Capítulo 6

Polinomios

6.1 Construcción

Definición 6.1.1 (Variable)**.** Definimos una variable como un símbolo o letra (signo) que representa a un objeto matemático que cumple una condición dada

Definición 6.1.2 (Variable numérica)**.** Definimos una variable numérica como una variable que representa un número de algún subconjunto de algún conjunto numérico $\mathbb{M}$.

Notación 6.1.3. A partir de ahora tomaremos a las letras del alfabeto como variables numéricas: "$x, y, z, \alpha, \beta, \omega, \theta, \gamma, ...$"

Comentario 6.1.4. Una variable es una representación de un conjunto de números, en ese sentido, si el conjunto es unitario, la variable representa a un número. Podemos tomar esta variable como dicho número. Es decir, podemos interpretar a los números como variables

A partir de ahora, tomaremos como conjunto de variables iniciales escogidas con respecto a un conjunto numérico $\mathbb{M}$ al conjunto X y a la de variables del conjunto numérico $\mathbb{M}$ como Var.

Definición 6.1.5. Una variable cuyo valor es único se dice constsnte

Ejemplo 6.1.6. La variable x que representa al conjunto $\{1\}$ es una constante y para efectos prácticos (cuando consideremos las operaciones de variables) es el mismo 1

Definición 6.1.7 (Operaciones de Variables)**.** Sean x, y variables numéricas en el conjunto de números $\mathbb{M}$. Sea $f : \mathbb{M}^m \to \mathbb{M}$ una operación de $\mathbb{M}$ y k un número en $\mathbb{M}$. Definimos:

1. Una operación de variables $\bar{f} : Var^m \to Var$ inducida por la variable f es aquella que opera sobre dos variables de la siguiente forma: La variable resultante representa a los números que cumplen que son los resultados de operar de números que son representados por x y números que son representados por y. Esto es:

$$\bar{f}(x_1, \dots, x_m) \sim \{f(a_1, \dots, a_m) \in \mathbb{M} : x_i \sim a_i\}$$

2. Una operación variable-número $\mathring{f} : Var \times \mathbb{M} \to Var$ inducida por f es aquella función que opera de la siguiente forma: Los números que cumplen son los resultados de operar números representados por x y el número k.

$$\forall k \in \mathbb{M}, \overset{\circ}{f}(x,k) \sim \{f(a,k) \in \mathbb{M} : a \in x\}$$

Ejemplo 6.1.8. El ejemplo más típico es a partir de las operaciones en $\mathbb{Z}$. A saber: Dados x, y variables numéricas en $\mathbb{Z}$, $n \in \mathbb{Z}$: $x + y$, $x.y$, nx, x^n son resultados de operar variables entre sí y variable-número respectivamente. $(x^n = \bar{\times}^{n}(x, \cdot)(1))$

Comentario 6.1.9. Notamos que las variables no son conjuntos, aunque pueden relacionarse con estos en el sentido de que son representantes de los objetos en el conjunto. Por eso en la definición anterior, no es correcto escribir $=$, sino que usamos la notación auxiliar $\sim$.

Cabe recalcar que la definición anterior no depende de que el conjunto sea numérico, sino que basta tomar un conjunto con sus respectivas operaciones $(A, \{f_i\}_{i\in I})$

Definición 6.1.10 (Generado)**.** Sea X variables de $(A, \{f_i\}_{i\in I})$ conjunto (no necesariamente numérico) con sus operaciones. Decimos que el generado de X es el conjunto de todas las imágenes de todas las composiciones de operaciones sobre el conjunto de variables. Es decir:

$$\langle X\rangle := \bigcup_{n\in\mathbb{N}} \bigcup_{j\in I^n} \bigcirc_{r=1}^{n} \bar{f}_{\pi_r(j)}(X)$$

Donde π_r proyección canónica ($r-$ésima coordenada) y $\bar{f}_\alpha(B) = \bar{f}_\alpha(B^{m(\alpha)})$ para todo $B \subseteq Var$ con m función que asigna a cada índice la cantidad de argumentos de su función asociada

Comentario 6.1.11. El generado se puede interpretar como el conjunto de todos los objetos resultado de haber manipulado las variables con nuestras operaciones. Una variable está en el generado si existe una cantidad finita de pasos y una cantidad finita de operaciones aplicadas para cada paso, de forma que esta variable sea resultado de haber aplicado dichas operaciones sobre el conjunto de variables reiteradas veces.

