Estructuras Algebraicas

Profesores: Angel Perez y Esther Garcia

Diego Rodriguez

Estudiante de Matemáticas e Ingeniería Informática en la URJC
GitHub
Wuolah

d.rodriguezto.2023@alumnos.urjc.es

Índice

1 Anillos

§1.1 Anillos. Generalidades.

§1.1.1 Definiciones basicas

Definición 1.1.1. Un grupo es un par $(G, \odot)$ donde:

- G es un conjunto no vacio.
- $\odot : G \times G \to G$ es una operacion interna

que cumplen:

1. Asociativa: $\forall a, b, c \in G \quad (a \odot b) \otimes c = a \odot (b \odot c)$
2. Existencia de neutro: $\exists e_G \in G$ tal que $\forall a \in G \quad a \odot e_G = e_G \odot a = a$
3. Existencia de inversos: $\forall a \in G \exists b \in G$ tal que $a \odot b = b \odot a = e_G$

Definición 1.1.2. Un grupo $(G, \odot)$ es abeliano o conmutativo si la operacion $\odot$ es conmutativa, es decir, $\forall a, b \in G \quad a \odot b = b \odot a$

Definición 1.1.3. Un anillo es una terna $(A, \oplus, \otimes)$ donde:

- A es un conjunto no vacio
- $\oplus$: $A \times A \to A$ es una operacion interna, denominada suma.
- $\otimes$: $A \times A \to A$ es una operacion interna, denominada producto.

que cumplen:

1. Suma asociativa: $\forall a, b, c \in A \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$
2. Existencia de neutro: $\exists 0_A \in A$ tal que $\forall a \in A \quad a \oplus 0_A = 0_A \oplus a = a$
3. Existencia de opuestos: $\forall a \in A \exists b \in A$ tal que $a \oplus b = b \oplus a = 0_A$
4. Suma conmutativa: $\forall a, b \in A \quad a \oplus b = b \oplus a$

5. Producto asociativo: $\forall a, b, c \in A \quad (a \otimes b) \otimes c = a \otimes (b \otimes c)$
6. Distributiva: $\forall a, b, c \in A \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c), (b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$

Definición 1.1.4 — Anillo conmutativo. Un anillo A es conmutativo si el producto $\otimes$ es conmutativo.

Definición 1.1.5 — Anillo unitario. Un anillo A es unitario o anillo con unidad si existe un neutro para el producto $\otimes$ distinto del neutro para la suma $\oplus$, es decir

$$\exists 1_A \in A \setminus \{0_A\} \,/\, \forall a \in A \quad a \otimes 1_A = 1_A \otimes a = a$$

Usualmente denotaremos la suma $a \oplus b$ como $a + b$ y el producto $a \otimes b$ como $a \cdot b$.
Si no hay ambiguedad, denotaremos los neutros como 0 y 1.

Definición 1.1.6 — Elemento invertible. En un anillo con unidad, decimos que $a \in A$ es invertible si $\exists b \in A$ tal que $ab = ba = 1$.

Definición 1.1.7 — Anillo de division. Un anillo de division es un anillo con unidad A tal que todo elemento distinto de 0 es invertible.

Definición 1.1.8 — Cuerpo. Un cuerpo es un anillo conmutativo con unidad A tal que todo elemento distinto de 0 es invertible.

Proposición 1.1.1.

1. Sea $(G, \odot)$ un grupo con elemento neutro e. Se cumple que e es el unico elemento de G con la propiedad que define al neutro.
2. Sea $(G, \odot)$ un grupo. Se cumplen las propiedades de cancelacion:

$$\forall a, b, c \in G \; a \odot b = a \odot c \Rightarrow b = c$$
$$b \odot a = c \odot a \Rightarrow b = c$$

3. En un grupo el inverso de cualquier elemento es unico.

   En un anillo con unidad el neutro para el producto es unico.

En un anillo con unidad el inverso de un elemento invertible es unico.

4. En un anillo A se cumple
$$\forall a \in A \quad 0a = a0 = 0$$

Proof. 1. Sea G un grupo y e un elemento neutro de G.

Supongamos que e' es un elemento de G con la propiedad que define el neutro. Vamos a ver que necesariamente $e = e'$.

$$e \overset{e' \text{ neutro}}{=} e \odot e' \overset{e \text{ neutro}}{=} e'$$

Observación 1.1.1. Como consecuencia, el neutro 0 de la suma para un anillo A es unico (porque $(A, \oplus)$ es un grupo).

2. Sean $a, b, c \in G$ tal que $a \cdot b = a \cdot c$.

Por el axioma de inversos $\Rightarrow$ existe $d \in G$ tal que $a \cdot d = e$.

$$d \cdot (a \cdot b) = d \cdot (a \cdot c) \overset{\text{Asociativa}}{\Rightarrow} (d \cdot a) \cdot b = (d \cdot a) \cdot c \Rightarrow e \cdot b = e \cdot c \overset{\text{Neutro}}{\Rightarrow} b = c$$

$b \cdot a = c \cdot a \Rightarrow b = c$ es analogo.

Observación 1.1.2. Como consecuencia, en un anillo A se tiene cancelacion para la suma: $\forall a, b, c \in A \quad a + b = a + c \Rightarrow b = c$

3. Sea $a \in G$. Supongamos que b, c son inversos de $a \Rightarrow a \cdot b = e$ y $a \cdot c = e$, siendo e el neutro de G.

Como $ab = ac$, por cancelacion $b = c$.

Observación 1.1.3. Esto implica que en un anillo el opuesto para la suma es unico.

–

Supongamos que $u, v \in A$ son neutros para el producto. Entonces $u \overset{v \text{ neutro}}{=} u \cdot v \overset{u \text{ neutro}}{=} v$. Luego el neutro es unico.

–

Sea $a \in A$ un elemento invertible. Supongamos que $b, c \in A$ son inversos de a. Entonces $a \cdot b = 1 = a \cdot c$. Multiplicando por b,

$$b \cdot a \cdot b = b \cdot a \cdot c \Rightarrow 1 \cdot b = 1 \cdot c \Rightarrow b = c$$

4. $a \cdot 0 = a \cdot (0 + 0) = a0 + a0 \Rightarrow 0 + \cancel{a0} = a0 + \cancel{a0} \overset{\text{Cancelacion}}{\Rightarrow} 0 = a0.$

■

Como notacion para el opuesto e inverso de un elemento, usaremos:

- $-a$ para el opuesto de a.
- a^{-1} para el inverso de a.

Para la resta, $a - b$ denota el elemento $a + (-b)$.

Definición 1.1.9 — Restriccion de una funcion. Sean $B \subseteq A$ y C tres conjuntos y $f\colon A \to C$ una funcion. Llamamos restriccion de f al conjunto B a la funcion

$$\begin{aligned} f|_B\colon B &\longrightarrow C \\ x &\longmapsto f|_B(x) = f(x) \end{aligned}$$

Definición 1.1.10 — Subanillo. Sea $(A, +, \cdot)$ un anillo y $\varnothing \neq B \subseteq A$. Decimos que B es subanillo de A si:

1. $\forall r, s \in B,\ r + s \in B$
2. $\forall r, s \in B,\ r \cdot s \in B$
3. $(B, +|_{B\times B}, \cdot|_{B\times B})$ cumple la definicion de anillo

Proposición 1.1.2 — Caracterizacion 1 de subanillo. Sea $(A, +, \cdot)$ un anillo y $B \subseteq A$. B es subanillo de A si y solo si se cumplen:

1. $0_A \in B$
2. $\forall r \in B \quad -r \in B$
3. $\forall r, s \in B \quad r + s \in B$
4. $\forall r, s \in B \quad r \cdot s \in B$

Proof.

