ÁLGEBRA I

PRIMER CUATRIMESTRE - AÑO 2016

COMPLEMENTO DEL TEÓRICO

El material de estas notas fue dictado en las clases teóricas pero no se encuentra en el texto que seguimos en las mismas ("Álgebra I - Matemática discreta I" de Miatello y Kisbye).

DIVISIBILIDAD

1. LOS NÚMEROS ENTEROS

Ejemplo 1. *Todo número entero divide a cero*

En efecto, $0 = 0x$ para todo $x \in \mathbb{Z}$ lo que demuestra la primera parte de la afirmación.

Lema 1 (Lema 1.4 (v))**.** *Sean a, b, $c \in \mathbb{Z}$ tales que $a|b$. Entonces $a|b \cdot c$.*

Demostración. Sea $x \in \mathbb{Z}$ tal que $b = xa$. Multiplicando a ambos lados de la igualdad por c obtenemos $bc = (xa)c = (xc)a$. Es decir, $a|b \cdot c$. □

Observación 1. *Sean a, b, $c \in \mathbb{Z}$ con $a \neq 0$. Si $ab = ac$, entonces $b = c$.*

Esta observación ya la hemos visto en el Capítulo referido a números reales. Se deduce multiplicando por el inverso de a, el cual no es un número entero salvo que a sea 1 ó -1.

Ejemplo 2. *Si $a|b$ y $b|a$, entonces $a = b$ ó $a = -b$.*

Demostración. Sean x e y enteros tales que: $b = xa$ y $a = yb$. Entonces

$$b = xa = x(yb) = (xy)b.$$

Luego, $xy = 1$ y por lo tanto $x = y = 1$ ó $x = y = -1$ por Proposición 1.2 (ii). Dado que $b = xa$ obtenemos que $a = b$ ó $a = -b$. □

Definición 1. *La función valor absoluto $|-| : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ es definida por*

$$|a| = \begin{cases} a, & \text{si } a \geq 0; \\ -a, & \text{si } a \leq 0. \end{cases}$$

Lema 2. *Si $b \neq 0$ y $a|b$, entonces $|a| \leq |b|$.*

Demostración. Sea $x \in \mathbb{Z}$ tal que $b = xa$. El valor absoluto respeta el producto, esto es: $|b| = |x||a|$. Como $|x| \geq 1$ el lema multiplicando a ambos lados por $|a|$ que es mayor o igual a 0. □

Ejemplo 3. *Si $m \leq n$, entonces m divide a $n!$*

En efecto, $n! = n(n-1)\cdots(m+1)\,m\,(m-1)! = m\big(n(n-1)\cdots(m+1)\,(m-1)!\big)$. □

El siguiente ejemplo da un criterio para decidir cuando un número es divisible por 9. Más adelante se verán más criterios como este.

Ejemplo 4. *Sean $0 \leq a, b, c \leq 9$ los dígitos de $x = abc \in \mathbb{N}$. Probar que 9 divide a $x-(a+b+c)$. En particular, $9|x$ si y sólo si $9|(a+b+c)$.*

Demostración. Podemos expresar a x de la siguiente forma $x = a \cdot 100 + b \cdot 10 + c$. Entonces

$$x - (a+b+c) = a \cdot 100 + b \cdot 10 + c - (a+b+c) = a \cdot 99 + b \cdot 9 = 9(a \cdot 11 + b).$$

Es decir, 9 divide a $x-(a+b+c)$.

La otra afirmación sigue de la propiedad: "si un entero divide a dos enteros entonces también divide a la suma y la resta de ambos". Pues, si 9 divide a x entonces divide a $a+b+c =$ □

2. Algoritmo de división

Corolario 1 (Teorema 2.1)**.** *Sean $a, b \in \mathbb{Z}$. Entonces existen enteros q y r tales que*

$$a = bq + r, \ \textit{con}\ 0 \leq r \leq |b|.$$

Además, q y r son únicos con esta propiedad, es decir, si

$$a = bq + r, \quad a = bq' + r', \ \textit{con}\ 0 \leq r, r' \leq |b|$$

entonces $q = q'$ y $r = r'$.

