

# lenguaje matemático

## 1. Nociones lógicas

- Expresiones matemáticas: proposiciones
  - Proposición lógicas simple
    - una proposición simple describe una propiedad de un objeto concreto y se le puede atribuir sin ambigüedad el valor verdadero o falso
    - para hacer referencia sintáctica a una proposición simple se le suele emplear una letra minúscula, por ejemplo,  $p$ ,  $q$  e,  $s$ ... cada letra(proposición) posee un único valor semántico, verdadero o falso.
  - Proposiciones compuestas
    - Con proposiciones simples se construyen proposiciones compuestas, tanto si las proposiciones son simples como si son compuestas, nos referimos a ellas como preposiciones.
  - Marco lógico
    - Todo lenguaje tiene unas reglas sintácticas que tienen que cumplir para que tenga lógica lo que está diciendo.
- Conectores lógicos:
  - La negación: -
    - El cuatro no es un numero par
    - $\neg p$  es cierta si  $p$  es falsa y es falsa si  $p$  es cierta
  - Disyunción:  $p \vee q$ 
    - El cuatro es un numero par o un numero impar
    - La proposición  $p \vee q$  es falsa únicamente si  $p$  y  $q$  son falsa
  - Conjunción:  $p \wedge q$ 
    - El cuatro es un numero par y el nueve es un numero impar
    - La proposición  $p \wedge q$  es verdadera solo si  $p$  y  $q$  son verdaderas
  - Condicional:  $p \rightarrow q$ 
    - Si ocho es un numero par, entonces ocho es suma de dos números iguales
    - La proposición  $p \rightarrow q$  es fals únicamente si  $p$  es verdadera y  $q$  es falsa
    - A la proposición condicional se le asocia tres nuevas proposiciones condicionales:
      - El condicional  $q \rightarrow p$  se denomina condicional reciproco
      - El condicional  $\neg p \rightarrow \neg q$  se denomina condicional contrario
      - El condicional  $\neg q \rightarrow \neg p$  se denomina condicional contrarrecíproco
  - Bicondicional:  $p \leftrightarrow q$ 
    - Ocho es un numero para si y solo si ocho es divisible entre dos
    - La proposición  $p \leftrightarrow q$  es verdadera solo si  $p$  y  $q$  toman es mismo valor
  - Dos proposiciones  $p$  y  $q$  son equivalentes si  $p$  y  $q$  toman el mismo valor
- Construcción de proposiciones
  - De entre todas las posibles tablas de verdad que se pueden obtener para una proposición compuesta, destacamos las siguientes:
    - Contradicción: es la proposición que solo toma el valor 0, la notaremos 0.
    - Tautología: es la proposición que solo toma el valor 1, y la notaremos 1.
  - Recordemos que dos proposiciones son equivalentes si y solo si el bicondicional de ambas,  $p \leftrightarrow q$ , es una tautología.
- Leyes lógicas
  - Existe el convenio que cuando se escribe una equivalencia entre proposiciones con un único símbolo  $\Leftrightarrow$ , las expresiones situadas a la derecha e izquierda del símbolo constituyen las proposiciones equivalentes.
  - Leyes lógicas equivalentes con una proposición
    - Con una única proposición atómica  $p$  y el conector negación
      - Ley de la doble negación: las proposiciones  $\neg \neg p$  y  $p$  son equivalentes

- Con una única proposición  $p$  y un conector distinto de  $\neg$ 
    - Leyes de identidad
  - Con una única proposición  $p$  y varios conectores distintos
    - Ley del tercio excluido
    - Ley de contradicción
- Leyes lógicas equivalentes con dos proposiciones
  - Leyes de simplificación
  - Leyes conmutativas
  - Leyes de Morgan
  - Leyes del condicional
  - Ley del bicondicional
  - Ley de reducción a lo absurdo
  - Leyes de trasposición
- Leyes lógicas equivalentes con tres proposiciones
  - Leyes asociativas
  - Leyes distributivas
- Leyes lógicas condicionales
  - Leyes de simplificación condicional
  - Leyes de inferencia
  - Ley modus ponendo ponens
  - Ley modus tollendo tollens
- Validación de proposiciones
  - Validación mediante tabla de verdad
  - Validación mediante refutación: consiste en aplicar la ley a lo absurdo, es decir se debe suponer que es falsa y comprobar que aparece una contradicción
  - Ley del silogismo
- Forma clausulada de proposiciones
  - Se trata de encontrar una proposición equivalente a la primera, que este escrita únicamente como conjunción  $\wedge$  de proposiciones disyuntivas  $\vee$
  - Comprobación de una tautología mediante una forma clausulada
  - Tabla de verdad mediante la forma clausulada
- Comentario
  - Un axioma es una sentencia bien formada que se considera verdadera
  - Un teorema es una sentencia bien formada que es cierta, es decir, una tautología
- Presentación de resultados en matemáticas
  - Un teorema
  - Una proposición
  - Un lema
  - Un corolario
- Métodos de demostración empleados en matemáticas
  - Deducción directa
  - Negación consecuente
  - Reducción a lo absurdo
  - Método inductivo