D1: Cerrado para la suma
D2: Cerrado para el producto
D3: Cumple la def de anillo
D1,D2,D3 $\Leftrightarrow$ 1,2,3,4
"$\Rightarrow$" D1 = 3 y D2 = 4.
Como B es anillo por $D3 \Rightarrow \exists 0_B \in B$. Vamos a demostrar que $0_B = 0_A$.

$$\begin{cases} 0_B + 0_A = 0_B \text{ (porque } 0_A \text{ es el neutro para la suma en } A) \\ 0_B = 0_B +_B +0_B = 0_B + 0_B \end{cases}$$

Igualando, $0_B + 0_A = 0_B + 0_B \Rightarrow 0_A = 0_B$.
Por tanto, $0_A \in B$. Hemos demostrado 1.
Nos queda demostrar 2.
Sea $r \in B$. Como por D3 B es un subanillo, r tiene opuesto en $B \Rightarrow \exists s \in B / r +_B s = 0_B \Rightarrow r + s = 0_A$ (usamos que $0_A = 0_B$ y que $+_B$ es la operacion restringida). Por unicidad del opuesto, $s = -r \Rightarrow -r \in B$.
"$\Leftarrow$" Se tienen D1 y D2 porque se cumplen 3 y 4.
$B \neq \varnothing$ porque $0_A \in B$.
Me falta demostrar D3 que son los 6 axiomas de la definicion de anillo: A1, A2, A3, A4, A5, A6.
A1, A4, A5, A6 se cumplen para la $+_B$ y $\cdot_B$ porque se cumplen para todos los elementos de A y las operaciones en B son las de A restringidas. Es decir, las propiedades se "heredan" en B.
Vamos a demostrar A2 (existencia de neutro para la suma). Como por 1 se tiene que $0_A \in B$ tengo que 0_A funciona como neutro para la suma en B.
Ademas, se que $0_A = 0_B$.
Vamos a demostrar A3 (existencia de opuestos).
Sea $r \in B$, tengo que demostrar que r tiene opuesto en B. Sea s el opuesto de r en A. Se que $r + s = 0_A$. Por 2, se que $s \in B$.
Por tanto, $r +_B s = 0_A = 0_B \Rightarrow s$ es el opuesto de r en B. ■

Ejemplo 1.1.1. Demostrar que $A = \{n + \sqrt{2}m / n, m \in \mathbb{Z}\}$ es un anillo.
Vamos a demostrar que A es un subanillo de $\mathbb{R}$ aplicando la proposicion 2.

1. $0 \in A$ porque se obtiene con $n = m = 0$.
2. El opuesto de $n + m\sqrt{2}$ es $-(n + m\sqrt{2}) = (-n) + (-m)\sqrt{2} \in A$
3. Sean $n + m\sqrt{2} \in A$ y $p + q\sqrt{2} \in A$, $(n + m\sqrt{2}) + (p + q\sqrt{2}) = n + p + (m + q)\sqrt{2} \in A$.
4. Dados los elementos anteriores, $(n + m\sqrt{2}) \cdot (p + q\sqrt{2}) = np + mp\sqrt{2} + nq\sqrt{2} + 2mq = (np + 2mq) + (np + mq)\sqrt{2} \in A$.

Luego A es subanillo de $\mathbb{R}$ y, por tanto, anillo.

Observación 1.1.4. A es el subanillo mas pequeño de $\mathbb{R}$ que contiene a $\mathbb{Z}$ y a $\sqrt{2}$ (no lo estamos demostrando). Se denota $A = \mathbb{Z}[\sqrt{2}]$.
Tomando $\mathbb{Z}[x]$, los polinomios con coeficientes en $\mathbb{Z}$, y sustituyendo $x = \sqrt{2}$, se obtiene dicho anillo.

Proposición 1.1.3 — Caracterizacion 2 de subanillo. Sea $(A, +, \cdot)$ un anillo y $B \subseteq A$. B es subanillo de A si y solo si se cumplen:

1. $0_A \in B$
2. $\forall r, s \in B \quad r - s \in B$
3. $\forall r, s \in B \quad r \cdot s \in B$

Proof.

Queda como ejercicio. ■

§1.1.2 Ejemplos de anillos

- $\mathbb{Z}$, con la suma y producto usuales, es un anillo conmutativo con unidad.
- $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$, con la suma y producto usuales, son cuerpos. Cada uno es subanillo de los que lo contienen.
- Sean A un anillo, $n \geq 2$ un entero.

  $\mathcal{M}_{n\times n}(A)$, el conjunto de las matrices cuadradas $n \times n$ con coeficientes en A, con la suma y producto usual de matrices, es un anillo.

  Si A es unitario, $\mathcal{M}_{n\times n}(A)$ tambien lo es.
- Sea A un anillo conmutativo.

  $A[x]$, el conjunto de los polinomios con coeficientes en A en la variable x, con la suma y producto usual de polinomios, es un anillo conmutativo.

  Si A es unitario, $A[x]$ tambien lo es.

  $A_3[x]$, el conjunto de los polinomios con grado menor o igual que 3 con coeficientes en A, no es un anillo por no ser cerrado para el producto.
- Dado $m \in \mathbb{Z}$, el conjunto $m\mathbb{Z} \coloneqq \{mx \mid x \in \mathbb{Z}\}$ es un subanillo de $\mathbb{Z}$.

  Proof.

  Usamos la caracterizacion 2.

  1. $0 \in m\mathbb{Z}$ tomando $x = 0$
  2. Sean $mx, mx' \in m\mathbb{Z}$, $mx - mx' = m(x - x') \in m\mathbb{Z}$
  3. Sean $mx, mx' \in m\mathbb{Z}$, $\underbrace{mx \cdot mx'}_{\in\mathbb{Z}} \in m\mathbb{Z}$.

  ■

  Observación 1.1.5. Si $n < 0$. Entonces $m\mathbb{Z} = (-m)\mathbb{Z}$.

Usaremos solo $m \geq 0$.

$$\left.\begin{array}{ll} m = 0 & 0\mathbb{Z} = \{0x \mid x \in \mathbb{Z}\} = \{0\} \\ m = 1 & 1\mathbb{Z} = \mathbb{Z} \end{array}\right\} \text{(son los dos subanillos triviales)}$$

Si $m \geq 2$, $m\mathbb{Z}$ tiene unidad?

$2\mathbb{Z}$ $a \cdot b = b \quad \forall b \in 2\mathbb{Z}$

$a = 2x \Rightarrow 2xb = b \Rightarrow 2x = 1$. Contradiccion.

Luego $2\mathbb{Z}$ no tiene unidad.

Ningun $m\mathbb{Z}$ con $m \geq 2$ tiene unidad.

- El anillo de los enteros modulo n.

§1.1.3 Divisores de cero. Dominios de integridad.

Definición 1.1.11 — Divisor de cero. Sean A un anillo conmutativo y $a \in A \setminus \{0\}$. Decimos que a es divisor de cero si $\exists b \in A \setminus \{0\}$ tal que $ab = 0$.

Definición 1.1.12 — Dominio de integridad. Un dominio de integridad (DI) es un anillo conmutativo con unidad (a.c.c.u.) que no tiene divisores de cero.

Observación 1.1.6. DI $\Leftrightarrow$ a.c.c.u. donde $\forall a, b \in A (a \neq 0, b \neq 0 \Rightarrow ab \neq 0)$

Teorema 1.1.1. Sean A un a.c.c.u. y $a \in A$

$$a \text{ invertible} \Rightarrow a \text{ no es divisor de cero}$$

Proof.

