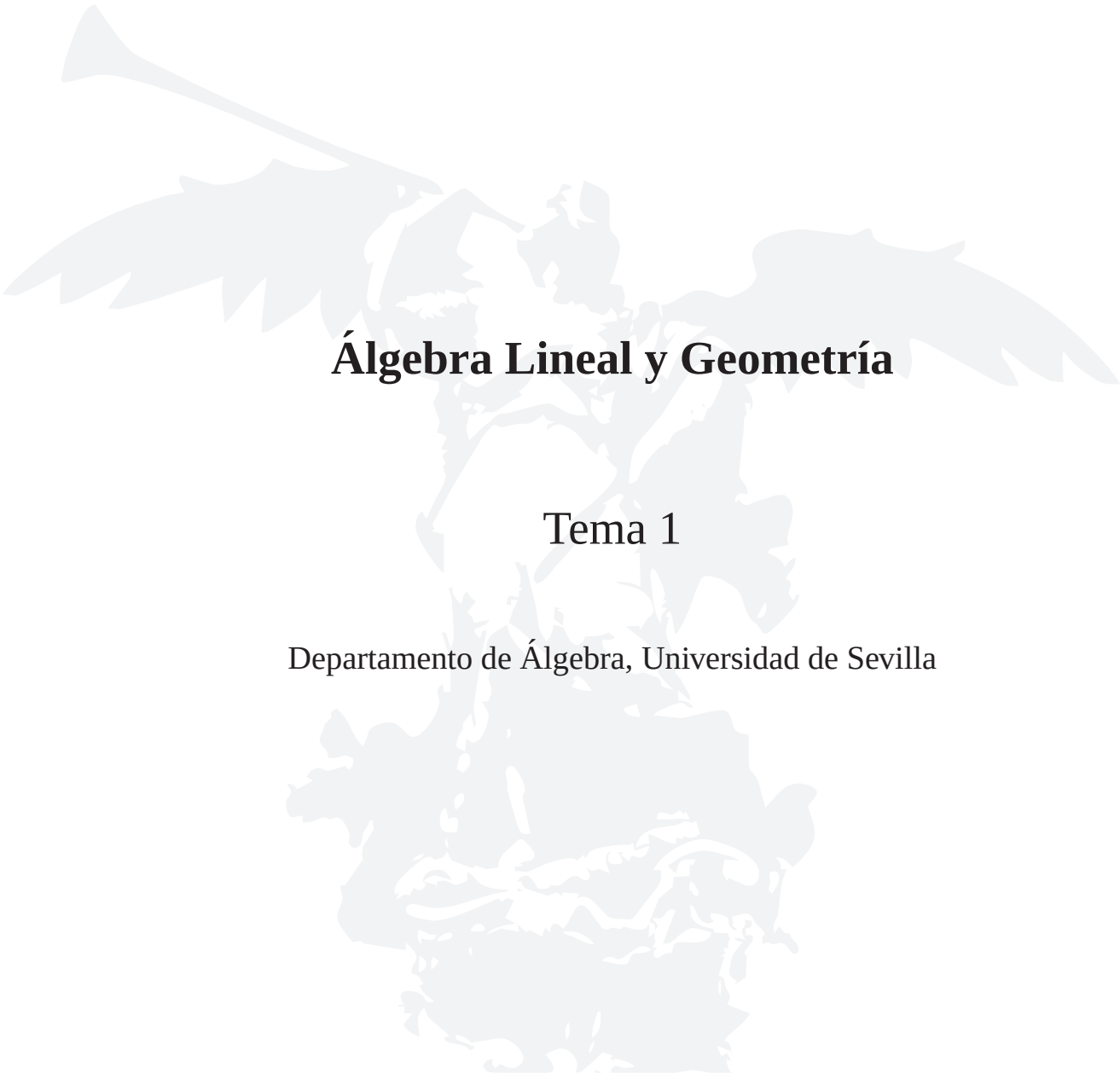

Álgebra Lineal y Geometría

Tema 1

Departamento de Álgebra, Universidad de Sevilla

UNIVERSIDAD DE SEVILLA

UNIVERSIDAD DE SEVILLA

El contenido de estas notas ha sido diseñado y redactado por el profesorado de la asignatura. Se permite su reproducción, única y exclusivamente para estudio *personal*. No se permite la copia indiscriminada, ni con fines lucrativos o diferentes del citado, de la totalidad o de parte de las presentes notas. © 2009.

Índice

UNIVERSIDAD DE SEVILLA

Tema 1: Estructuras básicas

1.1. Conjuntos: Definiciones y notaciones. Operaciones.

Definición.– Llamaremos conjunto a una colección de objetos que comparten una propiedad. Para que un conjunto esté bien definido debe ser posible discernir si un objeto arbitrario está o no en él.

Los conjuntos pueden definirse de manera explícita, citando todos sus elementos entre llaves, por ejemplo

$$A = \{1, 2, 3, 4, 5\},$$

o de manera implícita, dando una (o varias) característica(s) que determine(n) si un objeto dado está o no en el conjunto, por ejemplo

$$A = \{x \mid x \text{ es un número natural par}\},$$

que se leerá: A es el conjunto formado por los x tales que x es un número natural par. Esta última opción es obviamente imprescindible cuando el conjunto en cuestión tiene una cantidad infinita de elementos.

Notación.– Los conjuntos se notarán con letras mayúsculas: A, B,... y los elementos con minúsculas, en general. Si el elemento a pertenece al conjunto A escribiremos $a \in A$. En caso contrario escribiremos $a \notin A$.

Observación.– En ocasiones hay que considerar varios conjuntos en pie de igualdad. En estos casos es frecuente denotar los distintos conjuntos con la misma letra y un subíndice que los diferencia. Los subíndices pueden ser finitos y concretos, por ejemplo,

$$X_1, X_2, X_3, X_4, X_5;$$

finitos pero en cantidad desconocida,

$$X_1, X_2, ..., X_n,\ n \in \mathbf{N},$$

o arbitrarios; un ejemplo de esto sería considerar

$$\{A_i\}_{i \in I},$$

que se leería: la familia de conjuntos A_i donde i pertence a I. Aquí I es el conjunto de subíndices que puede o no ser finito (por ejemplo I podría ser todo $\mathbf{N}$).

Definición.– Un conjunto que carece de elementos se denomina el conjunto vacío y se denota por $\emptyset$. Un conjunto con un único elemento se denomina unitario.

Notemos que, si $X = \{x\}$ es un conjunto unitario, debemos distinguir entre el conjunto X y el elemento x.

Definición.– Dados dos conjuntos A y B, si todo elemento de A es a su vez elemento de B diremos que A es un subconjunto de B y lo notaremos $A \subset B$. En caso contrario se notará $A \not\subset B$.

Proposición.– Sean A, B y C tres conjuntos cualesquiera. Se tienen las siguientes propiedades:

(a) $A \subset A$, $\emptyset \subset A$.

(b) Si $A \subset B$ y $B \subset A$, entonces $A = B$.

(c) Si $A \subset B$ y $B \subset C$, entonces $A \subset C$.

Demostración.– La primera propiedad se sigue directamente de la definición.

Para probar (b), fijémonos en que dos conjuntos son iguales si tienen exactamente los mismos elementos. Pero esto es tanto como decir que todos los elementos de A están en B, y viceversa; eso es que $A \subset B$ y $B \subset A$.

