Resumen ALGEBRA I

Franco Pistasoli

December 23, 2009

1 Conjuntos, relaciones y funciones

1.1 Definiciones y propiedades

1.1.1 Propiedades de conjuntos

- $A - B = A \cap B^c$
- $A \triangle B = (A - B) \cup (B - A)$
- $A \subseteq B \iff B^c \subseteq A^c$
- *(Ley de De Morgan)* $(A \cap B)^c = A^c \cup B^c$
- *(Ley de De Morgan)* $(A \cup B)^c = A^c \cap B^c$

1.1.2 Conjunto de partes

El conjunto de partes $P(A)$ *es otro conjunto cuyos elementos son todos los subconjuntos de* A. *Si* n *es el cardinal de* A, *entonces* $\#P(A) = 2^n$.

1.1.3 Relación

Una relación R *de* A *en* B *es un subconjunto de* $A \times B$.

Propiedades de una relación: *Sea* $R : A \to B$,

- *Reflexividad:* $\forall a \in A,\ aRa$
- *Simetría:* $\forall a, b \in A,\ aRb \Rightarrow bRa$
- *Transitividad:* $\forall a, b, c \in A,\ aRb \wedge bRc \Rightarrow aRc$

- *Antisimetría:* $\forall a, b \in A,\ aRb \wedge bRa \Rightarrow a = b$

Relación de equivalencia: *Reflexiva, simétrica y transitiva.* Relación de orden: *Reflexiva, antisimétrica y transitiva.* Observación: $\emptyset$ *es simétrica, transitiva y antisimétrica, pero no es reflexiva.*

1.1.4 Partición

P es una partición de A si y sólo si se verifican las siguientes condiciones:

1. $P \neq \emptyset$
2. $x, y \in P \Rightarrow x \cap y = \emptyset$
3. $\forall a \in A,\ a \in P$

1.1.5 Clase de equivalencia

Sean R una relación de equivalencia en A y $a \in A$. Se define la clase de equivalencia C_a de a al conjunto $C_a = \{b \in A \,/\, bRa\}$

Propiedades:

1. $aRb \iff C_a = C_b$
2. *El conjunto de clases de equivalencia de A forman una partición de A.*
3. *Las particiones de A forman las clases de equivalencia de A.*

1.1.6 Función

Sean A y B conjuntos. Una función es una relación $f \subseteq A \times B$ tal que $\forall a \in A,\ \exists!\, b \in B$ tal que afb.

Clasificación de una función:

1. *Inyectiva:* $f(a) = f(b) \Rightarrow a = b$
2. *Suryectiva:* $\forall b \in B,\ \exists a \in A \,/\, f(a) = b$
3. *Biyectiva: si es inyectiva y suryectiva. Si f es biyectiva, $\exists f^{-1}$*

1.2 Teoremas más importantes

Proposición I: Sea R una relación de equivalencia en un conjunto A, y sean $a, b \in A$. Entonces $aRb \iff \exists c \in A \,/\, a, b \in C_c$.
Proposición II: Sea $f : A \to B$ una función. Entonces f es inversible si y sólo si f es biyectiva.

2 Números naturales. Principio de Inducción

2.1 Definiciones y propiedades

2.1.1 Algunas identidades

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$$\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1} \qquad a \neq 1, a \in \mathbb{N}$$

2.2 Teoremas más importantes

Binomio de Newton: Sean $a, b \in \mathbb{R}$. Entonces, $\forall n \in \mathbb{N}$

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

3 Combinatoria

3.1 Definiciones y propiedades

3.1.1 Bosones

La cantidad de maneras de ubicar k bolitas indistinguibles en n cajas numeradas es:

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

4 Números Enteros (Primera Parte)

4.1 Definiciones y propiedades

4.1.1 Propiedades de coprimos

Sean $a, b, c, d \in \mathbb{Z}$ y p un primo positivo.

