Álgebra Abstracta y Codificación

Clase 3: Polinomios, relaciones de equivalencia

by

Mauro Artigiani

14 agosto 2020

Polinomios

Polinomios

Un polinomio en al variable x es una fórmula del tipo

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0,$$

donde los a_i son números y pedimos que $a_n \neq 0$. El grado del polinomio es el exponente más alto de la variable x. Por ejemplo: $\deg p(x) = n$. El polinomio $p(x) = 0$ por definición no tiene grado.

Polinomios

Un polinomio en al variable x es una fórmula del tipo

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0,$$

donde los a_i son números y pedimos que $a_n \neq 0$. El grado del polinomio es el exponente más alto de la variable x. Por ejemplo: $\deg p(x) = n$. El polinomio $p(x) = 0$ por definición no tiene grado. Un polinomio define una función:

$$c \mapsto p(c) = \sum_{i=0}^{n} a_n c^n.$$

Polinomios

En general, es bueno distinguir entre la escritura de un polinomio y la función que define. De hecho

- Si dos polinomios son idénticos, pero uno tiene x como variable y otro y como variable, ¿son el *mismo* polinomio?
- Si dos polinomios dan origen a la misma función, ¿son el *mismo* polinomio?

Estas preguntas son más difíciles de lo que parece.

División entre polinomios

Como en los naturales, existe la división, con residuo, entre los polinomios.

División entre polinomios

Como en los naturales, existe la división, con residuo, entre los polinomios. Dados dos polinomios $f(x)$ y $g(x)$, con $g(x) \neq 0$, existen dos polinomios $q(x)$ y $r(x)$ tales que:

- $f(x) = g(x)q(x) + r(x)$;
- si el residuo $r(x) \neq 0$ se tiene $\deg r(x) < \deg g(x)$.

Esto será muy importante más adelante en el curso.

División entre polinomios

Ejemplo

$$
\begin{array}{rrrr|l}
x^3 & +x^2 & & -1 & x-1 \\
\cline{5-5}
-x^3 & +x^2 & & & x^2+2x+2 \\
\cline{1-2}
 & 2x^2 & & & \\
 & -2x^2 & +2x & & \\
\cline{2-3}
 & & 2x & -1 & \\
 & & -2x & +2 & \\
\cline{3-4}
 & & & 1 &
\end{array}
$$

Es decir, si $f(x) = x^3 + x^2 - 1$ y $g(x) = x - 1$, hay $q(x) = x^2 + 2x + 2$ y $r(x) = 1$.

Teorema del residuo

Teorema del residuo

El residuo de la división de un polinomio $f(x)$ por el polinomio $x - c$ es $f(c)$.

Teorema del residuo

Teorema del residuo

El residuo de la división de un polinomio $f(x)$ por el polinomio $x - c$ es $f(c)$.

Demostración

Se tiene $f(x) = (x - c)q(x) + r(x)$. Sabemos que $\deg r(x) < 1 = \deg(x - c)$. Substituyendo $x = c$ obtenemos $f(c) = r(c)$. $\square$

Hay un caso especial del teorema que es muy útil

Corolario (Teorema del factor)

Sea $f(x)$ un polinomio. El polinomio $x - c$ divide $f(x)$ si y solo si $f(c) = 0$

Polinomios irreducibles

Un polinomio no constante es irreducible si no se puede escribir como producto de dos polinomios de grado menor. Esto *depende* del conjunto numérico en donde viven los coeficientes del polinomio.

Polinomios irreducibles

Un polinomio no constante es irreducible si no se puede escribir como producto de dos polinomios de grado menor. Esto *depende* del conjunto numérico en donde viven los coeficientes del polinomio.
Por ejemplo $x^2 + 1$ es irreducible en $\mathbb{R}$, ya que debería tener factores de grado 1. Los polinomios de grado 1 se anulan en un punto. Pero $x^2 + 1 \neq 0$ para cualquier $x \in \mathbb{R}$.

Polinomios irreducibles

Un polinomio no constante es irreducible si no se puede escribir como producto de dos polinomios de grado menor. Esto *depende* del conjunto numérico en donde viven los coeficientes del polinomio.
Por ejemplo $x^2 + 1$ es irreducible en $\mathbb{R}$, ya que debería tener factores de grado 1. Los polinomios de grado 1 se anulan en un punto. Pero $x^2 + 1 \neq 0$ para cualquier $x \in \mathbb{R}$.
En los complejos se tiene $x^2 + 1 = (x - i)(x + i)$.

Polinomios irreducibles

Todos los polinomios de grado 1 son irreducibles (¿por qué?).

Polinomios irreducibles

Todos los polinomios de grado 1 son irreducibles (¿por qué?).
Un polinomio de grado 2 o 3 es irreducible si y solo si no tiene ceros (ejercicio).

Polinomios irreducibles

Todos los polinomios de grado 1 son irreducibles (¿por qué?).
Un polinomio de grado 2 o 3 es irreducible si y solo si no tiene ceros (ejercicio).
Un polinomio de grado 4 o mayor puede ser reducible sin tener ceros. Por ejemplo: $x^4 + 2x^2 + 1 \neq 0$ para cualquier $x \in \mathbb{R}$, pero $x^4 + 2x^2 + 1 = (x^2 + x + 1)^2 = (x^2 + x + 1)(x^2 + x + 1)$.

Relaciones y relaciones de equivalencia

Relaciones

Una relación R sobre un conjunto A es un subconjunto del producto cartesiano $A \times A$.

Relaciones

Una relación R sobre un conjunto A es un subconjunto del producto cartesiano $A \times A$.
Dados $a, b \in A$ escribimos aRb si $(a, b) \in R \subseteq A \times A$ y decimos que *a está en relación* R con b.

