Índice general

Parte I

Induccion y Divisibilidad

Capítulo 1

Induccion matematica

1.1. Conceptos previos

1.1.1. Numeros reales

1.1.1.1. Definicion

Llamamos $\mathbb{R}$ a un conjunto que satisface los siguientes axiomas:

Asociatividad $a + (b + c) = (a + b) + c \ \forall a, b, c \in \mathbb{R}$

Conmutatividad $a + b = b + a \ \forall a, b \in \mathbb{R}$

Neutro $a + 0 = a \ \forall a \in \mathbb{R}$

Opuesto $a + a' = 0$

Asociatividad $a\,(bc) = (ab)\,c \ \forall a, b, c \in \mathbb{R}$

Conmutatividad $ab = ba \ \forall a, b \in \mathbb{R}$

Neutro $a1 = a \ \forall a \in \mathbb{R}(1 \neq 0)$

Inverso $aa'' = 1 \ \forall a \in \mathbb{R} - \{0\}$

Distributividad $a\,(b + c) = ab + ac \ \forall a, b, c \in \mathbb{R}$

Tricotomia $a < b \veebar a = b \veebar a > b \ \forall a, b \in \mathbb{R}$

Transitividad $a < b \wedge b < c \Rightarrow a < c \ \forall a, b, c \in \mathbb{R}$

Consistencia $a < b \Rightarrow a + c < b + c \ \forall a, b, c \in \mathbb{R}$

Consistencia $a < b \wedge c > 0 \Rightarrow ac < bc \ \forall a, b, c \in \mathbb{R}$

Supremo $H \neq \emptyset \subseteq \mathbb{R}$ es acotado superiormente en $\mathbb{R} \Rightarrow H$ tiene supremo en $\mathbb{R}$

1.1.1.2. Propiedades

- El 0 es unico
- El opuesto de a es unico y se denota $-a$
- Ley cancelativa: $a + b = a + c \Rightarrow b = c$
- $a0 = 0$
- $ab = 0 \Rightarrow a = 0 \vee b = 0$
- Regla de los signos: $(-a)\, b = a\, (-b) = -\, (ab)$
- $a^2 = b^2 \Rightarrow a = b \vee a = -b$
- $(-1)\, a = -a$
- El inverso de $a \neq 0$ es unico y se denota $1/a$

1.1.2. Conjunto bien ordenado

Definicion

Decimos que A es un conjunto *bien ordenado* si todo subconjunto no vacio de A posee primer elemento.

1.1.3. Definiciones recursivas

Definicion Definimos una sucesion $u_1, u_2, u_3, \ldots$ donde el termino n-esimo es en funcion de los anteriores.

Ejemplo

1. $u_1 = 1$
2. $u_n = 2u_{n-1}$ $(\forall n > 1)$

Es decir: $u_1 = 1, u_2 = 2, u_3 = 4, u_4 = 8, \ldots$

1.1.4. Sumatoria

1.1.4.1. Definicion

Dada una sucesion de numeros reales $\{x_i : i \in \mathbb{N}\}$ se define la sumatoria desde 1 hasta n como:

1. $\sum_{i=1}^{1} x_i = x_1$
2. $\sum_{i=1}^{k+1} x_i = \sum_{i=1}^{k} x_i + x_{k+1}$

1.1.4.2. Propiedades

- Aditividad: $\sum_{k=1}^{n} (a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k$
- Homogeneidad: $\sum_{k=1}^{n} ca_k = c \sum_{k=1}^{n} a_k$
- Telescopica: $\sum_{k=1}^{n} (a_k - a_{k-1}) = a_n - a_0$
- $\sum_{k=1}^{n} c = nc$
- $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{i,j}$

1.2. Conjunto inductivo

1.2.1. Definicion

Un conjunto $H \subseteq \mathbb{R}$ se dice inductivo si:

- $1 \in H$
- $k \in H \Rightarrow k+1 \in H$

1.2.2. Ejemplos

- $\mathbb{R}$
- $\mathbb{N}$
- $\mathbb{Z}$
- $\bigcup_{i=1}^{\infty}(i-\epsilon, i+\epsilon)$

1.2.3. Lema: interseccion de conjutnos inductivos

La interseccion arbitraria de conjuntos inductivos es un conjunto inductivo.

1.2.3.1. Demostracion

Sean $X_i \subseteq \mathbb{R}$ subconjuntos inductivos con $i \in I$ y sea $X = \bigcap_{i \in I} X_i$

- Como X_i son inductivos: $1 \in X_i \Rightarrow 1 \in X$
- Sea $k \in X \Rightarrow k \in X_i \Rightarrow k+1 \in X_i \Rightarrow k+1 \in X$

1.3. Principio de induccion

1.3.1. Principio de induccion

1.3.1.1. Induccion conjuntista

Enunciado Sea $H \subseteq \mathbb{N} / 1 \in \mathbb{N} \wedge (h \in H \Rightarrow h+1 \in H)$ entonces $H = \mathbb{N}$.

Demostracion Por hipotesis H es inductivo $\overset{1.4.1}{\Longrightarrow} \mathbb{N} \subseteq H$ y como asumimos $H \subseteq \mathbb{N}$ entonces $H = \mathbb{N}$.

1.3.1.2. Induccion clasica

Enunciado Sea $P(n)$ una propiedad de $n \in \mathbb{N}$ tal que:

1. $P(1)$ es verdadera.
2. $P(k)$ verdadera $\Rightarrow P(k+1)$ verdadera.

entonces $P(n)$ es verdadera $\forall n$.

Demostracion Sea $H = \{n \in \mathbb{N} : P(n)\}$.

1. Por hipotesis $P(1)$ es verdadera, luego $1 \in H$.
2. Si $k \in H$ por definicion de H, $P(k)$ es verdadera y por hipotesis $P(k) \Rightarrow P(k+1) \Rightarrow k+1 \in H$

Hemos demostrado que H es inductivo, luego $\mathbb{N} \subseteq H$ y como $H \subseteq \mathbb{N}$ entonces $H = \mathbb{N} \therefore P(n)$ es verdadera $\forall n \in \mathbb{N} = H$.

1.3.1.3. Induccion desplazada

Enunciado Sea $P(n)$ una propiedad de $n \in \mathbb{N}$ y sea $N \in \mathbb{N}$, si $P(N)$ es cierta y $P(k) \Rightarrow P(k+1)$ para cada $k \geq N$ entonces $P(n)$ es cierta $\forall n \geq N$.

Demostracion Sea $H = \{n \in \mathbb{N} : P(n+N-1)\}$.

1. Notemos que $1 \in H$ pues $P(1+N-1) = P(N)$ que es cierta por hipotesis.
2. Si $k \in H$ entonces por definicion de H, $P(k+N-1)$ es cierta y por hipotesis: $P(k+N-1) \Rightarrow P(k+N-1+1) = P[(k+1)+N-1]$ luego $k+1 \in H$.

$\therefore H = \mathbb{N}$

1.3.1.4. Induccion fuerte conjuntista

Enunciado Sea $H \subseteq \mathbb{N} / 1 \in H \wedge [\![1,k]\!] \subseteq H \Rightarrow [\![1,k+1]\!] \subseteq H$ entonces $H = \mathbb{N}$

Demostracion Sea $H \subset \mathbb{N} \Rightarrow \overline{H} \neq \emptyset$ luego por el principio del buen orden $\overline{H}$ tiene primer elemento $p > 1$ (pues $1 \in H$ por hipotesis), entonces $[\![1,p-1]\!] \subseteq H$ pero por hipotesis si $[\![1,p-1]\!] \subseteq H \Rightarrow [\![1,p]\!] \subseteq H$ por lo que $p \in H$. Sin embargo $p \in \overline{H}$ (pues es su primer elemento). ¡Contradiccion!

1.3.1.5. Induccion fuerte clasica

Enunciado Sea $P(n)$ una propiedad de $n \in \mathbb{N}$ tal que:

1. $P(1)$ es cierta.
2. Si $P(1), P(2), P(3), \ldots, P(k)$ son ciertas, tambien lo es $P(k+1)$.

entonces $P(n)$ es cierta $\forall n \in \mathbb{N}$.

Demostracion Sea $H = \{n \in \mathbb{N} : P(n)\}$

1. Por hipotesis $P(1)$ es cierta luego $1 \in H$.
2. Ademas como $P(1), P(2), P(3), \ldots, P(k) \Rightarrow P(k+1)$ entonces $[\![1,k+1]\!] \subseteq H$.

y por el principio de induccion fuerte $H = \mathbb{N}$

1.4. Numeros naturales

1.4.1. Definicion

$\mathbb{N}$ es el conjunto de todos los subconjuntos inductivos de $\mathbb{R}$.

1.4.2. Propiedades

1. $n \in \mathbb{N} \wedge n \neq 1 \Rightarrow n-1 \in \mathbb{N}$ o en forma equivalente $\exists m \in \mathbb{N}/m+1=n$
2. $a, b \in \mathbb{N} \Rightarrow a+b \in \mathbb{N} \wedge ab \in \mathbb{N}$
3. $a, b \in \mathbb{N} \wedge a < b \Rightarrow b-a \in \mathbb{N}$
4. $n \in \mathbb{N}_0 \wedge a \in \mathbb{R}/n < a < n+1 \Rightarrow a \notin \mathbb{N}$
5. $\mathbb{N}$ es un conjunto bien ordenado (principio del buen orden).

