, sabemos que la aplicacion $\Psi : K[X] \to K^K_{Pol}$, $P \mapsto f_P$, es un morfismo sobreyectivo por construcción; es claro además que si $Q \in ker(\Psi)$ entonces f_Q se anula en K por lo que, si consideramos K infinito, obligadamente $Q = 0$ (pues en caso contrario tendríamos un polinomio con infinitas raíces....absurdo). Luego $ker(\Psi) = \{0\}$ y por tanto Ψ es inyectiva, con lo que se demuestra la segunda afirmación.

112. En el anillo $\mathbb{Z}[X]$ demuestre que: el ideal $\langle X \rangle$ es primo pero no es un ideal maximal. El ideal $\langle 3, X \rangle$ es maximal.

Solución. Como todo polinomio se puede escribir como $k + XP$ se infiere que $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$; luego, $\langle X \rangle$ es un ideal primo que no es maximal.

En cuanto a la segunda pregunta, veamos que un polinomio de $\mathbb{Z}[X]$ se puede escribir de la manera siguiente: $r + 3k + XP$ con $k \in \mathbb{Z}$ y $r = 0, 1, 2$.

Como en el anillo cociente $\mathbb{Z}[X]/\langle 3, X \rangle$ se tiene $X = 3 = 0$, concluimos que $\mathbb{Z}[X]/\langle 3, X \rangle = \{0, 1, 2 \ / \ 3 = 0\}$; luego, el ideal $\langle 3, X \rangle$ es maximal.

113. En el anillo $\mathbb{Q}[X]$ estudie si los ideales $\langle X^2-1, X-X^2\rangle$ y $\langle 2X^2-6\rangle$ son maximales.

Solución. Es claro que en el anillo $\mathbb{Q}/\langle X^2-1, X-X^2\rangle$ se infiere que $X=1$, luego $\mathbb{Q}/\langle X^2-1, X-X^2\rangle \approx \mathbb{Q}$; por tanto $\langle X^2-1, X-X^2\rangle$ es maximal.

En cuanto al otro ideal, en $\mathbb{Q}/\langle 2X^2-6\rangle$ se tiene $X^2=3$, luego los elementos del anillo cociente son de la forma $r+sX$, con $r,s\in\mathbb{Q}$ y $X^2=3$. Ahora bien, $r+sX=0$ si y sólo si $r=s=0$; con esto y como $r^2-3s^2\neq 0$ rapidamente se comprueba que $(r+sX)^{-1}=(r^2-3s^2)^{-1}(r-sX)$.

Luego $\mathbb{Q}/\langle 2X^2-6\rangle$ es un cuerpo y, por ende, $\langle 2X^2-6\rangle$ es también un ideal maximal.

114. Si $n\in\mathbb{Z}$ definimos: $L_n=\{kn+XP \;/\; k\in\mathbb{Z}, P\in\mathbb{Z}[X]\}$.

a) Compare L_n y L_{-n}. Demuestre que L_n es un ideal de $\mathbb{Z}[X]$.

b) Determine el ideal $L=\bigcap_{n\in\mathbb{Z}} L_n$.

c) Determine los enteros n para los cuales L_n es un ideal principal.

Solución. Puesto que $kn=(-k)(-n)$, es inmediato que $L_n=L_{-n}$.

Por otro lado, $(kn+XP)+(ln+XQ)=(k+l)n+XPQ$ lo que muestra que L_n es estable para la suma; además como todo polinomio puede escribirse como $m+XT$ se tiene:

$$(kn+XP)(m+XT)=(mk)n+X(mP+knT+XPT)$$

Todo esto muestra que L_n es un ideal.

La parte común a todos los L_n con $n\in\mathbb{Z}$, es el conjunto formado por los XP, $P\in\mathbb{Z}[X]$, es decir:

$$L=\bigcap_{n\in\mathbb{Z}} L_n=L_0=\langle X\rangle$$

Con respecto a la última pregunta, es claro que $L_1=\mathbb{Z}[X]$ que es trivialmente principal puesto que $\langle 1\rangle=\mathbb{Z}[X]$. El ideal L_2 no es principal: de serlo, necesariamente este sería engendrado por el elemento

no nulo de menor grado, lo que significa, entonces, que tendríamos $L_2 = \langle 2 \rangle = 2\mathbb{Z}[X]$; ahora bien, es inmediato que L_2 tiene polinomios cuyos coeficientes no son todos enteros pares.

Lo argumentado anteriormente permite responder a la última pregunta: los únicos ideales principales de esta familia son $L_0 = \langle X \rangle$ y $L_1 = \mathbb{Z}[X]$.

115. Establezca los isomorfismos siguientes:

   a) $K[X]/\langle X+1 \rangle \cong K$ donde K es un cuerpo.

   b) $\mathbb{R}[X]/\langle X^2+1 \rangle \cong \mathbb{C}$.

   Solución. Si $P \in K[X]$, podemos escribir : $P = (X+1)Q + \alpha_P$ (¿porqué?). Luego la aplicación $K[X]/\langle X+1 \rangle \to K$, $P \to \alpha_P$, es un epimorfismo de anillos, cuyo nucleo es $\langle X+1 \rangle$.

   Por tanto $K[X]/\langle X+1 \rangle \cong K$.

   Los elementos de $\mathbb{R}[X]/\langle X^2+1 \rangle$ son del tipo $\alpha + \beta\overline{X}$ con $\overline{X}^2 = -1$. Luego es inmediato que la aplicación de $\mathbb{R}[X]/\langle X^2+1 \rangle$ en $\mathbb{C}$, definida por $\alpha + \beta\overline{X} \to \alpha + \beta i$, es trivialmente un isomorfismo.

116. Se define: $End_A[X] = \{f \in End(A[X]), f(a) = a, \forall a \in A\}$.

   a) Caracterice los elementos de $End_A(A[X])$

   b) Suponga ahora que A es un anillo íntegro. En tal caso:

   - Caracterice los elementos inyectivos de $End_A(A[X])$.
   - Demuestre que si $f \in End_A(A[X])$ es sobreyectivo, entonces es biyectivo. Caracterice $Aut_A(A[X])$.
   - Constate que $Aut_A(A[X]$ no es un grupo conmutativo.

   Solución. No presenta dificultad en constatar que todo $f \in End_A(A[X])$ queda determinado al conocer $f(X)$: concretamente, si $f(X) = S \in A[X]$, entonces $f(P(X)) = P(S)$ (por lo que f se llama un morfismo de sustitución).

   Respecto a (b), si $S = \sigma_s X^s + ...$ y $P = \alpha_n X^n + ...$, entonces se tiene que $P(S) = \alpha_n \sigma_s^n X^{ns} + .. \neq 0$ si y sólo si $s \geq 1$.

   En cuanto a lo que sigue, como f es sobre, existe $Q = \beta_m X^m + ..$ tal que $Q(S) = X$; necesariamente $s \geq 1$ por lo que f es inyectiva.

