Notas de Álgebra I

Primer Cuatrimestre 2022

por *Joan Gonzalez*

Índice

I Teoría 1

1 Conjuntos, Relaciones y Funciones 1
- 1.1 Grupos 1
- 1.2 Grupos finitos y cíclicos 3
- 1.3 Anillos 3

2 Números Naturales e Inducción 5
- 2.1 Principio de Inducción 6
- 2.2 Inducción corrida 8
- 2.3 Inducción completa 9

3 Números Enteros 10
- 3.1 Teorema Chino del Resto 10

4 Números Complejos 11
- 4.1 Raíces n-ésimas de la unidad 11

II Práctica 12

1 Problemas 12
- 1.1 Final 03/08/2022 12

III Fórmulas y Definiciones 15

1 Grupos y Anillos 15
- 1.1 Definición – Grupo 15

1.2 Definición – Orden 15
1.3 Definición – Anillo 15
1.3.1 Conmutatividad de la multiplicación 16
1.3.2 Elemento identidad 16
1.3.3 Elemento inversible 16

2 Números Naturales **17**
2.1 Suma de Gauss 17
2.2 Serie geométrica 17

3 Combinatoria **18**
3.1 Cardinalidad de un conjunto 18
3.2 Cantidad de funciones inyectivas 18
3.3 Número combinatorio 18
3.3.1 Forma recursiva 18
3.4 Binomio de Newton 18

4 $\mathbb{Z}$ y $\mathbb{Z}/p\mathbb{Z}$ **20**
4.1 Ecuaciones de Congruencia 20
4.2 Inversibles en $\mathbb{Z}/n\mathbb{Z}$ 20
4.3 Pequeño Teorema de Fermat 20
4.4 Función $\varphi(n)$ de Euler 20
4.5 Teorema de Euler 20
4.6 Inverso multiplicativo módulo n 21
4.7 Potencias módulo m 21

5 Números Complejos **21**
5.1 Fórmula de De Moivre 21

IV Bibliografía **22**

Parte I
Teoría

1 Conjuntos, Relaciones y Funciones

1.1 Grupos

[1] El término *grupo* fue usado por Évariste Galois alrededor del año 1830 para describir conjuntos de funciones inyectivas en conjuntos finitos, que pudieran ser agrupadas para formar un conjunto cerrado con la operación de *composición* de funciones. Aunque el término existía previamente, a partir del siglo XX empezó a cobrar relevancia, ya que resultó útil para hablar sobre lo que ahora es una *estructura algebraica*.

Definición – Una estructura algebraica está compuesta por:

- Un conjunto no vacío, denominado el *dominio* de la estructura.
- Un conjunto de operaciones definidas sobre los elementos del dominio.
- Un conjunto finito de axiomas o identidades.

Una *operación binaria* sobre los elementos de un dominio G es simplemente un método (o una fórmula) a través de la cual los elementos de un par ordenado de elementos de G se combinan para dar un nuevo elemento perteneciente a G, a esto se lo conoce como *ley de composición*.

Las operaciones binarias más conocidas son la adición o suma y la multiplicación, o producto de los números enteros. La división de números enteros no es una operación binaria que siga la ley de composición, ya que no necesariamente un entero dividido por otro resulta en un nuevo entero.

Luego, un *grupo* es una estructura algebraica compuesta por un dominio, donde se define una operación binaria asociativa tal que exista el elemento identidad para dicha operación. Además, todo elemento debe tener inverso, y cualquier par de elementos deben poder ser combinados a través de la misma operación sin salirse del dominio.

Definición – Grupo: Sea G un dominio donde se define una operación binaria que asigna a cada par ordenado (a, b) con $a, b \in G$, otro elemento de G designado ab. Decimos que G es un grupo bajo ésta operación si las siguientes propiedades se cumplen:

1. **Asociatividad** – La operación es asociativa, tal que
   $(ab)c = a(bc) \quad \forall a, b, c \in G$
2. **Identidad** – Existe un elemento e, llamado *identidad* en G tal que
   $ae = ea = a \quad \forall a \in G$
3. **Inverso** – Para cada elemento $a \in G$ existe un elemento a^{-1} en G, llamado *inverso* tal que
   $ab = ba = e$

Adicionalmente, si un grupo tiene la propiedad de que para todo par ordenado (a, b) se cumple $ab = ba$ es decir, la **conmutatividad**, entonces decimos que se trata de un grupo *Abeliano*.