## 2. Conjuntos

- Principio de inducción
- Cuantificadores
  - Para todo valor:  $\forall$
  - Para solo un valor  $\exists$
- Complementarios y partes de un conjunto
- Operaciones entre conjuntos

### 3. Relaciones y aplicaciones entre conjuntos

- Las relaciones de equivalencia de en un conjunto permiten clasificar los elementos del conjunto, creando partición del propio conjunto, el conjunto cociente. Este concepto es de gran utilidad en casi todas las ramas de las matemáticas. Las relaciones de orden también aparecen por todas partes, desde la ordenación de números hasta la ordenación de palabras para disponerlas en un diccionario
- Por otro lado, y dentro de l marco de las relaciones binarias, estudiaremos las aplicaciones entre conjuntos. Son las relaciones para las que la imagen de cada elemento del con junto inicial es el único conjunto final
- **propiedades básicas de una relación**
  - una relación  $r$  definida en un conjunto  $U$ ,  $R \subset U \times U$ , puede tener las propiedades:
    - propiedad **reflexiva**: la relación  $R$  es reflexiva si y solo si  $\{(x,x) \mid x \text{ pertenece } U\} \subset R$  es decir: para todo  $x$  perteneciente a  $U$  se verifica  $xRx$
    - propiedad **simétrica**: la relación  $R$  es simétrica si y solo si  $RR^{-1} \subset R$ , es decir: para todo valor  $x, y$  perteneciente a  $U$  se verifica que si  $xRy$ , entonces  $yRx$
    - propiedad **antisimétrica**: la relación  $R$  es antisimétrica si y solo si  $R^{-1} \cap R \subset \{(x,x) \mid x \text{ perteneciente } U\}$ , es decir: para todo valor de  $x,y$  perteneciente a  $U$  se verifica que si  $xRy$  e  $yRx$ , entonces  $x = y$
    - propiedad **transitiva**: la relación  $R$  es transitiva si y solo si  $R \circ R \subset R$ , es decir: para todo valor de  $x,y,z$  perteneciente a  $U$  se verifica que si  $xRy$  e  $yRz$ , entonces  $xRz$
- **Relaciones de equivalencias**
  - Las relaciones de equivalencia en un conjunto sirven fundamentalmente para obtener clasificaciones de los elementos del conjunto. Estas clasificaciones se hacen mediante las clases de equivalencia. La identificación de todos los elementos de una clase de equivalencia conduce al concepto del conjunto cociente.
  - Una relación  $E$  en el conjunto  $U$  se denomina relación de equivalencia si posee las siguientes propiedades:
    - P. Reflexiva: para todo valor de  $x$  perteneciente a  $U$   $xEx$
    - P. simétrica : para todo valor de  $x,y$  perteneciente a  $U$  si  $xEy$ , entonces  $yEx$
    - P. transitiva: para todo valor de  $x,y,z$  perteneciente a  $U$  si,  $xEy$  e  $yEz$ , entonces  $xEz$
  - Clases de equivalencia
    - Dada una relación de equivalencia  $E$  en el conjunto  $U$ , se denomina clase de equivalencia del elemeto  $x$  perteneciente a  $U$  al conjunto imagen de  $X$ , que denoitaemos  $xE$  o  $[x]$ , es decir:  $[x] = \{y \text{ perteneciente } U \mid xEy\}$
  - Conjunto cociente
    - Dada una relación de equivalencia  $E$  en el conjunto  $U$ , se denomina conjunto conciente, y se denota por  $U/E$ , al conjunto de todas las clases que genera la relación de equivalencia  $E$
  - Partición de un conjunto
    - Una partición de un conjunto  $U$  es una familia  $P$  e subconjunto de  $U$  diisjuntos dos a dos y cuya unión es el conjunto  $U$ , es decir:  
para cualquier  $A,B$  perteneciente a  $P$  se tiene que  $A \cap B = \emptyset$  y  $\bigcup_{A \text{ pert } P} A = U$ 
      - Toda relación de equivalence  $E$  es un conjunto  $U$  genera una partición en ese conjunto, puesto que las clases de  $U/E$  son subconjuntos de  $U$  disjuntos dos a dos y la unión de estos es el conjunto  $U$
      - Recíprocamente, toda partición  $P$  del conjunto  $U$  permite definir una relación de queivalencia  $E$  en el conjunyo  $U$  mediante:  
 $xEy$  si y solo si existen algún  $A$  perteneciente a  $P$  tal qu  $\{x,y\}$  esta contenido en  $A$
- **Relación de orden**

