UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA MATEMÁTICA

Álgebra III
525201
9 de abril de 2025
Prof.: Anahí Gajardo

Enteros y polinomios

1. Enteros

Recordemos un teorema importante, aunque simple.

Teorema 1 (division entera) *Para todo par de enteros a, b, con $b \neq 0$ existe un único par de enteros d, r, tales que:*

- $a = db + r$, *y*
- $0 \leq r < b$.

El número d es llamado cuociente y r resto.

Recordemos ahora algunas definiciones clásicas.

Definición 1 *Dados dos enteros m, n, decimos que $m \mid n$ si y solo si $\exists k \in \mathbb{Z}, mk = n$. En otras palabras, si el resto de dividir n por m es 0.*

Definición 2 *Dados dos naturales a, b, se define lo siguiente.*

- $a \neq 1$ *es primo si* $\forall c \in \mathbb{Z} \setminus \{a, 1\}, c \nmid a$.
- $MCD(a, b) = g$ *si y solo si*
  - $g \mid a$ *y* $g \mid b$, *y*
  - *para todo c tal que $c|a$ y $c|b$, se cumple $c|g$.*
- *a y b son primos relativos si* $mcd(a, b) = 1$.
- $MCM(a, b) = g$ *si y solo si*
  - $a \mid g$ *y* $b \mid g$, *y*
  - *para todo c tal que $a|c$ y $b|c$, se cumple $g|c$.*

La relación $\mid$ es una relación de orden en $\mathbb{Z}$. El $MCD(a, b)$ es el máximo según $\mid$ en el conjunto de los divisores comunes de a y b. Análogamente, $MCM(a, b)$ es el mínimo de $\mid$ en el conjunto de los múltiplos comunes de a y b.
Como la relación $\mid$ ("divide a") es de orden parcial, no es claro que el MCD (ni el MCM) exista, pues el conjunto de divisores comunes podría tener varios maximales y ningún máximo. Para demostrar su existencia usamos el **Algoritmo de Euclides**.

```
entrada: a, b.
definir r_0 = a, r_1 = b e i = 1;
mientras r_i ≠ 0, hacer:
.    definir r_{i+1} ≥ 0 tal que r_{i-1} = d_i r_i + r_{i+1} y r_{i+1} < r_i; (división entera)
.    i := i + 1;
responder: MCD{a, b} es r_{i-1}.
```

Teorema 2 *El Algoritmo de Euclides es correcto y se detiene en un número finito de pasos.*

Se prueba así, de manera constructiva, la existencia del MCD. Como subproducto se obtiene la propiedad 1) del siguiente teorema, el cual reune las propiedades más importantes de los números naturales y enteros.

Teorema 3

1. *Para todo a, b naturales, existen e, f enteros tales que $MCD\{a, b\} = ea + fb$.*
2. *Si a y b son primos relativos y $a \mid bc$, entonces $a \mid c$.*
3. *Para todo $n \in \mathbb{N}$ existen únicos primos $p_1, ..., p_k$ y enteros $i_1, ..., i_k$ tales que*
$$n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}.$$
4. *$ab = MCD(a, b) * MCM(a, b)$.*
5. *Hay infinitos números primos.*

Volviendo a las relaciones de equivalencia, podemos observar, que dado un natural cualquiera p, la siguiente relación es de equivalencia en $\mathbb{Z}$.

$$a \sim_p b \Leftrightarrow p \mid a - b$$

Obtenemos por lo tanto el conjunto cuociente, que llamaremos $\mathbb{Z}_p = \mathbb{Z}/\sim_p$. Vemos que $\mathbb{Z}_p$ tiene solo p elementos (clases de equivalencia), $\mathbb{Z}_p = \{[0], [1], \ldots, [p - 1]\}$.
Allí se pueden definir la suma y la multiplicación de la siguiente forma.

$$\begin{aligned} [a] \oplus [b] =& [a + b] \\ [a] \odot [b] =& [ab] \end{aligned}$$

Se puede demostrar que están bien definidas, es decir, que la definición es coherente no depende de los representantes a y b de las clases. Obtenemos así una nueva estructura: $(\mathbb{Z}_p, \oplus, \odot)$. Gracias a al Teorema 3 parte 1, se demuestra lo siguiente.