1.4.3. Demostraciones

1. Sea $H = \{1\} \cup \{x \in \mathbb{N} : x = y+1\}$ (para algun $y \in \mathbb{N}$).
   - *a)* $1 \in H$
   - *b)* Si $h \in H$ entonces $h = y+1$, luego $h+1 = (y+1)+1$ por lo que $h+1 \in H$
     $\therefore H = \mathbb{N}$
2. Sea $b \in \mathbb{N}$ fijo y sea $P(n)$: "$n+b \in \mathbb{N}$"
   - *a)* $P(1)$ es cierta pues $b \in \mathbb{N}$ y $\mathbb{N}$ es inductivo.
   - *b)* Supongamos $P(k)$ cierta luego $k+1+b = (k+b)+1 \in \mathbb{N}$
     Finalmente $P(n)$ es verdadera $\forall n, b \in \mathbb{N}$
3. Sea $P(n)$: "$n < b \Rightarrow b-n \in \mathbb{N}$"
   - *a)* $P(1)$ es cierta por la propiedad 1.
   - *b)* Supongamos $P(k)$ cierta luego si $k+1 < b \Rightarrow k < b-1 < b \Rightarrow b-k \in \mathbb{N}$ (por H. I.)
     $b-(k+1) = (b-k)-1 \in \mathbb{N}$ (por propiedad 1).
     $\therefore P(k) \Rightarrow P(k+1)$ si $k+1 < b$

4. Si $0 < a < 1$ entonces $a \notin \mathbb{N}$ pues $\mathbb{R}_{\geq 1}$ es inductivo y $a \notin \mathbb{R}_{\geq 1}$.
   Como $\mathbb{N} \subseteq \mathbb{R}_{\geq 1}$ sigue $a \notin \mathbb{N}$.
   Si $n < a < n+1$ con $n \in \mathbb{N}$ y $a \in \mathbb{N}$ entonces $0 < a - n < 1$.
   Por un lado $a - n \in \mathbb{N}$ (por propiedad 3) pero acabamos de ver que no existen naturales entre 0 y 1. ¡Absurdo!
   $\therefore a \notin \mathbb{N}$

5. Debemos ver que si $H \subseteq \mathbb{N} \Rightarrow H$ tiene primer elemento.
   Supongamos por el absurdo que H no tiene primer elemento.
   Sea $K = \left\{n \in \mathbb{N} : [\![1, n]\!] \subseteq \overline{H}\right\}$

   a) $1 \in K$ pues de lo contrario 1 seria primer elemento de H.

   b) Supongamos $k \in K$ es decir $[\![1, k]\!] \subseteq \overline{H}$ $(i \notin H \forall i \in [\![1, k]\!])$
   Si $k+1 \in H \Rightarrow k+1$ seria primer elemento de H. Esto no puede ser, luego $k+1 \notin H \Rightarrow [\![1, k+1]\!] \subseteq H$, es decir $k+1 \in K$

   Por lo tanto K es inductivo y como $K \subseteq \mathbb{N}$ entonces $K = \mathbb{N}$ y en conclusion $H = \emptyset$. ¡Contradiccion!

Capítulo 2

Divisibilidad

2.1. Numeros enteros

2.1.1. Definicion

Definimos al conjunto de los numeros enteros como $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$

2.1.2. Propiedades

1. $a, b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z} \wedge ab \in \mathbb{Z}$
2. $ab = 1 \Rightarrow \begin{cases} a = b = 1 \\ a = b = -1 \end{cases} \quad \forall a, b \in \mathbb{Z}$
3. $a, b \in \mathbb{Z} \Rightarrow a - b \in \mathbb{Z}$

2.1.3. Demostraciones

1. Analizaremos distintos casos.
   - *a*) $a, b \in \mathbb{N}$: ya vimos $a + b \in \mathbb{N} \wedge ab \in \mathbb{N}$
   - *b*) $a = 0 \wedge b \in \mathbb{Z}$:
     - 1) $a + b = 0 + b = b \in \mathbb{Z}$
     - 2) $ab = 0b = 0 \in \mathbb{Z}$
   - *c*) $a \in \mathbb{Z} \wedge b = 0$: Analogo al caso anterior.

d) $-a, -b \in \mathbb{N}$:

1) $a+b = -\left[\underbrace{-a}_{\in \mathbb{N}} \quad \underbrace{+(-b)}_{\in \mathbb{N}} \right] \in -\mathbb{N}$

2) $ab = [(-a)(-b)] \in \mathbb{N}$

e) $a \in \mathbb{N} \wedge b \in -\mathbb{N}$:

1) $a+b = a-(-b) \begin{cases} Si & a = -b \Rightarrow a+b = 0 \in \mathbb{Z} \\ Si & a > -b \Rightarrow a+b = a-(-b) \in \mathbb{N}(1.4.2) \\ Si & a < -b \Rightarrow a+b = a-(-b) = -(-b-a) \in \mathbb{N} \end{cases}$

2) $ab = [a(-b) \in -\mathbb{N}]$

f) $a \in -\mathbb{N} \wedge b \in \mathbb{N}$: Analogo al caso anterior.

2. Podemos asumir $a, b \neq 0$ pues de lo contrario $ab = 0 \neq 1$

a) Si $a, b \in \mathbb{N}$ entonces $ab = 1 \Rightarrow a = b = 1$ de lo contrario $ab > 1$

b) Si $a \in \mathbb{N} \wedge b \in -\mathbb{N}$ entonces $ab < 0 \Rightarrow ab \neq 1$ por lo que este caso no se da.

c) Si $a, b \in -\mathbb{N}$ entonces $-a, -b \in \mathbb{N}$. Por hipotesis tenemos $ab = 1 = (-a)(-b)$ y por el caso a) $-a = -b = 1$ por lo que $a = b = -1$.

3.

a) $1 \in \mathbb{N} \Rightarrow -1 \in \mathbb{Z}$

b) $a - b = a + \underbrace{(-1)b}_{\in \mathbb{Z}}$

2.2. Divisibilidad

2.2.1. Definicion

Sean $a, b \in \mathbb{Z}$ decimos que «*a divide a b*» y lo notamos $a|b$ si $\exists c \in \mathbb{Z} / b = ac$

2.2.2. Propiedades

1. $1|a \wedge a|a \wedge a|0 \ \forall a \in \mathbb{Z}$
2. $a|b \wedge b|c \Rightarrow a|c$
3. $a|b \wedge a|c \Rightarrow a|(b+c) \wedge a|(b-c)$
4. $a|b \wedge a|(b+c) \Rightarrow a|c$
5. $a|b \wedge b|a \Rightarrow a = \pm b$
6. $a|b \Rightarrow a|bx \ \forall x \in \mathbb{Z}$
7. $a|b \wedge a|c \Rightarrow a|(bx+cy) \ \forall x, y \in \mathbb{Z}$

2.2.3. Demostraciones

1. $a = 1a \Rightarrow 1|a \wedge a|a$ ademas $0 = 0a \Rightarrow a|0$
2. $a|b \Rightarrow b = ax$ ademas $b|c \Rightarrow c = by$ luego $c = by = a\,(xy) \Rightarrow a|c$
3. $a|b \Rightarrow b = ax$ ademas $a|c \Rightarrow c = ay$ luego:
   a) $b + c = ax + ay = a\,(x+y) \Rightarrow a|\,(b+c)$
   b) $b - c = ax - ay = a\,(x-y) \Rightarrow a|\,(b-c)$
4. Por la propiedad 3) $a|b \wedge a|\,(b+c) \Rightarrow a|\,[(b+c)-b]$ es decir $a|c$

2.2.4. Algoritmo de la division

2.2.4.1. Teorema

Enunciado Sean $a, b \in \mathbb{Z}$ $(b \neq 0)$ entonces $\exists q, r \in \mathbb{Z}/a = bq + r$ con $0 \leq r < b$ y ademas q, r son unicos.

Observacion $b|a \iff r = 0$

2.2.4.2. Demostracion

Existencia

1. Supongamos $a > 0$. Sea $H = \{h \in \mathbb{N} : hb > a\}$. Notemos que $H \neq \emptyset$ pues $(a+1)\,b > a$.
   Por el principio del buen orden H tiene primer elemento h_0; luego $h_0 - 1 \notin H$ es decir $(h_0 - 1)\,b \leq a < h_0 b$.
   Llamemos $q = h_0 - 1$ y $r = a - bq$. Restando bq miembro a miembro: $0 \leq a - bq < b$ por lo que $0 \leq r < b$ y claramente $a = bq + r$.

2. Si $a < 0$ entonces $-a > 0$. Luego por la parte anterior $\exists q, r / -a = bq + r$ con $(0 \leq r < b)$. Luego $a = b\,(-q) - r$.

   a) Si $r = 0 \Rightarrow a = b\,(-q)$.

   b) Si $0 < r < b \Rightarrow 0 > -r > -b \Rightarrow -b < -r < 0 \Rightarrow 0 < b - r < b$.
   Luego: $a = b\,(-q) - r = b\,(-q) - b + b * r = b\underbrace{(q-1)}_{\widetilde{q}} + \underbrace{b - r}_{\widetilde{r}}$.