Demostración. Si $b > 0$ el corolario sigue del Teorema 2.1. Si $b < 0$, entonces $-b = |b| > 0$. Luego, existen únicos enteros $\tilde{q}$ y $\tilde{r}$ tales que

$$a = (-b)\tilde{q} + \tilde{r}, \ \text{con}\ 0 \leq \tilde{r} \leq |b|.$$

por el Teorema 2.1. Si decretamos $q = -\tilde{q}$ y $r = \tilde{r}$, entonces

$$a = bq + r, \ \text{con}\ 0 \leq r \leq |b|.$$

Probemos la unicidad. Supongamos que

$$a = bq' + r', \text{ con } 0 \leq r' \leq |b|.$$

Entonces

$$a = (-b)(-q') + r', \text{ con } 0 \leq r' \leq |b|.$$

Por la unicidad del Teorema 2.1 aplicado a la división de a por $-b$, deducimos que $r = r'$ y $-q' = \tilde{q}$. Por lo tanto $q' = q$ y el corolario queda demostrado. □

Ejemplo 5. *La ecuación* $2x^2 - 1 = 3y$ *no tiene soluciones enteras.*

Demostración. Basta ver que si x es un entero, entonces $n = 2x^2 - 1$ no es divisible por 3. Probaremos esto en tres casos diferentes, dependiendo del resto r de la división de x por 3.

Si $r = 0$, entonces $n = 2 \cdot 9q^2 - 1 = (6q^2) \cdot 3 - 1 = 3 \cdot (6q^2 - 1) + 2$. Es decir, n no es divisible por 3.

Si $r = 1$, entonces $n = 2 \cdot (9q^2 + 6q + 1) - 1 = 3 \cdot (3q^2 + 2q) + 1$. Es decir, n no es divisible por 3.

Si $r = 2$, entonces $n = 2 \cdot (9q^2 + 12q + 4) - 1 = 3 \cdot (3q^2 + 4q + 2) + 1$. Es decir, n no es divisible por 3. □

3. Desarrollo en base b

No hay material complementario.

4. Máximo común divisor

4.1. **El máximo común divisor existe.**

A continuación probaremos algunos resultados que ayudan a esclarecer la demostración del Teorema 4.3.

Fijemos $a, b \in \mathbb{Z}$. Recordar que el máximo común divisor del par $\{a, b\}$ es un $d \in \mathbb{N}$ que satisface:

(i) d divide a a y b.

(ii) Si $c \in \mathbb{Z}$ divide a a y b, entonces c divide a d.

Lema 3. $(a, b) = (a + tb, b)$ *para todo* $t \in \mathbb{Z}$.

Demostración. Veamos que $d = (a, b)$ satisface las propiedades del máximo común divisor para el par $\{a + tb, b\}$ y por lo tanto es su máximo común divisor.

(i) d divide a $a + tb$ porque d divide a a y b. Entonces d es un divisor común de $a + tb$ y b.

(ii) Sea c un divisor de $a+tb$ y b. Entonces c divide a $a = (a+tb)-(tb)$. Luego, c es un divisor común de a y b por lo tanto debe dividir al máximo común divisor de ambos, que es d. Es decir, $c|d$. □

Corolario 2. *Sean q y r el cociente y el resto de la división de a por b, es decir $a = qb + r$ con $0 \leq r < |b|$. Entonces $(a, b) = (b, r)$.*

Demostración. Usar $t = -q$ en el lema anterior. □

Supongamos $b > 0$. La sucesión (finita) de números enteros $\{r_i\}_{1 \leq i \leq n-1}$ definida en la demostración del Teorema 4.3 es una sucesión del tipo recursiva. Puede ser definida como sigue:

$$\begin{aligned} r_0 &= a, \\ r_1 &= b, \\ r_{i-1} &= q_{i+1}r_i + r_{i+1} \quad \text{para todo} \quad i \geq 2, \end{aligned}$$

donde r_{i+1} es el resto de la división de r_{i-1} por r_i.

Observemos que estos números satisfacen:

- $r_1 > r_2 > \cdots > r_\ell > \cdots \geq 0$ por el algoritmo de la división.

Luego, dado que estos son números naturales, existe un n tal que $r_{n-1} \neq 0$ y $r_n = 0$.

La demostración de la existencia del máximo común divisor en el Teorema 4.3 es entonces garantizada por la siguiente afirmación.