Para terminar, como $Q(S) = \beta_m \sigma_s^m X^{ms} + ... = X$, se tiene obligadamente que $ms = 1$, luego $m = s = 1$ y, obviamente, $\beta_1 \sigma_1 = 1_A$.

En conclusión, $f \in Aut_A(A[X])$ si y sólo si $f(X) = \sigma_1 X + \sigma_0$ con σ_1 invertible en A.

Construcción de Cuerpos

117. Sea J un ideal propio de $K[X]$ y $\pi : K[X] \to K[X]/J$, el epimorfismo canónico. Demuestre que $\pi_{|K}$, la restricción de π a K, es inyectiva.

Deduzca de ello que K puede ser considerado un subcuerpo del anillo cociente $K[X]/J$.

Solución. Sea $\alpha \in K$ tal que $\pi(\alpha) = \overline{0}$; esto significa que $\alpha \in J$, lo que es posible sólo si $\alpha = 0$ (¿porqué?).

Respecto de la segunda pregunta, sabemos que π es sobreyectiva por definición; luego $\pi(K)$ es una imágen isomórfica de K, lo que significa que tales estructuras son algebraicamente indistinguibles. Es natural, por tanto considerar a K como un subcuerpo de $K[X]/J$.

118. Sea K un cuerpo, $car(K) \neq 2, 3$. Demuestre los siguientes isomorfismos de anillos:

a) $K[X]/\langle X^2 - 1\rangle \simeq K[X]/\langle X^2 - 4\rangle$.

b) $K[X]/\langle X^2 + 1\rangle \simeq K[X]/\langle X^2 + 2X + 2\rangle$.

Solución. Hagamos el segundo:.

Si $f : K[X]/\langle X^2 + 1\rangle \to K[X]/\langle X^2 + 2X + 2\rangle$ es un morfismo de anillos, entonces $f(\overline{X}) = \alpha\overline{X} + \beta$, con $\alpha \neq 0$ y $f(1) = 1$. Como $\overline{X}^2 = -1$ en $K[X]/\langle X^2 + 1\rangle$ y además $\overline{X}^2 = -2X - 2$ en $K[X]/\langle X^2 + 2X + 2\rangle$, se tiene $-1 = \left(\alpha\overline{X} + \beta\right)^2 = \alpha^2(-2X - 2) + 2\alpha\beta X + \beta^2$, de donde obtenemos las ecuaciones $-2\alpha(\alpha - \beta) = 0$ y $-2\alpha^2 + \beta^2 = -1$.

Se infiere que con $\alpha = \beta = \pm 1$, f es un isomorfismo.

119. Sea $P \in K[X]$. Entonces P es irreducible en K si y solamente sí $K[X]/\langle P\rangle$ es un cuerpo.

Solución. Sea $\overline{Q} \in K[X]/\langle P\rangle$, tal que $\overline{Q} \neq 0$. Por tanto $P \nmid Q$ y como P es irreducible, se infiere que P es primo con Q. Luego existen

$R, S \in K[X]$ tales que $PR + QS = 1$; en el anillo cociente $K[X]/\langle P\rangle$ esto significa que $\overline{Q}$ es invertible.

Recíprocamente, si P no fuera irreducible, entonces se tendría $P = RS$ con $R, S \in K[X]$ y $gr(R)$, $gr(S) \geq 1$; es claro que $P \nmid R, S$. Esto significa que en el cuerpo $K[X]/\langle P\rangle$ se obtiene $\overline{R}\,\overline{S} = 0$, lo que es una contradicción.

Cabe hacer notar este ejercicio trivializa de cierta manera gran parte de los ejercicios relativos a ideales maximales de $K[X]$ que han sido propuestos y/o resueltos anteriormente.

120. (Teorema de Kronecker) Sean F un cuerpo y P un polinomio irreducible de $F[X]$. Infiera del ejercicio anterior que sienpre existen un cuerpo K y $\alpha \in K$ de manera que $F < K$ y $P(\alpha) = 0$. Establezca que siempre se puede construir un cuerpo en el cual P tenga todas sus raices.

Solución. Como P es irreducible, $K = F[X]/\langle P\rangle$ es un cuerpo que contiene a F. Sea $\lambda = \overline{X}$: es claro que $\lambda \in K$, como también es inmediato que $P(\lambda) = 0$. Lo anterior significa que podemos factorizar P en $K[X]$, es decir se tiene $P = (X - \lambda)Q$ para algún $Q \in K[X]$. Si Q es irreducible en $K[X]$, sea $K_1 = K[X]/\langle P\rangle$; por lo anteriormente expuesto, $K < K_1$ y $\lambda_1 = \overline{X}$ es un elemento de K_1 que anula a P. Por tanto existe $Q_1 \in K_1[X]$ tal que $P = (X - \lambda)(X - \lambda_1)Q_1$. Reiterando este procedimiento a lo más n veces, donde $n = gr(P)$, encontraremos un cuerpo que contiene todas las raices de P.

Extensiones de Cuerpos

121. Sea V un espacio vectorial de dimensión finita sobre un cuerpo K. Si se provee a V de un producto para el cual es un anillo íntegro, demuestre que V es un cuerpo.

Solución. Sea v un elemento no nulo de V. Como V es de dimensión finita, existe $n > dim(V)$ tal que la familia $\{v, v^2, ..., v^n\}$ es linealmente dependiente; dicho de otra manera, existen polinomios que tienen a v como raíz. Sea $P \in K[X]$, de grado mínimo $m \leq n$, tal que $P(v) = 0$, $P = \alpha_m X^m + .. + \alpha_1 X + \alpha_0$; como V es íntegro, necesariamente $\alpha_0 \neq 0$ ya que en caso contrario $\alpha_m X^{m-1} + .. + \alpha_1$ admitiría a v como raíz, contradiciéndose la condición de minimalidad impuesta a P. Se obtiene así que $(\beta_m v^{m-1} + .. + \beta_1)v = 1$, donde $\beta_k = -\alpha_0^{-1}\alpha_k$.

Una mejor demostración es la siguiente: Sea $v \in V,\ v \neq 0_V$. La función $L_v : V \to V,\ x \to vx$ es trivialmente lineal; como V es íntegro, L_v es además inyectiva. Dado que $dim_K(V) < \infty$, concluimos que L_v es biyectiva, por lo que existe $w \in A$ tal que $vw = 1_V$. Se establece así que V es un cuerpo.

122. Sean $p \in \mathbb{N}$, primo, K un cuerpo, $car(K) = p$, y $f : K \to K,\ f(x) = x^p$. Demuestre que:

   a) La aplicación f es un monomorfismo.

   b) De un ejemplo en donde f no sea biyectiva.

   c) Si K es finito, f es sobreyectiva.