- De esta forma cada número natural distinto de cero es definido como es siguiente de otro número natural, y esto nos permite realizar la siguiente representación de  $\mathbb{N}$ :
  - Una relación  $R$  en el conjunto  $U$  se denomina relación de orden si posee las propiedades:
    - P. Reflexiva: para todo valor de  $x$  perteneciente a  $U$   $xRx$
    - P. simétrica : para todo valor de  $x,y$  perteneciente a  $U$  si  $xRy$ , entonces  $yRx$
    - P. transitiva: para todo valor de  $x,y,z$  perteneciente a  $U$  si,  $xRy$  e  $yRz$ , entonces  $xRz$
  - La relación de orden  $R$  se dice que es una relación de orden total si posee la propiedad  $R^{-1} \cup R = U \times U$ , es decir: para todo  $x,y$  perteneciente a  $U$   $xRy$  o  $yRx$
  - Para subrayar que una relación de orden no es total se indica con el término parcial: relación de orden parcial.
  - El par formado por un conjunto y una relación de orden definida sobre el se denomina conjunto ordenado.
  - A menudo las relaciones de orden se denotan por  $\leq$ , de manera que la expresión  $a \leq b$  se lee como  $a$  precede a  $b$  o  $a$  antecede a  $b$ . también se utiliza indistintamente la notación  $b \geq a$  para indicar  $a \leq b$  y se lee  $b$  sucede a  $a$  o  $b$  es posterior a  $a$ . la notación  $a < b$  o  $b > a$  se utiliza para indicar que  $a \leq b$  y  $a$  es distinto de  $b$
- Intervalos en un conjunto ordenado dados un conjunto ordenado  $(U, \leq)$ , y  $a,b$  pertenecen a  $U$  tales que  $a \leq b$ , se denomina:
  - Intervalo abierto  $(a,b)$ : es el conjunto  $(a,b) = \{ x \text{ pertenece } U \mid a < x < b \}$
  - Intervalo cerrado  $[a,b]$ : es el conjunto  $[a,b] = \{ x \text{ pertenece } U \mid a \leq x \leq b \}$
  - Intervalo semiabierto: es cada uno de los siguientes conjuntos:
    - $(a,b] = \{ x \text{ pertenece } U \mid a < x \leq b \}$
    - $[a,b) = \{ x \text{ pertenece } U \mid a \leq x < b \}$
- Intervalos iniciales y finales dado un conjunto ordenado  $(U, \leq)$ , se denomina intervalos a cada uno de los siguientes conjuntos:
  - Intervalo inicial abierto:
  - Intervalo final abierto:
  - Intervalo inicial cerrado:
  - Intervalo final cerrado:
- Conjunto acotado dados un conjunto ordenado  $(U, \leq)$ , y un subconjunto  $A$  contenido en  $U$ , se denomina :
  - Cota superior del conjunto  $A$ : una cota superior de  $A$  es cualquier elemento de  $U$  perteneciente a  $U$  que verifica que para todo  $x$  perteneciente a  $A$   $x \leq u$
  - Cota inferior del conjunto  $A$ : una cota inferior de  $A$  es cualquier elemento de  $U$  perteneciente a  $U$  que verifica que para todo  $x$  perteneciente a  $A$   $d \leq x$
  - $A$  un conjunto acotado superiormente: el conjunto  $A$  es acotado superiormente si existe una cota superior de  $A$
  - $A$  un conjunto acotado inferiormente: el conjunto  $A$  es acotado inferiormente si existe una cota inferior de  $A$
  - $A$  un conjunto acotado: el conjunto  $A$  es acotado si lo es tanto superiormente como inferiormente.
- Dados un conjunto  $(U, \leq)$  y subconjunto  $A$  contenido en  $U$ , se denomina:
  - Máximo del conjunto  $A$ : es un elemento  $M$  perteneciente a  $A$  tal que para todo  $x$  perteneciente a  $A$   $x \leq M$  y se denota  $\max(A)$
  - Mínimo del conjunto  $A$ : es un elemento  $m$  perteneciente a  $A$  tal que para todo valor de  $x$  perteneciente a  $A$   $m \leq x$  y se denota  $\min(A)$
  - Supremo del conjunto  $A$ : es una cota superior  $s$  perteneciente a  $U$  tal que  $s \leq u$  para toda cota superior  $u$  de  $A$  y se denota  $\sup(A)$
  - Infimo del conjunto  $A$ : es una cota inferior  $i$  perteneciente a  $U$  tal que  $d \leq i$  para toda cota inferior  $d$  de  $A$  y se denota  $\inf(A)$