Afirmación 1. *El máximo común divisor de a y b es r_{n-1}.*

Demostración. Aplicando sucesivamente el corolario anterior obtenemos que

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{i-1}, r_i) = (r_i, r_{i+1}) = \cdots = (r_{n-2}, r_{n-1}) = r_{n-1}$$

donde la última igualdad es consecuencia de que $r_{n-2} = q_n r_{n-1} + r_n = q_n r_{n-1}$, es decir $r_{n-1}|r_{n-2}$. □

4.2. **Números coprimos.**

Lema 4 (NOTA 4.3)**.** *Sean $a, b \in \mathbb{Z}$. Si existen $s, t \in \mathbb{Z}$ tales que $1 = sa + tb$, entonces a y b son coprimos.*

Demostración. Si d divide a a y b, entonces divide a cualquier combinación lineal de ambos. Luego $d|1$ y por lo tanto son iguales. □

Lema 5. *Si $a, b \in \mathbb{Z}$ son no nulos, entonces $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$ son coprimos.*

Demostración. Sean $s, t \in \mathbb{Z}$ tales que $(a, b) = sa + tb$. Entonces $1 = s\frac{a}{(a,b)} + t\frac{b}{(a,b)}$ y el lema sigue por el lema anterior. □

Observación 2. *Sean a y b coprimos. Todo número entero se puede escribir como combinación lineal entera de a y b.*

En efecto, esto sigue del hecho que 1 es una combinación lineal de a y b, es decir, existen $s, t \in \mathbb{Z}$ tales que $1 = sa + tb$. Luego,

$$c = sca + tcb \tag{1}$$

para todo $c \in \mathbb{Z}$. □

Lema 6. *Sean a y b coprimos. Si $a \mid b \cdot c$, entonces $a \mid c$.*

Demostración. Sean $s, t \in \mathbb{Z}$ como en la demostración anterior. Por hipótesis, a divide a los dos sumandos del lado derecho de (1). Por lo tanto $a|c$. □

5. Números primos

Observación 3. *Sea p un número primo y $a \in \mathbb{Z}$. Entonces, $(p, a) = 1$ si y sólo si $p \not| a$.*

En efecto, los divisores positivos de p son 1 y p por definición de númeor primo. Luego, el máximo común divisor de p y a es 1 ó p. Si es 1, entonces $p \not| a$. Si es p, entonces $p|a$ y la observación queda demostrada. □

La siguiente afirmación es utilizada en la demostración de la Proposición 5.8, la cual da una forma de calcular el máximo común divisor usando su factorización en primos.

Lema 7. *Sean c y a enteros positivos cuya factorización en primos es*

$$c = \prod_{j=1}^{r} p_j^{l_j} \quad y \quad a = \prod_{j=1}^{r} p_j^{k_j}$$

donde los exponentes pueden ser nulos. Entonces $c|a$ si y sólo si $l_j \leq k_j$ para todo j.

Demostración. Asumamos que $c|a$. Entonces existe un entero positivo x tal que $a = cx$. Sea

$$x = \prod_{j=1}^{r} p_j^{t_j}$$

la factorización en primos de x donde algún exponente puede ser nulo. Entonces

$$a = \prod_{j=1}^{r} p_j^{k_j} = \prod_{j=1}^{r} p_j^{l_j+t_j} = cx.$$

Dado que la factorización es única (por TFA), $l_j + t_j = k_j \geq l_j$ para todo j.

Ahora asumimos que $l_j \leq k_j$ para todo j. Luego,

$$a = \prod_{j=1}^{r} p_j^{k_j} = \prod_{j=1}^{r} \left(p_j^{l_j} p_j^{k_j-l_j}\right) = \left(\prod_{j=1}^{r} p_j^{l_j}\right)\left(\prod_{j=1}^{r} p_j^{k_j-l_j}\right) = c\left(\prod_{j=1}^{r} p_j^{k_j-l_j}\right),$$

es decir $c|a$. □

6. Mínimo común múltiplo

Observación 4. *Sean a, b, c enteros. Si $(a, b) = 1$, $a \mid c$ y $b \mid c$, entonces $a \cdot b \mid c$.*

En efecto, por la definición de mínimo común multiplo sabemos que $[a, b]|c$ y por ser coprimos $[a, b] = ab$.

□

Congruencias

7. La relación de congruencia

No hay material complementario.

8. Ecuaciones en congruencias

Las congruencias facilitan en cierto modo algunos problemas, como el siguiente que es equivalente al Ejemplo 5.

Ejemplo 6. *La ecuación $2x^2 \equiv 1\,(3)$ no tiene solución.*

Demostración. Si $x \equiv 0\,(3)$, no puede ser solución pues $2x^2 \equiv 0\,(3)$. Mientras que si $x \equiv 1\,(3)$ ó $x \equiv 2\,(3)$, entonces $2x^2 \equiv 2\,(3)$.