Podemos considerar a la identidad Id_A como una operación propia de cualquier conjunto, de donde se tiene $X \subseteq \langle X\rangle$. En lo sucesivo asumiremos que la identidad forma parte de las operaciones, así no sea escrito.

Ejemplo 6.1.12. El generado de $\{x\}$ en $(\mathbb{M}, \{\times(a, \cdot)\}_{a\in\mathbb{M}})$

$$\begin{aligned}
\langle\{x\}\rangle &= \bigcup_{n\in\mathbb{N}} \bigcup_{j\in I^n} \bigcirc_{r=1}^{n} \bar{\times}\,(a_{\pi_r(j)}, \cdot)(\{x\}) \\
&= \{ax\}_{a\in\mathbb{M}} \cup \bigcup_{n\in\mathbb{N}-1} \bigcup_{j\in\mathbb{M}^{n-1}} \bigcirc_{r=1}^{n-1} \bar{\times}\,(a_{\pi_r(j)}, \cdot)(\{ax\}_{a\in\mathbb{M}}) \\
&= \bigcup_{n\in\mathbb{N}} \{\Pi_{i=1}^{n} a_i x : a_i \in \mathbb{M}\} \\
&= \{ax : a \in \mathbb{M}\}
\end{aligned}$$

Proposición 6.1.13 (Generado Invariante)**.** *El generado es invariante bajo las operaciones del conjunto sobre el cual se construye. Es decir:*

$$x_1, \ldots, x_m \in \langle X \rangle \Rightarrow f(x_1, \ldots, x_m) \in \langle X \rangle$$

Proof. Por definición de generado. □

Definición 6.1.14. El generado de un conjunto es el generado por variables constantes asociadas a un conjunto dado.

Notación 6.1.15. Cuando nos refiramos al generado de un conjunto de variables unitario $\{x\}$, usaremos la expresión $\langle x \rangle$

De manera similar, cuando sea una cantidad finita, podemos usar $\langle x_1, \ldots, x_n \rangle$

Ejemplo 6.1.16. Vemos que el generado de 4 y 5 en $(\mathbb{N}, +)$ es:

$$\begin{aligned}
\langle 4, 5 \rangle &:= \bigcup_{n \in \mathbb{N}} \bigcup_{j \in I^n} \bigcirc_{r=1}^{n} \bar{+} (\{4, 5\}) \\
&= \{4, 5, 4+5\} \cup \bigcup_{n \in \mathbb{N}} \bigcirc_{r=1}^{n-1} \bar{+} (\{4, 5, 4+5\}) \\
&= \{4, 5, 4+5, 4+4, 4+4+5, 5+5, 4+5+5, 4+5+4+5\} \\
&\cup \bigcup_{n \in \mathbb{N}} \bigcirc_{r=1}^{n-2} \bar{+} (\{4, 5, 4+5, 4+4, 4+4+5, 5+5, 4+5+5, 4+5+4+5\}) \\
&= \{4n + 5m : n, m \in \mathbb{N}\} = 4\mathbb{N} + 5\mathbb{N}
\end{aligned}$$

De modo análogo $\langle 4 \rangle = 4\mathbb{N}$ y $\langle 4, 5 \rangle$ en $(\mathbb{Z}, +, -, \cdot)$ es $\{4n + 5m : n, m \in \mathbb{Z}\}$, y por identidad de Bezout es el mismo $\mathbb{Z}$

Proposición 6.1.17 (Generado de un conjunto de números)**.** *El generado de un conjunto de variables constantes resulta en el mismo conjunto que el generado por un conjunto de números.*

Demostración. Resulta de la igualdad del conjunto con respecto a su posible valor. □

Proposición 6.1.18 (Generado bajo sumas)**.** *El generado de una variable numérica x bajo suma resulta de la forma $\bigcup_{n \in \mathbb{N}} \{nx\}$*

Demostración.

$$\begin{aligned}
\langle x \rangle &= \{x\} \cup \bigcup_{n \in \mathbb{N}} \bigcup_{j \in I^n} \bigcirc_{r=1}^{n} \bar{+} (\{x\}) \\
&= \{x\} \cup \bigcup_{n \in \mathbb{N}} \bigcirc_{r=1}^{n} \bar{+} (\{x\}) \\
&= \{x\} \cup \{x, 2x\} \cup \bigcup_{n \in \mathbb{N} - \{1\}} \bigcirc_{r=1}^{n-1} \bar{+} (\{x, 2x\}) \\
&= \{nx\}_{n \in \mathbb{N}} = \mathbb{N}x
\end{aligned}$$