   Solución. Sabemos que todo morfismo entre cuerpos es inyectivo. Como en el caso que nos convoca, trivialmente se tiene $(xy)^p = x^p y^p$, basta establecer que $(x+y)^p = x^p + y^p$; ahora bien, como p es primo, ello se deduce de que para todo $0 < k < p$ se tiene $\binom{p}{k} = 0$ (¿porqué?).

   Si $K = \mathbb{Z}_p(X)$, cuerpo de fracciones de $\mathbb{Z}_p[X]$, la función f no es sobreyectiva (¿porqué?). La última pregunta es inmediata.

123. En el cuerpo $\mathbb{C}$, demuéstrese que los siguientes números son algebraicos: $\sqrt{2}+\sqrt{3}$, $\sqrt{7}+\sqrt{12}$, $2+i\sqrt{3}$, $cos(\frac{2\pi}{k}) + isen(\frac{2\pi}{k})$ con k entero positivo.

   Solución. Hagamos dos casos: si $\alpha = 2+i\sqrt{3}$; se tiene $(\alpha^2-1)^2 = -48$ de donde $Q = X^4 - 2X^2 + 49$ se anula con α.

   Sin embargo tal polinomio no es el de grado mínimo: en efecto, se tiene $\alpha^2 - 1 = 4(\alpha - 2)$, luego $P = X^2 - 4X + 7$ también se anula con α.

   Sea ahora $\beta = cos(\frac{2\pi}{k}) + isen(\frac{2\pi}{k})$; para $k \leq 2$ es trivial. Si $k > 2$, el polinomio mínimo que se anula en β es $Q = X^{k-1} + X^{k-2} + ... + 1$.

124. Sean F un subcuerpo de K, $a \in K$, y $P \in F[X]$, P no constante. Demuestre que si $P(a)$ es algebraico también lo es a.

   Solución. Si $P(a)$ es algebraico sobre F, entonces existe $Q \in F[X]$ tal que $Q(P(a)) = 0$. Es claro que $T(X) = Q(P(X))$ se anula en a.

125. Si la característica de un cuerpo no es nula, entonces es un número primo.

Solución. Sabemos que la característica de un cuerpo K la determina el generador del nucleo del morfismo de anillos $\mathbb{Z} \to K$, $n \to n1_K$; esto quiere decir que $car(K)$ es el menor entero tal que $n1_K = 0$. Si tal morfismo es inyectivo, $car(K) = 0$; en caso contrario, $car(K) = p$ donde p es necesariamente un número primo (¿porqué?).

126. Si K es una extensión finita de F, entonces es algebraica.

Solución. K es un espacio vectorial de dimensión finita sobre F por lo que dado $k \in K$, para cierto entero $n \in \mathbb{N}$, la familia $k, k^2, ..., k^n$ es linealmente dependiente, es decir, existe una combinacion lineal no trivial $\alpha_1 k + \alpha_2 k^2 + ... + \alpha_n k^n = 0$, donde los α_i son elementos de F.

Es claro que el polinomio $P(X) = \sum \alpha_i X^i$ se anula en k.

127. Sean $F < K$ cuerpos, $a \in K$, $F[\,a\,] = \{\ P(a) : P \in F[X]\}$ y $F(a)$ el sub-cuerpo de K engendrado por F y a. Demuestre que:

   a) $F[\,a\,]$ es un sub-anillo de K.

   b) a es algebraico sobre F si y sólo si $F(a) = F[\,a\,]$.

   c) a es trascendente sobre F si y sólo si $F(a) = Frac(F[\,a\,])$.

Solución. La aplicación $\varphi : F[X] \to K, \varphi(P) = P(a)$, es trivialmente un morfismo de anillos cuya imagen es $F[\,a\,]$; esto responde a la primera pregunta. En cuanto a las otras, sabemos que $F[X]/ker(\varphi)$ es isomorfo a $Im(\varphi)$. Ahora bien, si φ no es inyectiva (equivalente a decir que a es algebraico sobre F), $ker(\varphi)$ es un ideal maximal por lo que $Im(\varphi)$ es un cuerpo; esto responde a la segunda pregunta. Por último, se deduce de lo anterior que a es trascendente sobre F si y sólo si φ es inyectiva y esto es equivalente a decir que $F[X] \cong F[\,a\,]$ o, lo que es lo mismo, que se tenga $Frac(F[X]) \cong Frac(F[\,a\,])$ de donde $F(a) = Frac(F[\,a\,])$.

128. Constrúyase dos cuerpos, $F < K$, de manera que K sea una extensión algebraica no finita de F.

Solución. Un ejemplo está dado por $\mathbb{Q} < Alg_{\mathbb{Q}}(\mathbb{C})$.

Otra extensión algebraica infinita de $\mathbb{Q}$ lo da $\mathbb{Q}(\sqrt{\mathbb{P}})$, el menor cuerpo que contiene a $\mathbb{Q}$ y a todos los elementos $\sqrt{p}$, donde p es un número primo La existencia de $\mathbb{Q}(\sqrt{\mathbb{P}})$ está garantizada por el hecho de que $Alg_{\mathbb{Q}}(\mathbb{C})$ es un cuerpo que contiene a los elementos $\sqrt{p}$, $p \in \mathbb{P}$.

129. Sean a y b algebraicos sobre F, de grados n y m respectivamente. Si n y m son primos entre sí, demuestre que $[F(a,b) : F] = nm$.

Solución. En demostraciones anteriores vimos que $[F(a,b) : F] \leq nm$.

Como n y m son primos entre sí, de las igualdades $[F(a,b) : F] = [F(a,b) : F(a)] \cdot n = [F(a,b) : F(b)] \cdot m$, se infiere que existe $s \in N$ tal que $[F(a,b) : F] = snm$. A fortiori, $s = 1$.

130. De un ejemplo de números algebraicos a y b, de grados respectivos 2 y 3 sobre $\mathbb{Q}$, de manera que ab tenga sobre $\mathbb{Q}$, un grado menor que 6.

Solución. Este es el tipo de solución que puede demorar días en encontrarse y que, una vez escrita, es de una penosa pero enriquecedora trivialidad. Quien lo haya hecho, habrá aprendido mucho.

Es claro que $a = \sqrt[3]{2}$ es de grado 3 sobre $\mathbb{Q}$; compruebe que $b = 1 - i\sqrt{3}$ es de grado 2. Por último, verifique que ab es de grado 3 sobre $\mathbb{Q}$.

131. Sea F un subcuerpo de K. Si $[K : F] = p$ es un número primo, demuestre que para todo $a \in K$ se tiene $F(a) = F$ o $F(a) = K$.

Solución. La respuesta se deduce de $[K : F] = [K : F(a)][F(a) : F]$: en efecto, si $a \in F$ entonces $F(a) = F$. En caso contrario, $F(a)$ es un $F-$subespacio vectorial de K de dimensión p; luego, $F(a) = K$.

Contructibilidad con Regla y Compás

132. Demuestre que si la cantidad α es constructible, también lo es $\sqrt[2^n]{\alpha}$.

Solución. Sabemos que si α es contructible $\sqrt{\alpha}$ tambien lo es; luego $\sqrt{\sqrt{\alpha}}$ también y así sucesivamente.