Esta propiedad se utiliza muy frecuentemente para demostrar igualdades de conjuntos por el procedimiento denominado *doble inclusión*. Éste consiste en, dados los dos conjuntos, probar primero que todo elemento del primero está en el segundo, y luego que todo elemento del segundo está en el primero. Aplicando entonces el apartado (b), queda demostrado que ambos conjuntos son iguales.

La demostración de (c) se sigue de la definición de subconjunto: todo elemento de A está en B, por ser $A \subset B$ y, dado que es elemento de B, está en C por ser $B \subset C$. Así todo elemento de A está en C y hemos finalizado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Definición.– Dado dos conjuntos $A \subset X$ se define el complementario de A en X (o simplemente el complementario de A, si el conjunto X no se presta a confusión) como

$$X \setminus A = \{x \mid x \in X,\, x \notin A\},$$

esto es, el conjunto de elementos de X que no están en A. Otras notaciones que se puede encontrar para $X \setminus A$ (donde X se obvia) son $\overline{A}$ o cA.

Observación.– Dados $A \subset X$, se dan las siguientes igualdades obvias:

$$\overline{\emptyset} = X,\ \overline{X} = \emptyset,\ \overline{\overline{A}} = A.$$

Nos detendremos solamente en la tercera de las anteriores propiedades. En efecto, por definición

$$\overline{\overline{A}} = \{x \mid x \in X,\, x \notin \overline{A}\},$$

pero para un $x \in X$, $x \notin \overline{A}$ si y sólo si $x \in A$, por tanto los elementos de $\overline{\overline{A}}$ son precisamente los de A.

Notación.– Cuando A es un conjunto finito, el número de elementos de A se denomina cardinal de A y se notará $\sharp(A)$.

UNIVERSIDAD DE SEVILLA

Definición.– Dados dos conjuntos A y B se define la unión de A y B, notado $A \cup B$ como el conjunto formado por aquéllos elementos que pertencen al menos a uno de los dos conjuntos, A ó B.

Se definen de forma equivalente la unión de una cantidad finita de conjuntos $A_1, ..., A_n$, que denotaremos

$$A_1 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i,$$

y la unión de una familia arbitrariamente grande de conjuntos $\{A_i\}_{i \in I}$, que denotaremos

$$\bigcup_{i \in I} A_i.$$

Proposición.– La unión de conjuntos verifica las siguientes propiedades, para cualesquiera conjuntos A, B y C:

(a) Conmutativa: $A \cup B = B \cup A$.

(b) Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$.

(c) $\emptyset \cup A = A$.

(d) $A \subset B \iff A \cup B = B$.

(e) Si $A \subset B$, entonces $A \cup (B \setminus A) = B$.

Demostración.– Todas las pruebas son sencillas, y son un buen ejercicio para que el alumno comience a tratar de plasmar demostraciones rigurosas. Como ilustración de cómo se ataca una doble implicación, probaremos (d).

Comenzaremos suponiendo que $A \subset B$. Entonces todos los elementos de A están en B, por tanto $A \cup B = B$ de manera inmediata. Recíprocamente, supongamos que $A \cup B = B$. Entonces todo elemento que esté en A ó en B está forzosamente en B, con lo que se tiene $A \subset B$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Definición.– Dados dos conjuntos A y B se define la intersección de A y B, notado $A \cap B$, como el conjunto formado por aquéllos elementos que pertencen al mismo tiempo a ambos conjuntos, A y B.

Se definen de forma equivalente la intersección de una cantidad finita de conjuntos $A_1, ..., A_n$, y la intersección de una familia arbitrariamente grande de conjuntos $\{A_i\}_{i \in I}$, que denotaremos, respectivamente,

$$A_1 \cap ... \cap A_n = \bigcap_{i=1}^{n} A_i, \text{ y } \bigcap_{i \in I} A_i.$$

Si A y B son dos conjuntos tales que $A \cap B = \emptyset$ se dice que A y B son disjuntos.

Proposición.– La intersección de conjuntos verifica las siguientes propiedades, para cualesquiera conjuntos A, B y C:

(a) Conmutativa: $A \cap B = B \cap A$.

UNIVERSIDAD DE SEVILLA

(b) Asociativa: $(A \cap B) \cap C = A \cap (B \cap C)$.

(c) $\emptyset \cap A = \emptyset$.

(d) $A \subset B \iff A \cap B = A$.

(e) Si $A \subset B$, entonces $A \cap (B \setminus A) = \emptyset$.

Demostración.– Las demostraciones se dejan como ejercicios. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Proposición.– Dados tres conjuntos A, B y C se verifican las siguientes igualdades:

(a) Leyes distributivas:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

(b) Leyes de De Morgan (supongamos $A, B \subset C$):

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B), \quad C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$$

Demostración.– Probaremos una de las leyes distributivas y una de las leyes de De Morgan; las restantes quedan como ejercicio por ser simétricas a las probadas. Ambos resultados se probarán por doble inclusión.

Veamos que $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Para ello tomemos un elemento arbitrario $x \in A \cap (B \cup C)$. Esto quiere decir que x está en A y además en B ó en C. Esto implica que, bien está en $A \cap B$, bien está en $A \cap C$. En cualquier caso $x \in (A \cap B) \cup (A \cap C)$.

Demostremos ahora que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Si consideramos un elemento cualquiera $y \in (A \cap B) \cup (A \cap C)$, y ha de pertencer a $A \cap B$ o a $A \cap C$. Por tanto, bien está en A y en B o en A y en C. En cualquier circunstancia ha de estar en A y al menos en uno de los otros dos conjuntos B ó C. De aquí $y \in A$ y además $y \in B \cup C$.

Pasemos a probar la segunda ley de De Morgan. Veamos primero $C \setminus (A \cap B) \subset (C \setminus A) \cup (C \setminus B)$. Un elemento x de $C \setminus (A \cap B)$ ha de estar en C, pero no en $A \cap B$, por lo que no puede estar en al menos uno de los dos conjuntos A ó B. Así, x ha de pertenecer, bien a $C \setminus A$, bien a $C \setminus B$. En cualquier caso $x \in (C \setminus A) \cup (C \setminus B)$.

Si tomamos ahora un elemento $z \in (C \setminus A) \cup (C \setminus B)$, observemos que z ha de estar, bien en $C \setminus A$, bien en $C \setminus B$, por lo que debe estar en C y *no estar* en A ó en B. Así, $z \in C$, pero nunca puede estar en $A \cap B$, por lo que $z \in C \setminus (A \cap B)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

1.2. Producto cartesiano. Relaciones de equivalencia.

Definición.– Dados dos conjuntos A y B, se define el producto cartesiano de A y B como el conjunto de pares ordenados formados (por este orden) por un elemento de A y uno de B y se denota

$$A \times B = \{(a, b) \mid a \in A,\, b \in B\}.$$

UNIVERSIDAD DE SEVILLA

Dado $(a, b) \in A \times B$, el elemento $a \in A$ (respectivamente $b \in B$) se suele denominar primera (segunda) componente del par.