Efectivamente, este problema es equivalente al Ejemplo 5 dado que $2x^2 \equiv 1\,(3)$ si y sólo si $2x^2 - 1 = 3y$ paa algún $y \in \mathbb{Z}$. □

La Proposición 2.4 nos da condiciones necesarias y suficientes para que una ecuación lineal tenga solución. Más aún en la prueba se construyen las soluciones. A continuación damos explícitamente los pasos a seguir para encontrar las soluciones basándonos en esa demostración.

Observación 5. *Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$ tales que $(a, n)|b$. El conjunto de soluciones de $ax \equiv b\,(n)$ se construye siguiendo los siguientes pasos:*

(1) Calcular $s, t \in \mathbb{Z}$ tales que $(a, n) = sa + tn$.

(2) $x_0 = \dfrac{sb}{(a, n)}$ es una solución.

(3) $\left\{x_0 + q\dfrac{n}{(a, n)} \mid q \in \mathbb{Z}\right\}$ es el conjunto de soluciones.

(4) La menor solución positiva es el resto de la división de x_0 por $\dfrac{n}{(a, n)}$.

9. Sistemas de ecuaciones en congruencias

Como en la Observación 5, a continuación damos un algoritmo para encontrar las soluciones de un sistema de dos ecuaciones basándonos en la demostración de la Proposición 3.1

Observación 6. *Sean $b_1, b_2 \in \mathbb{Z}$ y $n_1, n_2 \in \mathbb{N}$ tales que $(n_1, n_2)|b_1 - b_2$. El conjunto de soluciones del sistema*

$$\begin{cases} x \equiv b_1\,(n_1) \\ x \equiv b_2\,(n_2), \end{cases}$$

se construye siguiendo los siguientes pasos:

(1) Calcular una solución $h \in \mathbb{Z}$ de la ecuación $n_1 y \equiv b_1 - b_2\,(n_2)$.

(2) Calcular $k \in \mathbb{Z}$ tal que $n_1 h = b_1 - b_2 + kn_2$.

(3) $x_0 = b_1 - hn_1 = b_2 - kn_2$ es una solución.

(4) $\left\{x_0 + q\,[n_1, n_2] \mid q \in \mathbb{Z}\right\}$ es el conjunto de soluciones.

(5) La menor solución positiva es el resto de la división de x_0 por $[n_1, n_2]$.

Podemos hacer lo mismo para más ecuaciones siguiendo la demostración del Teorema Chino del Resto. A modo de ejemplo se puede seguir las cuentas realizadas en la página 83 del texto de Miatello-Kisbye para resolver el sistema (14) de la página 82.

Observación 7. *Sean $n_1, n_2, \ldots, n_h \in \mathbb{N}$ todos coprimos entre si. El conjunto de soluciones del sistema*

$$\begin{cases} x \equiv b_1 \, (n_1) \\ x \equiv b_2 \, (n_2) \\ \quad \vdots \\ x \equiv b_h \, (n_h), \end{cases}$$

se construye siguiendo los siguientes pasos:

(1) Calcular $n_i' = \dfrac{\prod_{j=1}^{h} n_j}{n_i}$ para todo $i = 1, \ldots, h$.

(2) Calcular, para cada $i = 1, \ldots, h$, una solución y_i de la ecuación $n_i' \, y \equiv b_i \, (n_i)$.

(3) $x_0 = \sum_{j=1}^{h} y_j \, n_j'$ es una solución.

(4) $\left\{ x_0 + q \prod_{j=1}^{h} n_j \mid q \in \mathbb{Z} \right\}$ es el conjunto de soluciones.

(5) La menor solución positiva es el resto de la división de x_0 por $\prod_{j=1}^{h} n_j$.

9.1. **Pequeño Teorema de Fermat.** La demostración dada en la clase es diferente a la del texto porque no utilizamos números combinatorios. Esta demostración tiene como principal ingrediente el siguiente lema.

Lema 8. *Sean $p \in \mathbb{N}$ primo y $b \in \mathbb{Z}$ no divisible por p, equivalentemente $(b, p) = 1$. Entonces $x \equiv y \, (p)$ si y sólo si $bx \equiv by \, (p)$.*

Demostración. Si $x \equiv y \, (p)$, entonces $bx \equiv by \, (p)$ por una de las primeras propiedades de congruencia.