133. Demuestre que es imposible trisectar un ángulo de 60^o utilizando regla y compás.

Solución. Eston implicaría poder construir un triángulo rectángulo de hipotenusa de largo 1 y catetos de largos $cos(20)$ y $sen(20)$. Demuestre la identidad $cos(3\alpha) = 4cos^3() - 3cos(\alpha)$ y luego utilicela para probar que $cos(20)$ no es constructible.

134. Dada una circunferencia de superficie S, demuestre que es imposible construir un cuadrado que tenga la misma superficie, utilizando regla y compás.

Solución. Esto equivale a decir que $\sqrt{\pi}$ es constructible, y por tanto también π, lo que significaría que sería algebraico.

135. Dado un cubo de volumen V, demuestre que es imposible construir con regla y compás, un cubo con el doble de volumen.

Solución. Tal problema implica construir raices para el polinomio $X^3 - 2a^3$, donde a es el lado del cubo de volumen V. La extensión de cuerpo correspondiente es por tanto de grado 3, lo que muestra la imposibilidad de la construcción pedida.

136. Demuestre que el número real δ es constructible si y sólo si $\sqrt{\delta + \sqrt{\delta}}$ también lo es.

Solución. La demostración directa es inmediata pues el cuerpo de los números constructibles es estable por acción de raiz cuadrada. Para el recíproco ponemos: $\lambda = \sqrt{\delta + \sqrt{\delta}}$; Un cálculo menor nos lleva a que

$$\delta = \frac{2\lambda^2 + 1 \pm \sqrt{4\lambda^2 + 1}}{2}$$

lo que muestra que δ es constructible.

Cuerpos Finitos

137. Sea K un cuerpo finito, $|K| = q$. Demuestre que:

   a) El polinomio $\alpha X^q + \beta X$, $\beta \neq 0$, no tiene raices múltiples.

   b) Si n es primo con q, $\alpha X^n + \beta$, $\beta \neq 0$, no tiene raices múltiples.

Solución. Demostremos la segunda afirmación: el polinomio derivado $(\alpha X^n + \beta)' = \alpha n X^{n-1}$ el cual acepta como única raiz al 0, que no es raiz de $\alpha X^n + \beta$. Luego, $\alpha X^q + \beta X$ no tiene raíces múltiples.

138. Sea K un cuerpo finito y F un subcuerpo de K tal que $[K : F] = m$. Si $|F| = q$, demuestre que $|K| = q^m$.

Concluya que todo cuerpo finito tiene p^n elementos, donde p es un número primo.

Solución. K es un espacio vectorial de dimensión m sobre F, por tanto $K \cong F^m$ (isomorfismo de esp. vects). Como F es finito, $|K| = |F|^m$.

Para responder a la segunda pregunta, tengamos presente que si la característica de K es p entonces $\mathbb{Z}_p < K$.

Como K es finito, este es necesariamente una extensión finita de $\mathbb{Z}_p$, es decir $[K : \mathbb{Z}_p] = n$; luego $|K| = p^n$.

139. Demuestre que para todo p, $n \in \mathbb{N}^*$, p primo, existe un cuerpo K tal que $|K| = p^n$.

Solución. Sea $q = p^n$ y consideremos en $\mathbb{Z}_p[X]$ el polinomio $X^q - X$; éste no tiene raíces múltiples pues su polinomio derivado es igual a -1. En un cuerpo conveniente (el menor, es decir el cuerpo de descomposición de $X^q - X$) tal polinomio admite q raíces distintas: $0,\ 1,\ \alpha_2, \cdots,\ \alpha_q$. Si β y γ son dos de esas raíces entonces $\beta \pm \gamma$, $\beta\gamma$ y $\dfrac{\beta}{\gamma}$ (si $\gamma \neq 0$) tambien son raices de $X^q - X$ (¿porqué), es decir $\{0,\ 1,\ \alpha_2, \cdots,\ \alpha_q\}$ es un cuerpo de q elementos, extensión de $\mathbb{Z}_p$.

140. Construya dos cuerpos con 9 elementos y verifique que son isomorfos.

Solución. Si tomamos el anillo $\mathbb{Z}[\,i\,]$, entonces $J = 3\mathbb{Z}[\,i\,]$ es un ideal maximal (compruébelo); es claro que el cuerpo cociente $\mathbb{Z}[\,i\,]/J$ tiene 9 elementos. Por otro lado, el polinomio $X^2 + 1$ es irreducible en $\mathbb{Z}_3[X]$; constate que el cuerpo $\mathbb{Z}_3[X]/\langle X^2 + 1\rangle$ también tiene 9 elementos. Verifique usted si hay relación isomórfica entre estos dos cuerpos.

141. Construya cuerpos con 25, 27, 49, 81 y 125 elementos.

Solución. Construyamos uno de los cuerpos pedidos: como $X^2 + 1$ es irreducible en $\mathbb{Z}_7[X]$ (¡compruébelo!), verifique que el cuerpo cociente $\mathbb{Z}_7[X]/\langle X^2 + 1\rangle$ tiene 49 elementos.

142. Compruebe que $X^2 + 4X + 5$ es irreducible sobre $\mathbb{R}$ y estudie si los cuerpos $\mathbb{Q}(i)$ y $\mathbb{Q}[X]/\langle X^2 + 4X + 5\rangle$ son isomorfos.

Si no es el caso, argumente con claridad la imposibilidad; si lo fuese, precise los isomorfismos posibles.

Solución: recordemos que en el cociente $\mathbb{Q}[X]/\langle X^2 + 4X + 5\rangle$ la base está dada por $1, \overline{X}$; es decir, los elementos son de la forma $\gamma + \delta\overline{X}$, teniendo en cuenta para operar la relación $\overline{X}^2 = -4\overline{X} - 5$.

Si $f : \mathbb{Q}(i) \to \mathbb{Q}[X]/\langle X^2 + 4X + 5\rangle$ es un isomorfismo, de $f(i^2) = f(i)^2$ se obtiene $(5b^2 - a^2 - 1) + 2b\,(2b - a)\,\overline{X} = 0$ de donde $a = \pm 2$ y $b = \pm 1$.

Concluimos que los cuerpos $\mathbb{Q}(i)$ y $\mathbb{Q}[X]/\langle X^2+4X+5\rangle$ son isomorfos y los isormorfismos posibles están dados por:

$$\begin{aligned} \alpha+\beta i &\mapsto (\alpha+2\beta)+\beta\overline{X} \\ \alpha+\beta i &\mapsto (\alpha-2\beta)-\beta\overline{X} \end{aligned}$$

143. Demuestre que dos cuerpos finitos con el mismo número de elementos son isomorfos.

Solución. Además de que los respectivos grupos multiplicativos son isomorfos, si dos cuerpos tienen q elementos, ambos son cuerpos de descomposición del polinomio $X^q - X$.