Ejemplos:

- Los conjuntos numéricos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ son todos grupos con la adición. En cada caso, el elemento neutro es el 0, y el inverso de a es siempre $-a$.
- Ahora bien, $\mathbb{Z}$ con la multiplicación no es un grupo. Siendo el número 1 la identidad, falla la propiedad del inverso para cada elemento de $\mathbb{Z}$. Por ejemplo, no existe $b \in \mathbb{Z}$ tal que $5b = 1$.

Ahora bien, aunque los ejemplos dados de grupos son fundamentalmente distintos, comparten algunas propiedades que podemos deducir. Ya desde su definición podemos plantearnos algunas preguntas. Por ejemplo,

- Todo grupo tiene *algún* elemento identidad.
  ¿Podría un grupo tener *más* de una?
- Todo elemento de un grupo tiene su inverso.
  ¿Podría tener más de uno?

Los ejemplos sugieren que la respuesta es *no* a ambas preguntas, pero en sí no prueban nada. Es imposible probar que cada grupo tiene una única identidad sólo mirando los ejemplos, ya que cada ejemplo tiene propiedades inherentes que no comparte con otros grupos. Para poder responder a algunas de esas preguntas, miremos primero a los siguientes teoremas:

1. **Unicidad de la identidad:**
   En un grupo G, existe un único elemento identidad.

Demostración: Supongamos que e y e' son ambas identidades en G. Luego,

- $ae = a$ para todo $a \in G$
- $e'a = a$ para todo $a \in G$

$\implies$ $e'e = e \ \wedge \ e'e = e'$

$\implies$ Por ende, e al igual que e' son iguales. Teniendo este teorema en cuenta, cuando hablamos de la identidad de un grupo, y la denotamos con la letra e (Del alemán *einheit*, identidad), sabemos que estamos hablando de la única que existe en el grupo.

2. **Cancelación de términos**
   En un grupo G, se pueden cancelar a la derecha y a la izquierda. Es decir, vale lo siguiente:

$$ba = ca \implies b = c \wedge ab = ac \implies b = c$$

   Demostración: Supongamos que $ba = ca$. Asumamos que a' es el inverso de a. Luego, multiplicar a la derecha por a' resulta en $(ba)a' = (ca)a'$. A través de la asociatividad, sabemos que $b(aa') = c(aa')$. Luego, $be = ce$ y por ende $b = c$. La prueba para la multiplicación por la izquierda es análoga.

   Una consecuencia de éste teorema es la unicidad de los inversos.

3. **Unicidad de los inversos**
   Para cada elemento $a \in G$, si G es un grupo, entonces existe un único elemento $b \in G$ tal que $ab = ba = e$

   Demostración: Supongamos que b y c son ambos inversos de a. Luego, $ab = e \wedge ac = e$ es verdadero, además $ac = e$ tal que $ab = ac$. Cancelando en ambos lados, llegamos a que $b = c$.

1.2 Grupos finitos y cíclicos

1.3 Anillos

[1] Anteriormente, vimos que los conjuntos sobre los que se define una sola operación pueden ser denominados grupos si se cumplen las propiedades de asociatividad, identidad e inverso sobre la operación definida. Ahora bien, sobre bastantes conjuntos podemos definir dos operaciones binarias, en particular la adición y la multiplicación. Los ejemplos típicos pueden ser los enteros módulo n ($\mathbb{Z}/n\mathbb{Z}$), los números reales ($\mathbb{R}$), los polinomios ($K[X]$) y las matrices. Cuando considerábamos a estos conjuntos como dominios de grupos, sólo mirabamos una sola operación, la adición; ahora nos gustaría ver la adición y la multiplicación simultáneamente definida en dichos dominios. En este caso, la estructura algebraica pertinente es la de los *anillos*, término utilizado por primera vez por David Hilbert en 1897.