Sea $a \in A$ invertible. Sabemos que si a es invertible, $a \neq 0$.
Supongamos que a es divisor de cero $\Rightarrow \exists b \neq 0 \mid a \cdot b = 0$.
En la igualdad multiplico por a^{-1} y tengo

$$a^{-1}ab = a^{-1}0 \Rightarrow b = 0$$

Esto es una contradiccion porque hemos supuesto que $b \neq 0$.
Luego a no es divisor de cero. ■

Observación 1.1.7. Esto es equivalente a

$$a \text{ es divisor de cero} \Rightarrow a \text{ no es invertible}$$

Observación 1.1.8. El reciproco del teorema 1 no es cierto.

$$a \text{ no divisor de cero} \not\Rightarrow a \text{ invertible}$$

Veamos un ejemplo en $\mathbb{Z}$. 2 es divisor de cero?
$2x = 0 \Rightarrow x = 0$.
Luego 2 no es divisor de cero. Es 2 invertible?
$2x = 1$ no tiene solucion en $\mathbb{Z}$. Luego no es invertible.

Teorema 1.1.2.

$$A \text{ cuerpo} \Rightarrow A \text{ dominio de integridad}$$

Proof.

Si A es un cuerpo, tambien es un a.c.c.u.
Ademas, como A es un cuerpo se cumple que $\forall a \neq 0, a$ es invertible. Por el teorema 1, $\forall a \neq 0$, a no es divisor de cero $\Rightarrow A$ es D.I. ■

Observación 1.1.9. El reciproco del teorema 2 no es cierto.
Un contraejemplo es el conjunto de los numeros enteros. Como $\mathbb{Q}$ es un cuerpo, $\mathbb{Q}$ es D.I. Ademas, $\mathbb{Z} \subseteq \mathbb{Q}$. Por tanto, $\mathbb{Z}$ tambien es D.I. (si hubieran divisores de cero en $\mathbb{Z}$ tambien los habria en $\mathbb{Q}$).
Y sabemos que $\mathbb{Z}$ no es un cuerpo (por ejemplo, 2 no es invertible).

Observación 1.1.10. Los unicos elementos invertibles de $\mathbb{Z}$ son 1 y -1.

$$ab = 1 \Rightarrow |a||b| = 1 \Rightarrow |a| = |b| = 1 \Rightarrow |a| = |b| = 1$$

Lema 1.1.1. Sea A a.c.c.u.
A es un dominio de integridad $\Leftrightarrow$ A tiene la propiedad de cancelacion para el producto: $\forall a, b, c \in A$ tales que $a \neq 0$ y $ab = ac$ se tiene $b = c$.

Proof.

"$\Rightarrow$" Tenemos que $a \neq 0$ y $ab = ac$. Entonces

$$ab - ac = 0 \Rightarrow a(b-c) = 0 \overset{\substack{A\,D.I.\\ a\neq 0}}{\Rightarrow} b - c = 0 \Rightarrow b = c$$

"$\Leftarrow$" Tengo que demostrar que A no tiene divisores de cero.
Lo demostramos por reduccion al absurdo. Supongamos que si hay divisores de cero. Entonces $\exists a, b \neq 0 \mid a \cdot b = 0$.

$$ab = 0 = a \cdot 0 \overset{\substack{a\neq 0\\ \text{Cancelacion}}}{\Rightarrow} b = 0$$

Esto es una contradiccion porque $b \neq 0$.
Luego no hay divisor de cero en $A \Rightarrow A$ es D.I. ■

Observación 1.1.11. La cancelacion para el producto es falsa en general.
Ejemplo: en $\mathbb{Z}_6$, $[2][3] = [4][3] = [0]$. No puedo cancelar $[3]$ porque $[2] \neq [4]$.

Teorema 1.1.3. *A dominio de integridad finito $\Rightarrow$ A cuerpo.*

Proof.

Quiero demostrar que A es un cuerpo. Como A es D.I. $\Rightarrow$ A es un anillo conmutativo con unidad. Tengo que demostrar que todo elemento no nulo de A tiene inverso.
Sea $a \in A$ con $a \neq 0$, veamos que a tiene inverso.
Defino una funcion, que consiste en multiplicar por a

$$\begin{aligned} f\colon A &\longrightarrow A \\ x &\longmapsto f(x) = a \cdot x \end{aligned}$$

Si consigo demostrar que f es suprayectiva $\Rightarrow 1 \in Imf \Rightarrow \exists b \in A \mid f(b) = 1 \Rightarrow ab = 1 \Rightarrow b = a^{-1}$ y a es invertible.
Vamos a demostrar que f es inyectiva. Sean $b_1, b_2 \in A$ tales que $f(b_1) = f(b_2) \overset{DEF}{\Rightarrow} ab_1 = ab_2 \overset{\text{Lema 1}}{\Rightarrow} b_1 = b_2 \Rightarrow f$ es inyectiva.
Como f es una funcion inyectiva entre dos conjuntos finitos del mismo cardinal, f tiene que ser suprayectiva. ■

Teorema 1.1.4 — Wedderburn. *A anillo de division finito $\Rightarrow$ A cuerpo*

Proposición 1.1.4. Sea $[a] \in \mathbb{Z}_n$.
$[a]$ es invertible $\Leftrightarrow mcd(a,n) = 1$.

Proof.

$[a]$ tiene inverso $\Leftrightarrow ax \equiv 1 \bmod n$ tiene solucion $\Leftrightarrow ax - 1 = n \cdot y$ tiene solucion $\Leftrightarrow ax + (-n)y = 1$ tiene solucion $\Leftrightarrow mcd(a,n) = 1$. ■

Corolario 1.1.1. $\mathbb{Z}_n$ es un cuerpo $\Leftrightarrow n$ es primo

Proof.

n primo $\Rightarrow 1, 2, \ldots, n-1$ tienen $mcd = 1$ con n.
n compuesto $\Rightarrow \exists d \in 1, 2, \ldots, n-1$ tal que d tiene un factor comun con $n \Rightarrow mcd(b,n) \geq 2 \Rightarrow [d]$ no es invertible. ■

Corolario 1.1.2. Sea $[a] \in \mathbb{Z}_n$, $[a] \neq [0]$.
$[a]$ no es invertible $\Rightarrow [a]$ es divisor de cero.

Ejemplo 1.1.2. En $\mathbb{Z}_{12}$, $[10]$ no es invertible porque $mcd(10,12) = 2$.
Por otro lado $[10] = [2] \cdot [5]$
$[10] \cdot [6] = [2] \cdot [5] \cdot [6] \overset{[2][6]=[0]}{=} [0] \Rightarrow [10]$ es divisor de cero.
En general si en $\mathbb{Z}_n$ $mcd(d,n) = x \geq 2$
$[d] \neq [0]$
$[d]\left[\frac{n}{x}\right] = \left[\frac{d}{x}\right][n] = [0]$. Luego d es divisor de cero.

§1.1.4 Homomorfismos de anillos

Definición 1.1.13 — Homomorfismo. Sean A y B dos anillos y $f\colon A \to B$ una funcion. Decimos que f es un homomorfismo de anillos si cumple:

- $\forall x, y \in A \quad f(x+y) = f(x) + f(y)$
- $\forall x, y \in A \quad f(x \cdot y) = f(x) \cdot f(y)$

Definición 1.1.14 — Isomorfismo. Sean A y B dos anillos y $f\colon A \to B$ una funcion. Decimos que f es un isomorfismo de anillos si f es un homomorfismo biyectivo.