□

Proposición 6.1.19 (Generado bajo producto)**.** *El generado de una variable numérica x bajo producto resulta de la forma $\bigcup_{n \in \mathbb{N}} \{x^n\}$*

Demostración. Análoga a la de la suma □

Definición 6.1.20 (Monomio en una variable)**.** Sea x una variable numérica. Definimos un monomio como la imagen de la composición de la operación entre variable y número inducida por la potencia con la operación entre variable y número inducida producto. Esto es, una variable de la forma

$$ax^n = a \cdot (x^n) = \overset{\circ}{\times}(\overset{\circ}{\hat{}}\,(x, n), a)$$

Un monomio en dos variables es un monomio en una variable construido sobre el conjunto de monomios en una variable.

De forma recursiva se construye para el conjunto de monomios en una cantidad arbitraria de variables

Comentario 6.1.21. Si bien la definición anterior es correcta en el conjunto $(\mathbb{M}, \overset{\circ}{\hat{}}\,(\cdot, n), \overset{\circ}{\times})$ a partir de un conjunto dado, podemos aprovechar la definición de generado para lograr explicar de forma más concisa (y general) la naturaleza de monomios/polinomios

Proposición 6.1.22 (Conjunto de Monomios)**.** *El conjunto de monomios sobre el conjunto de variables X es el generado de X en $(\mathbb{M}, \times, \{\times(a, \cdot)\}_{a\in\mathbb{M}})$. Al reducirse a una variable cada elemento es un monomio en una variable y al iterar con respecto al conjunto de monomios en una variable definido como antes, ambas definiciones coinciden*

Demostración. El conjunto de monomios tiene la forma: $\{a \cdot x^n : a \in \mathbb{M}, n \in \mathbb{N}\}$

De donde el generado verifica por ejemplo anterior y proposición anterior. □

Definición 6.1.23 (Polinomio en una variable)**.** Sea x una variable numérica. Decimos que p (variable numérica) es un polinomio en una variable si es una suma de monomios.

De manera análoga al caso del monomio se define el polinomio de varias variables.

Definición 6.1.24 ($\mathbb{M}[X]$)**.** Se puede tomar al conjunto de polinomios sobre el conjunto de variables X como el generado de X en $(\mathbb{M}, +, \times, \{\times(a, \cdot)\}_{a\in\mathbb{M}})$. En este caso se denota al conjunto de polinomios con respecto a las variables X como $\mathbb{M}[X]$.

Ejemplo 6.1.25. Tomemos los monomios: $4x^2, 3x^7, 2x^2, 9x, x^4, 1$

El polinomio que resulta de sumar todos estos es: $4x^2 + 3x^7 + 2x^2 + 9x + x^4 + 1$

Ahora, sabemos que esto representa un número entero. Por propiedad distributiva, podemos agrupar términos con el x^n en común. Es decir: $ax^n + bx^n = (a + b).x^n$

De donde, ordenando el polinomio y agrupando tenemos:

$4x^2 + 3x^7 + 2x^2 + 9x + x^4 + 1 = 3x^7 + x^4 + (4+2)x^2 + 9x + 1 = 3x^7 + x^4 + 6x^2 + 9x + 1$

Definición 6.1.26 (Álgebra de términos)**.** El mínimo conjunto de la clase de variables de un conjunto numérico que verifique que contiene al generado y es cerrado bajo las operaciones que constituyen al generado se dice el álgebra de términos asociada al conjunto de variables y al conjunto numérico. Dicho conjunto se denota por $\mathcal{T}_{\mathbb{M}}(X)$

Notación 6.1.27 (Notación de Polinomios)**.** Escribimos $\mathbb{M}[X] := \{p \in \mathcal{T}_{\mathbb{M}}(X) : p = \sum_{\text{finita}} a_i x_i^{n_i}\}$ conjunto de polinomios en una cierta cantidad de variables

Definición 6.1.28 (Función polinomial)**.** Decimos que una función $p : \mathbb{M} \to \mathbb{M}$ es una función polinomial si su regla de correspondencia es la de reemplazar en las variables de un polinomio el número de entrada. En este caso escribimos el polinomio como $p(\{x_i\}_{i=1}^n) = \sum_{i=1}^n a_i \Pi_{j=1}^{m(i)} x_j^{n_j}$.

Ejemplo 6.1.29. Pongamos $p(x) = 4x^2 + 7x$. podemos determinar sus imágenes de forma análoga a: $p(3) = 4 \times (3)^2 + 7 \times 3 = 4 \times 9 + 21 = 57$.