Definición – Anillo: Sea R un conjunto con dos operaciones binarias. En particular, la adición y la multiplicación, de forma tal que para todo $a, b, c \in R$ se cumplan las siguientes propiedades:

1. **Conmutatividad de la adición**
   $a + b = b + a$
2. **Asociatividad de la adición**
   $(a + b) + c = a + (b + c)$
3. **Existencia del neutro aditivo**
   $a + 0 = a$
4. **Existencia del inverso aditivo**
   $a + (-a) = 0$
5. **Asociatividad de la multiplicación**
   $a(bc) = (ab)c$
6. **Distribución de la multiplicación respecto de la adición**
   $a(b + c) = ab + ac \wedge (b + c)a = ba + ca$

De esta manera, un anillo es un grupo Abeliano con la adición, multiplicación asociativa y distributiva a la izquierda y a la derecha sobre la adición. Nótese que la multiplicación no tiene por qué ser conmutativa. Cuando lo es, decimos que se trata de un *anillo conmutativo*. De la misma manera, notemos que un anillo no necesita tener un elemento identidad en la multiplicación. Cuando lo tiene, decimos que es un *anillo con unidad*, o *con 1*. Un elemento distinto del 0 de un anillo conmutativo con unidad, no necesariamente tiene inverso multiplicativo. Cuando lo tiene, decimos que es *inversible*. Es decir, si a es inversible en un anillo R, entonces existe a^{-1}.

2 Números Naturales e Inducción

[2] El conjunto de los números naturales $\mathbb{N} = 1, 2, 3, 4...$ se define axiomáticamente a partir de la teoría de conjuntos (Axiomas de Peano, 1890 1899 y *Models of the Arithmetic*, Heane)

Luego, $(N, +, \cdot)$ se definen axiomáticamente:

La suma $(+)$ es conmutativa: $a + b = b + a$
y asociativa: $a + (b + c) = (a + b) + c$

El producto $(\cdot)$ es conmutativo: $a \cdot b = b \cdot a$
y asociativo $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Además, el *neutro multiplicativo* es el 1:
$1 \cdot a = a \cdot 1 = a$

Y finalmente, el producto es distributivo respecto de la suma:
$a \cdot (b + c) = a \cdot b + a \cdot c$

Sobre el conjunto de los números naturales $\mathbb{N}$ podemos hacer predicados, tal que $p(n)$ con $n \in \mathbb{N}$ es una proposición que versa sobre los $\mathbb{N}$.

Ejemplos de proposiciones:

- p(n) : $n \geqslant 7$ p(5) = Falso p(23) = Verdadero
- p(n) : $n^2 + 1 \geqslant n$ p(n) = Verdadero siempre
- p(n) : $x^n + y^n = z^n$ con $x, y, z \in \mathbb{Z}$, $n \in \mathbb{N}$ y no todos 1 $\vee$ -1. Tiene soluciones $\iff$ $n = 2$.
- p(n) : Todo número par es la suma de dos primos.

2.1 Principio de Inducción

Sea A $\in \mathbb{N}$ conjunto, tal que $1 \in$ A. Si $n \in$ A $\Rightarrow n+1 \in$ A, entonces A $= \mathbb{N}$. Muchas veces A es el conjunto dado por una proposición. Por ejemplo:

$$\text{A} = \{n : \text{p}(n) \text{ es verdadero}\}$$

Uno quiere demostrar que p es siempre verdadera, y para eso se intenta demostrar que A $= \mathbb{N}$, mostrando que $1 \in$ A (O sea, p(1) es verdadero) y que si p(n) es verdad, entonces p(n) también lo es. Es decir,

$$\text{p}(1) \wedge \text{p}(n) \Longrightarrow \text{p}(n+1)$$

Ejemplo: Demostrar que p(n) es verdadero siempre.

$$\text{p}(n) : \frac{(2n)!}{n!^2} \leqslant (n+1)! \tag{1}$$

Caso base:

$$\text{p}(1) : \frac{(2)!}{1!^2} \leqslant (1+1)! \tag{2}$$

$$\iff \frac{2}{1} \leqslant 2 \Longrightarrow \text{p}(1) \text{ es verdadero.}$$

Paso Inductivo: Veamos que p(h) $\implies$ p(h+1).
Nuestra *hipótesis inductiva* es que p(h) es verdadero. Queremos ver que si es verdadero, entonces p(h+1) también lo es.

