Aritmética

Clase 1

Primeras Nociones

- El objeto principal de estudio de este curso son los números naturales y los enteros, definidos como:
- $\mathbb{N} = \{1, 2, 3, 4, \ldots\ldots\ldots\ldots\}$
- $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\ldots\}$

- Es importante recordar que entre los axiomas que definen a estos conjuntos, con sus operaciones (suma, resta, multiplicación), formalizados por G. Peano, se tiene el:
- **Principio de Inducción:** Sea P una propiedad acerca de los elementos de $\mathbb{N}$. Si se cumple que:

- A) P(1) es verdadera, y
- B) Para todo j >1, si P(z) es verdadera para todo z < j, entonces P(j) es verdadera.
- Entonces, P(n) es verdadera para todo n en ℕ.
- Observación: También puede aplicarse un argumento similar para probar que una cierta propiedad P es cierta para todo natural mayor o igual que un valor inicial w, verificando primero P(w) y luego el paso (B) del principio de inducción (pero ahora para j > w y z con: w ≦ z < j).
- Ejemplo: verificar que $2^n > n^2$ para todo n ≧ 5.

G. Peano

- **División entera:** Sean a,b enteros con b diferente de 0. Entonces existen enteros únicos c y r tales que:
  - $a = c \cdot b + r,\ 0 \leqq r < |b|$
- Observación: A un tal c se le llama "cociente" y a r "resto" de la división.
- Demostración: Supondremos que $b > 0$, el caso $b < 0$ queda como ejercicio.
- Caso (1): $a > 0$. En la sucesión: 0, b, 2b, 3b, …. , kb, (k+1)b,…….
- hay elementos mayores que a, por ejemplo para k= a+1 es evidente que
- $(a+1)\,b > ab \geqq a$. Luego, si cogemos k+1 como el primero natural con esta propiedad se tiene:
  - $kb \leqq a < (k+1)b$

- Si escribimos: $a - kb = r$, tenemos entonces que:
  - $0 \leqq a - kb = r < b$
- Con lo cual tomando $k=c$ se tiene $a = c\,b + r$ con un r que satisface las condiciones para ser el resto de la división.
- Veamos ahora unicidad (de cociente y resto): Si se tiene:
- $a = c\,b + r$, y también $a = c'\,b + r'$, con $0 \leqq r, r' < b$, restando tenemos:
- $c\,b - c'b + r - r' = 0$, de donde: $r - r' = (c' - c)b$. Como $|r-r'| < b \Longrightarrow$
- $r - r' = 0$ (pues 0 es el único múltiplo de b más pequeño que b), es decir que $r = r'$, y por lo tanto de la fórmula anterior también $c = c'$.

- Caso (2): $a = 0$: Podemos escribir $0 = 0 \cdot b + 0$, es decir que el cociente y el resto son 0. Para ver unicidad, si se tiene:
  - $0 = c\,b + r$ con $0 \leqq r < b$,
- Esta cota para r junto con la igualdad $r = -cb$ prueban que $r = 0$, y de aquí se deduce que $c = 0$.

- Caso (3): $a < 0$: Tomamos $-a > 0$ y aplicando lo visto en el caso (1) tenemos:
  - $-a = c\,b + r$, con $0 \leqq r < b$
- De aquí: $a = (-c)b - r$, con $-b < -r \leqq 0$
- Si $r=0$ esto ya resuelve la división entera. Si $r > 0 \Longrightarrow -r + b < b$, además como
- $r < b$, se tiene $-r + b > 0$, por lo tanto escribimos:
- $a = -c\,b - b - r + b = b(-c - 1) + (-r + b)$, y por lo tanto llamando $c' = -c-1$ y
- $r' = -r + b$, hemos obtenido:
  - $a = b \cdot c' + r'$ con $0 < r' < b$.
- Que es lo que queríamos: la unicidad se prueba exactamente igual que en el caso (1).
  - Q.E.D.


desmotivaciones.es
¿Alguna pregunta?

Polinomios (sobre un cuerpo K)

- Sea K un cuerpo, que puede ser $\mathbb{R}$, $\mathbb{Q}$ o $\mathbb{C}$. Lo importante es que se tienen dos operaciones, suma y producto, con neutros 0 y 1 respectivamente, ambas conmutativas y asociativas (además vale la propiedad distributiva del producto respecto de la suma), y que todo elemento tiene opuesto para la suma y todo elemento diferente del 0 tiene inverso para el producto.
- Definición: Sea K un cuerpo. Un polinomio P(x) a coeficientes en K (en una variable) es una expresión de la forma:
- $a_n\, x^n + \ a_{n-1}x^{n-1} \ + \ \dots \dots + \ \ a_1\ x + \ a_0$
- con n $\geqq$ 0 y a_0 , a_1, . … … . , a_n en K. Se dice que x es la variable y que los a_i son los coeficientes de P(x).