Si $bx \equiv by \, (p)$, entonces p divide a $b(x - y)$. Dado que $(b, p) = 1$, p debe dividir a $x - y$ por Lema 6. Es decir $x \equiv y \, (p)$. □

Teorema 1 (Pequeño Teorema de Fermat)**.** *Sean $p \in \mathbb{N}$ primo y $a \in \mathbb{Z}$. Entonces $a^p \equiv a \, (p)$.*

Demostración. Si $a \equiv 0 \, (p)$, entonces $a^p \equiv 0 \equiv a \, (p)$.

Asumamos que $a \not\equiv 0 \, (p)$ o, lo que es lo mismo, p no divide a a. En este caso, por el lema anterior (usando $b = a$), deducimos que los números $a \cdot 1$, $a \cdot 2$, ..., $a \cdot (p - 1)$ son todos no

congruentes módulo p. Luego, para cada $i \in \{1, ..., p-1\}$ existe un único $j \in \{1, ..., p-1\}$ tal que $i \equiv a \cdot j\ (p)$. Por lo tanto,

$$1 \cdot 2 \cdots (p-1) \equiv (a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1))\ (p)$$

pues en ambos lados de la congruencia aparecen los "mismos números" (es decir, iguales con respecto a la congruencia módulo p).

Usando la conmutatividad del producto podemos reordenar el lado derecho de la congruencia y obtenemos que

$$(p-1)! \equiv a^{p-1} \cdot (p-1)!\ (p).$$

Por otro lado, p no divide a ningún número $\leq p-1$. Dado que es primo, tampoco divide al producto de los mismos. Por lo tanto $(p, (p-1)!) = 1$ y por el lema anterior (usando $b = (p-1)!$) deducimos que $1 \equiv a^{p-1}\ (p)$. Multiplicando por a llegamos a lo que queremos probar $a^p \equiv a\ (p)$.

□

CONTEO

10. TÉCNICAS DE CONTEO

Es conveniente ser más explicito en la demostración del Corolario 1.10. Por lo que damos aquí una demostración alternativa a la del texto.

Teorema 2 (Corolario 1.10)**.** *Sea $f : [1, n] \mapsto [1, n]$. Entonces f es inyectiva si y sólo si es f suryectiva.*

Demostración. Supongamos que f es inyectiva. Si f no fuera suryectiva, existiría $h \in [1, n]$ tal que h no está en la imagen de f. Entonces podemos definir la función $\tilde{f} : [1, n+1] \mapsto [1, n]$ dada por:

$$\tilde{f}(k) = \begin{cases} f(k) & \text{si } k \leq n \\ h & \text{si } k = n+1 \end{cases}$$

Entonces $\tilde{f}$ es inyectiva pues f lo es y porque h no está en la imagen de f. Esto es absurdo por el Teorema 1.8, ya que $n+1 > n$, y por lo tanto f debe ser suryectiva.

Ahora supongamos que f es suryectiva. Definimos una "inversa" g de f de la siguiente manera: Para cada $k \in [1, n]$, consideramos el conjunto

$$H_k = \{x \in [1, n] \mid f(x) = k\}.$$

H_k es un subconjunto de los naturales, y es no vacío pues f es suryectiva. Luego tiene primer elemento. Definimos $g(k) =$ primer elemento de H_k.

Entonces $g : [1, n] \mapsto [1, n]$ es inyectiva, y por la primera parte del teorema debe ser suryectiva.

Ahora bien, si f no fuera inyectiva, entonces existirían x_1 y x_2, con $x_1 < x_2$ tal que $f(x_1) = f(x_2) = k$ para algún k. Entonces x_2 no pertenecería a la imagen de g, y por lo tanto g no sería suryectiva. Luego debe ser f inyectiva. □

A continuación haremos algunas demostraciones que el apunte deja como ejercicios.

Corolario 3 (Corolario 1.14)**.** *Si A_1, ..., A_m son conjuntos finitos disjuntos dos a dos, entonces*

$$|A_1 \cup \cdots \cup A_m| = \sum_{i=1}^{m} |A_i|.$$

Demostración. Haremos inducción fuerte en la cantidad m de conjuntos. Si $m = 1$ no hay nada que probar. Si $m \leq k$ asumimos que la igualdad es cierta y probamos el caso $m = k + 1$.