   Finalmente: $a = b\widetilde{q} + \widetilde{r}$ con $0 \leq \widetilde{r} < b$

Unicidad

Supongamos $\begin{cases} a = bq + r & (0 \leq r < b) \\ a = bq' + r' & (0 \leq r' < b) \end{cases}$

Como $r \neq r'$ supongamos $r' \leq r$. Restando las ecuaciones anteriroes: $0 = b\,(q - q') + r - r'$ con $(0 < r - r' < b) \Rightarrow r - r' = b\,(q' - q)$. Luego:

- $q' - q = 0 \Rightarrow r - r' = 0 \Rightarrow q = q' \wedge r = r'$
- o bien $q' - q \in \mathbb{N} \Rightarrow r - r' = b\,(q' - q) \geq b$ ¡Contradiccion!

$\therefore q = q' \wedge r = r'$.

2.2.4.3. Corolario

Dados $a, b \in \mathbb{Z}, \exists q, r \in \mathbb{Z} / a = bq + r$ con $(0 \leq r < |b|)$

2.2.4.4. Ejemplos

- Para$19/6$ tenemos $19 = 6.3 + 1$
- Para $-19/6$ tenemos $-19 = 6\,(-3) - 1 = 6\,(-3) - 6 + 6 - 1 = 6\,(-4) + 5$
- Para $-19/-6$ tenemos $-19 = (-6)\,4 + 5$

2.2.5. Sistemas de numeracion posicionales

En general para representar un numero en base $b \geq 2$ se utilizan b simbolos $\{S_0, S_1, \ldots, S_{b-1}\}$ que representan los numeros $0, 1, \ldots, b-1$.

Un numero a en base b se escribe

$$a : (a_k a_{k-1} \cdots a_1 a_0)_b = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 k + a_0$$

Luego $a = b \underbrace{\left(a_k b^{k-1} + a_{k-1} b^{k-2} + \ldots + a_1\right)}_{q'} + \underbrace{a_0}_{r'}$ con $(0 \leq a_0 < b)$

2.2.6. Maximo comun divisor

2.2.6.1. Definicion

Dados $a, b \in \mathbb{Z}$ con $(b \neq 0)$ decimos que d es un MCD de a y b si $d \in \mathbb{N}$ y:

1. $d|a \wedge d|b$
2. $c|a \wedge c|b \Rightarrow c|d$

Observacion Si existe el MCD es unico.

Demostracion Supongamos que d_1 y d_2 son MCD de a y b entonces $d_2|d_1 \Rightarrow d_2 \leq d_1$. Analogamente $d_1|d_2 \Rightarrow d_1 \leq d_2 \therefore d_1 = d_2$

2.2.6.2. Teorema

Dados $a, b \in \mathbb{Z}$ no simultaneamente nulos, entonces:

1. $\exists! d$ que satisface las condiciones de la definicion.
2. $MCD(a, b)$ es combinacion lineal de a y b. Es decir $\exists s, t \in \mathbb{Z} / MDC(a, b) = sa + tb$

2.2.6.3. Demostracion

1. Supongamos sin perder generalidad que $b \neq 0$. Mas aun, como $MCD(a,b) = MCD(a,-b)$ se puede suponer $b > 0$.

   Divido por b: $a = bq_1 + r_1 \ (0 \leq r_1 < b)$
   Si $r_1 \neq 0$ *divido por* r_1*:* $b = r_1q_2 + r_2 \ (0 \leq r_2 < r_1)$
   Si $r_2 \neq 0$ *divido por* r_2*:* $r_1 = r_2q_3 + r_3 \ (0 \leq r_3 < r_2)$
   $\ldots$
   Como $b = r_0 > r_1 > r_2 > \ldots \geq 0$ llegamos a $r_n = 0$. Luego:
   $r_{n-3} = r_{n-2}q_{n-1} + \underbrace{r_{n-1}}_{MCD}$ con $(0 \leq r_{n-1} < r_{n-2})$
   $r_{n-2} = r_{n-1}q_n$

   $$\text{Notar que:} \quad \begin{array}{c} r_{n-1}|r_{n-2} \Rightarrow r_{n-1}|r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \ \Rightarrow \\ r_{n-1}|r_{n-4} = r_{n-3}q_{n-2} + r_{n-2} \ \Rightarrow \\ r_{n-1}|r_0 = b \Rightarrow r_{n-1}|a = bq_1 + r_1 \end{array}$$

   $$\text{Reciprocamente si } c|a \wedge c|b \text{ entonces } \begin{array}{c} c|r_1 = a - bq_1 \ \Rightarrow \\ c|r_2 = b - r_1q_2 \Rightarrow c|r_3 \ \Rightarrow \\ c|r_{n-1} \end{array}$$

   Por lo tanto $MCD(a,b) = r_{n-1}$

2. Finalmente r_{n-1} es combinacion lineal entera de r_{n-2} y r_{n-3}:

   $$r_{n-1} = r_{n-3} - r_{n-2}q_{n-1} = r_{n-3} - (r_{n-4} - r_{n-3}q_{n-2})\, q_{n-1} = -r_{n-4} + q_{n-1} + r_{n-3}\,(1 + q_{n-2}q_{n-1})$$

   Continuando asi encontramos $s, t \in \mathbb{Z} / r_{n-1} = sa + tb$.

2.2.7. Primalidad

2.2.7.1. Numeros coprimos

Definicion Dos numeros $a, b \in \mathbb{Z}$ no simultaneamente nulos, se dicen coprimos si $MCD(a, b) = 1$

Observacion

- 1 es corpimo con todos los enteros.
- a y b son coprimos $\iff$ no tienen divisores comunes $\neq 1$

Corolario a y b son corpimos $\iff \exists s, t \in \mathbb{Z}/1 = sa + tb$.

Demostracion

- $\Rightarrow$) a, b coprimos $\Rightarrow MCD(a, b) = 1 \Rightarrow \exists s, t/1 = sa + tb$
- $\Leftarrow$) Si $c|a \wedge c|b \Rightarrow c|\,(sa + tb) = 1$, luego $c = \pm 1 \therefore MDC(a, b) = 1$

2.2.7.2. Numeros primos

Definicion Un numero $p \in \mathbb{Z}$ se dice primo si tiene exactamente cuatro divisores. Equivalentemente p es primo si $p \neq \pm 1$ y solo es divisible por $\pm 1, \pm p$.

Observacion p es primo $\iff$ $-p$ es primo (p y $-p$ tienen los mismos divisores).

Lema Sea $p \in \mathbb{Z}$ un numero primo, entonces: $p|ab \Rightarrow p|a \vee p|b$

Demostracion Supongamos $p \nmid a \Rightarrow MCD(a, p) = 1$ por lo tanto $\exists s, t \in \mathbb{Z}/1 = sa + tp$ y como $b = b.1$ entonces $b = b\,(sa + tp) = sab + tpb$.

Como $p|ab \Rightarrow p|sab$ y ademas $p|tpb$, entonces $p|sab \wedge p|tpb \Rightarrow p|\,(sab + tpb) = b$.

Lema

1. Si p es primo y divide a un producto de enteros $a_1, a_2, \ldots, a_n$ entonces $p|a_j$ para algun $1 \leq a_j \leq n$.
2. Si p, q son primos positivos y $p|q \Rightarrow p = q$.

2.2.8. Teorema fundamental de la aritmetica

Sea $m \in \mathbb{Z}, m \neq -1, 0, 1$ entonces existen primos positivos $p_1, p_2, \ldots, p_r / m = \epsilon \prod_{j=1}^{r} p_j$ con $\epsilon = \pm 1$ y esta factorizacion es unica (salvo por el orden).

2.2.8.1. Demostracion

Existencia Consideremos $m \geq 2$. Debemos probar $Q(m)$:«m es producto de primos».

1. $Q(2)$ es verdadera.
2. Supongamos $Q(2), Q(3), \ldots, Q(m)$ son ciertas y veamos que pasa con $Q(m+1)$
   Si $m+1$ es primo ya esta. De lo contrario $m+1$ tiene un divisor a tal que $1 < a < m+1$. Luego $m+1 = ab$ con $1 < b < m+1$.
   Como $Q(a)$ y $Q(b)$ son verdaderas, tanto a como b son producto de primos y en consecuencia $m+1 = ab$ es producto de primos.

Unicidad Sea $P(r)$: «Todo $m \in \mathbb{N}$ que es producto de primos positivos tiene una unica factorizacion en primos positivos, salvo por el orden».

1. Veamos que $P(1)$ es cierta.
   Supongamos $m = \prod_{j=1}^{1} p_j = p_1$. Luego m es primo.
   Si por otro lado $m = \prod_{j=1}^{s} p'_j$ con $p'_j > 0$, por el lema previo: $m | p'_j$ para algun j y por la segunda parte del lema $m = p'_j = p_1$.
   Por lo tanto $s = 1 \wedge m = p_1$.
2. Veamos que $P(k) \Rightarrow P(k+1)$. Supongamos cierta $P(k)$ y sea $m = \prod_{j=1}^{k+1} p_j = \prod_{j=1}^{s} p'_j$.
   $p_{k+1} \left| m = \prod_{j=1}^{s} p'_j \right. \Rightarrow p_{k+1} | p'_h$ para algun $1 \leq h \leq s \therefore p_{k+1} = p'_h$.

Luego $\frac{m}{p_{k+1}} = \prod_{j=1}^{k} p_j = \prod_{\substack{j=1 \\ j \neq k}}^{s} p'_j$ con $j \neq h$ y en consecuencia $\frac{m}{p_{k+1}}$ es producto de k primos. Finalmente por hipotesis inductiva esta factorizacion es unica $\Rightarrow k+1 = s \wedge p_1, \ldots, p_{k+1}$ coinciden con $p'_1, \ldots, p'_{k+1}$ salvo en el orden.