- Notación: K[x] = {Polinomios a coeficientes en K}
- Dos polinomios son iguales cuando lo son coeficiente a coeficiente. Cuando un coeficiente es 0, el sumando correspondiente puede o no escribirse, así: $x^2 + 1 = \quad x^2 + 0\,x + 1$
- Polinomios Constantes: son aquellos que se pueden escribir como arriba con n=0: P(x) = $a_0 \in K$. Un caso particular es el Polinomio Nulo: P(x) = 0.
- Propiedad: Todo polinomio no nulo se escribe de forma única como:
- $a_n x^n + \; a_{n-1}x^{n-1} + \; \ldots \ldots + \; a_1\, x + \; a_0$
- con $a_n \neq 0$, n ≧ 0. Llamamos a este n Grado del polinomio, y lo denotamos gr(P(x)). También convenimos en que el grado del polinomio nulo es -∞.

- Suma y Producto de Polinomios: Para sumar polinomios, se suman coeficiente a coeficiente (con la suma de K), y para multiplicar, se aplica la propiedad distributiva, aplicando la regla $x^n x^m = x^{n+m}$ y agrupando luego términos donde la x tenga el mismo exponente:
- Ejemplos:
- $(x^2 + 1) + (x^3 + 7x^2 + 3\,x + 4) = x^3 + 8x^2 + 3x + 5$
- (x+3)$(2x^3 + x^2\,) = 2x^4 + x^3 + 6x^3 + 3x^2 = 2x^4 + 7x^3 + 3x^2$
- Nótese que el polinomio constante 1 es el neutro del producto, y el polinomio nulo 0 el neutro de la suma.

Clase 2

- Propiedad: Sean P(x) y Q(x) polinomios en K[x].
  - (1) $\operatorname{gr}(P(x) \pm Q(x)) \leqq \max\{\operatorname{gr}(P(x)), \operatorname{gr}(Q(x))\}$
    - (2) $\operatorname{gr}(P(x) \cdot Q(x)) = \operatorname{gr}(P(x)) + \operatorname{gr}(Q(x))$
- Demostración: es evidente si recordamos como se suman y se multiplican polinomios (para (2), recordar que al multiplicar dos elementos no nulos de K, el resultado no puede dar 0).
- Corolario: Los polinomios P(x) que tienen inverso, es decir, tales que existe un polinomio Q(x) con:
- P(x) · Q(x) = 1, son los polinomios constantes no nulos (y sólo ellos).

- Demostración: Si $P(x) = c \in K$, $c \neq 0$, entonces $Q(x) = 1/c$ es su inverso.
- El polinomio nulo no tiene inverso puesto que para todo polinomio $Q(x)$, se tiene $0 \cdot Q(x) = 0 \neq 1$.
- Sea ahora $P(x)$ con $gr(P(x)) > 0$. Supongamos razonando por el absurdo que existe un polinomio $Q(x)$ con $P(x) \cdot Q(x) = 1$. Calculamos el grado de ambos miembros de esta igualdad y aplicamos la propiedad anterior:
- $gr(P(x)) + gr(Q(x)) = gr(P(x) \cdot Q(x)) = gr(1) = 0$
- Por otro lado tenemos que $gr(P(x)) > 0$ por hipótesis y $gr(Q(x)) \geqq 0$ (pues claramente $Q(x)$ no puede ser el polinomio nulo), luego:
- $gr(P(x)) + gr(Q(x)) > 0$, contradiciendo lo que pone tres líneas arriba!!
- Esta contradicción prueba lo que queríamos: $P(x)$ no posee inverso.

  - Q.E.D.

- Veamos ahora que al igual que en el caso de los enteros, para los polinomios también es posible efectuar divisiones con resto:
- Teorema (División Euclídea de polinomios): Si $a(x)$, $b(x) \in K[x]$ con $b(x) \neq 0$, existen polinomios únicos $q(x)$ y $r(x)$, llamados cociente y resto, tales que:
- $a(x) = b(x) \cdot q(x) + r(x)$ con $gr(r(x)) < gr(b(x))$.
- Demostración: La demostración de existencia es algorítmica:
- Si $gr(a(x)) < gr(b(x))$, la igualdad: $a(x) = b(x) \cdot 0 + a(x)$ resuelve el problema con $q(x)=0$ y $r(x) = a(x)$.