Como los conjuntos son disjuntos dos a dos, la unión $A_1 \cup \cdots \cup A_k$ tiene intersección vacía con A_{k+1}. Luego, como la igualdad vale para $m = 2$, deducimos que

$$|\{A_1 \cup \cdots \cup A_k\} \cup A_{k+1}| = |\{A_1 \cup \cdots \cup A_k\}| + |A_{k+1}| = \sum_{i=1}^{k} |A_i| + |A_{k+1}| = \sum_{i=1}^{k+1} |A_i|,$$

donde la segunda igualdad vale por el caso $m = k$ y la última igualdad es por definición de sumatoria. Hemos probado el caso $m = k + 1$ y por inducción fuerte vale para todo $m \in \mathbb{N}$. □

Lema 9 (Ejercicio 1.3 (a))**.** *Probar que si A y B son conjuntos finitos, entonces*

$$|A \cup B| + |A \cap B| = |A| + |B|.$$

Demostración. Denotemos por A' el complemento de $A \cap B$ en A. Es decir, $A = (A \cap B) \cup A'$ y $(A \cap B) \cap A' = \emptyset$. Sea B' el complemento $A \cap B$ en B. Por el principio de adición obtenemos que

$$|A| = |A \cap B| + |A'| \quad \text{y} \quad |B| = |A \cap B| + |B'|. \tag{2}$$

Por otro lado, $A \cup B = A' \cup (A \cap B) \cup B'$ y estos tres conjuntos son disjuntos dos a dos. Luego, usando nuevamente el principio de adición y (2), obtenemos

$$|A \cup B| = |A'| + |A \cap B| + |B'| = |A| + |B| - |A \cap B|.$$

La igualdad que queremos se obtiene sumando $|A \cap B|$ en ambos miembros. □

Corolario 4 (Corolario 1.16)**.** *Si A_1, ..., A_m son conjuntos finitos, entonces*

$$|A_1 \times \cdots \times A_m| = \prod_{i=1}^{m} |A_i|.$$

Demostración. Es por inducción fuerte en la cantidad m de conjuntos, análogamente a la del Corolario 3 pero cambiando las uniones por productos cartesianos las sumas por productos.

Si $m = 1$ no hay nada que probar. Si $m \leq k$ asumimos que la igualdad es cierta y probamos el caso $m = k + 1$. Como la igualdad vale para $m = 2$, deducimos que

$$|\{A_1 \times \cdots \times A_k\} \times A_{k+1}| = |\{A_1 \times \cdots \times A_k\}| \cdot |A_{k+1}| = \prod_{i=1}^{k} |A_i| \cdot |A_{k+1}| = \prod_{i=1}^{k+1} |A_i|,$$

donde la segunda igualdad vale por el caso $m = k$ y la última igualdad es por definición de productoria. Hemos probado el caso $m = k + 1$ y por inducción fuerte vale para todo $m \in \mathbb{N}$. □

Teorema 3 (Teorema 1.21)**.** *Sean $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$, con $n \leq m$. Entonces*

$$|\mathcal{F}_i(A, B)| = \frac{m!}{(m-n)!} = m(m-1)\cdots(m-n+1).$$

Demostración. La prueba del Teorema 1.21 del apunte es informal y propone cambiar el "Así sucesivamente" por una demostración inductiva. La propiedad a demostrar por inducción es:

$$P(m): \text{ Si } n \leq m, \text{ entonces } |\mathcal{F}_i(A, B)| = \frac{m!}{(m-n)!} = m(m-1)\cdots(m-n+1)$$

para cualesquiera conjuntos A y B de cardinal n y m, respectivamente.

Si $m = 1$, n sólo puede tomar el valor 1 y hay sólo una función. Luego, $|\mathcal{F}_i(A, B)| = 1 = \frac{1!}{0!}$.

Supongamos que $P(m-1)$ vale y probemos $P(m)$.

Si $n = 1$, entonces $A = \{a_1\}$ y por lo tanto toda función de A en B es inyectiva. Además, hay tantas funciones como elementos en B. Es decir,

$$|\mathcal{F}_i(A, B)| = m - 1 = \frac{(m-1)!}{(m-2)!}.$$

Sea $1 < n \leq m$. Una forma de interpretar matemáticamente la frase "$f(a_1)$ tiene como posibles valores a $b_1, \ldots, b_m$, o sea m posibilidades. Ahora, fijado $f(a_1)$ hay $(m-1)$ posibles valores para ..." –ver la prueba en el apunte– es descomponiendo el conjunto de funciones inyectivas $\mathcal{F}_i(A, B)$

como unión de subconjuntos parametrizados de acuerdo al valor que toman las funciones en a_1. Esto es,

$$\mathcal{F}_i(A,B) = \bigcup_{\ell=1}^{m} \big\{ f \in \mathcal{F}_i(A,B) \,:\, f(a_1) = b_\ell \big\}.$$