Teorema 4 *$(\mathbb{Z}_p, \oplus, \odot)$ es un cuerpo si y solo si p es primo.*

2. Polinomios

En este curso, los polinomios serán vistos como expresiones algebraicas en x, no como funciones, adoptaremos entonces la nomenclatura $\mathbb{K}[x]$ para denotar el conjunto de los polinomios a coeficientes en el cuerpo $\mathbb{K}$, en la indeterminada x. Veremos que cumplen muchas de las propiedades antes vistas para los enteros, y que las mismas metodologías se pueden aplicar. Si recordamos, a cada polinomio no nulo $p(x)$ se le puede asociar un natural, su grado: $gr(p(x))$, que cumple:

- $gr(p(x) + q(x)) = max\{gr(p(x), gr(q(x))\}$
- $gr(p(x)q(x)) = gr(p(x)) + gr(q(x))$

El primer teorema importante es el siguiente.

Teorema 5 (de la división) *Para todo par de polinomios $p(x)$, $q(x) \neq 0$ existe un único par de polinomios $d(x)$, $r(x)$, tales que:*

- *$p(x) = d(x)q(x) + r(x)$, y*
- *$gr(r(x)) < gr(q(x))$ o bien $r(x)$ es el polinomio nulo.*

Se pueden definir conceptos análogos a los definidos en $\mathbb{Z}$.

Definición 3 *Si $p(x), q(x) \in \mathbb{K}[x]$, entonces se define:*

- *$q(x)|p(x)$ si y solo si $\exists d(x) \in \mathbb{K}[x], q(x)d(x) = p(x)$.*
- *$p(x)$ es mónico si su coeficiente principal es 1.*
- *$p(x)$ no constante es irreducible en $\mathbb{K}[x]$ si no tiene divisores en $\mathbb{K}[x]$ no constantes de grado estríctamente menor.*
- *$MCD(p(x), q(x)) = d(x)$ si y solo si*
  - *$d(x) \in \mathbb{K}[x]$ es mónico,*
  - *$d(x)|p(x)$ y $d(x)|q(x)$, y*
  - *para todo $h(x)$ tal que $h(x)|p(x)$ y $h(x)|q(x)$, se cumple $h(x)|d(x)$.*
- *$p(x)$ y $q(x)$ son primos relativos si $MCD(p(x), q(x)) = 1$.*

La relación $|$ es una relación de orden en el conjunto de los polinomios mónicos. El algoritmo de Euclides funciona igualmente en este caso, y se tienen las siguientes propiedades.

Teorema 6 *1. Para todo $p(x)$, $q(x) \in \mathbb{K}[x]$, existen $e(x)$, $f(x) \in \mathbb{K}[x]$ tales que $MCD\{p(x), q(x)\} = e(x)p(x) + f(x)q(x)$.*

2. Si $p(x)$ y $q(x)$ son primos relativos y $p(x) \mid q(x)r(x)$, entonces $p(x) \mid r(x)$.

3. Para todo $q(x) \in \mathbb{K}[x]$ existen únicos polinomios irreducibles mónicos $p_1(x), ..., p_k(x) \in \mathbb{K}[x]$ y enteros $i_1, ..., i_k$ y constante a tales que

$$q(x) = ap_1(x)^{i_1}p_2(x)^{i_2} \cdots p_k(x)^{i_k}.$$

4. Dado $a \in \mathbb{K}$ fijo, el polinomio $(x - a)$ divide a $p(x)$ sí y solo si $p(a) = 0$.

5. Todo polinomio $p(x) \neq 0$ tiene a lo más $gr(p)$ raíces.

Finalmente, se tiene el siguiente importante resultado, cuya demostración requiere herramientas que están fuera de los contenidos de este curso.

Teorema 7 (fundamental del álgebra) *Los únicos polinomios irreducibles en $\mathbb{C}$ son los polinomios de grado 1.*

De aquí se deduce el siguiente teorema, importante también.

Teorema 8 *Los únicos polinomios irreducibles en $\mathbb{R}$ son:*

- *los polinomios de grado 1, y*
- *los polinomios de grado 2, $ax^2 + bx + c$, tales que $b^2 - 4ac < 0$.*