Definición 1.1.15 — Anillos isomorfos. Sean A y B dos anillos. Decimos que A y B son anillos isomorfos si existe algun isomorfismo $f\colon A \to B$.

Proposición 1.1.5. Sea $f\colon A \to B$ un homomorfismo de anillos. Se cumple:

1. $f(0_A) = 0_B$
2. $\forall a \in A \quad f(-a) = -f(a)$

Proof.

1. $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \Rightarrow 0_B + f(0_A) = f(0_A) + f(0_A) \Rightarrow 0_B = f(0_A)$
2. $f(a) + f(-a) = f(a + (-a)) = f(0_A) = 0_B$. Por la unicidad del elemento opuesto, llegamos a que $f(-a) = -f(a)$.

■

Proposición 1.1.6. Sean $f\colon A \to B$ y $g\colon B \to C$ homomorfismos de anillos. Entonces $g \circ f$ es un homomorfismo de anillos.

Proof.

Sean $a, b \in A$

$$(g \circ f)(a + b) = g(f(a + b)) = g(f(a) + f(b)) = g(f(a)) + g(f(b)) = \\ = (g \circ f)(a) + (g \circ f)(b)$$

Esto es analogo para el producto. ■

Observación 1.1.12. En la definicion de homomorfismo, si la quiero "bien escrita",

$$f(a +_A b) = f(a) +_B f(b)$$

Proposición 1.1.7. Sea $f\colon A \to B$ un isomorfismo de anillos. Se cumple:

1. f^{-1} es isomorfismo de anillos.
2. A conmutativo $\Rightarrow B$ conmutativo.

3. A unitario $\Rightarrow$ B unitario. Ademas:
   - $f(1_A) = 1_B$
   - a invertible $\Rightarrow$ $f(a)$ invertible y $(f(a))^{-1} = f(a^{-1})$
4. A cuerpo $\Rightarrow$ B cuerpo.

Proof. 1. f es isomorfismo. Como f es biyectiva $\Rightarrow \exists f^{-1}\colon B \to A$ otra funcion biyectiva. Tengo que demostrar que f^{-1} es isomorfismo. Falta ver que preserva suma y producto.

Tenemos que demostrar que $\forall b_1, b_2 \in B\ f^{-1}(b_1 + b_2) = f^{-1}(b_1) + f^{-1}(b_2)$.

Como f es biyectiva, sabemos que $\exists a_1, a_2 \in A \mid f(a_1) = b_1,\ f(a_2) = b_2$. Luego

$$f^{-1}(b_1 + b_2) = f^{-1}(f(a_1) + f(a_2)) = f^{-1}(f(a_1 + a_2)) = a_1 + a_2 = \\ = f^{-1}(b_1) + f^{-1}(b_2)$$

La demostracion para el producto es analoga.

2. Supongamos que A es conmutativo.

   Sean $b_1, b_2 \in B$ cualesquiera. Tenemos que ver si $b_1 \cdot b_2 = b_2 \cdot b_1$

   Sean $a_1, a_2 \in A$ tales que $f(a_1) = b_1$, $f(a_2) = b_2$ (existen por ser f biyectiva). Entonces

$$b_1 \cdot b_2 = f(a_1) \cdot f(a_2) = f(a_1 \cdot a_2) = f(a_2 \cdot a_1) = f(a_2) \cdot f(a_1) = b_2 \cdot b_1$$

3. Por el enunciado, se que el candidato a neutro del producto en B es $f(1_A)$. Voy a comprobar que funciona.

   Tengo que ver que $\forall b \in B\ f(1_A) \cdot b = b$ y $b \cdot f(1_A) = b$.

   Como f es biyectiva $\Rightarrow \exists a \in A \mid f(a) = b$. Entonces

$$f(1_A) \cdot b = f(1_A) \cdot f(a) \overset{fhom}{=} f(1_A \cdot a) \overset{\text{Neutro}}{=} f(a) = b$$

   Analogamente, $b \cdot f(1_A) = b$.

   Por tanto B es unitario $1_B = f(1_A)$.

   Observación 1.1.13. Es suficiente con que f sea un homomorfismo suprayectivo.

   Sea ahora $a \in A$ invertible. Tengo que ver que $f(a)$ es invertible en B. El enunciado me da el candidato $f(a^{-1})$. Pruebo que funciona.

   Multiplico $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1_A) = 1_B$.

   Analogamente $f(a^{-1}) \cdot f(a) = 1_B \Rightarrow$ los dos elementos son inversos uno de otro, es decir, el inverso de $(f(a))^{-1} = f(a^{-1})$.

4. Si A es cuerpo,
$$\begin{cases} A \text{ conmutativo} \overset{2}{\Rightarrow} B \text{ conmutativo} \\ A \text{ unitario} \overset{3}{\Rightarrow} B \text{ unitario} \end{cases}$$
Sea $b \in B, b \neq 0_B$, tengo que ver que b es invertible.

Como f es biyectiva, existe $a \in A$ tal que $f(a) = b$. Como $f(0_A) = f(0_B)$, $b \neq 0_B$ y f es biyectiva, $a \neq 0_A \Rightarrow a$ es invertible. Por la propiedad 3 y que $b = f(a)$, b es invertible.

■

Observación 1.1.14. Si $\exists f\colon A \to B$ isomorfismo, decimos que A es isomorfo a B y lo denotamos
$$A \cong B$$

Proposición 1.1.8. La relacion de isomorfia de anillos es una relacion de equivalencia.

Proof. 1. Reflexiva: $id\colon A \to A$ es obviamente biyectiva y homomorfismo $\Rightarrow A \cong A$

2. Simetrica:

Si $A \cong B \Rightarrow \exists f\colon A \to B$ isomorfismo $\Rightarrow f^{-1}\colon B \to A$ isomorfismo (prop 11) $\Rightarrow B \cong A$

3. Transitiva:

Supongamos que $A \cong B$ y $B \cong C \Rightarrow \exists f\colon A \to B$ y $\exists g\colon B \to C$ isomorfismos $\Rightarrow g \circ f$ homomorfismo.

Veamos que la composicion de funciones biyectivas es biyectiva
$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$
porque
$$(g \circ f)(f^{-1} \circ g^{-1}) = g \circ id_B \circ g^{-1} = g \circ g^{-1} = id_C$$
$$(f^{-1} \circ g^{-1})(g \circ f) = f^{-1} \circ id_B \circ f = f^{-1} \circ f = id_A$$
Luego $g \circ f\colon A \to C$ isomorfismo $\Rightarrow A \cong C$

■

Definición 1.1.16. Sea $f\colon A \to B$ un isomorfismo de anillos. Se definen el nucleo y la imagen de f como:

- $Ker f \coloneqq \{x \in A \mid f(x) = 0_B\}$

- $Imf \coloneqq \{y \in B \mid \exists x \in A \mid f(x) = y\}$

Proposición 1.1.9. 1. $Kerf$ es un subanillo de A

2. f es inyectiva $\Leftrightarrow Kerf = \{0_A\}$
3. Imf es un subanillo de B
4. f es suprayectiva $\Leftrightarrow Imf = B$

Proof. 1. Veamos que $Kerf$ es subanillo de A

- $0_A \in Kerf$ porque $f(0_A) = 0_B$
- Cerrado para la resta: Sean $a, b \in Kerf$,

$$f(a-b) = f(a+(-b)) = f(a) + f(-b) = f(a) - f(b) = 0_B - 0_B = 0_B$$

Luego $a - b \in Kerf$.