- Dados un conjunto ordenado  $(U, \leq)$  y un subconjunto  $A$  contenido  $U$ , se tiene:
  - Si existe el máximo, o el mínimo, del conjunto  $A$ , entonces este es único
  - Si existe el supremo, o infimo, del conjunto  $A$ , entonces este es único
  - Si existe el supremo  $s$  del conjunto  $A$  y  $s$  pertenece  $A$ , entonces  $s$  es el máximo de  $A$
  - Si existe el infimo  $i$  del conjunto  $A$  e  $i$  pertenece a  $A$ , entonces  $i$  es el mínimo de  $A$ .
- Propiedad del buen orden
  - Se dice que un conjunto  $(U, \leq)$  es un conjunto bien ordenado, o que la relación  $\leq$  es una buena ordenación, si cualquier subconjunto no vacío posee mínimo. El elemento mínimo de cada subconjunto  $A$  también se denomina primer elemento de  $A$
- Propiedad del supremo
  - Se dice que un conjunto ordenado  $(U, \leq)$  verifica la propiedad del supremo si y solo si cualquier subconjunto no vacío  $A$  acotado superiormente posee supremo.
- Dados un conjunto ordenado  $(U, \leq)$  y un subconjunto  $A$  de  $U$  se denomina:
  - Maximal del conjunto  $A$ : es un elemento  $M$  perteneciente  $A$  tal que no existe  $x$  perteneciente  $A$ ,  $x$  distinto de  $M$ , que cumpla  $M \leq x$
  - Minimal del conjunto  $A$ : es un elemento  $m$  perteneciente  $A$  tal que no existe  $x$  perteneciente  $A$ ,  $x$  distinto de  $M$ , que cumpla  $x \leq m$

#### 4. Operaciones y estructuras algebraicas

- Definiremos las estructuras básicas para operaciones internas: grupos, anillos y cuerpos. A lo largo de estudios posteriores, tanto en física como en matemáticas, se encontrarán muy a menudo este tipo de estructuras, por eso este capítulo supone una economía importante de medios intelectuales.
- Operaciones internas
  - Sea  $E$  un conjunto. una operación interna, o ley de composición interna, en  $E$  es una aplicación de  $E \times E$  en  $E$ . es decir, es una ley que asocia a todo par  $(a, b)$  de elementos de  $E$  en un único de  $E$ , que notaremos,  $a*b$ .
  - Son operaciones internas conocidas:
    - $\cap$  intersección en el conjunto  $P(\Omega)$  de las partes de un conjunto  $\Omega$
    - $\cup$  unión en el conjunto  $P(\Omega)$  de las aplicaciones de un conjunto  $\Omega$  en si mismo
    - $\circ$  composición de el conjunto  $F(\Omega)$  de las aplicaciones de un conjunto  $\Omega$  en si mismo
    - $+$  suma en los conjuntos  $N, Z, Q, R$
    - $-$  resta en los conjuntos  $Z, Q, R$
    - $\times$  producto en los conjuntos  $N, Z, Q, R$
    - $/$  división en los conjuntos  $Q^*$  o  $R^*$
    - $+$ ,  $\times$  suma y producto en el conjunto de matrices cuadradas de orden  $n$ .
    - $\wedge, \vee$  conjunción y disyunción en el conjunto de proposiciones lógicas
    - $\wedge, \vee$  máximo común divisor y mínimo común múltiplo en  $N^*$
    - $\wedge$  producto vectorial en el espacio euclideo tridimensional
  - Propiedades: sea  $E$  un conjunto y  $*$  una operación interna definida en  $E$ 
    - La operación  $*$  es asociativa si para todo  $a, b, c \in E$
    - La operación  $*$  es conmutativa si para todo  $a, b \in E$
    - Se denomina elemento neutro de la operación interna  $*$  en  $E$ , a un elemento  $e \in E$  que cumple para todo  $a \in E$ 
      - Sea  $*$  una operación interna en  $E$ . si existen elemento de  $*$  en  $E$ , este es único
    - Se denomina elemento simétrico del elemento  $a \in E$  a un elemento  $a' \in E$  tal que:
      - En el conjunto  $F(\Omega)$  de las aplicaciones de un conjunto dado en si mismo, solo tiene simétrico respecto de la composición las aplicaciones biyectivas. El simétrico de la biyección  $f$  es la biyección inversa. En el conjunto de matrices cuadradas de orden  $n$  solo tiene simétrico respecto del producto, las matrices cuyo determinante es distinto de 0.

- Sea  $*$  una operación interna asociativa en  $E$  con elemento neutro  $e \in E$ . si  $a \in E$  tiene elemento simétrico, este es único.