También se puede definir el producto cartesiano de una cantidad finita de conjuntos (para cantidades infinitas hay dos posibles generalizaciones y no las veremos aquí) de la forma natural

$$A_1 \times ... \times A_n = \prod_{i=1}^{n} A_i = \{(a_1, ..., a_n) \mid a_i \in A_i, \text{ para } i = 1, ..., n\}.$$

Definición.– Una correspondencia G de A en B es un subconjunto del producto $A \times B$. Equivalentemente se puede definir como una regla que asocia algunos elementos de A con algunos elementos de B. Concretamente, G asocia $a \in A$ con $b \in B$ si $(a, b) \in G$.

Definición.– Sea A un conjunto. Una relación R definida en A es una correspondencia de A en sí mismo.

Si el par $(x, y) \in A \times A$ está en R, diremos que x está R–relacionado con y, o relacionado con y por R. Esto se notará frecuentemente xRy (nótese que el orden es importante).

Definición.– Sea R una relación en A. Entonces diremos que R es:

(a) Reflexiva cuando para todo $x \in A$ se tiene que xRx.

(b) Simétrica cuando xRy implica yRx.

(c) Antisimétrica cuando xRy e yRx implican $x = y$ necesariamente.

(d) Transitiva cuando xRy e yRz implican xRz.

Las relaciones reflexivas, simétricas y transitivas se denominan relaciones de equivalencia. Las relaciones reflexivas, antisimétricas y transitivas se denominan relaciones de orden, pero no las trataremos aquí.

Ejemplos.– En el conjunto $\mathbf{Z}$ definimos la relación siguiente, notada S:

$$xSy \iff x - y \text{ es par},$$

Entonces R es una relación de orden (de hecho, las relaciones de orden se denominan así por ser éste el ejemplo fundamental), T también lo es y S es una relación de equivalencia. De hecho, notemos que S es de equivalencia si sustituimos la condición "$x - y$ es par" por la condición "$x - y$ es múltiplo de p", para cualquier número p que fijemos con antelación.

Definición.– Si R es una relación de equivalencia en A, denominamos clase de equivalencia de un elemento $x \in A$ al conjunto de todos los elementos de A relacionados con x, esto es,

$$\overline{x} = R(x) = \{y \in A \mid xRy\},$$

donde la primera notación se usa si R se sobreentiende, y la segunda si no es así.

Proposición.– Sea A un conjunto, R una relación de equivalencia en A. Entonces se verifican las siguientes propiedades:

UNIVERSIDAD DE SEVILLA

(a) Todo elemento pertenece a una clase de equivalencia.

(b) Dos clases de equivalencia son disjuntas o iguales.

Esto es, la relación R divide completamente al conjunto A en subconjuntos disjuntos (las clases de equivalencia).

Demostración.– La afirmación (a) es trivial, ya que R es reflexiva. Para probar (b) supongamos que tenemos dos clases de equivalencia $R(x)$ y $R(y)$ de tal forma que existe $z \in R(x) \cap R(y)$. Tenemos que demostrar entonces que $R(x) = R(y)$, y lo haremos por doble inclusión. De hecho, sólo probaremos que $R(x) \subset R(y)$, porque la otra inclusión es absolutamente simétrica.

Tomamos entonces $a \in R(x)$. Como $z \in R(x)$, tenemos que aRx y xRz, por lo que aRz. De la misma forma, como $z \in R(y)$, se verifica que zRy. Así tenemos aRy, luego $a \in R(y)$. Observemos que hemos usado tanto la propiedad simétrica como la transitiva para demostrar (b). $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Definición.– Dada una relación de equivalencia R definida sobre un conjunto A, el conjunto cuyos elementos son las clases de equivalencia de A por R se denomina conjunto cociente de A por R. La notación ususal es

$$A/R = \{R(x) \mid x \in A\}.$$

Ejemplo.– Volviendo al ejemplo anterior, tomamos un entero p, fijado para lo que sigue, y consideramos

$$xSy \iff x - y \text{ es múltiplo de } p.$$

Entonces se tiene que, para todo $x \in \mathbf{Z}$

$$S(x) = \{y \in \mathbf{Z} \mid \ x \text{ e } y \text{ dan el mismo resto al dividirlos entre } p\},$$

por lo que

$$\mathbf{Z}/S = \{S(0), S(1), ..., S(p-1)\}.$$

1.3. Aplicaciones.

Una aplicación f de A en B es una correspondencia donde todo elemento de A tiene asociado un único elemento de B. Esto es, en notación matemática, una correspondencia G es una aplicación si y sólo si se verifica que

$$\forall a \in A \quad \exists! b \in B \ \text{ tal que } (a, b) \in G.$$

Notación.– Es habitual denotar una aplicación entre conjuntos A y B de la forma $f : A \longrightarrow B$. En estas condiciones, dado $a \in A$ el único b verificando $(a, b) \in f$ se denota $f(a)$ y se denomina imagen de a (por f).

De esta notación surge la terminología, comúnmente usada, de llamar a A conjunto original (o dominio) y a B conjunto imagen.

En según qué contextos (por ejemplo, en Análisis Matemático, o cuando el conjunto de llegada es $\mathbf{R}^n$) es habitual llamar a las aplicaciones funciones, pero durante este curso utilizaremos la denominación aplicaciones.

Definición.– Dada una aplicación $f : X \longrightarrow Y$ y subconjuntos $A \subset X$ y $B \subset Y$, definimos:

(a) La imagen de A, notada $f(A)$, como

$$f(A) = \{y \in Y \mid \exists x \in A \text{ con } f(x) = y\} \subset Y,$$

esto es, el conjunto de elementos del conjunto imagen que son imagen de un elemento de A.

(b) La anti–imagen (o contraimagen, o imagen recíproca) de B, notada $f^{-1}(B)$, como

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subset X,$$

esto es, el conjunto de elementos del conjunto original cuya imagen está en B.

Proposición.– Sea $f : X \longrightarrow Y$ una aplicación, $A_1, A_2 \subset X$ y $B_1, B_2 \subset Y$. Se verifica:

(a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.

(b) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(c) $f(f^{-1}(B_1)) \subset B_1$, $A_1 \subset f^{-1}(f(A_1))$.

Demostración.– Vamos a probar, por ejemplo, la segunda afirmación de (a) y la primera de (c). Las demás son similares. Consideremos $y \in f(A_1 \cap A_2)$. Entonces existe $x \in A_1 \cap A_2$ tal que $y = f(x)$. Por tanto, $y \in f(A_1)$ e $y \in f(A_2)$, por lo que se tiene el resultado.

Es importante entender que, para afirmar que la otra inclusión no es cierta, basta con dar un contraejemplo; esto es, un caso particular donde no sea cierto el enunciado. Para ello consideremos $f : \mathbf{N} \longrightarrow \mathbf{N}$ definida por

$$f(x) = \begin{cases} x/2 + 1 & \text{si } x \text{ es par} \\ x + 2 & \text{si } x \text{ es impar} \end{cases}$$

Tomamos $A_1 = \{1, 3, 5\}$, $A_2 = \{2, 4, 6\}$. Claramente $f(A_1 \cap A_2) = f(\emptyset) = \emptyset$, pero $f(A_1) \cap f(A_2) = \{3\}$.

Probemos ahora que $f(f^{-1}(B_1)) \subset B_1$. Si $y \in f(f^{-1}(B_1))$, es porque existe $x \in f^{-1}(B_1)$ tal que $y = f(x)$. Pero, al ser $x \in f^{-1}(B_1)$, por definición tenemos que $y = f(x) \in B_1$.