- Cerrado para el producto: Sean $a, b \in A$

$$f(a \cdot b) = f(a) \cdot f(b) = 0_B \cdot 0_B = 0_B \Rightarrow a \cdot b \in Kerf$$

2. f inyectiva $\Leftrightarrow Kerf = \{0_A\}$
"$\Rightarrow$" Se que $0_A \in Kerf$.
Sea $a \neq 0_A \Rightarrow f(a) \neq f(0_A) = 0_B \Rightarrow Kerf = \{0_A\}$
"$\Leftarrow$" Voy a ver que f es inyectiva.
Sea $a, b \in A$. Supongamos que $f(a) = f(b)$. Entonces

$$f(a) - f(b) = 0_B \Rightarrow f(a-b) = 0_B \Rightarrow a - b \in Kerf \Rightarrow a - b = 0_A \Rightarrow a = b$$

3. Veamos que Imf es subanillo de B.

- $0_B \in Imf$ porque $f(0_A) = 0_B$
- Sean $b_1, b_2 \in Imf \Rightarrow \exists a_1, a_2 \in A \mid f(a_1) = b_1$ y $f(a_2) = b_2$.

$$b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \Rightarrow b_1 - b_2 \in Imf$$

- $b_1 \cdot b_2 = f(a_1) \cdot f(a_2) = f(a_1 \cdot a_2) \Rightarrow b_1 \cdot b_2 \in Imf$

4. Es la definicion de suprayectiva.

■

§1.2 Ideales y anillos cociente. Teoremas de isomorfía

§1.2.1 Ideales

Definición 1.2.1. Sea A un anillo. Decimos que I es un ideal de A si cumple:

1. I es un subanillo de A
2. I tiene la propiedad de absorcion:
   $\forall a \in A, \forall r \in I$:
   - $ar \in I$
   - $ra \in I$

Proposición 1.2.1 — Caracterizacion de ideal. Sean A un anillo e $I \subseteq A$, I es ideal de A si y solo si

- $0_A \in I$
- $\forall a, b \in I \quad a - b \in I$
- I tiene la propiedad de absorcion.

Proof.

Usar la caracterizacion que teniamos de subanillo y darse cuenta de que la absorcion implica que el producto sea cerrado. ■

Proposición 1.2.2. Sean A un anillo conmutativo y $c \in A$. El conjunto

$$I_c \coloneqq \{ac \mid a \in A\}$$

es un ideal de A.

Proof.

1. $0_A \in I_c$ porque $0_A = c \cdot 0_A$.
2. Sean $x, y \in I_c \Rightarrow \exists a, b \in A \mid x = c \cdot a$ y $y = c \cdot b \Rightarrow x - y = c \cdot a - c \cdot b = c(a - b) \in I_c$
3. Sea $x \in I_c$ y $a \in A$, $\exists b \in A \mid x = cb$.
   Entonces $x \cdot a = c \cdot b \cdot a \in I_c$.

■

Observación 1.2.1. $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$ porque, con la notacion que estamos usando, $n\mathbb{Z} = I_n$.

Observación 1.2.2. En general, $c \in I_c$ no se cumple.
Como contraejemplo, $A = 2\mathbb{Z}$ no tiene unidad y $I_2 = \{2x \mid x \in 2\mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, \ldots\} = 4\mathbb{Z}$. En este caso $2 \notin I_2$.

Proposición 1.2.3. Si A es un a.c.c.u. y $c \in A$, entonces I_c se llama el ideal principal generado por c. Es el minimo ideal (respecto de la relacion de contenido) al que c pertenece.
Notacion: En este caso se usa la notacion $I_c = (c)$.

Proof.

Sabemos, por la proposicion 2, que I_c es ideal de A.
Cumple que $c \in I_c$ porque $c = c \cdot 1_A \in I_c$.
Falta "es el minimo ideal con respecto la propiedad de ser ideal al que c pertenece".
Demostrar eso se puede formalizar de la siguiente forma: Dado cualquier ideal J de A tal que $c \in J$, entonces $I_c \subseteq J$.
Sea J ideal de A tal que $c \in J$. Quiero ver que $I_c \subseteq J$.
Sea $x \in I_c \Rightarrow \exists a \in A \mid x = c \cdot a \Rightarrow$ Como J es ideal y $c \in J$, por absorcion $x = c \cdot a \in J$. ■

Ejemplo 1.2.1.

- Sea A un anillo cualquiera. A y $\{0_A\}$ son ideales de A. Se consideran los ideales triviales de A.
- $7\mathbb{Z}$ es ideal de $\mathbb{Z}$. Hemos visto en general que $\forall n \in \mathbb{Z}$, $n\mathbb{Z}$ es ideal de $\mathbb{Z}$ (por la proposicion 2).
- $\{0, 3\}$ es ideal de $\mathbb{Z}_6$.

  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Veamos que $\{0, 3\}$ es ideal:

  1. $0 \in I$
  2. Cerrado para la resta:
     - $0 - 0 = 0 \in I$
     - $0 - 3 = -3 = 3 \in I$
     - $3 - 0 = 3 \in I$
     - $3 - 3 = 0 \in I$
  3. Cumple la propiedad de absorcion.

  Luego $I = \{0, 3\}$ es ideal de $\mathbb{Z}_6$.

  Como alternativa, se puede demostrar teniendo en cuenta que $I = \{0, 3\} = I_3 = (3)$. $\{0, 3\}$ es el conjunto de todos los multiplos de 3.

- $\{x^2p(x) \mid p \in \mathbb{Z}[x]\}$ es ideal de $\mathbb{Z}[x]$.

  Para demostrar que I es ideal basta con darse cuenta de que I es el conjunto de todos los multiplos de $\mathbb{Z}[x]$ del polinomio x^2 y utilizar la propiedad 2. $I = (x^2)$.

- $\{2a + xp(x) \mid a \in \mathbb{Z}, p \in \mathbb{Z}[x]\}$ es ideal de $\mathbb{Z}[x]$.

  I consiste en todos los polinomios con termino independiente par.

  Vamos a demostrar que I es ideal de $\mathbb{Z}[x]$:

  1. $c(x) = 0$, el polinomio constante 0, es el neutro para la suma de este anillo.

     $0 \in I$ porque se obtiene tomando $a = 0$ y $p(x) = 0$.

  2. Cerrado para la resta:

     $$\left.\begin{array}{l} 2a + xp(x) \in I \\ 2b + xq(x) \in I \end{array}\right\} \Rightarrow (2a+xp(x))-(2b+xq(x)) = 2\underbrace{(a-b)}_{\in\mathbb{Z}} + x\underbrace{(p(x)-q(x))}_{\in\mathbb{Z}[x]} \in I$$

  3. Absorcion:

     $$\left.\begin{array}{l} (x) = 2a + a_1x + a_2x^2 + \cdots \in I \\ g(x) = b_0 + b_1x + \cdots \in \mathbb{Z}[x] \end{array}\right\} \Rightarrow f(x) \cdot g(x) = 2 \cdot a \cdot b_0 + \cdots \in I$$

     Luego I es ideal de $\mathbb{Z}[x]$

  Vamos a demostrar que I no es principal, es decir, que I no esta generado por un solo elemento. Por reduccion al absurdo, vamos a suponer que I es principal, es decir, que existe $q(x)$ tal que $I = (q(x))$.

  Observamos que $f(x) = 2$ (polinomio constante).

  Como $2 \in I$ y estoy suponiendo que $q(x)$ genera $I \Rightarrow \exists p(x) \in \mathbb{Z}[x] \mid 2 = p(x)q(x)$.

  La unica opcion es que tanto $p(x)$ como $q(x)$ sean polinomios constantes.

  Solo hay 4 opciones: $p(x) = 1$ y $q(x) = 2$, $p(x) = 2$ y $q(x) = 1$, $p(x)-1$ y $q(x) = -2$, y $p(x) = -2$ y $q(x) = -1$.