144. Para todo cuerpo finito K, donde $|K| = q$, se tiene $\prod_{a\in K^*} a = (-1)^q$.

Solución. Como $(K^*, \cdot)$ es un cuerpo de orden $q-1$, si $a \in K^*$ entonces $a^{q-1} = 1$; de ello se infiere que a es raíz del polinomio $X^{q-1} - 1$ y por tanto que $X^{q-1} - 1 = \prod_{a\in K^*}(X - a)$. El resultado sale de tomar $X = 0$.

145. Si p es primo, encuentre el resto de la división de $(p-1)!$ por p.

Solución. Sale del ejercicio anterior tomando $K = \mathbb{Z}_p$. El resto es $p-1$.

Sobre Códigos de Longitud Constante

146. Demuestre que un código C es e-corrector si y solamente si las bolas cerradas centradas en los elementos de C y de radio e son disjuntas dos a dos.

Solución: Consideremos las bolas $B(a,e)$ y $B(b,e)$ donde $a, b \in C$; si estas no fueran disjuntas, existiría $x \in A^n$ tal que $d(a,x), d(b,x) \leq e$, de donde se inferiría que $a, b \in B(x,e)$ lo que es imposible. Recíprocamente, si dado $x \in A^n$ la bola $B(x,e)$ contuviera $a, b \in C$ entonces $x \in B(a,e) \cap B(b,e)$, lo que contradice la hipótesis.

147. Dado $A = \{\alpha, \beta\}$ construya un código perfecto de longitud 3.

Solución: $C = \{\alpha\alpha\alpha, \beta\beta\beta\}$. Se tiene aquí: $\delta_C = 3$ y $e_C = \rho_C = 1$.

Más precisamente, se tiene que $B(\alpha\alpha\alpha, 1) = \{\alpha\alpha\alpha, \alpha\alpha\beta, \alpha\beta\alpha, \beta\alpha\alpha\}$ y $B(\beta\beta\beta, 1) = \{\beta\beta\beta, \beta\beta\alpha, \beta\alpha\beta, \alpha\beta\beta\}$ constituyen una partición de A^3.

148. Sea C un código de longitud n sobre A tal que $d(x,y) = 1$ para todo $x, y \in C$. Demuestre que $|C| \leq |A|$.

Solución: Consideramos obviamente que se tiene $|A| > 1$.

Sean $a = (\cdot, \cdot, \ldots, x, \ldots, \cdot, \cdot)$ y $b = (\cdot, \cdot, \ldots, y, \ldots, \cdot, \cdot) \in C$, tales que $d(a,b) = 1$. Si $c \in C$ es tal que $d(a,c) = d(b,c) = 1$, el elemento c no puede difierir de a en una coordenada distinta de x pues en tal caso automaticamente sería distinto de b en dos coordenadas; luego c difiere de a en la coordenada x lo que obliga a tener $c = (\cdot, \cdot, \ldots, z, \ldots, \cdot, \cdot)$ con $z \neq x, y$. Y así sucesivamente, encontrar un cuarto elemento de C obliga a disponer de un cuarto elemento de A.

Con este análisis se concluye lo pedido.

149. Sea $\mathbb{K}$ un cuerpo de q elementos y $n \in \mathbb{N}^*$. Calcule $\sum_{x \in \mathbb{K}^n} w(x)$.

Solución: Ya que en $\mathbb{K}^n$ hay q^n elementos, cada uno con n coordenadas, se escriben nq^n letras al hacer la lista de los elementos de $\mathbb{K}^n$.

Por razones de homogeneidad en tal lista cada letra aparece el mismo número de veces, es decir, nq^{n-1}. Concluimos por tanto que dada una letra, las otras ocupan $nq^n - nq^{n-1}$ lugares de coordenada en tal lista.

Luego $\sum_{x \in \mathbb{K}^n} w(x) = n(q-1)q^{n-1}$.

150. Conociendo $k \geq 1$ y $q = |\mathbb{K}|$ determine el menor n para que, dado un código lineal de tipo (n,k) sobre $\mathbb{K}$, la cota de Plotkin sea más fina que la cota de Singleton.

Solución: de la desigualdad $\dfrac{n(q-1)q^{k-1}}{q^k - 1} \leq n - k + 1$ se obtiene:

$\dfrac{(k-1)(q^k-1)}{q^{k-1}-1} \leq n$. Luego, $n = \left\lceil \dfrac{(k-1)(q^k-1)}{q^{k-1}-1} \right\rceil$.

151. Sea $C < \mathbb{K}^n$ un código lineal. Demuestre que todas las matrices generadoras de C tienen las mismas columnas nulas.

Solución: Sea G una matriz generadora de C. Recordemos que los vectores línea de G forman una base de C; luego, si la j-ésima columna de G es nula, todo elemento de C tendrá nulo el j-ésimo coeficiente y por tanto toda otra matriz generadora tendrá nula la misma columna.

152. Sea $C < K^n$ un código lineal no trivial.

Demuestre que nunca se tiene $C \cup C^\perp = K^n$. Determine las condiciones necesarias y suficientes para que:

(a) $C + C^\perp = \mathbb{K}^n$. (b) El código $C \cap C^\perp$ sea auto-dual.

Solución: Sean $|\mathbb{K}| = q$ y $dim(C) = k$. Suponiendo que tenemos maximalidad en la reunión, o sea que $C \cap C^\perp = \{0\}$, se tiene $\left|C \cup C^\perp\right| = |C| + \left|C^\perp\right| - 1$ es decir que $\left|C \cup C^\perp\right| = q^k + q^{n-k} - 1$, lo que es siempre menor que $|\mathbb{K}^n| = q^n$.

En cuanto a las otras preguntas, para la primera la condición es que la suma sea directa, es decir que $C \cap C^\perp = \{0\}$

Para la última, sabemos que en general para dos subespacios tenemos $(U + W)^\perp = U^\perp \cap W^\perp$, por tanto $\left(C \cap C^\perp\right)^\perp = C + C^\perp$; así las cosas, la auto-dualidad de $C \cap C^\perp$ implica que C y $C^\perp$ estan contenidos en $C \cap C^\perp$, es decir que C sea auto-dual, la cual es una condición necesaria y suficiente.

153. Sea C un código lineal de tipo $(3, 5)$ sobre $\mathbb{Z}_3$ definido por:

$$C = \{(x, y, z, t, u),\ x + 2y + z = 0,\ y + 2t + u = 0\}$$

Encuentre la matriz generadora normalizada de C (o de un código equivalente). Determine w_C y ρ_C.