Relaciones

Una relación R sobre un conjunto A es un subconjunto del producto cartesiano $A \times A$.
Dados $a, b \in A$ escribimos aRb si $(a, b) \in R \subseteq A \times A$ y decimos que *a está en relación R* con b.

Ejemplo

En los reales hay la relación "menor o igual", que se denota $\leq$.
Vivir en el mismo barrio es una relación entre los estudiantes de esta clase.

Relaciones de equivalencia

Dada una relación R sobre un conjunto A decimos que R es

- Reflexiva si para todos $a \in A$ se tiene aRa;
- Simétrica si aRb implica bRa;
- Transitiva si aRb y bRc implican aRc.

Relaciones de equivalencia

Dada una relación R sobre un conjunto A decimos que R es

- Reflexiva si para todos $a \in A$ se tiene aRa;
- Simétrica si aRb implica bRa;
- Transitiva si aRb y bRc implican aRc.

Una relación que sea reflexiva, simétrica y transitiva se dice una relación de equivalencia.

Dada una relación de equivalencia R sobre A, definimos la clase de equivalencia de un elemento a (con respecto a la relación R) de la siguiente manera

$$[a]_R = \{b \in A, aRb\}.$$

Particiones

Dado un conjunto A una partición $\{A_1, A_2, \ldots\}$ es una colección de subconjuntos de A que satisface

1. $A_i \neq \varnothing$ para todos i;
2. Se tiene $\cup_i A_i = A$;
3. $A_i \cap A_j = \varnothing$ para todos $i \neq j$.

Particiones

Dado un conjunto A una partición $\{A_1, A_2, \dots\}$ es una colección de subconjuntos de A que satisface

1. $A_i \neq \varnothing$ para todos i;
2. Se tiene $\cup_i A_i = A$;
3. $A_i \cap A_j = \varnothing$ para todos $i \neq j$.

Teorema

Sea R una relación de equivalencia sobre un conjunto A. Entonces la colección de clases de equivalencia respecto a R es una partición de A.

Por otro lado, dada una partición $\{A_1, A_2, \dots\}$ de A existe una (única) relación de equivalencia R sobre A cuya clases de equivalencia son exactamente $A_1, A_2, \dots$.

Un ejemplo importante

Una relación importante

Un ejemplo importante de relación de equivalencia es la relación ser congruente módulo un entero.

Una relación importante

Un ejemplo importante de relación de equivalencia es la relación ser congruente módulo un entero.
Consideramos el conjunto de los enteros. Sea $m \geq 2$ un entero.
Decimos que dos enteros a y b son congruentes módulo m si y solo si

$$m \mid (b - a).$$

En este caso escribimos $b \equiv a \mod m$, o $b \equiv a \pmod{m}$.

Una relación importante

Un ejemplo importante de relación de equivalencia es la relación ser congruente módulo un entero.
Consideramos el conjunto de los enteros. Sea $m \geq 2$ un entero.
Decimos que dos enteros a y b son congruentes módulo m si y solo si

$$m \mid (b - a).$$

En este caso escribimos $b \equiv a \mod m$, o $b \equiv a \pmod{m}$.

Proposición

La relación ser congruente módulo m es una relación de equivalencia.

Una relación importante

Demostración

Empezamos demostrando *reflexividad*.

Dado un entero $a \in \mathbb{Z}$ se tiene $a - a = 0 = m \cdot 0$. Por eso $a \equiv a \mod m$.

Una relación importante

Demostración

Empezamos demostrando *reflexividad*.

Dado un entero $a \in \mathbb{Z}$ se tiene $a - a = 0 = m \cdot 0$. Por eso $a \equiv a \mod m$.

Ahora mostramos *simétria*.

Sean a y b dos enteros con $a \equiv b \mod m$. Por definición se tiene $m \mid (b - a)$, entonces existe un entero q tal que $b - a = mq$.

Equivalentemente

$$a - b = -mq = m(-q).$$

Es decir $m \mid (a - b)$, lo que nos dice $b \equiv a \mod m$.

Una relación importante

Demostración

Finalmente, mostramos *transitividad*.
Sean a, b y c tres enteros tales que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$. Entonces existen enteros q y s tales que $b - a = mq$ y $c - b = ms$. Tenemos

$$c-a = c-b+b-a = (c-b)+(b-a) = ms+mq = m(s+q) = mt.$$

Es decir $m \mid (c - a)$ y por esto $a \equiv c \mod m$. □

Dos ejemplos

Sea $m = 2$. La relación ser congruente módulo 2 es una manera complicada de decir si los dos números tienen la misma *paridad*.

Dos ejemplos

Sea $m = 2$. La relación ser congruente módulo 2 es una manera complicada de decir si los dos números tienen la misma *paridad*.
Sea $m = 4$ Ya sabemos que ser congruente módulo 4 es una relación de equivalencia. Las clases de equivalencia son la siguientes:

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

Dos ejemplos

Sea $m = 2$. La relación ser congruente módulo 2 es una manera complicada de decir si los dos números tienen la misma *paridad*.
Sea $m = 4$ Ya sabemos que ser congruente módulo 4 es una relación de equivalencia. Las clases de equivalencia son la siguientes:

$$
\begin{aligned}
[0] &= \{\dots, -8, -4, 0, 4, 8, \dots\} \\
[1] &= \{\dots, -7, -3, 1, 5, 9, \dots\} \\
[2] &= \{\dots, -6, -2, 2, 6, 10, \dots\} \\
[3] &= \{\dots, -5, -1, 3, 7, 11, \dots\}
\end{aligned}
$$

En general, hay m clases de equivalencia módulo m. Son exactamente las clases $[0]$, $[1]$, $\dots$, $[m-1]$ (ejercicio).