- Supongamos ahora gr(a(x)) ≧ gr(b(x)). Si a es constante, entonces b también es constante y: a = b · (a/b) + 0 resuelve el problema, con cociente q(x) = a/b y r(x) = 0.
- Veamos pues el caso gr(a(x)) = k > 0 (y recordar que tenemos gr(b)≦gr(a)).
- Aplicaremos el principio de inducción sobre k: para el caso de grado k= 0 la proposición ya la hemos visto (esta es una inducción que comienza en 0 en lugar de comenzar el 1, la cual es válida por el mismo principio). Suponemos pues (hipótesis de inducción) que es cierta para todo k' < k.

- Si a(x) $= a_k x^k + \;\ldots\ldots. + a_1 x + \; a_0\;,\; b(x) = \; b_m x^m + \;\ldots\ldots. + b_1\; x + \; b_0\;,\; con\; a_k \neq 0, b_m \; \neq 0, k \; \geq m \; \geq 0, k > 0,$ procedemos con la división imitando el algoritmo de división en enteros:
- $a_k x^k + a_{k-1} x^{k-1} + \cdots + \; a_0 \;\big|\; b_m x^m + \; b_{m-1}\, x^{m-1} + \cdots + \; b_0$
- $- \, a_k x^k - \frac{a_k b_{m-1}}{b_m} \; x^{k-1}$-........ $\qquad \frac{a_k}{b_m} \, x^{k-m} +$ ....
- $c_{k-1} x^{k-1} + \; \ldots \ldots$

- Como el polinomio que queda como "valor provisional del resto" es:
- $$c(x) = a(x) - (\frac{a_k}{b_m} \; x^{k-m}) \, b(x) \qquad (*)$$

- Con $\mathrm{gr}(\mathrm{c}(\mathrm{x})) < \mathrm{gr}(\mathrm{a}(\mathrm{x})) = \mathrm{k}$ podemos aplicarle la hipótesis de inducción y deducir que existen e(x) y r(x) polinomios tales que:
- $\mathrm{c}(\mathrm{x}) = \mathrm{b}(\mathrm{x})\ \mathrm{e}(\mathrm{x})\ + \mathrm{r}(\mathrm{x})$, con $\mathrm{gr}(\mathrm{r}(\mathrm{x})) < \mathrm{gr}(\mathrm{b}(\mathrm{x}))$ (**)
- Combinando (*) y (**) obtenemos:
- $\mathrm{a}(\mathrm{x})$ - $(\frac{a_k}{b_m}\ x^{k-m})\ \mathrm{b}(\mathrm{x}) = \mathrm{b}(\mathrm{x})\ \mathrm{e}(\mathrm{x})\ + \mathrm{r}(\mathrm{x})$, de donde:
- $\mathrm{a}(\mathrm{x}) = (\frac{a_k}{b_m}\ x^{k-m} + \mathrm{e}(\mathrm{x})\ )\ \mathrm{b}(\mathrm{x})\ + \mathrm{r}(\mathrm{x})$, que como $\mathrm{gr}(\mathrm{r}(\mathrm{x})) < \mathrm{gr}(\mathrm{b}(\mathrm{x}))$ resuelve el problema.

- Veamos ahora la unicidad: Si:
- $a(x) = b(x) \cdot q(x) + r(x)$ con $gr(r(x)) < gr(b(x))$, y:
- $a(x) = b(x) \cdot q'(x) + r'(x)$ con $gr(r'(x)) < gr(b(x))$, restando obtenemos:
- $b(x)\ (q(x) - q'(x)) = r'(x) - r(x)$ (😀)
- Si $q(x)-q'(x) \neq 0$, gr(LADO IZQUIERDO DE 😀) $\geqq gr(b(x))$, pero por otro lado:
- gr (LADO DERECHO DE 😀) $\leqq \max\{gr(r(x)), gr(r'(x))\} < gr(b(x))$
- Luego la igualdad (😀) daría lugar a una contradicción, con lo cual necesariamente se tiene que: $q(x) = q'(x)$, y por lo tanto de (😀) se deduce también que $r(x) = r'(x)$
- Q. E. D.