  Como $1, -1 \notin I$ pero $q(x) \in I$, esto no es una opcion.

  Puede ser $I = (2) = (-2)$.

  $g(x) = x \notin (2)$.

  Pero $x \in I$ porque tiene termino independiente par. Esto es una contradiccion. Por tanto, I no es principal.

- $\mathbb{Z}$ es subanillo pero no ideal de $\mathbb{Z}[x]$.

  Puedo ver $\mathbb{Z}$ como un subanillo de $\mathbb{Z}[x]$ identificando $\mathbb{Z}$ como el conjunto de los polinomios constantes.

  $\mathbb{Z}$, obviamente, es subanillo. Sin embargo, no tiene la propiedad de absorcion:

  $$\left.\begin{array}{l} f(x) = 1 \in \mathbb{Z} \\ g(x) = x \in \mathbb{Z}[x] \end{array}\right\} \Rightarrow f(x) \cdot g(x) = x \notin \mathbb{Z}$$

Esto es un contraejemplo a la absorcion.

- $K \coloneqq \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ es subanillo pero no ideal de $\mathcal{M}_{2\times 2}(\mathbb{R})$.

  Se puede verificar facilmente que cumple la caracterizacion de subanillo. Veamos que no tiene absorcion.

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a \cdot a' & b \cdot b' \\ 0 & 0 \end{pmatrix}$$

  Pero no se tiene la absorcion por el otro lado:

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a \cdot a' & b \cdot b' \\ c' \cdot a & c' \cdot b \end{pmatrix} \notin K$$

  Por ejemplo, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \notin K$.

  Luego K no es ideal.

§1.2.2 Anillo cociente

Definición 1.2.2 — Congruencia modulo un ideal. Sean A un anillo e I un ideal de A. Se dice que dos elementos $a, b \in A$ son congruentes modulo I si

$$a - b \in I$$

Notacion: $a \equiv b \bmod I$

Proposición 1.2.4. La relacion de la definicion anterior es una relacion de equivalencia.

Proof. 1. Reflexiva: $\forall a \in A \; a \equiv a \bmod I$?

$a - a = 0_A \in I$ (porque I es subanillo).

2. Simetrica: $\forall a, b \in A$ si $a \equiv b \bmod I \Rightarrow a - b \in I \Rightarrow -(a-b) = b - a \in I$ (I es cerrado para opuestos) $\Rightarrow b \equiv a \bmod I$.

3. Transitiva: $\forall a, b, c \in A$ si $a \equiv b \bmod I$ y $b \equiv c \bmod I \Rightarrow a - b \in I$ y $b - c \in I \Rightarrow a - b + b - c = a - c \in I$ (porque es cerrado para la suma) $\Rightarrow a \equiv c \bmod I$.

■

Las clases de equivalencia de la relacion anterior son $[a]_I \coloneqq \{b \in A \mid a \equiv b \bmod I\}$.

Proposición 1.2.5 — Descripcion de las clases de equivalencia.

$$[a]_I = \{a + r \mid r \in I\}$$

Proof.

Lo demostraremos por doble contenido.
"$\subseteq$" $x \in [a]_I \Rightarrow a \equiv x \bmod I \Rightarrow x - a \in I \Rightarrow \exists r \in I \mid x - a = r \Rightarrow x = a + r$.
"$\supseteq$" Si $x = a + r$ con $r \in I$, entonces $x - a = r \in I \Rightarrow x \equiv a \bmod I \Rightarrow x \in [a]_I$. ■

La Proposicion 1.2.5 sugiere la siguiente notacion, que sera la que usaremos a partir de ahora para las clases de equivalencia de la relacion anterior:

$$[a]_I \coloneqq a + I$$

Definición 1.2.3. Sean A un anillo e I un ideal de A. Denotamos el cociente de A bajo la relacion de la Definicion 1.2.2 como

$$A/I \coloneqq \{a + I \mid a \in A\}$$

Proposición 1.2.6. Sean A un anillo e I un ideal de A. Las operaciones en el cociente A/I definidas como:

- $(a + I) + (b + I) \coloneqq (a + b) + I$
- $(a + I) \cdot (b + I) \coloneqq (a \cdot b) + I$

son operaciones internas bien definidas en el cociente A/I.
El cociente A/I dotado de estas dos operaciones es un anillo. Ademas:

- Si A es conmutativo, A/I tambien lo es.
- Si A es unitario, A/I tambien lo es.

Proof.

Empezamos viendo que las operaciones esten bien definidas.
Supongamos $a + I = c + I$ y $b + I = d + I$.
Tengo que ver que $(a+b)+I = (c+d)+I$. Esto es lo mismo que ver si $(a+b)-(c+d) \in I$.

$$\underbrace{a - c}_{\substack{\in I \\ (a+I=c+I)}} + \underbrace{b - d}_{\substack{\in I \\ (b+I=d+I)}} \in I \text{ (cerrado para la suma)} \Rightarrow (a + b) + I = (c + d) + I.$$

He visto que la suma esta bien definida.
Veamos si tambien el producto: $(a \cdot b) + I \stackrel{?}{=} (c \cdot d) + I \Rightarrow ab - cd \stackrel{?}{\in} I$.

$$ab - ad + ad - cd = \underbrace{a\underbrace{(b-d)}_{\in I}}_{\substack{\in I \\ \text{(absorcion)}}} + \underbrace{\underbrace{(a-c)}_{\in I} d}_{\substack{\in I \\ \text{(absorcion)}}} \in I \Rightarrow ab + I = cd + I$$

Observación 1.2.3. Hemos necesitado absorcion para demostrar que el producto esta bien definido.

Tenemos que ver que A/I con esta suma y este producto es un anillo.

- Suma conmutativa: $(a+I)+(b+I) \stackrel{DEF}{=} (a+b)+I$. Como la suma es conmutativa en A, $(a+b)+I = (b+a)+I \stackrel{DEF}{=} (b+I)+(a+I)$.

  Analogamente, se demuestra que la suma es asociativa, el producto asociativo y la propiedad distributiva del producto respecto de la suma.

- Neutro de la suma: 0_A+I porque $\forall a+I \in A/I\ (a+I)+(0_A+I) = (a+0_A)+I = a+I$.

- Opuestos: Dado $a+I \in A/I$, su opuesto es $-a+I$ porque $(a+I)+(-a+I) = (a+(-a))+I = 0_A+I$.

Por lo tanto, A/I es un anillo.
Tenemos que demostrar que si A es conmutativo, la propiedad se hereda a $A/I \Rightarrow A/I$ tambien es conmutativo.
Si A es unitario, vamos a ver que $1_A + I$ es neutro para el producto en A/I.
Para todo $a + I \in A/I$ se tiene que $(a+I)(1_A+I) \stackrel{DEF}{=} (a \cdot 1_A) + I = a + I$.
Tambien $(1_A + I)(a + I) = (1_A \cdot a) + I = a + I$. ■

Observación 1.2.4. Como conjunto, quien es $0_A + I$?
$0_A + I = \{0_A + r \mid r + I\} = \{r \mid r \in I\} = I$.

Ejemplo 1.2.2. Veremos cuales son los anillos cociente de los anillos en el ejemplo 1.2.1.

- Sea A un anillo cualquiera y $I = A$. Dados $x, y \in A$, $x \equiv y \bmod I \Leftrightarrow x - y \in I = A$. Luego en A/A solo hay una clase: $0_A + A$.

  $A/A = \{0_A + A\}$ es un anillo con un unico elemento.