## ○ Grupos

- Sea  $G$  un conjunto no vacío y  $*$  una operación interna en  $G$ . se dice que el par  $(G, *)$  tiene estructura de grupo. O que  $(G, *)$  es un grupo, si satisfacen las siguientes propiedades:
  - La operación  $*$  es asociativa
  - Existe elemento neutro de  $*$  en  $G$
  - Para todo elemento  $a \in G$ , existe en  $G$  el elemento simétrico de  $a$  respecto de  $*$ .
    - Si además la operación  $*$  es conmutativa se dice que el grupo es conmutativo o abeliano
  - Nota aditiva: cuando la operación de un grupo se representa con el símbolo  $+$ , el grupo se llama aditivo.
  - Notación multiplicativa: cuando la operación se representa con el símbolo  $\cdot$ , el grupo se dice multiplicativo
- Ejemplos de grupos conocidos
  - Veremos en capítulos posteriores que los conjuntos  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  y  $\mathbb{C}$  son grupos conmutativos respecto de la suma
  - Los conjuntos  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$  y  $\mathbb{C}^*$  son grupos conmutativos respecto del producto.
  - El conjunto de matrices de orden  $n \times m$  respecto de la suma de matrices es un grupo conmutativo
  - El conjunto de matrices cuadradas invertibles de orden  $n$  es un grupo no conmutativo respecto del producto
  - El conjunto  $B(\Omega)$  de las aplicaciones biyectivas de un conjunto  $\Omega$  en si mismo es el grupo no conmutativo respecto de la composición de aplicaciones.
- Propiedades de un grupo
  - Para todo  $a, b, c \in G$ ,  $a * b = a * c \implies b = c$  (propiedad cancelativa)
  - Para todo  $a, b \in G$ , existe un único  $x \in G$  tal que  $a * x = b$
  - Si  $a^{-1}$  y  $b^{-1}$  son simétricos de  $a$  y  $b$ , entonces  $(a * b)^{-1} = b^{-1} * a^{-1}$
  - observaciones: la propiedad cancelativa indica que un grupo, la aplicación ... es inyectiva.

## ○ Subgrupos

- Sean un grupo  $(G, *)$  y un subconjunto  $\emptyset \neq H \subset G$ .  $H$  es un subgrupo de  $G$  si y solo si para todo  $a, b \in H$ ,  $a * b^{-1} \in H$

## ○ congruencia de modulo un subgrupo

- sea  $(G, *)$  un grupo conmutativo y sea  $H$  un subgrupo. La relación  $R_h$  en  $G$  definida para todo  $a, b \in G$  por,  $a R_h b$  si y solo si  $a * b^{-1} \in H$ , es una relación de equivalencia denominada congruencia modulo  $H$ .
  - es reflexiva, pues para todo  $a \in G$ ,  $a * a^{-1} = e \in H$  y en consecuencia  $a R_h a$ .
  - Es simétrica, pues si  $a R_h b$  entonces  $a * b^{-1} \in H$ . en consecuencia,  $(a * b^{-1})^{-1} = b * a^{-1} \in H$ . por tanto  $b R_h a$ .
  - Es transitiva...
- Toda clase de equivalencia de la relación  $R_h$  es equipotente a  $H$ .
- Si  $\text{card}(G)$  es finito, entonces cualquier subgrupo  $H$  cumple que  $\text{card}(H)$  es divisor de  $\text{card}(G)$ .
- En un grupo con un número finito de elementos, a  $\text{card}(G)$  se le denomina orden del grupo  $G$ .

## ○ Anillo

- Consideramos ahora conjuntos donde están definidas dos operaciones internas. Por analogía con las operaciones internas y por comodidad, denotaremos la primera operación como suma,  $+$ , mientras que a la segunda la llamaremos producto  $\cdot$ .
- Sea  $A$  un conjunto y sean  $+$  y  $\cdot$  dos operaciones internas definidas en  $A$ . diremos que  $(A, +, \cdot)$  es un anillo si se satisfacen:
  - $(A, +)$  es un grupo conmutativo
  - La operación  $\cdot$  es asociativa