Solución: Dadas las relaciones coordenadas que definen al código C, tenemos: $C = \{(x, x + z, z, x + z + u, u);\ x, z, u \in \mathbb{Z}_3\}$, por lo que una base de C es $(1, 1, 0, 1, 0)$, $(0, 1, 1, 1, 0)$, $(0, 0, 0, 1, 1)$; esta base nos da la matriz generadora:

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

y, operando con la biyección $\overline{\sigma}$ inducida por $\sigma = (3, 4)$, obtenemos:

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

luego restando la segunda linea a la primera y la tercera a la segunda terminamos con la matriz normalizada de un código C', equivalente al código C:

$$G = \begin{pmatrix} 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Así, el elemento tipo de C' es $(\alpha, \beta, \gamma)\, G = (\alpha, \beta, \gamma, 2\alpha + \beta, 2\beta + \gamma)$ con $\alpha, \beta, \gamma \in \mathbb{Z}_3$; un pequeño análisis nos indica que w_C es 2. En cuanto al radio ρ_C, de la cota de Hamming se deduce que: $\sum_{k=0}^{\rho_C} \binom{5}{k} 2^k \geq 3^2$.y, por tanto, $\rho_C = 1$.

154. Establezca que para un código lineal C sobre $\mathbb{Z}_2$ se tiene una de las situaciones siguientes: (a) todas las palabras de C son de peso par; (b) la mitad de las palabras de C son de peso par.

Solución: Es inmediato (a causa del vector nulo) que C tiene palabras de peso par. Si C contiene un elemento i de peso impar consideremos el subespacio P de C formado por las palabras de peso par; el espacio cociente C/P tiene trivialmente dos clases: P e $I = i + P$ (las palabras de peso impar). De esto se infiere el resultado, pues sabemos que todas las clases tienen el mismo cardinal

155. Demuestre que el código dual de un código de chequeo de paridad de tipo $(n, n-1)$ es un código de repetición de tipo $(n, 1)$ (son sobre $\mathbb{Z}_2$). Argumente razonablemente el recíproco.

Utilice lo anterior para demostrar que la capacidad de corrección de un código de repetición de tipo $(2q + 1, 1)$ es q.

Solución: La matriz normalizada de un código de repetición R está dada por: $(1\,1\,\ldots\,1) = (I_1, \mathbf{1}_{n-1})$. Luego su matriz de control es $({}^t\mathbf{1}_{n-1}, I_{n-1})$, por lo que la matriz normalizada de $R^\perp$ es.$(I_{n-1}, {}^t\,\mathbf{1}_{n-1})$.

Es inmediato que se tiene:

$$(a_1, a_2, \cdots, a_{n-1})(I_{n-1}, {}^t\,\mathbf{1}_{n-1}) = (a_1, a_2, \cdots, a_{n-1}, a_1 + a_2 + \cdots + a_{n-1}),$$

lo que muestra que $R^\perp$ es un código de chequeo de paridad de tipo $(n, n-1)$.

Reciprocamente, puesto que $\left(V^{\perp}\right)^{\perp} = V$ para todo subespacio, el dual de un código de chequeo de paridad es un código de repetición.

Por último, dada la matriz de control de un código de repetición, su peso mínimo es n (número mínimo de columnas dependientes); con esto se deduce la última pregunta: en el caso $n = 2q + 1$, se obtiene $e_C = q$.

156. Dado un código de Hamming C, de longitud $2^k - 1$, determine e_C (la capacidad de corrección) y ρ_C (el radio de recubrimiento). ¿Cual es su conclusión?.

Solución: Sabemos que la dimensión de C es $2^k - k - 1$ y que la capacidad de corrección es $e_C = 1$.

En cuanto al radio de recubrimiento, como $|A| = 2$ y $|C| = 2^{2^k-k-1}$, utilizando la cota de Hamming tenemos:

$$2^{2^k-k-1} \sum_{i=0}^{\rho_C} \binom{2^k-1}{i} \geq 2^{2^k-1} \text{ es decir, } \sum_{i=0}^{\rho_C} \binom{2^k-1}{i} \geq 2^k$$

de donde se deduce inmediatamente que $\rho_C = 1$. Concluimos que todo código de Hamming es perfecto.

157. Demuestre que los códigos cíclicos binarios de tipo (7,4) son códigos de Hamming.

Solución.

Sobre $\mathbb{Z}_2$ se tiene: $x^7-1 = (x-1)(x^3+x+1)(x^3+x^2+1)$. Los polinomios generadores de códigos cíclicos de tipo (7,4) son por tanto $x^3 + x + 1$ y $x^3 + x^2 + 1$, y sus respectivos los polinomios de control $x^4 + x^3 + x^2 + 1$ y $x^4 + x^2 + x + 1$

Asi las cosas, las matrices de control asociadas, inducidas por los polinomios de control, son:

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

cuyas columnas, como vemos, describen en base 2 los enteros de 1 a 7.

158. Sean A un alfabeto y n un entero mayor que 1. Denotamos por s la función $A^n \to A^n$ definida por $s(x) = shift(x)$. Para todo entero $m \in \mathbb{N}$ decimos que la función s^m es una m-circularidad; (se acepta a Id, la función identidad, como **la** circularidad trivial, sin acción). Así mismo, decimos que un código $C \subset A^n$ es m-circular si $s^m(C) \subset C$; si $m = 1$ hablamos simplemente de código circular

a) Dado n, ¿cuantos tipos de m-circularidades no triviales existen?. Además, si $x = x_1 \dots x_n$ explícite $s^m(x)$.

b) Diga cuantos códigos circulares hay cuando $|A| = 2$ y $n = 3$ (se apreciará mucho más el argumento reflexivo que la construcción de la lista exhaustiva). Si $A = \mathbb{Z}_2$, ¿cuales de esos códigos circulares son códigos ciclicos no triviales?

Solución

a) Es inmediato que $s^n = Id$; luego, por la división euclidiana por n tenemos $m = qn + r$ con $0 \leq r < n$, de donde $s^m = s^{qn+r} = (s^n)^q s^r = s^r$. Debemos descartar $r = 0$ pues obtenemos la función identidad; por tanto hay $n - 1$ m-circularidades no triviales. Con respecto a lo segundo, por lo anterior podemos considerar $m < n$. Luego se tiene: $s^m(x_1 \dots x_n) = x_{n-m+1} \dots x_{n-m}$.

b) Obtenemos los códigos circulares minimales iterando la función s sobre cada elemento x.

Así las cosas, si $A = \{a, b\}$ tenemos $C_1 = \{aaa\}$, $C_2 = \{aab, baa, aba\}$, $C_3 = \{bba, abb, bab\}$ y $C_4 = \{bbb\}$.

Todo código circular será reunión de los C_i; como estos son disjuntos dos a dos, el número de reuniones posibles coincide con el número de subconjuntos no vacíos de $\{C_1, C_2, C_3, C_4\}$.

Por tanto hay 15 códigos circulares.

Respecto de la segunda pregunta, si $A = \mathbb{Z}_2$, con $a = 0$ y $b = 1$ se tiene $C_1 = \{000\}$, $C_2 = \{001, 100, 010\}$, $C_3 = \{110, 011, 101\}$ y $C_4 = \{111\}$. Ahora bien, como $\langle C_2 \rangle = \mathbb{Z}_2^3$, no es difícil ver que los códigos circulares que son cíclicos no triviales son: $\{000, 111\}$ y $\{000, 110, 011, 101\}$.