  Si $I = \{0_A\}$, $x \equiv y \bmod \{0_A\} \Rightarrow x - y = 0_A \Rightarrow x = y$.

  Luego $a + \{0_A\} = \{a\}$. Cada clase tiene un unico elemento.

  Obtengo un anillo que es practicamente A. La diferencia es que en lugar de ser los elementos de A, son sus clases.

En general, la funcion

$$\begin{aligned} f\colon A &\longrightarrow A/\{0_A\} \\ a &\longmapsto f(a) = \{a\} \end{aligned}$$

es isomorfismo de anillos ($A/\{0_A\} \cong A$).

- Sea $\mathbb{Z}$ y $I = 7\mathbb{Z}$. Las clases son $0+7\mathbb{Z}$, $1+7\mathbb{Z}$, $2+7\mathbb{Z}$, $3+7\mathbb{Z}$, $4+7\mathbb{Z}$, $5+7\mathbb{Z}$, $6+7\mathbb{Z}$.

  En este caso $\mathbb{Z}/7\mathbb{Z} = \mathbb{Z}_7$.

  $x \equiv y \bmod 7\mathbb{Z} \Leftrightarrow x - y \in 7\mathbb{Z} \Rightarrow x - y$ es multiplo de $7 \Leftrightarrow x \equiv y \bmod 7$.

  En general, si $n \geq 2$, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

- $\mathbb{Z}_6 = \{[0],[1],[2],[3],[4],[5]\} \leftarrow$ es un anillo cociente de $\mathbb{Z}$ porque $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$.

  $I = \{[0],[3]\}$ es un ideal de $\mathbb{Z}_6$.

  Veamos quien es $\mathbb{Z}_6/I$.

  $[0] + I = \{[0]+[0], [0]+[3]\} = \{[0],[3]\}$.

  $[1] + I = \{[1]+[0], [1]+[3]\} = \{[1],[4]\}$.

  $[2] + I = \{[2]+[0], [2]+[3]\} = \{[2],[5]\}$.

  Ya estan todos los elementos de $\mathbb{Z}_6$.

  $$\mathbb{Z}_6/I = \{0+I, 1+I, 2+I\}.$$

  Ademas, se tiene que $\mathbb{Z}_6/I \cong \mathbb{Z}_3$ (se puede comprobar haciendo tabla para la suma y el producto, observando que son modulo 3).

- $A = \mathbb{Z}[x]$ y $I = (x^2) = \{x^2 \cdot p(x) \mid p(x) \in \mathbb{Z}[x]\}$.

  $A/I = \{q(x) + I \mid q(x) \in \mathbb{Z}[x]\}$.

  Dada una clase, cual sera el representante mas sencillo?

  Un ejemplo de polinomio es $q(x) = 3 + 7x - 8x^2 + 15x^4$. Si tomo $g(x) = 3 + 7x$, tengo que $g(x)+I = q(x)+I$ porque $q(x)-g(x) = 3+7x-8x^2+14x^4-(3+7x) = -8x^2+15x^4 = x^2(-8+15x^2) \in I$.

  En general, dado $q(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ el polinomio $g(x) = a_0 + a_1x$ esta en la misma clase porque $q(x) - g(x) = a_2x^2 + \cdots + a_nx^n = x^2(a_2 + \cdots) \in I$.

  Mi cociente lo puedo expresar como $A/I = \{a_0 + a_1x + I \mid a_0, a_1 \in \mathbb{Z}\}$.

  Ademas, estos representantes forman un "conjunto completo de representantes", es decir, estan todas las clases y no hay clases repetidas.

  Supongamos que $a_0+a_1x+I = b_0+b_1x+I$. Entonces $a_0+a_1x-b_0-b_1x$ es multiplo de x^2. La unica forma es que sea $0 \Rightarrow a_0 + a_1x = b_0 + b_1x$.

  Este cociente es el que tiene como representantes a todas las clases de polinomios de grado ≤ 1.

- $A = \mathbb{Z}[x]$ y $I = \{2a + xp(x) \mid a \in \mathbb{Z}, p \in \mathbb{Z}[x]\}$.

$f(x) \equiv g(x) \bmod I \Leftrightarrow f(x) - g(x) \in I \Leftrightarrow f(x) - g(x)$ tiene termino independiente par.

Quien es $0 + I$? $0 + I = I$.

Si $f(x), g(x) \neq I \Rightarrow$ tienen termino independiente impar $\Rightarrow$ su resta tiene termino independiente par $\Rightarrow f(x) \equiv g(x) \bmod I$.

Solo hay 2 clases de equivalencia.

$A/I = \{0 + I, 1 + I\}$.

Ya sabemos que $A/I \cong \mathbb{Z}_2$ (porque es el unico anillo unitario con 2 elementos).

- $\mathbb{Z}$ es subanillo de $\mathbb{Z}[x]$.

  $f(x) \equiv g(x) \bmod \mathbb{Z}$.

  Supongamos que en el cociente que queda intento definir la multiplicacion operando representantes: $((x + 1) + \mathbb{Z})((x + 2) + \mathbb{Z}) = (x^2 + 3x + 2) + \mathbb{Z}$.

  Cambiando representante, $((x + 2) + \mathbb{Z})((x + 2) + \mathbb{Z}) = (x^2 + 4x + 4) + \mathbb{Z}$ pero $(x^2 + 3x + 2) + \mathbb{Z} \neq (x^2 + 4x + 4) + \mathbb{Z}$

  Esta operacion no esta bien definida porque depende de la eleccion de representante (no ha funcionado porque $\mathbb{Z}$ no es ideal de $\mathbb{Z}[x]$).

§1.2.3 Teoremas de isomorfía para anillos

Proposición 1.2.7. Sean A un anillo y C un subanillo de A. La funcion inclusion de C en A definida como

$$\begin{aligned} i \colon C &\longrightarrow A \\ x &\longmapsto x \end{aligned}$$

es un homomorfismo inyectivo de anillos (o monomorfismo).

Proof.

Trivial. ■

Proposición 1.2.8. Sean A un anillo e I un ideal de A. La funcion proyeccion sobre el cociente definida como

$$\begin{aligned} \pi \colon A &\longrightarrow A/I \\ x &\longmapsto x + I \end{aligned}$$

es un homomorfismo suprayectivo de anillos (o epimorfismo).

Proof.

Usando las propiedades de la suma y producto de clases,

Suma: $\pi(x+y) = (x+y)+I \overset{DEF}{=} (x+I)+(y+I) = \pi(x)+\pi(y)$.
Producto: $\pi(x\cdot y) = (x\cdot y)+I \overset{DEF}{=} (x+I)\cdot(y+I) = \pi(x)\cdot\pi(y)$.
Luego es un homomorfismo.
Veamos que π es suprayectiva.
Sea $z \in A/I$, z es de la forma $z = x+I$ para algun $x \in A$.
Entonces $\pi(x) = x+I = z$.
Luego z tiene una preimagen que es $x \Rightarrow \pi$ es suprayectiva. ■

Proposición 1.2.9. Sea $f\colon A \to B$ un homomorfismo de anillos. $Kerf$ es un ideal de A.

Proof.

Veamos que $Kerf$ es ideal de A.
Sabemos, por el tema 1, que $Kerf$ es subanillo de A. Falta demostrar la propiedad de absorcion.
Sean $a \in A, r \in Kerf$. Comprobemos si $a\cdot r \in Kerf$.

$$f(a\cdot r) = f(a)\cdot f(r) \overset{r\in Kerf}{=} f(a)\cdot 0_B = 0_B \Rightarrow a\cdot r \in Kerf$$

Analogamente, $r\cdot a \in Kerf$. ■

Teorema 1.2.1 — Primer teorema de isomorfia de anillos. Sea $f\colon A \to B$ un homomorfismo de anillos suprayectivo. Entonces la siguiente funcion es un isomorfismo de anillos:

$$\begin{aligned} \overline{f}\colon A/Kerf &\longrightarrow B \\ a+Kerf &\longmapsto \overline{f}(a+Kerf) \coloneqq f(a) \end{aligned}$$

Proof.