Para demostrar que la inclusión contraria no es cierta en general podemos tomar la misma aplicación que en el caso anterior y considerar $B_1 = \{1, 3, 5\}$ nuevamente. Entonces $f^{-1}(B_1) = \{1, 3, 4, 8\}$ (por convenio, no incluimos el 0 en $\mathbf{N}$). Pero $f(f^{-1}(B_1)) = \{3, 5\}$, por lo que hemos acabado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Definición.– Sea una aplicación $f : X \longrightarrow Y$.

(a) f se dice inyectiva si dos elementos distintos de X siempre tienen imágenes distintas. Dicho de otro modo, f es inyectiva si, de $f(x) = f(x')$, para $x, x' \in X$, se deduce que $x = x'$.

(b) f se dice sobreyectiva (o sobre) si todo elemento de Y es imagen de algún elemento de X. O sea, f es sobre si $f(X) = Y$.

(c) f se dice biyectiva si es inyectiva y sobreyectiva.

Observación.– Así, podemos decir que:

(a) f es inyectiva si y sólo si para todo $y \in Y$ $f^{-1}(\{y\})$ consta, a lo más, de un elemento.

(b) f es sobre si y sólo si para todo $y \in Y$ $f^{-1}(\{y\})$ consta, a lo menos, de un elemento.

(c) f es biyectiva si y sólo si para todo $y \in Y$ $f^{-1}(\{y\})$ consta, exactamente, de un elemento.

De esta forma, si f es biyectiva, existe una aplicación, denominada aplicación inversa y notada $f^{-1} : Y \longrightarrow X$, definida por $f^{-1}(y) = x$ si y sólo si $f(x) = y$.

Las aplicaciones inyectivas, sobres o biyectivas verifican algunas propiedades más concretas de las que enunciamos con anterioridad.

Definición.– Dadas dos aplicaciones $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ se define la composición de f y g, notada $g \circ f$, de X en Z como

$$(g \circ f)(x) = g(f(x)), \text{ para todo } x \in X.$$

Obviamente $g \circ f$ es una aplicación.

Definición.– Dada una aplicación $f : X \longrightarrow Y$ y un subconjunto $A \subset X$, se define la restricción de f a A como la aplicación

$$\begin{array}{rcl} f_{|A} : A & \longrightarrow & Y \\ x & \longmapsto & f_{|A}(x) = f(x) \end{array}$$

Esto es, $f_{|A}$ actúa exactamente como f, pero sólo sobre los elementos de A. Esto pone de manifiesto (o debería) lo importante que es, a la hora de definir una aplicación, determinar los conjuntos de partida y llegada, no sólo cómo se calcula la imagen de un elemento.

1.4. Grupos, anillos y cuerpos.

Definición.– Dado un conjunto G, una operación interna binaria, $\bullet$, en G es una aplicación

$$\begin{array}{rcl} \bullet : G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & \bullet(a, b) \end{array}$$

Habitualmente se utiliza la notación $\bullet(a,b) = a \bullet b$. Una operación externa (binaria) es exactamente lo mismo, salvo por el hecho de que el conjunto de partida es $X \times G$, para un cierto conjunto X distinto de G.

Un grupo es un par $(G, \bullet)$, compuesto por un conjunto G y una operación interna $\bullet$ en G, que verifica las siguientes propiedades:

(G.1) Asociativa: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$, para cualesquiera $a, b, c \in G$.

(G.2) Elemento neutro: Existe un $e \in G$ tal que $a \bullet e = e \bullet a = a$, para todo $a \in G$.

(G.3) Elemento opuesto: Dado $a \in G$ existe $b \in G$ tal que $a \bullet b = b \bullet a = e$, el elemento neutro antes mencionado.

Si $(G, \bullet)$ posee además la propiedad conmutativa (esto es $a \bullet b = b \bullet a$ para cualesquiera $a, b \in G$), se dice que el grupo es abeliano o conmutativo.

Proposición.– Dado un grupo $(G, \bullet)$, el elemento neutro es único. Además, fijado $a \in G$, el elemento opuesto de a también es único.

Demostración.– Supongamos que e' es otro elemento neutro. Entonces

$$e = e \bullet e' = e' \bullet e = e'.$$

Sean ahora entonces b y c dos elementos opuestos de un $a \in G$ arbitrario, pero fijado en lo que sigue. Entonces

$$e = a \bullet b \implies c = c \bullet e = c \bullet a \bullet b = e \bullet b = b.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Notación.– Existen dos notaciones usuales para la operación en un grupo: la notación aditiva y la notación multiplicativa, que heredan las notaciones para los grupos conocidos $(k, +)$ y $(k \setminus \{0\}, \cdot)$, donde k puede ser $\mathbf{Q}$ o $\mathbf{R}$.

Si escribimos un grupo en notación aditiva, $(G, +)$, denotaremos 0 al elemento neutro y $-a$ al opuesto de a. Por el contrario, si usamos la notación multiplicativa, $(G, \cdot)$ denotaremos por 1 al elemento neutro y por a^{-1} o por $1/a$ al opuesto de a (que se denominará entonces inverso de a). Muchas veces la operación $\cdot$ se denota por simple yuxtaposición, esto es, ab en lugar de $a \cdot b$.

Observación.– Dado un grupo (pongamos en notación multiplicativa) G y un elemento $g \in G$ se puede probar (ejercicio fácil de doble inclusión) que el conjunto $g \cdot G = \{gx \mid x \in G\}$ es de nuevo G.

Definición.– Un cuerpo k es un conjunto con dos operaciones binarias internas, denominadas usualmente suma o adición $(+)$ y producto o multiplicación $(\cdot)$, de tal forma que

(C.1) $(k, +)$ es un grupo abeliano.

(C.2) $(k \setminus \{0\}, \cdot)$ es un grupo abeliano.

(C.3) Se da la propiedad distributiva de la suma respecto del producto:

$$a(b + c) = ab + ac, \quad \text{para cualesquiera } a, b, c, \in k.$$

UNIVERSIDAD DE SEVILLA

Ejemplos.– Los ejemplos usuales de cuerpos son $\mathbf{Q}$ y $\mathbf{R}$. Veremos un ejemplo más adelante de gran impotancia: los números complejos.

En concreto el cuerpo $\mathbf{Q}$ podemos entenderlo como un buen ejemplo de relación de equivalencia. El conjunto base es, en este caso

$$X = \mathbf{Z} \times (\mathbf{Z} \setminus \{0\}) = \{\ (a,b) \mid a,b \in \mathbf{Z},\ b \neq 0\ \},$$

y la relación viene definida por

$$(a,b) \sim (a',b') \iff ab' = a'b.$$

En este contexto, la notación estndar para la clase de equivalencia del par (a,b) por la relación $\sim$ es, obviamente, a/b.

Definición.– Un anillo es un conjunto A dotado con dos operaciones binarias internas, usualmente denominadas suma o adición $(+)$ y producto o multiplicación $(\cdot)$, de tal forma que:

(A.1) $(A,+)$ es un grupo abeliano.

(A.2) La operación $(\cdot)$ es asociativa, conmutativa y posee elemento neutro (notado 1)[1].