- $(c:d)=1 \Rightarrow c|a \wedge d|a \iff cd|a$
- $(d:a)=1 \Rightarrow d|ab \iff d|b$
- $p \not| b \iff (p:b)=1$

4.1.2 Propiedades de divisibilidad

- $a|b+c \wedge a|b \Rightarrow a|c$
- $p|ab \Rightarrow p|a \vee p|b$
- $(a:b) \neq 1 \iff \exists p$ primo positivo tal que $p|a \wedge p|b$
- $a|b \Rightarrow a^n|b^n \, \forall n \in \mathbb{N}$
- $a-b|a^n-b^n \, \forall n \in \mathbb{N}$
- n par, $a+b|a^n-b^n$
- n impar, $a+b|a^n+b^n$
- $a \not| b \Rightarrow a^n \not| b \, \forall n \in \mathbb{N}$
- a impar, $2^{n+2}|a^{2^n}-1 \, \forall n \in \mathbb{N}$
- p, q primos distintos y $n \in \mathbb{N}$, $pq|a^n \Rightarrow pq|a$

4.1.3 Propiedades de máximo común divisor

- $(a:b)=1 \iff (a^n:b^n)=1$
- $(a:b)=d \iff (a^n:b^n)=d^n$
- $(a:b)=1 \Rightarrow (a:bc)=(a:c)$
- a y b no ambos nulos, $(\frac{a}{(a:b)}:\frac{b}{(a:b)})=1$
- $n, m \in \mathbb{N}$ y $a>1$, $(a^n-1:a^m-1)=a^{(n:m)}-1$
- $(a:b)\,[a:b]=|ab|$

4.2 Teoremas más importantes

Proposición I: Sea $a \in \mathbb{Z}, a \neq 1, -1$. Entonces existe un primo positivo p tal que $p|a$.
Teorema I: Existen infinitos primos.
Teorema II (Algoritmo de la división): Sean $a, b \in \mathbb{Z}, b \neq 0$. Entonces $\exists!\, q, r \in \mathbb{Z} \,/\, a = bq + r$ y $0 \leq r < |b|$
Teorema III (Máximo común divisor): Sean $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$. Entonces $\exists!\, d \in \mathbb{Z}$ tal que:

1. $d \in \mathbb{N}$
2. $d|a \wedge d|b$
3. Dado $c \in \mathbb{Z}$, si $c|a \wedge c|b \Rightarrow c|d$

Corolario: Sean $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$. Entonces $\exists t, s \in \mathbb{Z}$ tales que $(a : b) = at + bs$.
Proposición II (Algoritmo de Euclides): Sean $a, b \in \mathbb{Z}, b \neq 0$. Si $a = bq + r$, con $q, r \in \mathbb{Z}$, entonces $(a : b) = (b : r)$
Teorema IV (Mínimo común múltiplo): Sean $a, b \in \mathbb{Z}, a \neq 0 \wedge b \neq 0$. Entonces $\exists!\, m \in \mathbb{Z}$ tal que:

1. $m \in \mathbb{N}$
2. $a|m \wedge b|m$
3. Dado $c \in \mathbb{Z}$, si $a|c \wedge b|c \Rightarrow m|c$

5 Números Enteros (Segunda Parte)

5.1 Definiciones y propiedades

5.1.1 Congruencias

Sean $a, b, c \in \mathbb{Z}$ tales que $c \neq 0$. Entonces $a \equiv b \quad (c) \iff c|a - b$

Propiedad: $a \equiv b\,(c) \iff r_c(a) \equiv r_c(b) \quad (c)$

5.1.2 Ecuaciones diofánticas: Algoritmo

$$ax + by = c$$

1. *Hay solución* $\iff (a : b)|c$
2. *Coprimizamos la ecuación.*
3. *Buscamos una solución particular (Euclides o a ojo).*

4. *Buscamos las soluciones del sistema homogéneo, es decir* $ax + by = 0$

5. *La solución es* $S = \{$ *solución particular + solución del homogéneo* $\}$

5.1.3 Ecuaciones de congruencia: Algoritmo

$$ax \equiv c \quad (b)$$

1. *Reemplazo los coeficientes por sus restos módulo* b.