- La operación  $\cdot$  es distributiva respecto de la operación  $+$ . Esto es,  $a(b + c) = ab + ac$  y  $(a + c)a = ba + ca$
- Si además, la operación  $\cdot$  es conmutativa, se dice que  $(A, +, \cdot)$  es un anillo conmutativo
- Si, además,  $A$  tiene elemento neutro para el producto, siendo este distinto del elemento neutro de la suma, se dice que  $(A, +, \cdot)$  es un anillo unitario
- Elemento nulo, elemento neutro de la suma se designa por  $0$ .
- Elemento opuesto, elemento simétrico de  $a$  para la suma se designa por  $-a$
- Elemento unicidad, elemento neutro del producto y se designa por  $1$ .
- Elemento inverso, el elemento simétrico de  $a$  para el producto se designa por  $a^{-1}$ , en este caso se dice que  $a$  es un elemento invertible.
- Ejemplos de anillos conocidos
  - Veremos en capítulos posteriores que los conjuntos  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  y  $(\mathbb{C}, +, \cdot)$  son anillos conmutativos unitarios respecto de la suma y el producto habituales
  - El conjunto de matrices cuadradas de orden  $n$  respecto de la suma y del producto de matrices es un anillo unitario no conmutativo
- Propiedades de un anillo
  - Para todo  $a \in A$ ,  $a \cdot 0 = 0 \cdot a = 0$ . ( se dice que  $0$  es absorbente para el producto)
  - Para todo  $a, b \in A$ ,  $(-a)b = a(-b) = -(ab)$  y  $(-a)(-b) = ab$
  - Si además el anillo  $A$  es conmutativo se satisfacen las igualdades:
    - $(a + b)^2 = a^2 + b^2 + 2ab$
    - $(a + b)(a - b) = a^2 - b^2$
    - $(a + b)^n = \dots$
- Divisores de  $0$ 
  - Es un anillo  $(A, +, \cdot)$  se dice que el elemento  $a \in A$ ,  $a \neq 0$ , es un divisor de cero existe  $b \in A$ ,  $b \neq 0$ , tal que  $ab = 0$
- **Subanillos. Ideales**
  - Se dice que  $H$  es un subanillo de  $A$  si  $(H, +, \cdot)$  es a su vez un anillo. Cuando  $A$  es unitario entonces también se exige a todo subanillo que contenga el elemento unicidad de  $A$ .
  - Sea  $(A, +, \cdot)$  un anillo y sea  $H$  un subconjunto no vacío de  $A$ .  $H$  es un subanillo de  $A$  si y solo si para todo  $a, b$  perteneciente a  $H$  se verifica:
    - $a - b$  pertenece a  $H$
    - $ab$  pertenece a  $H$
    - si el anillo  $(A, +, \cdot)$  es unitario  $1$  pertenece a  $H$
  - sea  $(A, +, \cdot)$  un anillo conmutativo y  $\emptyset \neq I$  esta contenido en  $A$ .  $I$  es un ideal de  $A$  si se cumple:
    - $a - b$  pertenece a  $I$  para todo  $a, b$  perteneciente a  $I$
    - $ac$  pertenece a  $I$  para todo  $a$  perteneciente a  $I$  y para todo  $c$  perteneciente a  $A$
  - si  $(A, +, \cdot)$  es un anillo conmutativo y  $a$  pertenecer a  $A$  es un elemento fijo, el conjunto  $aA = \{ak \mid k \text{ pertenecientes a } A\}$  que también se denota por  $(a)$  es un ideal de  $A$  que se denomina ideal principal generado por  $a$ .
- **cuerpo**
  - un cuerpo es un anillo conmutativo unitario en el que todo elemento no nulo es inversible respecto del producto
  - sea  $K$  un conjunto y sean  $+$  y  $\cdot$  dos operaciones internas definidas en  $K$ .  $(K, +, \cdot)$  es un cuerpo si se satisfacen las siguientes propiedades:
    - las operaciones  $+$  y  $\cdot$  son asociativas en  $K$
    - las operaciones  $+$  y  $\cdot$  son conmutativas en  $K$
    - la operación  $\cdot$  es distributiva respecto de la operación  $+$  en  $K$
    - existen dos elementos distintos en  $K$  que se designan por  $0, 1$  que son elementos neutros de la suma y el producto respectivamente