$$\text{p}(h+1) : \frac{(2h+2)!}{(h+1)!^2} \leqslant (h+2)! \tag{3}$$

$$\iff \underbrace{\frac{(2h)!}{h!^2}}_{\text{p}(h)} \cdot \frac{(2h+1)(2h+2)}{(h+1)^2} \leqslant (h+1)! \cdot (h+2)$$

Luego, uso lo que sé de la hipótesis inductiva. Basta con probar que:

$$\begin{aligned}
(h+1)! \cdot \frac{(2h+1)(2h+2)}{(h+1)^2} &\leqslant (h+1)!(h+2) \\
\iff \quad \frac{2(2h+1)}{h+1} &\leqslant h+2 \\
\iff \quad 4h+2 &\leqslant (h+1)(h+2) \\
\iff \quad 0 &\leqslant h(h-1)
\end{aligned}$$

Resta ver que $h(h-1) \geqslant 0$, pero ésto es verdadero ya que $h \in \mathbb{N} \Rightarrow h \geqslant 1$ entonces $h(h-1)$ es como mínimo 0, y luego es producto de números positivos, que siempre será mayor a cero. Como ésto último es verdadero, entonces $\mathrm{p}(h+1)$ es verdadero y $\mathrm{p}(h+1) \implies \mathrm{p}(h) \implies \underline{\mathrm{p}(h) \text{ vale } \forall h \in \mathbb{N}.}$

2.2 Inducción corrida

Sea p una proposición tal que:

- p(n_0) es verdadera para algún $n_0 \in \mathbb{N}$
- p(h) es verdadero $\implies$ p($h+1$) es verdadero
- Entonces, p(h) es verdadero $\forall n \geqslant n_0$

Ejemplo: Sea p la siguiente proposición

p(n) : $2^n \geqslant n^3$

Luego,

- p(1) es verdad
- p(2) es falso
- p(3) es falso
- p(4) es falso
- p(5) es falso
- p(10) es falso
- p(11) es verdad

Demostremos $2^n \geqslant n^3 \quad \forall n \geqslant 10$.
Si $n_0 = 10 \implies p(n_0) =$ Verdadero

Luego, si p(h) es verdadero, quiero ver que p($h+1$) es verdad.

$$\begin{aligned} & p(h+1) : 2^{h+1} \geqslant (h+1)^3 \\ \iff & 2^h \cdot 2 \geqslant 2 \cdot h^3 \geqslant (h+1)^3 \end{aligned} \tag{4}$$

Alcanza con ver que

$$2h^3 \geqslant (h+1)^3 \tag{5}$$

Sea cierto para $h \geqslant 10$. Para demostrar esto, es lo mismo ver que:

$$\text{q}(h) : h^3 - 3h^2 - 3h - 1 \geqslant 0 \tag{6}$$

Vemos que q(10) verdadero, pues $2(10^3) \geqslant 11^3$. Ahora tomemos q(h) como hipótesis inductiva a nuestro nuevo problema de inducción, y probemos (6).

$$\text{q}(h+1) = (h+1)^3 - 3(h+1)^2 - 3(h+1) - 1 \geqslant 0 \tag{7}$$

$$h^3 + 3h^2 + 3h + 1 - 3h^2 - 6h - 3 - 3h - 3 - 1 \geqslant 0$$

$$\underbrace{h^3 - 3h^2 - 3h - 1}_{\text{Hipótesis}} - 6h - 3 + 3h^2 + 3h + 1 \geqslant 0$$

2.3 Inducción completa

3 Números Enteros

3.1 Teorema Chino del Resto

4 Números Complejos

4.1 Raíces n-ésimas de la unidad

Imaginemos que queremos resolver la siguiente ecuación, para $\omega \in \mathbb{C} \land n \in \mathbb{Z}$

$$\omega^n = 1 \tag{8}$$

Luego, el conjunto de soluciones de ésta ecuación son las raíces n-ésimas de la unidad. Si reescribimos al 1 en su forma exponencial usando la fórmula de De Moivre, vemos que:

$$\omega_k = e^{\frac{2k\pi}{n}i}, \quad 0 \leqslant k \leqslant n-1 \tag{9}$$

Parte II
Práctica

1 Problemas

1.1 Final 03/08/2022

1. Calcular la cantidad de funciones inyectivas

$$f : \{1, 2, ..., 20\} \to 1, 2, ..., 50$$

que verifican simultáneamente:

- $f(1) < f(3)$
- $f(2) < f(3)$

2. Sea (a_n) $n \in \mathbb{N}$ la sucesión definida recursivamente por:

$$a_1 = 42$$
$$a_2 = 90$$
$$a_n = 3a_{n-1} + (29^n - 11^n)a_{n-2} \text{ si n} \geqslant 3$$

Probar que $(6^n : a_n) = 2 \cdot 3^n$ para todo $n \in \mathbb{N}$.