2.2.8.2. Corolario

Enunciado Existen infinitos numeros primos.

Demostracion Supongamos que existen una cantidad finita de primos positivos. Digamos $p_1, p_2, \ldots, p_k$.

Sea $n = \prod_{j=1}^{k} p_j$, como $n+1 > 1$ por el teorema fundamental de la aritmetica existe un primo positivo p tal que $p|n+1$. Luego $p = p_j$ para algun j. Como $p|n+1 \wedge p|n \Rightarrow p|MCD(n, n+1)$. ¡Absurdo! (ver lema siguiente).

2.2.8.3. Lemas

Lema 1 Dado $n \in \mathbb{Z}$: n y $n+1$ son coprimos.

Demostracion $1 = 1\,(n+1) + (-1)\,n \therefore MCD(n, n+1) = 1$

Lema 2 Si $n \in \mathbb{N}$ no es primo, entonces existe un primo positivo p tal que $p|n \wedge p \leq n$

2.2.8.4. Proposicion

Enunciado Sean $a, b \in \mathbb{Z} - \{0\}$ tales que:

- $a = \epsilon \prod_{j=1}^{r} p_j^{kj}$
- $b = \epsilon' \prod_{j=1}^{r} p_j^{hj}$

con $\epsilon, \epsilon' = \pm 1, p_j$ primos positivos distintos y $k_j, h_j \geq 0$ entonces:

$$MCD(a, b) = \prod_{j=1}^{r} p_j^{min(k_j, h_j)}$$

Observacion Notese que $k_j = 0$ en el caso de que p_j no aparezca en la descomposicion en primos de a. (Analogamente si $h_j = 0$).

Demostracion Sea $d = \prod_{j=1}^{r} p_j^{min(k_j, h_j)}$, claramente $d|a \wedge d|b$. Sea c tal que $c|a \wedge c|b$. Notemos que si p es primo y $p|c$ entonces $p|a \wedge p|b$, luego $c = \epsilon'' \prod_{j=1}^{r} p_j^{l_j}$ con $\epsilon'' = \pm$ y $l_j \geq 0$. Como $c|a$, $l_j \leq k_j$ y como $c|b$, $l_j \leq h_j$ por lo que $l_j \leq min\,(k_j, h_j) \Rightarrow c|d \therefore d = MCD(a, b)$.

2.2.9. Minimo comun multiplo

2.2.9.1. Definicion

Dados $a, b \in \mathbb{Z} - \{0\}$, un numero $n \in \mathbb{N}$ se dice minimo comun multiplo de a y b si:

1. $a|m \wedge b|m$
2. $a|n \wedge b|n \Rightarrow m|n$

Al igual que el MCD el mcm debe ser unico.

2.2.9.2. Teorema

Enunciado Sean $a, b \in \mathbb{Z} - \{0\}$:

1. $mcm\,(a,b) = \frac{|ab|}{MCD(a,b)}$
2. Si $a = \epsilon\prod_{j=1}^{r} p_j^{k_j}$ y $b = \epsilon''\prod_{j=1}^{r} p_j^{h_j}$ con $\epsilon, \epsilon'' = \pm 1, p_j$ primos positivos y $k_j, h_j \geq 0$ entonces: $mcm\,(a,b) = \prod_{j=1}^{r} p_j^{max(k_j,h_j)}$

2.2.9.3. Demostracion

1. Como $mcm(a,b) = mcm(|a|,|b|)$ podemos suponer $a > 0 \wedge b > 0$.
   $MCD(a,b)|a \wedge MCD(a,b)|b \Rightarrow \frac{a}{MCD(a,b)}, \frac{b}{MCD(a,b)} \in \mathbb{N}$.
   Luego $\frac{ab}{MCD(a,b)} = \underbrace{a\frac{b}{MCD(a,b)}}_{\Rightarrow a\left|\frac{ab}{MCD(a,b)}\right.} = \underbrace{b\frac{a}{MCD(a,b)}}_{\Rightarrow b\left|\frac{ab}{MCD(a,b)}\right.}$.
   Por otro lado si $a|n \wedge b|n \Rightarrow \exists x, y \in \mathbb{Z}/n = xa = yb \Rightarrow x\frac{a}{MCD(a,b)} = y\frac{b}{MCD(a,b)}$.
   Como $\frac{a}{MCD(a,b)}$ y $\frac{b}{MCD(a,b)}$ son coprimos y $\frac{a}{MCD(a,b)}\left|\frac{b}{MCD(a,b)}\right.$ entonces $\frac{a}{MCD(a,b)}\left|y \Rightarrow y = \frac{a}{MCD(a,b)}z\right.$ con $z \in \mathbb{Z}$.
   Finalmente $n = yb = \frac{ab}{MCD(a,b)}z \Rightarrow \frac{ab}{MCD(a,b)}\,|n \therefore \frac{ab}{MCD(a,b)} = mcm(a,b)$.
2. $mcm(a,b) = \frac{|ab|}{MCD(a,b)} = \frac{\prod_{j=1}^{r} p_j^{k_j+h_j}}{\prod_{j=1}^{r} p_j^{min(k_j,h_k)}} = \prod_{j=1}^{r} p_j^{k_j+h_j-min(k_j,h_j)} = \prod_{j=1}^{r} p_j^{max(k_j,h_j)}$.

Parte II

Geometria lineal en el espacio

Capítulo 3

Vectores

Capítulo 4

Plano

Capítulo 5

Recta

Parte III

Analisis combinatorio

Capítulo 6

Cardinalidad

6.1. Funciones

6.1.1. Definiciones

6.1.1.1. Funcion inyectiva

Sean X, Y conjuntos y $f : X \to Y$ una funcion, decimos que f es inyectiva si

$$x \neq y \Rightarrow f(x) \neq f(y)$$

o en forma equivalente

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

6.1.1.2. Funcion sobreyectiva

Sean X, Y conjuntos y $f : X \to Y$ una funcion, decimos que f es sobreyectiva o suryectiva si

$$\forall y \in Y \exists x \in X / f(x) = y$$

6.1.1.3. Funcion biyectiva

Decimos que una funcion es biyectiva si es inyectiva y suryectiva.

6.1.1.4. Composicion

Si $f : X \to Y$, $g : Y \to Z$, la composicion $g \circ f : X \to Z$ se define como

$$(g \circ f)(x) = g(f(x))$$

6.1.1.5. Funcion caracteristica

Sea A un conjunto y $B \subseteq A$,definimos $\chi B : A \to \{0, 1\}$ tal que $\chi B(i) = \begin{cases} 0, & i \notin B \\ 1, & i \in B \end{cases}$

6.1.1.6. Notacion

- Denotamos con $\mathcal{F}(A, B)$ al conjunto de *todas* las funciones de A en B.
- Denotamos con $\mathcal{F}_i(A, B)$ al conjunto de todas las funciones *inyectivas* de A en B.
- Denotamos con $\mathcal{F}_b(A, B)$ al conjunto de todas las funciones *biyectivas* de A en B.
- $[\![m, n]\!] = \{m, m + 1, \ldots, n\} = \{k \in \mathbb{N} : m \leq k \leq n\}$.

6.1.2. Propiedades

- Si f, g son inyectivas/suryectivas entonces $g \circ f$ es inyectiva/suryectiva.
- Si $g \circ f$ es inyectiva/suryectiva entonces f/g es suryectiva.

6.1.3. Principio de las casillas

6.1.3.1. Teorema

Enunciado Si $m, n \in \mathbb{N}/n > m$, entonces no existe ninguna funcion inyectiva $f : [\![1, n]\!] \to [\![1, m]\!]$.

Demostracion Sea $H = \{n \in \mathbb{N} / \exists m < n, f : [\![1,n]\!] \to [\![1,m]\!] \, inyectiva\}$. Debemos ver que $H = \emptyset$. Supongamos lo contrario.

- Sea $h \in H$ el primer elemento de H (principio del buen orden).
- Por definicion de H sabemos que $\exists m < h$ y $f : [\![1,h]\!] \to [\![1,m]\!]$ inyectiva.
- Definimos:
  - $c = f(h)$
  - $g : [\![1,m]\!] \to [\![1,m]\!]$
    $$g(i) = \begin{cases} i, & i \neq c, m \\ m, & i = c \\ c, & i = m \end{cases}$$
- $g \circ g = id_{[\![1,m]\!]}$, luego g es biyectiva.
- $i \in [\![1,h-1]\!] \Rightarrow g[f(i)] \in [\![1,m-1]\!]$.
- Sea $\widetilde{f} : [\![1,h-1]\!] \to [\![1,m-1]\!]$ tal que $\widetilde{f}(i) = g[f(i)]$
- $\widetilde{f}$ es inyectiva, pues $g \circ f$ lo es (6.1.2).
- Luego $m - 1 < h - 1 \in H$. ¡Contradiccion!

6.1.3.2. Corolarios

- Si $n \neq m \Rightarrow \nexists f : [\![1,n]\!] \to [\![1,m]\!]$ biyectiva.
- $f : [\![1,n]\!] \to [\![1,n]\!]$ es inyectiva $\iff$ es sobreyectiva $\iff$ es biyectiva.

6.2. Cardinalidad

6.2.1. Definicion

Un conjunto X tiene cardinalidad $n \in \mathbb{N}$ si existe una funcion biyectiva $f : [\![1,n]\!] \to X$ y se denota $|X| = n$. Para $X = \emptyset$ definimos $|X| = 0$. Estos conjuntos se llaman *conjuntos finitos*.