- existencia de opuestos: para todo elemento  $a$  de  $K$  existen el simétrico de  $a$  respecto de la suma que se designa por  $-a$ .
- existencia de inversos: para todo elemento  $a$  distinto de  $0$  de  $K$  existe el simétrico de  $a$  para el producto que se designa por  $a$  elevado a menos uno.
- Sea  $K$  un conjunto y sea  $+$  y  $\cdot$  dos operaciones internas definidas en  $K$ 
  - $(K, +)$  es un grupo conmutativo
  - $(K^*, \cdot)$  es un grupo conmutativo
  - La operación  $\cdot$  es distributiva respecto de la operación  $+$  en  $K$
- Sea  $(K, +, \cdot)$  un cuerpo y  $H$  un subconjunto no vacío de  $K$ ,  $H$  es un subcuerpo de  $K$  si y solo si se verifica:
  - $a-b$  pertenece a  $H$  para todo  $a, b$  perteneciente a  $H$
  - $a$  elevado a  $-1$  perteneciente a  $H$  para todo  $a, b$  perteneciente a  $H^* = H/\{0\}$
- **Definición y propiedades de grupo, anillo y cuerpo ordenados**
  - Supongamos que tenemos un grupo conmutativo  $G$  donde por comodidad denotamos por  $+$  la operación interna de  $G$ , siendo  $0$  el elemento neutro de  $(G, +)$  y  $-a$  el elemento simétrico de  $a$ . sea una relación de orden  $\leq$  definida sobre  $G$ . se dice que  $(G, +, \cdot)$  es un grupo ordenado si la relación de orden es compatible con la suma, esto es:
    - Para todo  $a, b$  y  $c$  perteneciente a  $G$   $a \leq b \Rightarrow a + c \leq b + c$
  - En grupo ordenado  $(G, +, \leq)$  se satisfacen las siguientes propiedades:
    - $a \leq b$  si y solo si  $b - a$  pertenece a  $G^+$
    - Si  $a \leq b$  y  $a' \leq b'$  entonces  $a + a' \leq b + b'$
    - Si  $a \leq b$  entonces  $-b \leq -a$
  - Si la relación de orden es total se dice que el grupo es un grupo totalmente ordenado.
  - Ejemplos
    - Veremos en los capítulos 5 y 6 que  $(\mathbb{Z}, +, \leq)$ ,  $(\mathbb{Q}, +, \leq)$  y  $(\mathbb{R}, +, \leq)$  son grupos totalmente ordenados.
    - $(\mathbb{Q}^*, \cdot, \leq)$  no es un grupo ordenado pues el orden no es compatible con el producto, ya que  $2 \leq 2$  y sin embargo para  $c = -1$  no se cumple que  $1 \cdot (-1) \leq 2 \cdot (-1)$ . En cambio, si es un grupo totalmente ordenado el conjunto de los números racionales estrictamente positivos  $(\mathbb{Q}^{*+}, \cdot, \leq)$  pues veremos que si  $a, b$  y  $c$  pertenecen a  $\mathbb{Q}^{*+}$  si  $a \leq b$  entonces  $ac \leq bc$ .
  - Esta será la condición que se pide a la segunda operación de un anillo ordenado. Se dice que  $(A, +, \cdot, \leq)$  es un anillo ordenado si se cumple lo siguiente
    - Para todo  $a, b$  y  $c$  perteneciente a  $A$  si  $a \leq b$  entonces  $a + c \leq b + c$
    - Para todo  $a, b$  perteneciente a  $A$  si  $0 \leq a$  y  $0 \leq b$  entonces  $0 \leq ab$
  - Todo anillo ordenado es en particular un grupo ordenado
  - Si la relación de orden es total, se dice que el anillo es un anillo totalmente ordenado. Si además, el anillo es un cuerpo hablaremos de un cuerpo ordenado.
  - En un anillo totalmente ordenado  $(A, +, \cdot, \leq)$  se satisfacen las siguientes propiedades:
    - $a \leq b$  si y solo si  $b - a$  pertenecen a  $A^+$
    - Si  $a \leq b$  y  $a' \leq b'$  entonces  $a + a' \leq b + b'$
    - Si  $a \leq b$  entonces  $-b \leq -a$
    - Si  $a \leq b$  y  $0 \leq c$  entonces  $ac \leq bc$
    - Si  $a \leq b$  y  $c \leq 0$  entonces  $bc \leq ac$
    - Para todo  $a$  perteneciente a  $A$ ,  $a$  elevado a  $2 \geq 0$
    - Si  $A$  es un anillo unitario entonces  $0 < 1$
    - $|a| \geq |b|$  para todo  $a, b$  perteneciente a  $A$
    - $|a + b| \leq |a| + |b|$  para todo  $a, b$  perteneciente a  $A$ . si además  $(A, +, \cdot)$  es un cuerpo también se cumple:
      - Si  $a > 0$  entonces  $a$  elevado a  $-1 > 0$
      - Si  $0 < a \leq b$  entonces  $b$  elevado a  $-1 \leq a$  elevado a  $-1$
      - Si  $a < 0 < b$  entonces  $b$  elevado a  $-1 \leq a$  elevado a  $-1$