(A.3) Se verifica la propiedad distributiva de la suma respecto del producto:

$$a \cdot (b+c) = a \cdot b + a \cdot c, \text{ para cualesquiera } a,b,c \in A.$$

Observación.– En un anillo A, $0 \cdot a = 0$ para todo $a \in A$, ya que

$$a + 0 \cdot a = a \cdot (1+0) = a \cdot 1 = a.$$

De similar forma se puede probar, por ejemplo, que $(-1) \cdot a = -a$ para todo $a \in A$.

Ejemplo.– El ejemplo fundamental de anillo son los enteros, $\mathbf{Z}$, con la suma y el producto usuales. Un ejemplo enormemente similar (luego veremos por qué) es el de los polinomios con coeficientes en $\mathbf{Q}$ o en $\mathbf{R}$.

1.5. Grupos cíclicos. Permutaciones.

Ejemplo.– Un primer ejemplo de grupo que puede resultar nuevo (aunque no tanto, como veremos), es C_n, el grupo cíclico de n elementos generado por una variable a. Si usamos la notación multiplicativa

$$C_n = \left\{a^0 = 1, a^1 = a, a^2, ..., a^{n-1}\right\},$$

y la operación entre dos elementos del grupo es

$$a^m \cdot a^p = a^r,$$

[1] No creemos necesario establecer la definición más general posible de anillo, que admite la posibilidad de que el producto no sea abeliano ni posea elemento neutro.

UNIVERSIDAD DE SEVILLA

donde r es el resto de dividir $m+p$ entre n (por tanto un número entre 0 y $n-1$).

En notación aditiva tendremos

$$C_n = \{0, a, 2a, ..., (n-1)a\}$$

con la operación $ma + pa = ra$, donde r es el resto de dividir $m+p$ entre n de nuevo. En cualquiera de ambas notaciones es obvio que C_n es abeliano.

Entre las muchas encarnaciones de C_n en la vida diaria, tal vez sea C_{12} (o C_{24}, tanto da) en el sistema horario la más evidente. Con algo más de lenguaje, podemos considerar otros ejemplos como C_7 en los días de la semana.

Ejemplo.– Tomemos el conjunto $A = \{1, 2, ..., n\}$ y sea

$$S_n = \{f : A \longrightarrow A \mid f \text{ biyectiva } \}.$$

De la caracterización estudiada en 1.3. para las aplicaciones biyectivas se sigue que la composición de dos aplicaciones biyectivas es de nuevo biyectiva. Por tanto en S_n podemos definir una operación interna, que no es más que la composición de aplicaciones.

El par $(S_n, \circ)$ es entonces un grupo, como es sencillo de probar, con la aplicación, denominada identidad,

$$\begin{array}{rcl} \text{Id} : A & \longrightarrow & A \\ i & \longmapsto & i \end{array}$$

como elemento neutro y, dada $f \in S_n$, con f^{-1} como elemento inverso.

Es posible entender cada aplicación de S_n como una reordenación del conjunto $\{1, ..., n\}$. Es por esto que $(S_n, \circ)$ se denomina el grupo de permutaciones de n elementos. Cuidado: S_n *no tiene* n elementos, un cálculo combinatorio trivial nos dice que S_n es un grupo con $n!$ elementos. De aquí es usual denotar los elementos de S_n como una tabla con dos filas: en la primera aparecen los números del 1 al n (para saber cuál es el conjunto original) y en la segunda aparecen, bajo cada original, su imagen. Por ejemplo:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{bmatrix}$$

es la aplicación de $\{1, 2, 3, 4, 5\}$ en sí mismo que envía 1 en 4, 2 en 3, 3 en 2, 4 en 1 y 5 en sí mismo.

Casi cualquier ejemplo no trivial sirve para ver que $(S_n, \circ)$ no es abeliano para $n \geq 3$.

Una cierta forma de medir cuánto altera una permutación $\sigma \in S_n$ el orden natural en $\{1, 2, ..., n\}$ es ver el número de inversiones que σ efectúa: para cada $i \in \{1, 2, ..., n\}$ se cuenta una inversión por cada $j > i$ tal que $\sigma(i) > \sigma(j)$. En nuestro ejemplo anterior tenemos que contar:

- Tres inversiones porque $\sigma(1) > \sigma(2), \sigma(3), \sigma(4)$.
- Dos inversiones porque $\sigma(2) > \sigma(3), \sigma(4)$.
- Una inversión porque $\sigma(3) > \sigma(4)$.

Luego el número de inversiones de σ es 6. Este concepto será útil con posterioridad, para la definición de determinante.

UNIVERSIDAD DE SEVILLA

1.6. Los números complejos.

El cuerpo de los números complejos se puede definir como sigue: sea $\mathbf{C}$ el conjunto

$$\mathbf{C} = \{a + b\imath \mid a, b \in \mathbf{R}\},$$

donde $\imath$ es, por ahora una variable, esto es, un símbolo carente de significado propio, denominado unidad imaginaria.

Dado un complejo $z = a + b\imath$, el número real a se denomina parte real de z, notado $\Re(z)$, mientras que b se denomina parte imaginaria de z, notado $\Im(z)$.

Dotamos a $\mathbf{C}$ de una estructura de cuerpo con las siguientes operaciones:

$$(a + b\imath) + (c + d\imath) = (a + c) + (b + d)\imath,$$

$$(a + b\imath)(c + d\imath) = (ac - bd) + (ad + bc)\imath,$$

regla esta última que puede ser fácilmente recordada si decimos que $\imath$ representa $\sqrt{-1}$.

Comprobar que $\mathbf{C}$ con estas dos operaciones es un cuerpo es algo tedioso. Simplemente notaremos que el elemento neutro de la suma es $0 = 0 + 0\imath$ y el neutro del producto es $1 = 1 + 0\imath$. Así mismo, dado $a + b\imath$ el inverso aditivo es $-a + (-b)\imath$ y, si es distinto de 0, el inverso multiplicativo es precisamente $a/(a^2 + b^2) - (b/(a^2 + b^2))\imath$.

Observación.– Algunas propiedades interesantes de los número complejos son las siguientes:

(a) Si consideramos los números complejos de la forma $a + 0\imath$ veremos que podemos suponer $\mathbf{R} \subset \mathbf{C}$, identificando $a \in \mathbf{R}$ con $a + 0\imath \in \mathbf{C}$.

(b) Dado un complejo $z = a + b\imath$, el complejo $\overline{z} = a - b\imath$ se denomina su conjugado. La operación de conjugación, a pesar de su inofensivo aspecto, tiene una importancia enorme, incluso en el estudio de objetos reales. Un par de propiedades inmediatas, a partir de la definición, son las siguientes:

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \qquad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2},$$

de donde a su vez se deducen

$$\overline{-z} = -\overline{z}, \qquad \overline{1/z} = 1/\overline{z}.$$

(c) El producto $z\overline{z} = a^2 + b^2$ es un real positivo, y su raíz cuadrada se llama el módulo de z, denotado $|z|$. De hecho, la expresión del inverso multiplicativo de z resulta más sencilla usando $\overline{z}$:

$$\frac{1}{z} = \frac{\overline{z}}{\overline{z}} \cdot \frac{1}{z} = \frac{\overline{z}}{|z|}.$$

(c) Todo número complejo z se puede escribir de forma

$$z = |z|(a + b\imath),$$

donde $a^2 + b^2 = 1$ y, en consecuencia, existe un único ángulo $\alpha \in [0, 2\pi)$, llamado argumento de z, tal que $z = |z|(\cos(\alpha) + \text{sen}(\alpha)\imath)$.