Divisibilidad y Algoritmo de Euclides (en $\mathbb{Z}$)

- Definición: Dados enteros a y c tales que existe un entero b con:
  - $a \cdot b = c$
- decimos que “a divide a c” o que “c es divisible por a” o que “c es múltiplo de a”. Decimos en este caso que a es un divisor de c. La notación para esta relación es:
  - $a \mid c$
- El 0 es el único número que es divisible por cualquier otro entero.

- Clasifiquemos ahora a los enteros positivos de acuerdo a sus divisores:
- El 1 es el neutro del producto, y además el único entero positivo inversible, pues: $1 \cdot 1 = 1$. A un elemento inversible lo llamaremos unidad.
- Dado un entero n >1, decimos que es primo si sus únicos divisores positivos son 1 y n (a veces llamados divisores triviales). Es decir, un número positivo es primo si posee exactamente dos divisores positivos.
- En el caso complementario, un número n>1 se dice compuesto. Es decir, n es compuesto cuando posee más de dos divisores. Equivalentemente, n es compuesto si posee algún divisor d no trivial, es decir, un divisor d de n tal que 1 < d < n. En este caso, obsérvese que si llamamos c = n/d se tiene:
  - n = c · d, con 1 < c, d < n.
- Ergo, un número es compuesto cuando admite una factorización no trivial.

Propiedades básicas de la divisibilidad

- Sean a,b,c,m,n enteros. Entonces se tiene que:
- A) $a | a$ (propiedad reflexiva)
- B) $c | b$ y $b | a \Rightarrow c \mid a$ (propiedad transitiva)
- C) $a \mid b$ y $b \mid a \Rightarrow a = \pm b$
- D) $b \mid a$ y $b | c \Rightarrow b \mid a m + c n$ (linealidad)
- E) $b \mid a \Rightarrow c b \mid c a$ (multiplicatividad)
- F) si $c b \mid c a$ y $c \neq 0 \Rightarrow b \mid a$ (cancelativa)
- Demostración: las dejamos como ejercicio, todas se deducen fácilmente de la definición de divisibilidad. Probemos por ejemplo (D): la hipótesis implica que existen k y j enteros tales que: $a = b k$ y $c = b j$. Pero entonces se tiene que $a m = b (k m)$ y que $c n = b (j n)$, y por lo tanto que:
- $a m + c n = b (k m + j n)$, y por lo tanto que $b \mid a m + c n$.

- **Definición (Máximo Común Divisor):** Dados dos enteros a y b no ambos nulos, el Máximo Común Divisor de a y b, en símbolos, mcd(a,b), es el mayor de los enteros d que divide a ambos: es decir, el mayor entero d tal que $d|a$ y $d|b$.
- **Lema 1:** Si a y b son enteros no ambos nulos:
- $\mathrm{mcd}(a,b) = \mathrm{mcd}(\pm a, \pm b) = \mathrm{mcd}(a, b \pm a)$
- Demostración: La primera igualdad es trivial, para la otra basta con ver el caso $\mathrm{mcd}(a,b) = \mathrm{mcd}(a, b + a)$. Para ver esta igualdad, basta con ver que el conjunto de divisores comunes entre a y b es el mismo conjunto que el de divisores comunes entre a y b+a.
- Sea por lo tanto d tal que $d|a$ y $d|b$. Por las propiedades ya vistas de la divisibilidad (ítem (D)), de aquí se sigue que: $d \mid a + b$. Luego d es divisor común de a y b+a.
- Recíprocamente, aplicando la misma propiedad vemos que si $d|a$ y $d|b+a$ también divide a la resta de ambos que es b+a-a=b, luego d es divisor común de a y de b.

- Lema 2: Si a y b son enteros no ambos nulos y n es un entero, se tiene:
- mcd(a, b) = mcd(a, b – a n).
- Demostración: Podemos suponer que $n \neq 0$. Hagamos el caso $n > 0$, el caso $n < 0$ se prueba análogamente (ejercicio). Veámoslo por inducción: si $n=1$, la afirmación ya fue probada en el Lema 1. Si $n > 1$, podemos suponer por hipótesis de inducción que se tiene: mcd(a,b) = mcd(a, b- a (n-1)). Aplicando una vez más el Lema 1 (para el caso de la resta), tenemos que:
- mcd(a, b – a (n-1)) = mcd(a, b– a(n-1) – a) = mcd(a, b – n a). Luego concluímos que: mcd(a,b) = mcd(a, b - a n).
- Q.E.D.