2. *Hay solución* $\iff (a:b)|c$

3. *Coprimizamos la ecuación.*

4. *Simplificamos todo lo que sea posible.*

5. *Buscamos una solución particular* x_0 *(Euclides o a ojo).*

6. *La solución es* $S = \{x \in \mathbb{Z} : x \equiv x_0 \quad (b')\}$, donde $b' = \frac{b}{(a:b)}$

5.1.4 Pequeño Teorema de Fermat (PTF)

Sean $a \in \mathbb{Z}$ *y* p *primo positivo. Entonces,*

- $a^p \equiv a \quad (p)$
- Si $p \not| a \Rightarrow a^{p-1} \equiv 1 \quad (p)$

Propiedad I: Si p es un primo positivo, entonces $((p-1)! : p) = 1$

Propiedad II: $a \in \mathbb{Z}, n \in \mathbb{N}, p$ primo positivo. Si $p \not| a$ entonces

$$n \equiv r_{p-1}(n) \quad (p-1) \Rightarrow a^n \equiv a^{r_{p-1}(n)} \quad (p)$$

Propiedad III: p, q primos positivos distintos. Si $(a : pq) = 1$, entonces

$$pq | a^{(p-1)(q-1)} - 1$$

Propiedad IV: p primo positivo, $p > 2, a \in \mathbb{Z}, p \not| a$. Entonces

$$p^n | a^{(p-1)p^{n-1}} - 1 \ \forall n \in \mathbb{N}$$

5.2 Teoremas más importantes

Lema I: Sea p un primo positivo y sea $a \in \mathbb{Z}$ tal que $p \not| a$. Entonces,

$$\{r_p(a), r_p(2a), ..., r_p((p-1)a)\} = \{1, 2, ..., p-1\}$$

Teorema I: Pequeño Teorema de Fermat (PTF).
Teorema II: Teorema Chino del Resto.

6 Números Complejos

6.1 Definiciones y propiedades

6.1.1 Raíces n-ésimas de un complejo

$w = |w|(\cos\alpha + i\sin\alpha),\ z \in \mathbb{C}\,/\,z^n = w, \alpha = \arg(w)$
$z_k = \sqrt[n]{|w|}\,(\cos\frac{\alpha+2k\pi}{n} + i\sin\frac{\alpha+2k\pi}{n})$ $\qquad k = 0, 1, ..., n-1$

6.1.2 Grupo de raíces n-ésimas de la unidad

$G_n = \{z \in \mathbb{C}\,/\,z^n = 1\}$
$z = \cos\frac{2k\pi}{n} + i\ \sin\frac{2k\pi}{n}$ $\qquad k = 0, 1, ..., n-1$

6.1.3 Raíz n-ésima primitiva de la unidad

$w \in G_n$ es una raíz n-ésima primitiva de la unidad si y sólo si:

- $w^d \neq 1 \qquad \forall d \in \{1, 2, ..., n-1\}$
- $w^k = 1 \Longleftrightarrow n|k$
- $n = \text{mín}\{k \in \mathbb{N}\,/\,w^k = 1\}$

Observación: *Las tres definiciones anteriores son equivalentes.*

6.1.4 Propiedades de G_n

Sean $n, m \in \mathbb{N}$,

- $G_n \cap G_m = G_{(n:m)}$
- $G_n \subseteq G_m \Longleftrightarrow n|m$

6.1.5 Propiedades de congruencias de complejos

Sea $w \in G_n$

- $\overline{w}^k = w^{-k} = w^{n-k}$
- $\overline{w} = w^{n-1} = w^{-1}$

6.1.6 Suma y producto de raíces complejas

1. La suma de las raíces n-ésimas de la unidad es 0
2. La suma de las raíces de G_n:

$$\sum_{i=0}^{n-1} w^i = \frac{w^n - 1}{w - 1} \qquad \forall w \in \mathbb{C} - \{1\}$$

3. El producto de las raíces n-ésimas de la unidad es $(-1)^{n-1}$

Sea p un primo positivo,

1. La suma de las raíces p-ésimas primitivas de la unidad es -1.
2. La suma de las raíces p^2-ésimas primitivas de la unidad es 0.
3. Sea q un primo distinto de p. Entonces, la suma de las raíces pq-ésimas primitivas de la unidad es 1.