Claramente estos subconjuntos son disjuntos dos a dos por lo que podemos aplicar el principio de adición. Más aún, podemos identificar cada uno de ellos con conjuntos de funciones inyectivas usando la restricción de funciones. Es decir, la siguiente aplicación es biyectiva

$$\begin{aligned} \Theta : \{ f \in \mathcal{F}_i(A,B) \,:\, f(a_1) = b_\ell \big\} &\longrightarrow \mathcal{F}_i(A \setminus \{a_1\}, B \setminus \{b_\ell\}) \\ f &\longmapsto f_{|A\setminus\{a_1\}}, \end{aligned}$$

con inversa $g \longmapsto f(a_j) = \begin{cases} b_\ell & \text{si } j = 1 \\ g(a_j) & \text{si } 2 \leq j. \end{cases}$

Combinando todo lo anterior tenemos que:

$$\begin{aligned} |\mathcal{F}_i(A,B)| &= \sum_{\ell=1}^{m} |\big\{ f \in \mathcal{F}_i(A,B) \,:\, f(a_1) = b_\ell \big\}| \\ &= \sum_{\ell=1}^{m} |\mathcal{F}_i(A \setminus \{a_1\}, B \setminus \{b_\ell\})| \\ &= \sum_{\ell=1}^{m} \frac{(m-1)!}{((m-1)-(n-1))!} = \frac{m!}{(m-n)!}, \end{aligned}$$

donde la primera igualdad es por el principio de adición, la segunda es por la biyección Θ, la tercera por hipótesis inductiva aplicada a $n-1 \leq m-1$ y la última porque sumamos m veces el mismo número.

Por lo tanto la propiedad $P(m)$ vale $m \in \mathbb{N}$. □

10.1. **Número combinatorio.** En el apunte se afirma sin demostración (página 44) que la cantidad de maneras distintas de elegir n elementos de entre m dados (sin tener en cuenta el orden) es igual al número combinatorio

$$\binom{m}{n} = \frac{m!}{n!\,(m-n)!}.$$

A continuación probaremos esta afirmación.

Observemos que lo que queremos calcular es el cardinal del conjunto

$$C(n,m) = \big\{C \subseteq [1,m] \ : |C| = n\ \big\}.$$

Para esto usaremos el Teorema 3. Notemos que la imagen de una función inyectiva $f : [1,n] \to [1,m]$ define un subconjunto $\operatorname{Im} f$ de $[1,m]$ de cardinal n. Entonces, podemos descomponer el conjunto de funciones inyectiva de acuerdo a su imagen. Esto es,

$$\mathcal{F}_i([1,n],[1,m]) = \bigcup_{\{C\subseteq[1,m]\,:|C|=n\}} \big\{f \in \mathcal{F}_i([1,n],[1,m]) \ : \ \operatorname{Im} f = C\big\}$$

Claramente estos subconjuntos son disjuntos dos a dos y podemos aplicar el principio de adición. Calculemos el cardinal de cada uno de ellos reinterpretándolos de la siguiente forma. Fijado $C \subseteq [1,m]$ con $|C| = n$, entonces

$$\big\{f \in \mathcal{F}_i([1,n],[1,m]) \ : \ \operatorname{Im} f = C\big\} = \big\{f : [1,n] \to C \ : \ f \text{ es biyectiva}\big\}$$

y el cardinal de este último conjunto es $n!$, es decir las distintas formas de ordenar los elementos de la imagen.

Combinando lo anterior, resulta que

$$\begin{aligned}
\frac{m!}{(m-n)!} &= |\mathcal{F}_i([1,n],[1,m])| \\
&= \sum_{\{C\subseteq[1,m]\,:|C|=n\}} |\big\{f \in \mathcal{F}_i([1,n],[1,m]) \ : \ \operatorname{Im} f = C\big\}| \\
&= \sum_{\{C\subseteq[1,m]\,:|C|=n\}} |\big\{f : [1,n] \to C \ : \ f \text{ es biyectiva}\big\}| \\
&= \sum_{\{C\subseteq[1,m]\,:|C|=n\}} n! \\
&= n!|\{C \subseteq [1,m] \ : |C| = n\}|,
\end{aligned}$$

la última igualdad estamos sumando $n!$ tantas veces como el cardinal $\{C \subseteq [1,m] \ : |C| = n\}$. Dividiendo por $n!$ en ambos lados de la igualdad obtenemos lo que queríamos:

$$\binom{m}{n} = |\big\{C \subseteq [1,m] \ : |C| = n\ \big\}|. \tag{3}$$

En el Teorema 1.28 se prueban ciertas propiedades de los números combinatorios. La demostraciones de los incisos

(i) $\binom{m}{1} = m$, (ii) $\binom{m}{n} = \binom{m}{m-n}$ y (iii) $\binom{m}{n-1} + \binom{m}{n} = \binom{m+1}{n}$,

son aritméticas, pues consisten en sumar y multiplicar. En cambio la demostración de (iv) se dice que es combinatoria porque se basa en contar conjuntos. Las siguientes son demostraciones combinatorias de (i), (ii) y (iii).