3. Sea $w \in \mathrm{G}_{15}$ tal que $w \notin \mathrm{G}_3 \wedge w \notin \mathrm{G}_5$. Hallar el argumento del número complejo

$$(2 + w^3 + \bar{w}^3 + w^6 + \bar{w}^6 + i(2 + w^5 + w^{-5}))^{31}$$

4. Factorizar el polinomio

$$3X^2 + 210X + 5 \in (\mathbb{Z}/239\mathbb{Z})[X]$$

como producto de polinomios irreducibles en $(\mathbb{Z}/239\mathbb{Z})[X]$.

Nota: El el número 239 es primo.

1.

2.

3.

4. Factorizar en irreducibles en $(\mathbb{Z}/239\mathbb{Z})[X]$ al siguiente polinomio:

$$f(x) = 3X^2 + 210X + 5 \in (\mathbb{Z}/239\mathbb{Z})[X]$$

Al ser un polinomio cuadrático, miro su discriminante tal que:

$$\Delta = b^2 - 4 \cdot a \cdot c \Longrightarrow \Delta = \overline{210}^2 - \bar{4} \cdot \bar{3} \cdot \bar{5} = \overline{64}$$

Donde $\overline{64}$ es la clase de equivalencia del 64 módulo 239.

Queda ver que el discriminante sea un cuadrado perfecto módulo 239, es decir que $\Delta = w^2$. Noto que $\overline{64} = \bar{8}^2$, y como $8 \leqslant 239$, entonces 64 es un cuadrado perfecto módulo 239.

Por ende, puedo plantear:

$$\bar{x}_{1,2} = \frac{-\bar{b} \pm \bar{w}}{\overline{2a}} \qquad \text{con } \bar{a} \neq \bar{0} \wedge \bar{2} \neq \bar{0}$$

Luego,

$$\begin{aligned} &\text{Con } a = \bar{3},\ b = \overline{210} = \overline{-29},\ c = \bar{5} \\ &\bar{x}_{1,2} = \frac{-\bar{b} \pm \bar{w}}{\overline{2a}} \\ &\bar{x}_{1,2} = \frac{-\overline{29} \pm \bar{8}}{\bar{6}} \\ \Longrightarrow\ &x_1 \equiv \overline{37} \cdot \bar{6}^{-1} \pmod{239} \\ &x_2 \equiv \overline{21} \cdot \bar{6}^{-1} \pmod{239} \end{aligned}$$

Queda ver qué número es el inverso multiplicativo de 6 módulo 239. Es decir, buscamos un α tal que $\alpha \cdot 5 \equiv 1 \pmod{239}$

Para eso usamos el Teorema de Euler, tal que:

$$6^{-1} \equiv 6^{\varphi(239)-1} \pmod{239}$$

Pero como 239 es primo, entonces $\varphi(239) = 239 - 1 = 238$. Luego,

$$6^{\varphi(239)-1} \equiv 6^{237} \equiv 40 \pmod{239}$$

Podemos comprobarlo, ya que $6 \cdot 40 \equiv 240 \equiv 1 \pmod{239}$. Juntando todo, los valores de x_1 y x_2 son:

$$\begin{aligned} \implies x_1 &\equiv \overline{37} \cdot \bar{6}^{-1} \equiv \overline{37} \cdot \overline{40} \equiv \overline{46} \pmod{239} \\ x_2 &\equiv \overline{21} \cdot \bar{6}^{-1} \equiv \overline{21} \cdot \overline{40} \equiv \overline{123} \pmod{239} \end{aligned}$$

Por ende, como 46 y 123 son soluciones, y $46,\ 123 \in \mathbb{Z}/239\mathbb{Z}$, entonces $f(x)$ es reducible en $(\mathbb{Z}/239\mathbb{Z})[X]$ de la siguiente forma:

$$f(x) = (X - 123)(X - 46) \ \in (\mathbb{Z}/239\mathbb{Z})[X]$$

Siendo ésta su factorización en irreducibles en $(\mathbb{Z}/239\mathbb{Z})[X]$, ya que cada uno de sus factores es irreducible por ser de grado 1.