6.1.7 Otras propiedades

- $\Re(z) = 0 \iff \overline{z} = -z$
- $\Im(z) = 0 \iff \overline{z} = z$

Observación: $\Re(z)$ *y* $\Im(z)$ *denotan, respectivamente, a la parte real y la parte imaginaria de* z.

6.2 Teoremas más importantes

Demostraciones de las propiedades de G_n mencionadas en este apartado.

7 Polinomios

7.1 Definiciones y propiedades

7.1.1 Propiedades para polinomios $f \in \mathbb{K}[X]$, donde $\mathbb{K}$ es cualquier conjunto de números: naturales, enteros, racionales, irracionales, reales, complejos.

1. f tiene todas sus raíces simples si y sólo si $(f : f') = 1$
2. $a \in \mathbb{K}[X]$ es raíz con multiplicidad n de $f \iff a$ es raíz de f y a es raíz de f' con multiplicidad $n-1$
3. $a \in \mathbb{K}[X]$ es raíz múltiple de $f \iff a$ es raíz de f y de f'
4. $(f : f')$ tiene **exactamente** las raíces con multiplicidad mayor que 1 de f
5. $\frac{f}{(f:f')}$ tiene las mismas raíces que f pero con multiplicidad 1.
6. Si $f, g \in \mathbb{K}[X]$ tienen raíces comunes $\Longrightarrow (f : g) \neq 1$ y $(f : g)$ tiene como raíces a las raíces comunes.

7.1.2 Propiedades para polinomios $f \in \mathbb{Z}[X]$

1. $f(x) = g(x)\, h(x)$ para algún $g, h \in \mathbb{Q}[X]$
2. Puede aplicarse el Teorema de Gauss.

7.1.3 Propiedades para polinomios $f \in \mathbb{Q}[X]$

1. Sean $a, b, c \in \mathbb{Q}$, $\sqrt{c} \in \mathbb{R} - \mathbb{Q}$, $c > 0$. Si $a + b\sqrt{c}$ es raíz de f, entonces $a - b\sqrt{c}$ también lo es.

7.1.4 Propiedades para polinomios $f \in \mathbb{R}[X]$

1. Sea $z_0 \in \mathbb{C}$. Si z_0 es raíz de f entonces $\overline{z_0}$ también lo es.
2. f es irreducible en $\mathbb{R}[X]$ si y sólo si $gr(f) = 1$ ó 2

7.1.5 Propiedades para polinomios $f \in \mathbb{C}[X]$

1. **Teorema Fundamental del Álgebra:** Si $gr(f) \geq 1$, entonces $\exists \alpha \,/\, f(\alpha) = 0$
2. Si $gr(f) = n$ entonces f tiene n raíces en $\mathbb{C}$ contadas con multiplicidad.
3. Sean $g \in \mathbb{C}[X]$ y $a \in \mathbb{C}$. Entonces, a es raíz de f y g si y sólo si a es raíz de $(f : g)$
4. f es irreducible en $\mathbb{C}[X]$ si y sólo si $gr(f) = 1$
5. Si α es raíz de f, entonces $\overline{\alpha}$ es raíz de $\phi(X) = \overline{z_0} + \overline{z_1}X + \overline{z_2}X^2 + ... + \overline{z_n}X^n$