Definición 6.1.30 (Coeficientes)**.** Los números que multiplican a cada monomio en la escritura de polinomio son conocidos como coeficientes del monomio.

6.2 Identidades

Definición 6.2.1 (Igualdad de Polinomios)**.** Dos polinomios $p, q \in \mathbb{M}[X]$ se dicen iguales si sus coeficientes son idénticos con respecto a sus monomios. Es decir, si tienen la misma escritura.

Definición 6.2.2 (Identidad)**.** Decimos que una identidad es una igualdad de polinomios (que resulta de nuestras propiedades algebraicas) conveniente.

Dicha igualdad se verifica como proposición y se denota por $\mathbb{M} \vDash p = q$

Es decir, en el conjunto numérico $\mathbb{M}$, se verifica que los polinomios p y q con sus respectivas variables X son iguales

Notación 6.2.3. La igualdad depende de las propiedades, y por tanto de las operaciones, algebraicas. Por tanto están estrictamente asociadas al conjunto y las operaciones definidas sobre él. Por tanto, dado un álgebra $\mathcal{A} = \langle A, \mathcal{F} \rangle$ escribiremos que una identidad dada $p = q$ se cumple en $\mathcal{A}$ como $\mathcal{A} \vDash p = q$

Proposición 6.2.4. *Se cumplen las siguientes identidades:*

1. $(x + y)^2 = x^2 + 2xy + y^2$
2. $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$
3. *(Binomio de Newton)* $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$
4. *(Diferencia de cuadrados)* $(x + y)(x - y) = x^2 - y^2$
5. *(Identidad de Legendre)* $(x + y)^2 + (x - y)^2 = 2x^2 + 2y^2$
6. *(Identidad de Legendre 2)* $(x + y)^2 - (x - y)^2 = 4xy$
7. $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$
8. $\forall n \in 2\mathbb{N}\,,\ x^{n+1} + y^{n+1} = (x + y)\left(\sum_{i=0}^{n} (-1)^i x^{n-i} y^i\right)$

   (Equivalentemente podemos escribir:
9. $\forall n \in 2\mathbb{N} + 1\,,\ x^n + y^n = (x + y)\left(\sum_{i=0}^{n-1} (-1)^i x^{n-1-i} y^i\right)$

10. $x^{n+1} - y^{n+1} = (x-y)\left(\sum_{i=0}^{n} x^{n-i}y^i\right)$

Demostración. 1. $(x+y)^2 = x^2 + 2xy + y^2$

2. $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$

3. (Binomio de Newton) $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$

4. (Diferencia de cuadrados) $(x+y)(x-y) = x^2 - y^2$

5. (Identidad de Legendre) $(x+y)^2 + (x-y)^2 = 2x^2 + 2y^2$

6. (Identidad de Legendre 2) $(x+y)^2 - (x-y)^2 = 4xy$

7. $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$

8. $\forall n \in 2\mathbb{N}\,,\ x^{n+1} + y^{n+1} = (x+y)\left(\sum_{i=0}^{n}(-1)^i x^{n-i}y^i\right)$

   (Equivalentemente podemos escribir:

9. $\forall n \in 2\mathbb{N}+1\,,\ x^n + y^n = (x+y)\left(\sum_{i=0}^{n-1}(-1)^i x^{n-1-i}y^i\right)$

10. $x^{n+1} - y^{n+1} = (x-y)\left(\sum_{i=0}^{n} x^{n-i}y^i\right)$

□

6.3 Ecuaciones

Definición 6.3.1 (Ecuación)**.** Una ecuación es un problema matemático que consiste en hallar uno u varios objetos matemático cumpliendo una condición o propiedad.

El objeto que cumpla la condición se llama solución de la ecuación

El conjunto de todas las soluciones de una ecuación se dice conjunto solución

Comentario 6.3.2. Dado que el problema consiste en hallar todos los objetos tal que se cumple algo, podemos escribir la ecuación en forma conjuntista como el conjunto de todos los objetos que cumple dicha propiedad. Es decir, escribimos:

$$S = \{\alpha \in A : p(\alpha)\}$$

Dicho conjunto es el conjunto solución y la ecuación es el problema de determinar S mediante alguna otra propiedad más explícita.

Definición 6.3.3 (Ecuación algebraica)**.** Una ecuación algebraica es una ecuación que tienen la forma $P(x) = 0$ para algún (o algunos) polinomio(s) $P(x)$. Es decir, es una ecuación cuya solución es el conjunto de números que son envíados al 0 vía alguna función polinomial.