(i) sigue de la siguiente igualdad de conjuntos

$$\big\{C \subseteq [1,m] \,:\, |C| = 1\big\} = \big\{\{x\} \,:\, x \in [1,m]\big\}.$$

(ii) sigue de observar que cada vez que elegimos un subconjunto de cardinal n, por omición, estamos eligiendo un subconjunto de cardinal $m-n$, que es el complemento. En otras palabras, la siguiente función es biyectiva

$$\begin{aligned}\big\{C \subseteq [1,m] \,:\, |C| = n\big\} &\longrightarrow \big\{D \subseteq [1,m] \,:\, |D| = m-n\big\},\\ C &\longmapsto C^c.\end{aligned}$$

La demostración combinatoria de (iii) es similar a la de (iv). Dividimos los subconjuntos de $[1, m+1]$ de cardinal n en dos, aquellos que contienen a $m+1$ y los que no:

$$\begin{aligned}&\big\{C \subseteq [1,m+1] \,:\, |C| = n\big\} =\\ &= \big\{C \subseteq [1,m+1] \,:\, |C| = n \text{ y } m+1 \in C\big\} \bigcup \big\{C \subseteq [1,m+1] \,:\, |C| = n \text{ y } m+1 \notin C\big\},\end{aligned}$$

estos subconjuntos son disjuntos. Además,

$$\begin{aligned}&\big\{C \subseteq [1,m+1] \,:\, |C| = n \text{ y } m+1 \notin C\big\} = \big\{C \subseteq [1,m] \,:\, |C| = n\big\} \text{ y}\\ &\big\{C \subseteq [1,m+1] \,:\, |C| = n \text{ y } m+1 \in C\big\} = \big\{C' \cup \{m+1\} \,:\, C' \subseteq [1,m] \text{ y } |C'| = n-1\big\}.\end{aligned}$$

Tomando cardinal y usando el principio de adición obtenemos (iii).

10.2. **Binomio de Newton.** Nos explayaremos un poco más en la demostración combinatoria que se da al principio de la página 52.

Consideremos el producto cartesianos del conjunto $\{a,b\}$ consigo mismo n veces:

$$\mathcal{C} = \{a,b\} \times \cdots \times \{a,b\} = \big\{(x_1, \ldots, x_n) \,:\, x_i \in \{a,b\} \text{ para todo } i\big\}.$$

Separemos los elementos de este conjunto de acuerdo a la cantidad de a's que tienen. Es decir,

$$\mathcal{C} = \bigcup_{k=0}^{n} \big\{(x_1, \ldots, x_n) \in \mathcal{C} \,:\, x_i = a \text{ para exactamente } k \text{ valores de } i\big\}$$

Denotemos cada uno de esto subconjuntos por $\mathcal{C}_k$. Notar que son disjuntos dos a dos. Además,

$$|\mathcal{C}_k| = \binom{n}{k}$$

pues es la cantidad de maneras de elegir k lugares en donde poner a de entre los n dados.

Entonces la fórmula del binomio sigue por el siguiente razonamiento

$$\begin{aligned}(a+b)^n &= \sum_{(x_1,\ldots,x_n)\in\mathcal{C}} x_1\cdots x_n = \sum_{k=0}^{n} \sum_{(x_1,\ldots,x_n)\in\mathcal{C}_k} x_1\cdots x_n = \sum_{k=0}^{n} \sum_{(x_1,\ldots,x_n)\in\mathcal{C}_k} a^k b^{n-k} \\ &= \sum_{k=0}^{n} |\mathcal{C}_k|\, a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\end{aligned}$$

donde la primera igualdad es por la propiedad distributiva, la segunda es por la asociatividad de la suma y la tercera por la conmutatividad del producto. Notar si en $(x_1, \ldots, x_n)$ esta a repetida k veces, entonces b esta $n-k$ veces repetidas.