UNIVERSIDAD DE SEVILLA

De esta última escritura y de las fórmulas trigonométricas podemos deducir fácilmente que, dados $z_1, z_2 \in \mathbf{C}$, si escribimos

$$z_i = |z_1| \left(\cos(\alpha_i) + \text{sen}\alpha_i \imath\right), \quad i = 1, 2;$$

entonces

$$z_1 \cdot z_2 = |z_1|\ |z_2|(\cos(\alpha_1 + \alpha_2) + \text{sen}(\alpha_1 + \alpha_2)\imath).$$

Esto es, multiplicar números complejos equivale a multiplicar módulos y *sumar* argumentos. En particular esto prueba, por inducción, que

$$z = |z|(\cos(\alpha) + \text{sen}(\alpha)\imath) \implies z^n = |z|^n(\cos(n\alpha) + \text{sen}(n\alpha)\imath), \quad \forall n \in \mathbf{N}.$$

De esta forma demostramos que todo número complejo z tiene exactamente n raíces n–ésimas. En efecto, si z tiene módulo $|z|$ y argumento α, entonces sus raíces n–ésimas son las que tienen módulo $\sqrt[n]{|z|}$ (que es único si imponemos que sea un real positivo) y argumento β tal que $n\beta = \alpha$. Hay exactamente n de estos ángulos (distintos):

$$\beta \in \left\{ \frac{\alpha + 2k\pi}{n} \mid k = 0, ..., n-1 \right\}$$

En realidad lo que se puede decir es mucho más, pero no lo demostraremos.

Teorema fundamental del álgebra.– Toda ecuación de grado n en $\mathbf{C}[X]$ tiene, al menos, una solución en $\mathbf{C}$.

Corolario.– Toda ecuación de grado n en $\mathbf{C}[X]$ tiene, exactamente, n soluciones (eventualmente repetidas) en $\mathbf{C}$.

1.7. Polinomios.

Recordemos que un polinomio en la variable X con coeficientes en un cuerpo k es una expresión del tipo

$$p(X) = a_0 + a_1 X + ... + a_r X^r,$$

donde los a_i están en k. Cuando $a_r \neq 0$, decimos que el grado de $p(X)$ es r (por ahora supondremos que 0 no tiene grado alguno), notado $\text{gr}(p(X))$. La suma se hace sumando los coeficientes que acompañan a iguales potencias de X y el producto de dos polinomios se lleva a cabo multiplicando todos los sumandos del primero por todos los del segundo con la regla

$$aX^r \cdot bX^t = (ab)X^{r+t}$$

y sumando todos los resultados. Dado que el producto de dos elementos de k distintos de 0 es siempre distinto de 0 (porque $(k \setminus \{0\}, \cdot)$ es un grupo), tenemos que

$$\text{gr}(p(X)q(X)) = \text{gr}(p(X)) + \text{gr}(q(X)).$$

El anillo de los polinomios con coeficientes en k se denota $k[X]$.

Un parecido curioso entre $k[X]$ y $\mathbf{Z}$ es la existencia de una división. En efecto, dados dos enteros a y b, existen únicos q y r (denominados cociente y resto, respectivamente) verificando

$$a = qb + r, \;\; r = 0 \;\text{ó}\; 1 \leq r \leq b - 1.$$

De la misma forma, dados dos polinomios en $k[X]$, $a(X)$ y $b(X)$, existen polinomios únicos $q(X)$ y $r(X)$ (también denominados cociente y resto) en $k[X]$ verificando

$$a(X) = q(X)b(X) + r(X), \;\; r = 0 \text{ ó } 0 \leq \text{gr}(r(X)) \leq \text{gr}(b(X)) - 1.$$

Observación.– No todos los anillos poseen una división similar. Un primer ejemplo es el de los polinomios con coeficientes enteros, lógicamente notado $\mathbf{Z}[X]$. Observemos que la suma y el producto de polinomios con coeficientes enteros resulta de nuevo un polinomio con coeficientes enteros y todas las propiedades son triviales de verificar; por tanto $\mathbf{Z}[X]$ es un anillo. Además, sigue siendo cierta la propiedad de que el grado de un producto es la suma de los grados de los factores.

Sin embargo, dados $a(X)$ y $b(X)$ no siempre es posible hallar $q(X)$ y $r(X)$ en $\mathbf{Z}[X]$ verificando las propiedades anteriormente mencionadas. Por ejemplo, consideremos $a(X) = X^2 + X + 1$ y $b(X) = 2X + 1$. Si existieran $q(X)$ y $r(X)$ verificando las propiedades requeridas, tendría que darse:

$$\text{gr}(q(X)) = 1, \; r(X) = 0 \text{ ó } \text{gr}(r(X)) = 0,$$

esto es, $q(X) = \alpha X + \beta$, $r(X) = \gamma$, con $\alpha, \beta, \gamma \in \mathbf{Z}$. Pero además debe cumplirse $2\alpha = 1$, lo cual es imposible.

Un caso similar es el de los polinomios en más de una variable. Consideremos el conjunto $k[X, Y]$, formado por sumas finitas de términos de la forma

$$aX^iY^j, \; a \in k, \; i, j \in \mathbf{N} \cup \{0\},$$

denominados monomios.

En $k[X, Y]$ podemos definir, de manera análoga al caso $k[X]$, una suma (sumando coeficientes que acompañen a los mismos X^iY^j) y un producto que lo dotan de estructura de anillo. Una vez más, tampoco es posible definir una división análoga a la que se da en $k[X]$. Veamos ahora, para el caso de polinomios en una variable, otro concepto central: el de raíz.

Definición.– Si $P(X)$ es un polinomio, las soluciones de la ecuación $P(X) = 0$ se denominan raíces de $P(X)$.

Dado dos polinomios $P(X), Q(X) \in k[X]$, diremos que $Q(X)$ divide a $P(X)$ si el resto de la división de $P(X)$ entre $Q(X)$ es 0.

Sea $P(X) \in k[X]$, $\alpha \in k$. Se denomina multiplicidad de α en $P(X)$ al único entero $\nu \in \mathbf{N}$ que verifica que $(X - \alpha)^\nu$ divide a $P(X)$, pero $(X - \alpha)^{\nu+1}$ no divide a $P(X)$ (la unicidad es inmediata de las propiedades de la división.

La relación entre multiplicidad y raíces la da el siguiente resultado.

Lema.– El escalar α es raíz de $P(X) = 0$ si y sólo si $X - \alpha$ divide a $P(X)$.

Demostración.– La implicación inversa es muy simple, así que sólo haremos la directa. Supongamos que α es raíz de $P(X)$ y dividamos $P(X)$ entre $X-\alpha$ para obtener

$$P(X) = q(X)(X-\alpha) + r(X), \text{ con } r = 0, \text{ ó } \text{gr}(r) < \text{gr}(X-\alpha) = 1.$$

Entonces $r = \beta \in k$ y, al hacer $X = \alpha$ obtenemos

$$0 = P(\alpha) = q(\alpha)(\alpha - \alpha) + \beta = \beta.$$

Proposición.– Si $P(X)$ es un polinomio de grado m, con raíces (distintas) $\alpha_1, ..., \alpha_r$ de multiplicidades $\nu_1, ..., \nu_r$, entonces $\sum \nu_i \leq m$.