6.2.2. Principio de la suma

Si A, B son dos conjuntos finitos *disjuntos* entonces: $|A \cup B| = |A| + |B|$.

6.2.2.1. Demostracion

Sean A, B tales que $|A| = n, |B| = m$, sabemos entonces que existen $f : [\![1, n]\!] \to A$ y $g : [\![1, m]\!] \to B$ biyectivas.

Sea $X = A \cup B$. Queremos ver que $|X| = |A| + |B| = n + m$, es decir: existe una funcion biyectiva que parte de $[\![1, n + m]\!]$ y llega a X.

- Definimos $h(x) = \begin{cases} f(x), & x \in [\![1, n]\!] \\ g(x - n), & x \in [\![n + 1, n + m]\!] \end{cases}$
- Como f, g son biyectivas, h es biyectiva.
- Es facil ver que $Dom(h) = [\![1, n + m]\!]$ y $Im(h) = A \cup B = X$.

6.2.2.2. Corolario

Si $A_1, A_2, \ldots, A_n$ son conjuntos disjuntos entonces $|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i|$.

6.2.3. Principio del producto

Si A, B son dos conjuntos finitos *disjuntos* entonces: $|A \times B| = |A||B|$.

6.2.3.1. Demostracion

Sean $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$ entonces $|A| = n$ y $|B| = m$. Fijamos m y hacemos induccion en n.

1. $n = 1 \Rightarrow A \times B = \{(a_1, b_1), \ldots, (a_1, b_m)\}$.
2. La funcion $f : [\![1, m]\!] \to A \times B$ tal que $f(i) = (a_1, b_i)$ es biyectiva, luego $|A \times B| = m.1$
3. Supongamos que cierto para n y sea $A = \{a_1, \ldots, a_n, a_{n+1}\}$
4. $A \times B = [(A - \{a_{n+1}\}) \times B] \cup [\{a_{n+1}\} \times B]$ (disjunta).
5. Por hipotesis inductiva y el principio de la suma: $|A \times B| = nm + m = (n + 1)\, m$.

6.2.3.2. Corolario

Si $A_1, A_2, \ldots, A_n$ son conjuntos disjuntos entonces $|A_1 \times A_2 \times \ldots \times A_n| = \prod_{i=1}^{n} |A_i|$.

6.2.4. Conjuntos de funciones

6.2.4.1. Funciones de A en B

Enunciado Sean A, B dos conjuntos tales que $|A| = n, |B| = m$ entonces $|\mathcal{F}(A, B)| = m^n$.

Demostracion Sea $A = \{a_1, a_2, \ldots, a_n\}$. Toda $f : A \to B$ se identifica con $(f(a_1), f(a_1), \ldots, f(a_n)) \in \underbrace{B \times B \times \ldots \times B}_{n}$.

Luego $|\mathcal{F}(A, B)| = |B \times B \times \ldots \times B| = m^n$.

6.2.4.2. Funciones inyectivas de A en B

Enunciado Si $|A| = n, |B| = m$ y $n \leq m$ entonces $|\mathcal{F}_i(A, B)| = \frac{m!}{(m-n)!}$

Demostracion Ya vimos que si $n > m$ entonces $\mathcal{F}_i(A, B) = 0$ por el principio de las casillas.

Sea $A = \{a_1, a_2, \ldots, a_n\}$. Toda $f : A \to B$ se identifica con $(f(a_1), f(a_1), \ldots, f(a_n))$.
Si $f \in \mathcal{F}_i(A, B)$ entonces:

- $f(a_1)$ tiene m valores posibles,
- $f(a_2)$ tiene $m - 1$ valores posibles, pues $f(a_2) \neq f(a_1)$,
- $f(a_3)$ tiene $m - 2$ valores posibles,
- $\vdots$
- $f(a_n)$ tiene $m - (n - 1)$ valores posibles.

Por lo tanto $|\mathcal{F}_i(A, B)| = m(m-1)(m-2)\ldots[m-(n-1)] = \frac{m!}{(m-n)!}$

6.2.4.3. Funciones biyectivas de A en B

Enunciado Si $|A| = |B| = n$ entonces $|\mathcal{F}_b(A, B)| = m!$.

Demostracion Por el apartado anterior $|\mathcal{F}_i(A, B)| = \frac{m!}{(m-m)!} = m! = |\mathcal{F}_b(A, B)|$

6.2.4.4. Proposicion

Enunciado Sea A un conjunto tal que $|A| = n$, entonces $|\mathcal{P}(A)| = 2^n$.

Demostracion Sea $B = \{0, 1\}$, entonces $|B| = 2$. Todo conjunto $H \subseteq A$ se identifica con $\chi H : A \to B$. Luego $|\mathcal{P}(A)| = |\mathcal{F}(A, B)|$ y por 6.2.4.1 $|\mathcal{P}(A)| = 2^n$.

6.2.4.5. Ejemplos

- ¿Cuantas banderas se pueden hacer con tres bandas verticales de colores rojo, blanco, azul y verde, si se permiten dos o mas franjas del mismo color?
  Sean $A = \{1, 2, 3\}$ y $B = \{R, B, A, V\}$ entonces $|A| = 3$ y $|B| = 4$. Luego $|\mathcal{F}(A, B)| = 4^3 = 64$.

- ¿Cuantas pueden formarse si no se permiten franjas del mismo color? $|\mathcal{F}_b(A, B)| = 4! = 24$.

- Si en un colectivo hay 10 asientos vacios, ¿de cuantas maneras distintas pueden sentarse 7 personas?
  Sean $A = [\![1, 7]\!]$ y $B = [\![1, 10]\!]$ entonces $|A| = 7$ y $|B| = 10$. Luego $|\mathcal{F}_i(A, B)| = \frac{10!}{(10-4)!} = 640800$.

Capítulo 7

Arreglos, permutaciones y combinaciones

7.1. Arreglos

7.1.1. Arreglos

Si $|A| = m \geq n$, un *arreglo* o *seleccion ordenada* de n elementos del conjunto A es una funcion inyectiva $f : [\![1, n]\!] \to A$. Es comun representar un arreglo con una n-upla $(a_1, \ldots, a_n)$ en donde $a_i \in A$ son todos distintos.

La cantidad de arreglos de m elementos tomados de a n es entonces:

$$|A(n, m)| = \frac{m!}{(m-n)!}$$

7.1.1.1. Ejemplos

Si $A = \{a, b, c, d\}$ entonces:

1. (a, b, c)
2. (a, c, b)
3. (a, b, d)
4. (a, d, b)
5. (b, c, a)

6. (b, a, c)
7. (b, c, d)
8. (b, d, c)

son algunos de los arreglos de A tomados de a 3 elementos.

7.1.1.2. Aplicaciones

- En un grupo de 10 estudiantes, se escogera a cinco y se les sentara en fila para una foto. ¿Cuantas disposiciones lineales son posibles?
  $A(5, 10) = \frac{10!}{(10-5)!} = 30240$

7.1.2. Arreglos con repeticion

Si se pueden volver a elegir los elementos ya seleccionados entonces tenemos arreglos con repeticion. La cantidad de arreglos con repeticion de m elementos tomados de a n es: $|AR(n, m)| = m^n$.

7.1.2.1. Ejemplos

Si $A' = \{\alpha, \beta, \gamma\}$ entonces:

1. (α, β)
2. (α, γ)
3. (β, α)
4. (γ, α)
5. (β, γ)
6. (γ, β)
7. (α, α)
8. (β, β)
9. (γ, γ)

son todos los arreglos de A' elementos tomados de a 2.

7.1.2.2. Aplicaciones

- ¿Cuantos numeros de tres cifras se pueden formar con los digitos $1, 2, 3, 4, 5$?
  $AR(3, 5) = 5^3 = 125$

7.2. Permutaciones

7.2.1. Permutaciones

Si $|A| = m$, un arreglo de $n = m$ elementos del conjunto A se llama *permutacion*.

La cantidad de permutaciones de m elementos es entonces: $|A(n, m)| = \frac{m!}{(m-m)!} = m!$.

7.2.1.1. Ejemplos

Si $B = \{x, y, z\}$ entonces:

1. (x, y, z)
2. (x, z, y)
3. (y, x, z)
4. (y, z, x)
5. (z, x, y)
6. (z, y, x)

son todas sus permutaciones.

7.2.1.2. Aplicaciones

- ¿De cuantas formas distintas se puede ordenar una baraja de naipes españoles?
  $P(40) = 40!$

7.2.2. Permutaciones con repeticion

Cuando el conjunto posee elementos indistinguibles, tenemos permutaciones con repeticion. La cantidad de permutaciones con repeticion es: $\frac{m!}{m_1!,m_2!...m_r!}$ donde $m_1, m_2, \ldots, m_r$ son la cantidad de elementos repetidos de cada tipo.

Ejemplos Si $B' = \{\triangle, \square, \blacksquare\}$ y suponiendo que no podemos diferenciar $\square$ de $\blacksquare$:

1. $(\triangle, \square, \blacksquare) \approx (\triangle, \blacksquare, \square)$
2. $(\square, \blacksquare, \triangle) \approx (\blacksquare, \square, \triangle)$
3. $(\square, \triangle, \blacksquare) \approx (\blacksquare, \triangle, \square)$

son todas sus permutaciones con repeticion.