Parte III
Fórmulas y Definiciones

1 Grupos y Anillos

1.1 Definición – Grupo

1.2 Definición – Orden

Sea G un grupo. Sea a un elemento de G, tal que $a \in G$, definimos:

1. $|G|$ es la cantidad de elementos en G.
   Decimos que es el *orden* o la *cardinalidad* de G

   Ejemplos:

   - $|\mathbb{Z}| = \infty$
   - $|\mathbb{Z}/9\mathbb{Z}| = \#\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\} = 9$

2. $|a|$ es el entero positivo más chico tal que a^n sea el elemento identidad.
   Decimos que es el *orden* o el *periodo* de a.

   Ejemplo:

   - En $\mathbb{Z}/12\mathbb{Z}$, $|5| = 2$, pues $5^2 \equiv 1 \pmod{12}$

1.3 Definición – Anillo

Sea R un anillo. Luego R es un conjunto, donde se definen dos operaciones binarias: *adición* y *multiplicación*, tales que para todo a, b, c en R se cumpla:

1. **Conmutatividad de la adición:**
   $a + b = b + a$
2. **Asociatividad de la adición**
   $(a + b) + c = a + (b + c)$
3. **Existencia de neutro aditivo**
   Existe un elemento 0 en R tal que $a + 0 = a \ \forall a \in R$
4. **Existencia de inverso aditivo**
   $\exists\ -a$ tal que $a + (-a) = 0$
5. **Asociatividad de la multiplicación**
   $a(bc) = (ab)c$

6. **Distribución de la multiplicación respecto de la adición**
   $a(b+c) = ab + ac \wedge (b+c)a = ba + ca$

1.3.1 Conmutatividad de la multiplicación

Sea R un anillo. Luego, si para todo a, b, c en R se cumple: $ab = ba$
Entonces se dice que R es un *anillo conmutativo*.

1.3.2 Elemento identidad

Sea R un anillo, y sea e un elemento de R, luego si $e \neq 0$ y se cumple que

$$ae = a \ \ \forall a \in R$$

Entonces decimos que e es el *elemento identidad*. En particular, es la identidad de la multiplicación. También recibe el nombre de *unidad* ó *unity*, en inglés.

1.3.3 Elemento inversible

Sea R un anillo, y sea a un elemento de R, $a \neq 0$. Luego si existe un elemento $a^{-1} \in R$ tal que

$$a \cdot a^{-1} = e$$

Donde e es el elemento identidad de R.

Luego, a^{-1} es el *inverso multiplicativo* de a. Decimos que a es *inversible*.

Además, se cumple que:

1. El inverso multiplicativo es único para cada inversible de R.
2. El conjunto de los inversibles en R forman un grupo. Se suele notar $U(R)$.

Nota: Otro nombre para los elementos inversibles es *unidad* ó *unit*, en inglés, diferenciándose de *unity*, que es el nombre que recibe el elemento identidad. Es por eso que en éste texto *unidad* sólo refiere al elemento identidad.

2 Números Naturales

2.1 Suma de Gauss

Para todo $n \in \mathbb{N}$ vale que:

$$\sum_{k=1}^{n} k = 1 + 2 + \cdots + (n-1) + n = \frac{n(n+1)}{2}$$

2.2 Serie geométrica

Para todo $n \in \mathbb{N}$ y algún $q \in \mathbb{N}$ vale que:

$$\sum_{i=0}^{n} q^i = q^0 + q^1 + q^2 + \cdots + q^n = \begin{cases} n+1, & \text{si } q = 1 \\ \frac{q^{n+1}-1}{q-1} & \text{si } q \neq 1 \end{cases}$$

3 Combinatoria

3.1 Cardinalidad de un conjunto

3.2 Cantidad de funciones inyectivas

[3] Sean A_m y B_n conjuntos finitos, con m y n elementos respectivamente, donde $m \leqslant n$. Entonces la cantidad de funciones inyectivas $f : A_m \to B_n$ que hay es:

$$n \cdot (n-1) \cdots (n-m+1) = \frac{n!}{(n-m)!}$$

Cabe mencionar que no hay una fóormula tan simple como las anteriores para contar la cantidad de funciones sobreyectivas que hay de un conjunto A_n de n elementos en un conjunto B_m de m elementos, con $n \geqslant m$ cualesquiera. Existen fórmulas pero son más complicadas e involucran en general contar la cantidad de elementos de muchos conjuntos.