Demostración.– Resulta un poco artificial, por no recurrir a la conocida (y seguramente aceptada por el alumno sin mayor discusión) factorización única de los anillos de polinomios. Tal vez el docente opte por dar por supuesto este hecho y simplificar la prueba; en caso contrario aquí tiene una alternativa interesante desde el punto de vista formativo: lo haremos por inducción en el número de raíces de $P(X)$.

El caso de una raíz es sencillo, ya que si $P(X)$ tiene una sola raíz α_1 de multiplicidad ν_1, es

$$P(X) = (X-\alpha_1)^{\nu_1} Q(X),$$

y $\text{gr}(P) = \nu_1 + \text{gr}(Q)$, lo que prueba el resultado.

Escribimos, en el caso general,

$$P(X) = (X-\alpha_1)^{\nu_1} Q(X), \;\; P(X) = (X-\alpha_i)^{\nu_i} R_i(X), \; i = 2, ..., r$$

y veamos que α_i es raíz de $Q(X)$ con multiplicidad, al menos, ν_i.

Comenzamos sustituyendo $X = \alpha_i$ y vemos que

$$0 = P(\alpha_i) = Q(\alpha_i)(\alpha_i - \alpha_1)^{\nu_1},$$

de donde α_i es raíz de $Q(X)$ y entonces

$$Q(X) = (X-\alpha_i)Q_1^{(i)}(X) \implies (X-\alpha_i)^{\nu_i - 1} R_i(X) = (X-\alpha_1)^{\nu_1} Q_1^{(i)}(X).$$

Si hacemos de nuevo $X = \alpha_i$, comprobamos que $Q_1^{(i)}(\alpha_i) = 0$, y así

$$Q_1^{(i)}(X) = (X-\alpha_i)Q_2^{(i)}(X) \implies Q(X) = (X-\alpha_i)^2 Q_2^{(i)}(X),$$

y podemos seguir el proceso en ν_i ocasiones. Al final obtenemos una expresión de la forma

$$Q(X) = Q_{\nu_i}^{(i)}(X)(X-\alpha_i)^{\nu_i},$$

por lo que α_i es raíz de Q con multiplicidad, al menos, ν_i.

Obviamente $Q(X)$ no tiene más raíces que $\alpha_2, ..., \alpha_r$, porque α_1 no lo es (dado que su multiplicidad en $P(X)$ es ν_1) y $P(X)$ no tiene otras raíces. Así podemos aplicar a $Q(X)$ la hipótesis de inducción, para deducir $\text{gr}(Q) \leq \nu_2 + ... + \nu_r$. Como $\text{gr}(P) = \nu_1 + \text{gr}(Q)$, el resultado está probado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Corolario.– Un polinomio de grado n en $k[X]$ tiene, a lo más, n raíces (eventualmente repetidas) en k.

Observación.– Para finalizar esta lección, destacamos los resultados más útiles a la hora de calcular raíces de polinomios, que el docente puede entrar a demostrar o no, según su criterio. Los casos que tendrán más trascendencia en el futuro serán, obviamente $k = \mathbf{R}, \mathbf{C}$ y por ello se debería dedicar algún tiempo a éstos, al menos.

En cualquier caso, lo más importante es que el alumno entienda que cuál es el cuerpo base es esencial para el cálculo de las raíces de un polinomio, como se puede ver, por ejemplo con $P(X) = X^5 - 2X$ que tiene una raíz racional, tres raíces reales y cinco complejas.

Caso $k = \mathbf{C}$. Dado un polinomio $P(X) \in \mathbf{C}[X]$ de grado m, el teorema fundamental del álgebra, aplicado m veces nos indica que $P(X)$ tiene exactamente m raíces, si contamos cada una tantas veces como indica su multiplicidad (esto se expresa abreviadamente diciendo "m raíces contadas con multiplicidad").

Además, si $P(X) \in \mathbf{R}[X]$ y $z \in \mathbf{C}$ es una raíz, es inmediato que $\overline{z}$ también: para ver esto sólo hay que fijarse en que, dados $z_1, z_2 \in \mathbf{C}$ y $\alpha \in \mathbf{R}$,

$$\overline{z_1\, z_2} = \overline{z_1}\,\overline{z_2}, \quad \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \quad \overline{\alpha z_1} = \alpha \overline{z_1},$$

de donde $P(\overline{z}) = \overline{P(z)} = 0$. Usando esto, es simple ver, tras dividir por $(X - z)(X - \overline{z})$, que z y $\overline{z}$ han de tener la misma multiplicidad.

Caso $k = \mathbf{R}$. Si $k = \mathbf{R}$, todo polinomio se puede escribir como producto de polinomios de grado 1 (de la forma $X - \alpha$) por polinomios de grado 2 con sus dos soluciones complejas (y conjugadas, como hemos visto).

Esto es así porque un polinomio de grado m tiene m raíces complejas. Si una de esas raíces es real, pongamos α, dan un factor en $\mathbf{R}[X]$ de grado 1, $(X - \alpha)$. Si es compleja, $\alpha = a + bi$, entonces $a - bi$ también es raíz y, en la descomposición en $\mathbf{C}[X]$ aparecen los factores $(X - \alpha)$ y $(X - \overline{\alpha})$, que al multiplicarse dan el polinomio de segundo grado $(X^2 - 2aX + a^2 + b^2) \in \mathbf{R}[X]$.

Caso $k = \mathbf{Q}$. Si $k = \mathbf{Q}$, todas las raíces racionales de $P(X)$ han de ser números p/q donde p divida al término independiente y q al coeficiente de X^m o coeficiente líder (Regla de Ruffini).

En efecto, pongamos

$$P(X) = a_m X^m + a_{m-1} X^{m-1} + ... + a_1 X + a_0, \text{ con } a_i \in \mathbf{Z},$$

y $\alpha = p/q \in \mathbf{Q}$ una raíz escrita en forma irreducible. Entonces sustituyendo $X = \alpha$ y multiplicando por q^m tenemos

$$a_m p^m + a_{m-1} p^{m-1} q + ... + a_1 p q^{m-1} + a_0 q^m = 0,$$

de donde $a_0 q^m$ es múltiplo de p y $a_m p^m$ es múltiplo de q. Como p y q no tienen factores comunes a_m y a_0 tienen que ser, repectivamente, múltiplos de q y p.

Ejercicios del tema 1

Ejercicio 1.– Se consideran tres subconjuntos A, B y C de un conjunto Ω. El conjunto Ω y los subconjuntos A, B y C está representados en el diagrama 1. El diagrama se lee así la región encerrada dentro del rectángulo representa Ω, y los tres discos representan A, B y C (un tal diagrama se llama *diagrama de Venn*).