159. Sea $\mathbb{K}$ un cuerpo finito y $u = (1, 1, 0, 1, 1, 0) \in \mathbb{K}^6$.

a) Encuentre el menor código cíclico $C < \mathbb{K}^6$ que contiene a u.

b) Determine su peso mínimo, su polinomio generador y su matriz de control asociada.

Solución: Recordamos que para todo cuerpo se tiene en $\mathbb{K}[x]$:

$$x^6 - 1 = (x^3 + 1)((x^3 - 1) = (x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1)$$

Shifteando al elemento u obtenemos la colección

$$(1, 1, 0, 1, 1, 0), (0, 1, 1, 0, 1, 1), (1, 0, 1, 1, 0, 1).$$

Esta familia es libre salvo cuando la característica del cuerpo es 2 (de la suma de los primeros dos resulta el tercero), en cuyo caso los dos primeros vectores constituyen una familia libre.

Tenemos entonces:

► Si $car(\mathbb{K}) = 2$ el código buscado está dado por

$$C = \{(\alpha, \alpha + \beta, \beta, \alpha, \alpha + \beta, \beta);\ \alpha, \beta \in \mathbb{K}\}$$

y un simple análisis nos dice que $\omega_C = 2$. Por otro lado, es inmediato que $1 + x + x^3 + x^4$ es el polinomio generador y, dada la caracteristica del cuerpo, no es otra cosa que $(x + 1)(x^2 - x + 1)(x - 1)$, por lo que la matriz de control tiene como polinomio asociado a $x^2 + x + 1$, lo que nos da:

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

► Si $car(\mathbb{K}) \neq 2$ el código buscado está definido por

$$C = \{(\alpha + \gamma, \alpha + \beta, \beta + \gamma, \alpha + \gamma, \alpha + \beta, \beta + \gamma);\ \alpha, \beta, \gamma \in \mathbb{K}\}.$$

Sin embargo, podemos hacer un cambio de base que nos permita simplificar análisis y cálculos: otra base del código es:

$$(1, 0, 0, 1, 0, 0), (0, 1, 0, 0, 1, 0), (0, 0, 1, 0, 0, 1)$$

y con esto encontramos que $C = \{(\alpha, \beta, \gamma, \alpha, \beta, \gamma);\ \alpha, \beta, \gamma \in \mathbb{K}\}$ y obviamente que tenemos $\omega_C = 2$.

Así las cosas, como $1+x^3$ es el polinomio generador de C el polinomio de control es $-1+x^3$, por lo que la matriz de control esta dada por

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

160. Sean A un alfabeto y $n \in \mathbb{N}$. Consideremos el código de largo n sobre A definido por $\Pi = \{\pi;\ \pi \in A^n,\ \pi \text{ palíndrome}\}$.

a) Determine el cardinal de Π y su distancia mínima δ_Π.

b) Si $\pi_1, \pi_2 \in \Pi$ calcule $\left|\overline{B}(\pi_1, 1) \cap \overline{B}(\pi_2, 1)\right|$.

c) Demuestre que si $|A|, n \geq 3$ entonces $2 \leq \rho_\Pi \leq \left\lfloor \frac{n}{2} \right\rfloor$.

Solución.

(a) Para construir un palíndrome de largo $n = 2m$ basta escoger las primeras m letras y para $n = 2m+1$ las primeras $m+1$ letras (en ambos casos, las últimas m letras son las mismas que las m primeras, pero escritas en orden inverso). Esto nos dice que $|\Pi| = |A|^m$ si n es par y $|\Pi| = |A|^{m+1}$ si n es impar.

Por otro lado, para el caso par, si dos palíndromes diferieren en una letra entonces al menos difieren en dos, por lo que en tal caso $\delta_\Pi = 2$; en el caso impar, pueden diferir en la letra central por lo que $\delta_\Pi = 1$.

(b) Si $d(\pi_1, \pi_2) > 2$ es inmediato que $\left|\overline{B}(\pi_1, 1) \cap \overline{B}(\pi_2, 1)\right| = 0$

Supongamos que $d(\pi_1, \pi_2) \leq 2$ y que existe $c \in \overline{B}(\pi_1, 1) \cap \overline{B}(\pi_2, 1)$.

Caso $n = 2m$: supongamos que en cierta posición (por ejemplo, sin pérdida de generalidad por simetría, la posición $k \leq m$) el la palabra π_1 tiene un α y la palabra c tiene un β con $\alpha \neq \beta$; como sabemos que π_1 y c difieren en una letra la situación es la siguiente:

$$\pi_1 = \boxed{\cdots\cdots\alpha\cdots\cdots\cdots\cdots \mid \cdots\cdots\cdots\cdots\alpha\cdots\cdots}$$

$$c = \boxed{\cdots\cdots x\cdots\cdots\cdots\cdots \mid \cdots\cdots\cdots\cdots\alpha\cdots\cdots}$$

Ahora bien, como c es un quasi-palíndrome, (no es un palíndrome por acción de la letra x), en π_2 la posición k es obligadamente x pues en caso contrario se tendría:

$$c = \boxed{\cdots\cdots x \cdots\cdots\cdots\cdots \mid \cdots\cdots\cdots\cdots \alpha \cdots\cdots}$$

$$\pi_2 = \boxed{\cdots\cdots \beta \cdots\cdots\cdots\cdots \mid \cdots\cdots\cdots\cdots \beta \cdots\cdots}$$

lo que implicaría que $\beta = \alpha$ y en tal caso $\pi_1 = \pi_2$ lo que es una contradicción.

Concluimos que se tiene:

$$c = \boxed{\cdots\cdots x \cdots\cdots\cdots\cdots \mid \cdots\cdots\cdots\cdots \alpha \cdots\cdots}$$

$$\pi_2 = \boxed{\cdots\cdots x \cdots\cdots\cdots\cdots \mid \cdots\cdots\cdots\cdots x \cdots\cdots}$$

Es decir, la palabra c está absolutamente determinada por los palíndromes π_1 y π_2 y por tanto se tiene que $\overline{B}(\pi_1, 1) \cap \overline{B}(\pi_2, 1) = \{c\}$.

Caso $n = 2m + 1$: aquí, además, c puede diferir de π_1 y π_2 en la letra central. Si se difiere en una posición que no sea la central, el análisis es el mismo que el caso anterior; si la diferencia se constata en la letra central tenemos:

$$\pi_1 = \boxed{\cdots\cdots\cdots\cdots \mid \alpha \mid \cdots\cdots\cdots\cdots}$$

$$c = \boxed{\cdots\cdots\cdots\cdots \mid x \mid \cdots\cdots\cdots\cdots}$$

Es claro que en tales condiciones, c es un palíndrome por lo que obligadamente también difiere de π_2 en la posición central:

$$c = \boxed{\cdots\cdots\cdots\cdots \mid x \mid \cdots\cdots\cdots\cdots}$$

$$\pi_2 = \boxed{\cdots\cdots\cdots\cdots \mid \beta \mid \cdots\cdots\cdots\cdots}$$

Como $x \neq \alpha, \beta$ concluimos que en este caso $\left|\overline{B}(\pi_1, 1) \cap \overline{B}(\pi_2, 1)\right| = |A| - 2$.