7.1.6 Suma de raíces para polinomios de grado n

Sea $f = X^n + a_{n-1}X^{n-1} + ... + a_0$ (f mónico). Entonces,

$$a_{n-1} = -\sum_{i=1}^{n} \alpha_i \qquad\qquad \textit{donde } \alpha_i \textit{ son las raíces de } f$$

$$a_0 = (-1)^n \prod_{i=1}^{n} \alpha_i \qquad\qquad \textit{donde } \alpha_i \textit{ son las raíces de } f$$

7.2 Teoremas más importantes

Proposición I: Sea $f \in \mathbb{K}[X], f \neq 0$. Si $gr(f) = 1$ entonces f es irreducible.
Proposición II: Sea $f \in \mathbb{K}[X], f \neq 0$. Si $gr(f) > 0$ entonces $\exists h \in \mathbb{K}[X]$ irreducible tal que $h|f$
Teorema I (Algoritmo de la división para polinomios): Sean $f, g \in \mathbb{K}[X], g \neq 0$. Entonces $\exists!\, q, r \in \mathbb{K}[X]$ tales que $f = gq + r$ y $r = 0$ ó $gr(r) < gr(g)$
Teorema II (Teorema del Resto): Sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces, el resto de la división de f por $x - a$ es $f(a)$
Teorema III (Máximo común divisor para polinomios): Sean $f, g \in \mathbb{K}[X], f \neq 0 \vee g \neq 0$. Entonces, $\exists!\, d \in \mathbb{K}[X]$ tal que:

1. d es mónico.
2. $d|f \wedge d|g$
3. Dado $h \in \mathbb{K}[X]$, si $h|f \wedge h|g \Rightarrow h|d$

Proposición III (Algoritmo de Euclides): Sean $f, g \in \mathbb{K}[X], g \neq 0$. Si $f = gq + r$, con $q, r \in \mathbb{K}[X]$, entonces $(f : g) = (g : r)$
Teorema IV (Teorema de Gauss): Sea $f \in \mathbb{Z}[X],\ f = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$, con $a_n \neq 0$, y sean $p \in \mathbb{Z}$ y $q \in \mathbb{N}$ tales que $(p : q) = 1$. Si $\frac{p}{q}$ es raíz de f entonces $p|a_0, q|a_n$ y $p - kq|f(k)\, \forall k \in \mathbb{Z}$
Proposición IV: Sean $f \in \mathbb{R}[X]$ y $z \in \mathbb{C}$. Entonces z es raíz de f si y sólo si $\overline{z}$ es raíz de f.
Proposición V (Consecuencia inmediata del Teorema del Resto): Sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces a es raíz de f si y sólo si $x - a|f$
Corolario: Sea $f \in \mathbb{K}[X]$ tal que $gr(f) \geq 2$. Si f es irreducible en $\mathbb{K}[X]$ entonces f no tiene raíces en $\mathbb{K}[X]$.
Proposición VI: Sean $f, g \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces a es raíz de f y de g si y sólo si a es raíz de $(f : g)$
Corolario: Sean $f, g \in \mathbb{C}[X]$. Entonces f y g no tienen raíces comunes en $\mathbb{C}$ si y sólo si $(f : g) = 1$. **Sugerencia: usar el contrarrecíproco para probar este corolario.**
Proposición VII: Sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$. Entonces, dado $m \in \mathbb{N}, m \geq 2$ se verifica: a es raíz de f de multiplicidad $m \iff f(a) = 0$ y a es raíz de f' de multiplicidad $m - 1$.

Proposición VIII: Sea $f \in \mathbb{K}[X]$, y sea $a \in \mathbb{K}$. Entonces, dado $m \in \mathbb{N}$ se verifica: a es raíz de f de multiplicidad $m \iff f^{(k)}(a) = 0\,\forall 0 \leq k \leq m-1$ y $f^{(m)}(a) \neq 0$
Corolario: Sea $f \in \mathbb{Q}[X]$. Si f es irreducible en $\mathbb{Q}[X]$, entonces todas las raíces de f en $\mathbb{C}$ son simples.