Aplicaciones

- ¿Cuantos numeros distintos pueden armarse usando *todos* los dgitos 1112233345?
  $PR(3, 2, 3, 10) = \frac{10!}{3!2!3!} = 50400$

7.2.3. Permutaciones circulares

Las permutaciones circulares son un caso particular de las permutaciones con repeticion, donde las repeticiones son distintas rotaciones de la misma configuracion. La cantidad de permutaciones circualres es $\frac{m!}{m}$.

7.2.3.1. Aplicaciones

- ¿De cuantas formas distintas pueden sentarse 8 personas alrededor de una mesa circular?
  $PC(m) = \frac{8!}{8} = 5040$

7.3. Combinaciones

7.3.1. Combinaciones

Si $|A| = m \geq n$ y seleccionamos n objetos entre m sin tener en cuenta el orden, obtenemos una combinacion de n elementos tomados de un conjunto con m elementos.

La cantidad de combinaciones de m elementos tomados de a n es:

$$|C(n, m)| = \frac{|A(n, m)|}{|P(n)|} = \frac{m!}{n!\,(m-n)!} = \binom{m}{n}$$

7.3.1.1. Ejemplos

Si $C = \{1, 2, 3, 4, 5\}$ entonces:

1. $\{1, 2, 3\}$
2. $\{1, 2, 4\}$
3. $\{1, 2, 5\}$
4. $\{1, 3, 4\}$
5. $\{1, 3, 5\}$
6. $\{1, 4, 5\}$
7. $\{2, 3, 4\}$
8. $\{2, 3, 5\}$
9. $\{2, 4, 5\}$
10. $\{3, 4, 5\}$

son todas sus combinaciones de 3 elementos.

7.3.1.2. Aplicaciones

- ¿Cuantos comites distintos de 3 personas pueden armarse con un grupo de 9 personas?
  $C(3, 9) = \binom{9}{3} = \frac{10!}{3!(9-3)!} = 84$

7.3.2. Combinaciones con repeticion

Si podemos extraer varias veces el mismo elemento del conjunto, entonces tenemos combinaciones con repeticion. La cantidad de combinaciones con repeticion es $CR(n, m) = \binom{m+n-1}{n} = \frac{(m+n-1)!}{n!(m-1)!}$

7.3.2.1. Aplicaciones

- En una bodega hay en un cinco tipos diferentes de botellas. ¿De cuantas formas se pueden elegir cuatro botellas?
  $CR(4, 5) = \frac{8!}{4!4!} = 70$

7.4. Probabilidad

7.4.1. Definicion

Se define la probabilidad de un evento como $\frac{\text{casos favorables}}{\text{casos posibles}}$.

7.4.2. Ejemplos

- En el juego del truco: ¿Cual es la probabilidad de tener 33 para el envido?
  Manos posibles: $\binom{40}{3}$, Manos con el 6 y 7 de espadas: 38.
  Probabilidad: $\frac{4.38}{\binom{40}{3}} = \frac{152}{9880} \approx 0.015$ $(1,5\,\%)$

7.5. Numeros combinatorios

7.5.1. Teoremas

1. $\binom{m}{1} = m$
2. $\binom{m}{n} = \binom{m}{m-n}$
3. $\binom{m}{n-1} + \binom{m}{n} = \binom{m+1}{n}$ (triangulo de Pascal)
4. $\displaystyle\sum_{n=0}^{m} \binom{m}{n} = 2^m$
5. $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ $\forall a, b \in \mathbb{R}$ (teorema del binomio)
6. $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$
7. $(1+x)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} x^k$

7.5.2. Demostraciones

1. $\binom{m}{1} = \frac{m!}{1!(m-1)!} = \frac{m(m-1)!}{(m-1)!} = m$
2. $\binom{m}{n} = \frac{m!}{n!(m-n!)} = \frac{m!}{(n+m-m)!(m-n)!} = \frac{m!}{(m-n)!(m+n-m)!} = \frac{m!}{(m-n)![m-(m-n)]!} = \binom{m}{m-n}$
3. COMPLETAR.
4. COMPLETAR.
5. Haremos una prueba por induccion:

   a) Para $n = 1$: $\sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k} = \binom{1}{0} 1b^1 + \binom{1}{1} a^1 b^0 = b + a = (a+b)^1$

   b) Supongamos que vale para n y veamos que pasa para $n+1$:
   $(a+b)^{n+1} = (a+b)^n + (a+b) = (a+b)^n a + (a+b)^n b =$
   $= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}$
   Observemos que podemos escribir el primer termino de esta forma cambiando el indice:
   $\sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k}$.

   Retomando lo anterior: $(a+b)^{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} =$

   $= \underbrace{\binom{n}{0}}_{1} b^{n+1} + \sum_{k=1}^{n} \left[\underbrace{\binom{n}{k-1} + \binom{n}{k}}_{\text{triangulo de pascal}} \right] a^k b^{n+1-k} + \underbrace{\binom{n}{n}}_{1} a^{n+1} =$

   $= \binom{n+1}{0} b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + \binom{n+1}{n+1} a^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$

- $0 = 0^n = (-1+1)^n = \sum_{k}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k}^{n} (-1)^k \binom{n}{k}$

Parte IV

Matrices y determinantes

Parte V

Sistemas de ecuaciones lineales

Capítulo 8

Sistemas de ecuaciones

8.1. Definiciones

8.1.1. Ecuacion lineal

Una ecuacion con n variables $x_1, \ldots, x_n$ es lineal si puede escribirse en la forma: $a_1x_1 + a_2x_2 + \ldots + a_nx_n = y$.

Los a_i son los coeficientes, y y es el termino constante de la ecuacion. Si $b = 0$, la ecuacion se denomina homogenea.

Si se ordenan las variables, la primera variable cuyo coeficiente es distinto de cero se llama variable delantera, las demas son variables libres.

8.1.2. Sistema de ecuaciones lineales

Un sistema de m ecuaciones con n variables (o incognitas) $x_1, \ldots, x_n$ es un conjunto de m escuaciones lineales de la forma:

$$S) \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = y_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = y_2 \\ & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n & = y_m \end{cases} \tag{8.1}$$

Dado el sistema (1), si para cada $i = 1, \ldots, m$ llamamos L_i al primer miembro de su i-esima ecuacion: $L_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n$, entonces

podemos escribir S) mas brevemente asi:

$$S) \begin{cases} L_1 = & y_1 \\ L_2 = & y_2 \\ \vdots & \vdots \\ L_m = & y_m \end{cases}$$

8.1.3. Solucion de un sistema lineal

Una solucion $r_1, r_2, \ldots, r_n$ de escalares es una solucion (particular) de un sistema si todas las ecuaciones se satisfacen al sustituir $x_1 = r_1, \ldots, x_n = r_n$. El conjunto de todas las soluciones posibles es el conjunto solucion.

8.1.4. Sistemas equivalentes

Dos sistemas $(S1)$ y $(S2)$ se dicen equivalentes si tienen las mismas soluciones. O sea, toda solucion de $(S1)$ es solucion de $(S2)$ y viceversa.

8.2. Operaciones elementales en ecuaciones

8.2.1. Operaciones de eliminacion

Pasamos de un sistema (S) a un sistema (S') sumando la i-esima ecuacion α ves la k-esima ecuacion (con $k \neq i$).

Si la i-esima y la k-esima ecuacion de (S) son

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = y_i$$
$$a_{k1}x_1 + a_{k2}x_2 + \ldots + a_{kn}x_n = y_k$$

entonces la i-esima ecuacion de (S') es

$$(A_{i1} + \alpha A_{k1})x_1 + (A_{i2} + \alpha A_{k2})x_2 + \ldots + (A_{in} + \alpha A_{kn})x_n = y_i + \alpha y_k$$

8.2.2. Operaciones de escalamiento

Se pasa de un sistema (S) a un sistema (S') multiplicando la i-esima ecuacion por un escalar $\alpha \neq 0$. Si la i-esima ecuacion de (S) es

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = y_i$$

la i-esima ecuacion de (S') es

$$\alpha a_{i1}x_1 + \alpha a_{i2}x_2 + \ldots + \alpha a_{in}x_n = \alpha y_i$$

8.2.3. Operaciones de intercambio

Pasamos de un sistema (S) a un sistema (S') intercambiando dos ecuaciones.

8.2.4. Teorema fundamental de equivalencia de sistemas

Enunciado Dado un sistema de ecuaciones lineales, al realizar cualquier operacion elemental entre sus ecuaciones, obtenemos un sistema equivalente.

Demostracion

1. Lo afirmado es obvio si la operacion elemental es de intercambio.
2. Consideremos ahora una operacion elemental de escalamiento . Sea $S)$ el sistema de partida y sea $S')$ el obtenido de reemplazar la i-esima ecuacion de $S)$ por un multiplo $c \neq 0$ de ella:

$$S) \begin{cases} L_1 = & y_1 \\ \vdots & \vdots \\ L_i = & y_i \\ \vdots & \vdots \\ L_m = & y_m \end{cases} \rightarrow S') \begin{cases} L_1 = & y_1 \\ \vdots & \vdots \\ cL_i = & cy_i \\ \vdots & \vdots \\ L_m = & y_m \end{cases}$$

   a) Toda solucion de $S)$ lo es de $S')$: Sea $x = (x_1, \ldots, x_n)$ una solucion (particular) de $S)$, para ver que x es solucion de $S')$ solo hay que controlar que x verifica la i-esima ecuacion de $S')$ pues las restantes son las mismas.
   Como $a_{i1}x_1 + \ldots + a_{in}x_n = y_i$ (por verificar x_i la ecuacion $L_i = y_i$) multiplicando ambos miembros por c resulta $(ca_{i1})\, x_1 + \ldots + (ca_{in})\, x_n = cy_i$ y por lo tanto x verifica la ecuacion $cL_i = cy_i$.

   b) Toda solucion de $S')$ lo es de $S)$: Analogo multiplicando por $1/c$.