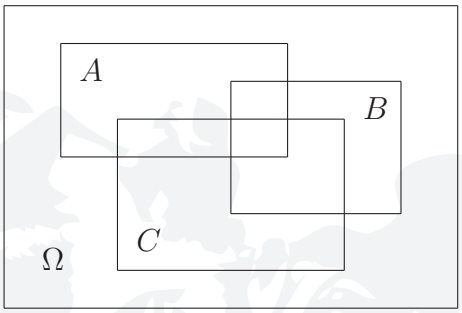

Diagrama 1

El diagrama 2 define los 8 subconjuntos S, T, U, V, W, X, Y, Z representados por las regiones delimitadas por los segmentos.

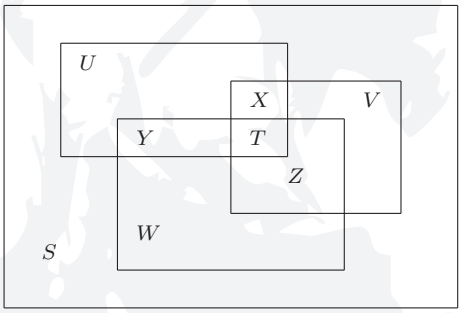

Diagrama 2

1. Cada subconjunto obtenido por unión de unos de estos 8 subconjuntos puede también obtenerse de A, B, C y Ω por medio de las operaciones $\cup$ (unión), $\cap$ (intersección) y $\setminus$ (complemento). Por ejemplo,

$$U \cup T = (A \setminus (B \cup C)) \cup (A \cap B \cap C).$$

   Hallar una tal descomposición, tan corta como sea posible, para los 4 subconjuntos siguientes:

$$X \cup Y \cup T, \quad X \cup Y \cup Z, \quad U \cup V \cup W, \quad U \cup Z.$$

   Prestar atención especial a poner paréntesis donde esta necesario.

2. Recíprocamente, todo subconjunto obtenido de Ω, A, B y C por medio de $\cup$, $\cap$ y $\setminus$ se escribe de manera única como unión de subconjuntos entre S, T, $\ldots$, Z. Por ejemplo:

$$(A \setminus B) \cup C = T \cup U \cup W \cup Y \cup Z.$$

Hallar una tal descomposición para los tres subconjuntos:

$$(A \cup B) \setminus (A \cap C),$$
$$((A \cap B) \cup (A \cap C)) \setminus (B \cap C),$$
$$((A \cup B) \cap C) \setminus ((A \cap B) \cup C).$$

Ejercicio 2.– Se supone que se conocen los números de elementos (o cardinal) de los conjuntos siguientes:

$$A, \quad B, \quad C, \quad A \cap B, \quad A \cap C, \quad B \cap C, \quad A \cap B \cap C.$$

Existe una fórmula expresando el numero de elementos de $A \cup B \cup C$ en función de estos siete números. Hallar esta fórmula, y demostrarla.

Ejercicio 3.– Consideremos una aplicación $f : X \longrightarrow Y$. Sea $A \subset X$ y $B \subset Y$.

1. Comparar, del punto de vista de la inclusión, $f(f^{-1}(B))$ con B.
2. Comparar, del punto de vista de la inclusión, $f^{-1}(f(A))$ con A.
3. Si se supone que f es inyectiva o que f es sobreyectiva, ¿cómo cambian las respuestas a las dos primeras preguntas?

Ejercicio 4.– Consideremos $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ dos aplicaciones.

1. Suponemos que la composición $g \circ f$ es sobreyectiva. ¿Qué implica para f y g?
2. Suponemos ahora que $g \circ f$ es inyectiva. ¿Qué implica para f y g?

Ejercicio 5.– Sean las aplicaciones:

$$\begin{array}{rcl} f : \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^2 - 2 \end{array} \qquad \begin{array}{rcl} g : (0, +\infty) & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \ln(x) \end{array} \qquad \begin{array}{rcl} h : \mathbf{R} & \longrightarrow & [-1, 1] \\ x & \longmapsto & \cos(x) \end{array}$$

Hallar, en cada caso, la imagen y la imagen inversa del intervalo $(0, 1]$.

Ejercicio 6.– Estudiar si las siguientes relaciones son o no de equivalencia sobre los conjuntos X dados:

1. En $X = \mathbf{R} \setminus \{0\}$, la relación xRy si y sólo si $xy > 0$.
2. En $X = \mathbf{Z}$, la relación xRy si y sólo si $x \geq y$.
3. En $X = \mathbf{R}^2$, la relación $(x, y)R(x', y')$ si y sólo si existe un $\lambda \in \mathbf{R} \setminus \{0\}$ tal que $x = \lambda x'$, e $y = \lambda y'$.

Ejercicio 7.– Probar que, en cada fila y columna de la tabla de un grupo G aparecen todos los elementos del grupo, cada uno exactamente una vez.

UNIVERSIDAD DE SEVILLA

Ejercicio 8.– Dado un grupo multiplicativo finito con n elementos $G = \{a_1, a_2, \ldots, a_n\}$, una tabla del grupo G es una tabla con n filas y n columnas, marcadas cada una de ellas con los elementos del grupo, que contiene, en la celda de fila a_i, columna a_j, el valor de $a_i \cdot a_j$ (notemos que decimos "una" tabla del grupo porque depende del orden de enumeración de los elementos del grupo).
Éste es el ejemplo de una tabla del grupo de simetrías $S_2 = \{\mathrm{Id}, \sigma\}$,

S_2	Id	σ
Id	Id	σ
σ	σ	Id

Hallar las tablas de S_3, C_2, C_3 y C_4.

Ejercicio 9.– Sea $\sigma \in S_n$. Recordemos que una inversión de σ es un par (i, j) con $1 \leq i < j \leq n$ y $\sigma(i) > \sigma(j)$.

1. Hacer la lista de todas las permutaciones elementos de S_3 y asociar a cada una su número de inversiones.
2. Misma pregunta para S_4.
3. En cada uno de los dos casos, ¿cuántas permutaciones tienen un número de inversiones par? ¿Cuántas tienen un número de inversiones impar?

Ejercicio 10.– Hallar un polinomio con coeficientes reales y grado mínimo que tenga al número complejo

$$\frac{1 + i\sqrt{3}}{2}$$

como raíz.

Ejercicio 11.– Determinar todos los números complejos z tales que $|z| = 1$ (el modulo de z sea 1) y $z^3 - z$ sea real.

Ejercicio 12.– Recordemos que *una raíz cuadrada* de un numero complejo z es cualquier numero α tal que $\alpha^2 = z$. Por ejemplo, las raíces cuadradas de 1 son 1 y -1. Hallar las raíces cuadradas de $1 + 4\,i\,\sqrt{3}$, y las de $1 + i$.
NOTA: Para hallar las raíces cuadradas *exactas* se pueden usar las fórmulas del ángulo mitad:

$$\mathrm{sen}\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1 - \cos(\alpha)}{2}}, \qquad \cos\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1 + \cos(\alpha)}{2}}.$$

Ejercicio 13.– Demostrar que un polinomio $P(x)$ con coeficientes reales de grado 3 tiene siempre por lo menos una raíz real.

Ejercicio 14.– Encontrar todas las raíces de $x^5 - x^4 - x^3 + x^2 - 2x + 2$.

Ejercicio 15.– Un polinomio $P(x)$ es *par* si $P(-x) = P(x)$, y es *impar* si $P(-x) = -P(x)$. Demostrar que cada polinomio se descompone en suma de un polinomio par y de un polinomio impar, y de sólo una manera.