3.3 Número combinatorio

Sea $n \in N_0$ y sea A_n un conjunto con n elementos. Para $0 \leqslant k \leqslant n$, la cantidad de subconjuntos con k elementos del conjunto A_n, o equivalentemente, la cantidad de maneras que hay de elegir k elementos en el conjunto A_n, es:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

3.3.1 Forma recursiva

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

3.4 Binomio de Newton

La fórmula del binomio de Newton produce polinomios con los coeficientes correspondientes a los números del triángulo de Pascal, tal que:

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

Ejemplos:

$$(x+y)^0 = 1$$
$$(x+y)^1 = x+y$$
$$(x+y)^2 = x^2+2xy+y^2$$
$$(x+y)^3 = x^3+3x^2y+3xy^2+y^3$$
$$(x+y)^4 = x^4+4x^3y+6x^2y^2+4xy^3+y^4$$
$$(x+y)^5 = x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5$$

4 $\mathbb{Z}$ y $\mathbb{Z}/p\mathbb{Z}$

4.1 Ecuaciones de Congruencia

Para $a, c \in \mathbb{Z}$, las ecuaciones de la forma

$$aX \equiv c \text{ (mod m)}$$

Tienen solución si y sólo si $(a : m) = 1$

4.2 Inversibles en $\mathbb{Z}/n\mathbb{Z}$

[3] es un Corolario de las Ecuaciones de Congruencia.
Sea $n \in \mathbb{N}$ y $r \in \mathbb{Z}/n\mathbb{Z}$ entonces n es inversible si y solo si r es coprimo con n.

Es decir:

$$r \text{ inversible mod } n \iff rx = 1 \text{ (mod } n) \text{ tiene solución} \iff (r : n) = 1$$

Un corolario de esto es que si $r, p \in \mathbb{N}$ y *pprimo*, luego r siempre es inversible módulo p.

4.3 Pequeño Teorema de Fermat

1. Dados a, $p \in \mathbb{Z}$ y p primo, entonces:

$$a^p \equiv a \text{ (mod p)}$$

2. Además, si $p \nmid a$

$$a^{p-1} \equiv 1 \text{ (mod p)}$$

4.4 Función $\varphi(n)$ de Euler

Dado $n \in \mathbb{N}$, entonces:

$$\varphi(n) = n \prod_{p|n} 1 - \frac{1}{p}$$

4.5 Teorema de Euler

Si a, $n \in \mathbb{N}$ tal que $(a : n) = 1$, entonces

$$a^{\varphi(n)} \equiv 1 \text{ (mod n)}$$

4.6 Inverso multiplicativo módulo n

Si a, $n \in \mathbb{N}$ tal que $(a : n) = 1$ y a inversible, entonces

$$a^{-1} \equiv a^{\varphi(n)-1} \text{ (mod n)}$$

Demostración: Por Teorema de Euler sabemos que:

$$a^{\varphi(n)} \equiv 1 \text{ (mod n)}$$

Luego, multiplicando todo por a^-1 obtenemos:

$$a^{-1} \cdot a^{\varphi(n)} \equiv 1 \cdot a^{-1} \text{ (mod n)}$$

$$a^{\varphi(n)-1} \equiv a^{-1} \text{ (mod n)}$$

4.7 Potencias módulo m

Dados $a, n, m \in \mathbb{N}$, si a es invertible módulo m, entonces

$$a^n \equiv 0 \text{(mod m)}$$

Nunca tiene soluciones.

5 Números Complejos

5.1 Fórmula de De Moivre

Parte IV
Bibliografía

[1] Joseph A. Gallian. Contemporary Abstract Algebra. Textbooks in Mathematics. Chapman & HallCRC Press, 2017.

[2] Román Sasyk. Álgebra 1, primer cuatrimestre, 2022.

[3] Teresa Krick. Álgebra I. Cursos de grado. Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, 2017.