3. Consideremos por ultimo una operacion elemental de eliminacion. Sea S) el sistema de partida y sea S') el obtenido de reemplazar la i-esima ecuacion de S) por la suma de ella mas la j-esima ecuacion de S) multiplicada por una constante $c \in \mathbb{R}$:

$$S) \begin{cases} L_1 = & y_1 \\ \vdots & \vdots \\ L_i = & y_i \\ \vdots & \vdots \\ L_j = & y_j \\ \vdots & \vdots \\ L_m = & y_m \end{cases} \rightarrow S') \begin{cases} L_1 = & y_1 \\ \vdots & \vdots \\ L_i + cL_j = & y_i + cy_j \\ \vdots & \vdots \\ L_j = & y_j \\ \vdots & \vdots \\ L_m = & y_m \end{cases}$$

   a) Toda solucion de S) lo es de S'): Sea x una solucion de S), como $a_{i1}x_1 + \ldots + a_{in}x_n = y_i$ y $a_{j1}x_1 + \ldots + a_{jn}x_n = y_i$ (por verificar x las ecuaciones $L_i = y_i$ y $L_j = y_j$) y sumando miembro a miembro ambas igualdades resulta: $(a_{i1} + ca_{j1})x_1 + \ldots + (a_{in} + ca_{jn})x_n = y_i + cy_j$, es decir x verifica la ecuacion $L_i + cL_j = y_i + cy_j$, que es la i-esima ecuacion de S')

   b) Toda solucion de S') lo es de S):

Capítulo 9

Representacion matricial

9.1. Notacion matricial de un sistema lineal

9.1.1. Definiciones

Sea $S)$ un sistema de m escuaciones lineales con n variables

$$S) \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = y_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = y_2 \\ & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n & = y_m \end{cases}$$

llamaremos:

- Matriz de los coeficientes a la matriz A, de tamnno $m \times n$, constituida por los coeficientes de las variables de $S)$
- Vector de las variables al vector columna X , de tamano n , formado por las incognitas
- Vector de las constantes al vector columna Y , de tamano m , con los terminos constantes del sistema.

$$A = \begin{pmatrix} a_{12} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

9.1.1.1. Matriz ampliada

Llamaremos matriz ampliada a la matriz $A'\,(A|Y)$, de tamaño $m\times(n+1)$, que se obtiene de aregarle a la matriz A la columna Y:

$$A' = \left(\begin{array}{cccc|c} a_{12} & a_{12} & \dots & a_{1n} & y_1 \\ a_{21} & a_{22} & \dots & a_{2n} & y_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & y_m \end{array}\right)$$

Podemos expresar un sistema en forma matricial $AX = Y$ como se puede comprobar efectuando el producto de las matrices del primer miembro y aplicando luego la de nicion de igualdad de matrices.

9.1.1.2. Sistema homogeneo

Un sistema se dice homogeneo si $y_1 = y_2 = \cdots = y_m = 0$. Un sistema homogeneo siempre admite la solucion trivial $x_1 = x_2 = \cdots = x_m = 0$ aunque podra tener soluciones no triviales.

9.1.1.3. Sistemas equivalentes

Dos sistemas $S1) AX = Y$ y $S2) A'X = Y'$ con $A, A' \in \mathbb{F}^{m\times n}$ y $Y, Y' \in \mathbb{F}^{m\times 1}$ se dicen equivalentes si tienen las mismas soluciones. O sea, toda solucion de $S1)$ es solucion de $S2)$ y viceversa.

9.1.1.4. Teorema

Enunciado Dado el sistema $S) AX = Y$ con $A \in \mathbb{F}^{m\times n}, Y \in \mathbb{F}^{m\times 1}$ y sea X_0 tal que $AX_0 = Y$, entonces el conjunto solucion de $S)$ es:

$$Sol = \{X_0 + X_h : X_h \text{ es solucion de } AX = 0\}$$

o en otras palabras toda solucion de $S)$ se escribe como una solucion particular mas una solucion del sistema homogeneo.

Demostracion

- Si $AX_h = 0$ entonces $A(X_0 + X_h) = AX_0 + AX_h = AX_0 + 0$ y por hipotesis: $AX_0 = Y$.
- Reciprocamente si $AX = Y$, escribimos $X = X_0 + (-X_0 + X)$. Luego $A(-X_0 + X) = -AX_0 + AX = -Y + Y = 0$.

9.1.2. Operaciones elementales por filas

Sea Auna matriz con m filas, definimos tres tipos de OEF sobre A:

- Tipo I: Se multiplica la fila r por un escalar $\alpha \neq 0$.
- Tipo II: Se suma a la fila r, α veces la sila s. (con $r \neq s$)
- Tipo III: Se intercambia la fila r con la fila s.

Mas precisamente, una OEF e sobre A devuelve la matriz $e(A)$ dada por:

- Tipo I: $e(A)_{ij} = \begin{cases} A_{ij}, & i \neq r \\ \alpha A_{rj}, & i = r \end{cases}$
- Tipo II: $e(A)_{ij} = \begin{cases} A_{ij}, & i \neq r \\ A_{rj} + A_{sj}, & i = r \end{cases}$
- Tipo III: $e(A)_{ij} = \begin{cases} A_{ij}, & i \neq r, s \\ A_{sj}, & i = r \\ A_{rj}, & i = s \end{cases}$

9.1.2.1. Teorema fundamental de equivalencia de sistemas

Sean $A \in \mathbb{F}^{m \times n}, Y \in \mathbb{F}^{m \times 1}$, si e es una OEF entonces los sistemas $AX = Y$ y $e(A)X = e(Y)$ son equivalentes.

9.1.2.2. Equivalencia por filas

Sean $A, B \in \mathbb{F}^{m \times n}$, se dice que B es equivalente por filas a A si se puede pasar de A a B por una sucecion finita de OEF.

9.1.2.3. Corolario

Enunciado Si B es equivalente por filas a A, entonces los sistemas $AX = 0$ y $BX = 0$ son equivalentes.

Demostracion Por hipotesis existen OEF $e_1, e_2, \ldots, e_k$ tales que $B = e_k [\ldots e_2 (e_1 [A])]$.

1. Toda solucion de $AX = 0$ es solucion de $BX = 0$: En efecto,
   $AX = 0 \Rightarrow e_1 (A) X = 0 \Rightarrow e_2 [e_1 (A)] X = 0 \Rightarrow \ldots \Rightarrow e_k [\ldots e_2 (e_1 [A])] = BX = 0$
2. Toda solucion de $BX = 0$ es solucion de $AX = 0$: En efecto, B es equivalente por filas a $A \Rightarrow B$ es equivalente por filas a B. Luego el argumento anterior tambien sirve para demostrar esto.

9.1.2.4. Matrices elementales

Sea e una OEF que aplica sobre matrices con m filas, la matriz elemental asociada a e es $E = e(I)$ en donde I es la matriz identidad $m \times m$.

Observacion Las matrices elementales son invertibles.

9.1.2.5. Teorema

Enunciado Sea e una OEF y sea $E = e(I_m)$ su correspondiente matriz elemental. Entonces para toda $A \in \mathbb{F}^{m \times n}$ vale $e(A) = EA$.

Demostracion

- Tipo I: Sea $e = "f_r \to \alpha f_r"$ $(\alpha \neq 0)$,
  - $E = e(I) = \begin{cases} \delta_{ij}, & i \neq r \\ \alpha \delta_{rj}, & i = r \end{cases}$
  - $(EA)_{ij} = \sum_{k=1}^{m} E_{ik} A_{kj} = \begin{cases} \sum_{k=1}^{m} \delta_{ik} A_{kj} = A_{ij}, & i \neq r \\ \sum_{k=1}^{m} \alpha \delta_{rk} A_{kj} = \alpha A_{rj}, & i = r \end{cases}$

- Tipo II: Sea $e = "f_r \to f_r + \alpha f_s"$ $(r \neq s)$,
  - $E = e(I) = \begin{cases} \delta_{ij}, & i \neq r \\ \delta_{rj} + \alpha\delta_{sj}, & i = r \end{cases}$
  - $(EA)_{rj} = \sum_{k=1}^{m} E_{rk}A_{kj} = \sum_{k=1}^{m} (\delta_{rk} + \alpha\delta_{sk}) A_{kj} =$
    $= \sum_{k=1}^{m} \delta_{rk}A_{kj} + \alpha \sum_{k=1}^{m} \delta_{sk}A_{kj} = A_{rj} + \alpha A_{sj}$
  - $(EA)_{ij} = \begin{cases} A_{ij}, & i \neq r \\ A_{rj} + \alpha A_{sj}, & i = r \end{cases}$

9.1.2.6. Lemas

Lema I Sea $E \in \mathbb{F}^{n\times n}$ una matriz elemental asociada a una OEF e, entonces:

1. Si $e = "f_r \to \alpha f_r" \Rightarrow |E| = \alpha$ (con $\alpha \neq 0$).
2. Si $e = "f_r \to f_r + \alpha f_s" \Rightarrow |E| = 1$ (con $r \neq s$).
3. Si $e = "f_r \leftrightarrow f_s" \Rightarrow |E| = -1$ (con $r \neq s$).