(c) Para establecer la cota superior, dada una palabra de A^n, donde $n = 2m$ o $2m+1$, esta difiere en a lo más en m letras de un palíndrome: en efecto, se construye el palíndrome cuyas m o $m+1$ primeras letras coinciden con la palabra dada y cuyas últimas m letras son las m primeras escritas inversamente. Como $\left\lfloor \frac{n}{2} \right\rfloor = m$, tenemos $A^n = \bigcup_{\pi \in \Pi} \overline{B}(\pi, \left\lfloor \frac{n}{2} \right\rfloor)$

Para la cota inferior veamos que $\left|\overline{B}(\pi, 1)\right| = n + 1$; se tiene, entonces:

$$\left| \bigcup_{\pi \in \Pi} \overline{B}(\pi, \left\lfloor \frac{n}{2} \right\rfloor) \right| \leq \bigcup_{\pi \in \Pi} \left| \overline{B}(\pi, \left\lfloor \frac{n}{2} \right\rfloor) \right| = (n+1) \left|\Pi\right|$$

Ahora bien:

$$(n+1)\,|\Pi| = \begin{cases} (2m+1)\,|A|^m & \text{si } n = 2m \\ 2\,(m+1)\,|A|^{m+1} & \text{si } n = 2n+1 \end{cases} < |A|^n$$

cuando $|A| \geq 3,\ n > 3$.

161. Sean m, n enteros positivos, K un cuerpo de característica p y M el código de largo mn sobre K definido por:

$$M = \left\{ \overbrace{ww\cdots w}^{m \text{ copias de } w}\ ;\ w \text{ de largo } n \right\}$$

Demuestre que:

a) M es un código lineal.

b) $M \subset M^{\perp} \Leftrightarrow p$ divide a m.

c) M es cíclico y deduzca que $\displaystyle\sum_{k=0}^{m-1} X^{kn}$ divide a $X^{mn} - 1$ en $K[X]$.

Solución.

a) Si $w = (w_1, w_2, \ldots, w_n)$ entonces:

$$ww\cdots w = (w_1, w_2, \ldots, w_n, w_1, w_2, \cdots\cdots, w_n, \ldots, w_1, w_2, \ldots w_n)$$

es decir, $ww\cdots w = \displaystyle\sum_{k=0}^{m-1} w_k e_k$ donde:

$$e_0 = (1, 0, \ldots, 0, 1, 0, \ldots, 0, \ldots),\ e_1 = (0, 1, 0, \ldots, 0, 1, \ldots, 0, \ldots),\ \text{etc.}$$

Concluimos que M es el subespacio generado por la familia $e_0, \ldots, e_{m-1}$ por lo que M es lineal. Hacemos notar que esta familia es trivialmente libre y que la matriz generadora de M está dada por:

$$G = \begin{pmatrix} \overbrace{1 & \cdots & 0}^{m \text{ copias de } I_n} & \overbrace{1 & \cdots & 0}^{} & \cdots\cdots\cdots & \overbrace{1 & \cdots & 0}^{} \\ 0 & \ddots & 0 & 0 & \ddots & 0 & \cdots\cdots\cdots & 0 & \ddots & 0 \\ 0 & \cdots & 1 & 0 & \cdots & 1 & \cdots\cdots\cdots & 0 & \cdots & 1 \end{pmatrix}$$

b) Dada la estructura de la base de M es inmediato que:

$$e_j \bullet e_k = \begin{cases} m & \text{si } \ j = k \\ 0 & \text{si } \ j \neq k \end{cases}$$

de donde sale sin dificultad la equivalencia pedida.

c) Que M es cíclico sale de comprobar que el shift sucesivo de e_0 produce todos los e_k. Además, de la forma de la matriz G sale que el polinomio generador de M está dado por:

$$1 + X^n + X^{2n} + \cdots + X^{(m-1)n}$$

por lo que $\displaystyle\sum_{k=0}^{m-1} X^{kn}$ divide a $X^{mn} - 1$ en $K[X]$.

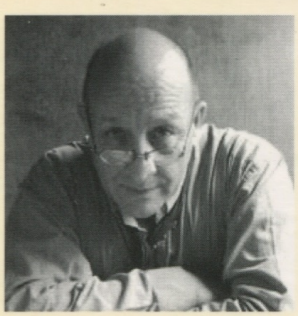
.

Referencias

- J.M. Arnaudiès, J. Bertin. *Groupes, Algèbre et Géométries*. Editions Ellipses, 1993.
- I. N. Herstein. *Algebra Abstracta*. Editorial Iberoamericana, 1986.
- A. Lentin, J. Rivaud. *Leçons d'Algèbre Moderne*.Vuibert, 1969.
- R. Lidl, H. Niederreiter: *Introduction to Finite Fields and their Applications*. Addisson Wesley, 1983.
- A. J. Kostrikin. *Introducción al Algebra*. Mc Graw-Hill, 1992.
- O. Papini, J. Wolfmann: *Algèbre Discrète et Codes Correcteurs*. Springer-Verlag, 1995.

Estas Notas introductorias son el fruto de enseñar el álgebra por más de una década en el marco de licenciaturas y pedagogías en Matemática, así como en el seno de la formación de variadas ingenierías, particularmente la Ingeniería Matemática. Los estudiantes encontrarán aquí la belleza y el rigor propios del álgebra, con sus dificultades y desafíos; les agradezco a ellos, de todo corazón, la curiosidad y la paciencia, cualidades necesarias a la pasión de aprender.

Los temas que presentamos aquí son ineludibles para una introducción formal al estudio del álgebra. El lector podrá formarse una idea básica pero exigente de las estructuras algebraicas –grupos, anillos, cuerpos, espacios vectoriales, etc.– y de sus propiedades y ramificaciones. Al respecto, hemos incorporado una mirada sobre la teoría de códigos en bloque, como una aplicación de varias de las herramientas algebraicas desarrolladas previamente. Por último, se incluye un set de ejercicios resueltos, aunque se aconseja utilizarlos solamente como ayuda y en caso alguno para reemplazar la reflexión personal.



El Dr. Cristián Mallol es Profesor Titular en la Universidad de La Frontera. Estudió en la Universidad de Montpellier (Francia), donde fue alumno de Alexander Grothendieck; llevó a cabo allí su formación superior (doctorados de Tercer Ciclo y de Estado). Durante veinte años fue académico de la Université Paul Valéry.

9 789562 362245