- Homomorfismos entre conjuntos dotados de una operación
  - Sean  $G$  y  $G'$  dos conjuntos donde se tiene respectivamente definidas dos operaciones internas que por comodidad denotaremos ambas  $+$ . Sea  $f: G \rightarrow G'$  una aplicación. Se dice que  $f$  es un homomorfismo si se cumple que:
    - $f(a + b) = f(a) + f(b)$  para todo  $a, b$  perteneciente  $G$
  - El homomorfismo se denomina endomorfismo cuando  $G = G'$  y la operación interna es la misma. Si el homomorfismo es biyectivo hablaremos de isomorfismo y finalmente todo endomorfismo biyectivo se denomina automorfismo.
  - Propiedades de un homomorfismo:
    - Si  $f: G \rightarrow G'$  es un homomorfismo entonces la operación de  $G'$  es una operación interna cuando se restringe al conjunto imagen  $f(G)$
    - Si  $f: G \rightarrow G'$  y  $g: G' \rightarrow G''$  son homomorfismos entonces la composición  $g \circ f: G \rightarrow G''$  es un homomorfismo
    - Si  $f: G \rightarrow G'$  es un isomorfismo entonces la aplicación inversa  $f^{-1}: G' \rightarrow G$  es un isomorfismo.
  - Como consecuencia de esta proposición se deduce que la existencia de un isomorfismo entre dos conjuntos dotados de sendas operaciones internas define una “relación” que satisface las siguientes propiedades:
    - Es reflexiva pues la aplicación identidad  $IG$  es un isomorfismo
    - Es simétrica pues existe un isomorfismo  $f: G \rightarrow G'$ , entonces la aplicación inversa  $f^{-1}: G' \rightarrow G$  es un isomorfismo
    - Es transitiva pues existen dos isomorfismos  $f: G \rightarrow G'$  y  $g: G' \rightarrow G''$  entonces la composición  $g \circ f: G \rightarrow G''$  es un isomorfismo
- **Homomorfismos de grupos**
  - En este apartado supondremos además que  $(G, +)$  y  $(G', +)$  son dos grupos tales que sus elementos neutros son respectivamente  $0G$  y  $0G'$  .... Se tiene:
    - $f(0G) = 0G'$
    - $f(-a) = -f(a)$  para todo  $a$  perteneciente  $G$
    - Si  $H$  es un subgrupo de  $G$  entonces,  $f(H) = \{ a' \text{ perteneciente } G' \mid \text{ existe } a \text{ perteneciente } G, f(a) = a' \}$  es un subgrupo de  $G'$
    - Si  $H'$  es un subgrupo de  $G'$  entonces,  $f^{-1}(H') = \{ a \text{ perteneciente } G \mid f(a) \text{ perteneciente } H' \}$  es un subgrupo de  $G$
  - Respecto de  $f(G)$  y  $\ker f$  se tiene:
  - Sea  $(G, +)$  y  $(G', +)$  dos subgrupos y  $f: G \rightarrow G'$  un homomorfismo. Se tiene:
    - $\text{Im } f$  es un grupo de  $G'$
    - $\ker f$  es un subgrupo de  $G$
    - $f$  es inyectivo si y solo si  $\ker f = \{0G\}$
    - $f$  es sobreyectivo si y solo si  $\text{Im } f = G'$
- **Homomorfismo de anillos y cuerpos**
  - Un homomorfismo de anillos de  $A$  en  $A'$  es una aplicación  $f: A \rightarrow A'$  tal que para todo  $a, b$  perteneciente  $A$  se cumple que :
    - $f(a+b) = f(a) + f(b)$
    - $f(ab) = f(a)f(b)$
  - Un homomorfismo de cuerpos no es más que un homomorfismo de anillos donde además  $(A, +, \cdot)$  y  $(A', +, \cdot)$  son dos cuerpos
- **Homomorfismos de conjuntos ordenados**
  - Cuando queremos hablar de identificaciones de estructuras ordenadas buscaremos biyecciones que conserven el orden. Con más precisión, si tenemos dos conjuntos ordenados  $(U, \leq)$  y  $(V, \leq)$ , una aplicación  $f: U \rightarrow V$  se denomina homomorfismo de estructuras de orden si es creciente, es decir:
    - Para todo  $u, u'$  perteneciente  $U$ , si  $u \leq u'$  entonces  $f(u) \leq f(u')$

- Cuando la aplicación  $f$  sea además biyectiva habalremos de un isomorfismo de estructuras ordenadas.
- **Aritmética de los números cardinales**
  - Sean  $a$  y  $b$  dos números cardinales y sean  $A$  y  $B$  dos conjuntos tales que :
    - $A \cap B = \emptyset$ ,  $a = \text{card}(A)$  y  $b = \text{card}(B)$  por definición:  
 $a + b = \text{card}(A \cup B)$
  - Sean  $a$  y  $b$  dos números cardinales y sean  $A$  y  $B$  dos conjuntos tales que :
    - $A \cap B = \emptyset$ ,  $a = \text{card}(A)$  y  $b = \text{card}(B)$  por definición:  
 $a \cdot b = \text{card}(A \times B)$

## 5. Los números naturales y los enteros

- Axiomas de Peano
- Propiedades de  $\mathbb{N}$
- El orden de  $\mathbb{N}$  en un buen orden
- Concepto conjunto finito e infinito
- Cardinal finito e infinito
- Teoremas y proposiciones (5.14 5.15 5.16 5.17 5.18 5.20 5.21 5.22 5.23 5.26)
- Resultados sobre conjuntos numerables
- Máximo común divisor
- Mínimo común múltiplo
- Algoritmo de Euclides
- Teorema de Bezout y teorema de Gauss

## 6. Los números Racionales y los números reales

- Propiedad arquimediana de  $\mathbb{R}$
- El orden en  $\mathbb{Q}$  es divisible
- Parte entera y aproximación decimal de un número real
- Propiedad arquimediana de  $\mathbb{R}$
- Caracterización de los intervalos
- $\mathbb{Q}$  y  $\mathbb{R} \setminus \mathbb{Q}$  son densos de  $\mathbb{R}$
- Propiedad de los intervalos encajados
- $\mathbb{R}$  no es un conjunto numerable

## 7. Los números Complejos

- Operar con números complejos
  - Biónica
  - Polar
  - Exponencial
- Conjugado, propiedades del conjugado
- Propiedades del módulo y argumento (representación geométrica)
- Potencia de un número complejo (fórmula de Moivre)
- Raíces  $n$ -ésima de un número complejo
- Resolución de ecuaciones de segundo grado
- Resolución de algunos tipos de problemas geométricos de movimientos mediante números complejos