Demostracion Sigue de las propiedades del determinante, pues $E = e(I)$.

Lema II Sea E una matriz elemental, entonces para toda $A \in \mathbb{F}^{n\times n}$ vale $|EA| = |E|\,|A|$.

Demostracion Por hipotesis $E = e(I)$ para alguna OEF e. Tenemos que analizar tres casos de acuerdo a si e es Tipo I, II o III:

- Tipo I: Si $e = "f_r \to \alpha f_r"$ (con $\alpha \neq 0$),
  - Como $EA = e(A)$ (por 9.1.2.5), $|EA| = |e(A)| = \alpha\,|A|$.
  - Luego por el lema previo, $\alpha\,|A| = |E|\,|A|$.
  - Por transitividad de la igualdad, $|EA| = |E|\,|A|$.
- Tipo II: COMPLETAR.
- Tipo III: COMPLETAR.

9.1.3. Reduccion de matrices

9.1.3.1. Matriz reducida por filas

Definicion Una matriz reducida por filas es una matriz que cumple las siguiente propiedades:

1. El primer elemento no nulo de cada fila es 1. Llamamos a este elemento «*pivote*».
2. Si una columna contiene un pivote, el resto de sus elementos son 0. Llamamos a esta columna, «columna pivote».

Ejemplos Sean

$$A = \begin{pmatrix} 1 & 0 & \mathbf{0} & 0 \\ 0 & 1 & \mathbf{-1} & 0 \\ 0 & 0 & \mathbf{1} & 0 \end{pmatrix} B = \begin{pmatrix} \mathbf{0} & \mathbf{2} & \mathbf{1} \\ 1 & 0 & -3 \\ 0 & 0 & 0 \end{pmatrix} C = \begin{pmatrix} 1 & 0 & \mathbf{-1} & 0 \\ 0 & 1 & \mathbf{2} & 0 \\ 0 & 0 & \mathbf{0} & 1 \end{pmatrix} D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- La matriz A no es RF pues la tercer columna pivote no tiene el resto de los elementos nulos.
- La matriz B no es RF pues la primer fila tiene un pivote distinto de 1.
- La matriz C es RF. Notese que la tercer columna no es columna pivote.
- La matriz D es RF.

9.1.3.2. Matriz escalonada reducida por filas

Definicion Una matriz se dice escalonada reducida por filas si cumple las siguiente propiedades:

1. Es reducida por filas.
2. Las filas nulas estan debajo de las no nulas.
3. El pivote de cada fila, se encuentra a la derecha del pivote de la fila anterior.

9.1.3.3. Existencia de matrices ERF

Enunciado Toda matriz $A \in \mathbb{F}^{m\times n}$ es equivalente por las a una matriz ERF. En otras palabras, existes matrices elementales $E_1, E_2, \ldots, E_k$ tales que $E_k E_{k-1} \cdots E_2 E_1 A$ es ERF. Esta matriz es ademas unica.

9.1.3.4. Teorema

Enunciado Si $A \in \mathbb{F}^{m\times n}$ con $m < n$ entonces el sistema homogeneo $AX = 0$ admite una solucion no trivial. En otras palabras, un sistema homogeneo con mas incognitas que ecuaciones tiene una solucion no trivial.

Demostracion COMPLETAR.

9.1.4. Clasificacion de sistemas

Los sistemas de ecuaciones se pueden clasificar segun el numero de soluciones que pueden presentar. De acuerdo con ese caso se pueden presentar los siguientes casos:

- *Sistema compatible* si tiene solución, en este caso además puede distinguirse entre:
  - Sistema compatible *determinado* cuando tiene una única solucion.
  - Sistema compatible *indeterminado* cuando admite mas de una solucion.
- Sistema incompatible si no tiene solucion.

9.1.4.1. Rango de una matriz

Dada una matriz A de tamano $m \times n$ llamaremos rango de A, y lo simbolizaremos $rg(A)$, al numero de columnas pivote de la forma ERF (o equivalentemente: al numero de filas no nulas).

9.1.4.2. Teorema Rouche-Frobenius

- Un sistema es incompatible si y solo si $rg\,(A') > rg\,(A)$.
- Un sistema es determinado si y solo si $rg\,(A') = rg\,(A) = n$
- Un sistema es indeterminado si y solo si $rg\,(A') = rg\,(A) < n$

9.2. Sistemas cuadrados

9.2.1. Teorema

Enunciado Sea $A \in \mathbb{F}^{n\times n}$, la siguientes formulaciones son equivalentes:

1. A es invertible ($|A| \neq 0$).
2. El sistema $AX = 0$ tiene solucion unica.
3. El sistema $AX = Y$ tiene solucion unica para cada $Y \in \mathbb{F}^{n\times 1}$.

Demostracion

- $1 \Rightarrow 2$: Como A es invertible, en $AX = 0$ multiplicando a izquierda por A^{-1} tenemos, $X = 0$.
- $1 \Rightarrow 3$: Analogo.
- $3 \Rightarrow 2$: Trivial tomando $Y = 0$.
- $2 \Rightarrow 1$: Sea R la forma ERF de A, R es triangular superior.
  Por equivalencia de sistemas, si $AX = 0$ tiene solucion unica entonces $RX = 0$ tambien y por lo tanto $R = I$.
  Luego A es equivalente por filas a $R = I$ y en consecuencia existen matrices elementales $E_1, E_2, \ldots, E_k$ tales que $E_k \ldots E_2 E_1 A = I$.
  A partir de aqui: $E_k \ldots E_2 E_1 A A^{-1} = A^{-1} \iff E_k \ldots E_2 E_1 = A^{-1}$.

9.2.2. Matriz inversa

La demostracion del teorema anterior nos da un metodo eficiente para calcular la inversa de una matriz A:

- Si A es invertible, por el teorema anterior, A es equivalente por filas a I.
- Si $e_1, e_2, \ldots, e_k$ son las OEF que aplicamos a A para llevarla a I, entonces: $A^{-1} = E_k \ldots E_2 E_1 = e_k \left[\ldots e_2 \left(e_1 \left[I \right] \right) \right]$.

En palabras: si aplicamos a la matriz identidad las mismas OEF que le aplicamos a A para llegar a I, lo que se obtiene es la matriz inversa A^{-1}.

9.2.3. Determinante del producto de matrices

Enunciado Dadas $A, B \in \mathbb{F}^{n \times n}$,se tiene que: $|AB| = |A|\,|B|$.

Demostracion

- Primer caso: $|A| = 0$,
  - Si $|B| = 0$, por 9.2.1, $\exists X \neq 0 / BX = 0$ y multiplicando miembro a miembro por A: $ABX = 0$ (con $X \neq 0$) por lo que $|AB| = 0 = |A||B|$
  - Si $|B| \neq 0$, B es invertible y ademas por 9.2.1, $\exists X \neq 0 / AX = 0$ y multiplicando al centro por I: $AB\left(B^{-1}X\right) = 0$. Como $X \neq 0 \wedge B^{-1} \neq 0$ entonces $\left(B^{-1}X\right) \neq 0$ y por lo tanto $|AB| = 0 = |A||B|$.
- Segundo caso: $|A| \neq 0$,
  - Por 9.2.1, $AX = 0 \Rightarrow X = 0$.
  - A es equivalente por filas a I luego existen matrices elementales $E_1, E_2, \ldots, E_k$ tales que $E_k \ldots E_2 E_1 A = I$.
  - $A = E_1^{-1} E_2^{-1} \ldots E_k^{-1}$ y E_i^{-1} son matrices elementales.
  - Por el lema II en 9.1.2.6, $|A| = \left|E_1^{-1}\right| \left|E_2^{-1}\right| \ldots \left|E_k^{-1}\right|$.
  - Como $AB = E_1^{-1} E_2^{-1} \ldots E_k^{-1} B$, $|AB| = \left|E_1^{-1}\right| \left|E_2^{-1}\right| \ldots \left|E_k^{-1}\right| |B| = |A||B|$.

9.2.4. Algotirmo de Gauss

El siguiente es un algoritmo para llevar una matriz $A \in n \times n$ a su forma ERF:

1. Ir a la columna no cero extrema izquierda.
2. Si la primera fila tiene un cero en esta columna, intercambiarlo con otra que no lo tenga.
3. Luego, obtener ceros debajo de este elemento delantero, sumando múltiplos adecuados del renglon superior a los renglones debajo de el.
4. Cubrir el renglon superior y repetir el proceso anterior con la submatriz restante. Repetir con el resto de los renglones.
5. Comenzando con el ultimo renglón no cero, avanzar hacia arriba: para cada renglon obtener un 1 delantero e introducir ceros arriba de este sumando múltiplos correspondientes a los renglones correspondientes.

9.2.5. Regla de Cramer

Enunciado Sea $A \in \mathbb{F}^{n \times n}$ una matriz inversible, entonces la unica solucion del sistema $AX = Y$ esta dada por

$$x_i = \frac{|A_i|}{|A|}$$

donde A_i esla matriz que se obtiene de A reemplazando la i-esima columna por el vector Y.

Demostracion COMPLETAR.

Parte VI

Cuerpos finitos

Capítulo 10

Cuerpos

Capítulo 11

Aritmetica Modular

Capítulo 12

Ecuaciones lineales en cuerpos finitos