Denotaremos con $K = Kerf$.
Definimos

$$\begin{aligned} \overline{f}\colon A/K &\to B \\ a+I &\to f(a) \end{aligned}$$

Como tengo una funcion definida sobre un cociente en terminos del representante, tengo que demostrar que esta bien definida.
Es decir, $\forall (a+K),(b+K) \in A/K$ si $a+K = b+K$, entonces $\overline{f}(a+K) = \overline{f}(b+K)$.

$$a+K = b+K \overset{DEF}{\Rightarrow} a-b \in K \Rightarrow f(a-b) = 0 \Rightarrow f(a)-f(b) = 0 \Rightarrow$$
$$\Rightarrow f(a) = f(b) \Rightarrow \overline{f}(a+K) = \overline{f}(b+K)$$

Veamos que es homomorfismo. Sean $(a+K),(b+K) \in A/K$,

$$\overline{f}((a+K)+(b+K)) \overset{\substack{DEF\\Suma\\A/K}}{=} \overline{f}((a+b)+K) \overset{\text{DEF } f}{=} f(a+b) \overset{fhom}{=} f(a)+f(b) = \overline{f}(a+K)+\overline{f}(b+K)$$

Esto es analogo para el producto.
Comprobamos que f es inyectiva: $\overline{f}(a+K) = \overline{f}(b+K) \overset{?}{\Rightarrow} a+K = b+K$.

$$\overline{f}(a+K) = \overline{f}(b+K) \Rightarrow f(a) = f(b) \Rightarrow f(a)-f(b) = 0_B \Rightarrow f(a-b) = 0_B \Rightarrow$$
$$\Rightarrow a-b \in K \Rightarrow a+K = b+K$$

Veamos que $\overline{f}$ es suprayectiva.
Sea $z \in B$, como f es suprayectiva $\Rightarrow \exists a \in A \mid f(a) = z$.
Entonces $\overline{f}(a+K) \coloneqq f(a) = z$. ■

Corolario 1.2.1. Sea $f\colon A \to B$ un homomorfismo de anillos. Entonces la siguiente funcion es un isomorfismo de anillos:

$$\begin{aligned} \overline{f}\colon A/Kerf &\longrightarrow Imf \\ a+Kerf &\longmapsto \overline{f}(a+Kerf) \coloneqq f(a) \end{aligned}$$

Proof.

Dado $f\colon A \to B$, defino una nueva funcion

$$\begin{aligned} \hat{f}\colon A &\longrightarrow Imf \\ x &\longmapsto \hat{f}(x) = f(x) \end{aligned}$$

Obviamente $\hat{f}$ es un homomorfismo suprayectivo de anillos.
Aplico el teorema 1 que acabo de demostrar a $\hat{f}$ y tenemos

$$\begin{aligned} \overline{f}\colon A/Ker\hat{f} &\longrightarrow Imf \\ a+Ker\hat{f} &\longmapsto \overline{f}(a+\underbrace{Ker\hat{f}}_{=Kerf} = \hat{f}(a) = f(a) \end{aligned}$$

Luego la funcion

$$\begin{aligned} \overline{f}\colon A/Kerf &\longrightarrow Imf \\ a+Kerf &\longmapsto \overline{f}(a+Kerf) = f(a) \end{aligned}$$

es isomorfismo de anillos.
En particular, $A/Kerf \cong Imf$. ■

Corolario 1.2.2. Sea $f\colon A \to B$ un homomorfismo de anillos. Entonces existen:

- π homomorfismo suprayectivo
- $\overline{f}$ isomorfismo
- i homomorfismo inyectivo

tales que $f = i \circ \overline{f} \circ \pi$.

Proof.

Sea $f\colon A \to B$ homomorfismo.
Por el corolario 2, $\overline{f}\colon A/Kerf \to Imf$ es un isomorfismo.

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ \downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle i} \\ A/Kerf & \xrightarrow{\quad \overline{f} \quad} & Imf \end{array}$$

Por tanto $f = i \circ \overline{f} \circ \pi$ porque $\forall a \in A\ i(\overline{f}(\pi(a))) = i(\overline{f}(a+K)) = i(f(a)) = f(a)$. ■

Ejemplo 1.2.3. Dada la funcion

$$\begin{aligned} f\colon \mathbb{Z}_{20} &\longrightarrow \mathbb{Z}_{10} \\ [x]_{20} &\longmapsto f([x]_{20}) = [6x]_{10} \end{aligned}$$

demostrar que esra bien definida y que es un homomorfismo de anillos. Hallar explicitamente $Kerf$, Imf, el anillo cociente $\mathbb{Z}_{20}/Kerf$ y la funcion $\overline{f}$ que aparece en el corolario 1 del primer teorema de isomorfia.
Vamos a ver que f esta bien definida (porque esta definida sobre un cociente y depende del representante).
$[x]_{20} = [y]_{20} \overset{?}{\Rightarrow} [6x]_{10} = [6y]_{10}$.
$[x]_{20} = [y]_{20} \Rightarrow x - y = 20 \cdot k \Rightarrow 6x - 6y = 120k = 10 \cdot 12 \cdot k \Rightarrow [6x]_{10} = [6y]_{10}$. Luego esta bien definida.
Veamos que f es homomorfismo.

$f([x]_{20}+[y]_{20}) = f([x+y]_{20}) = [6(x+y)]_{10} = [6x+6y]_{10} = [6x]_{10}+[6y]_{10} = f([x]_{2}0)+f([y]_{20})$

Para el producto, $f([x]_{20} \cdot [y]_{20}) = f([xy]_{2}0) = [6xy]_{10}$ y $f([x]_{20})f([y]_{2}0) = [6x]_{10} \cdot [6y]_{10} = [36xy]_{10} = [36]_{10} \cdot [xy]_{10} = [6]_{10} \cdot [xy]_{1}0 = [6xy]_{10}$.
Ya se que f es homomorfismo de anillos.

$Kerf?$, $Imf?$.

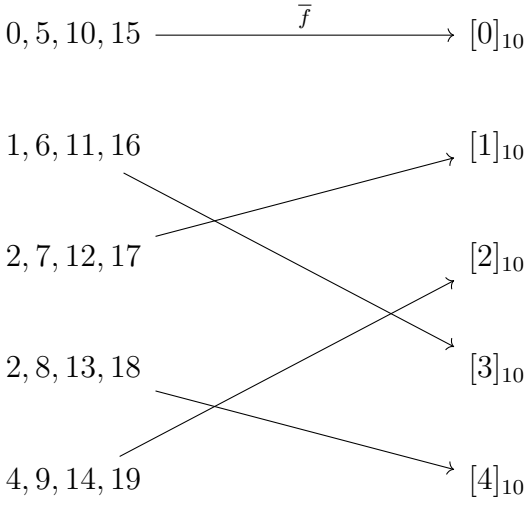
$$[0]_{20} \to [0]_{10}$$
$$[1]_{20} \to [6]_{10}$$
$$[2]_{20} \to [12]_{10} = [2]_{10}$$
$$[3]_{20} \to [18]_{10} = [8]_{10}$$
$$[4]_{20} \to [24]_{10} = [4]_{10}$$

Por tanto, $Imf = \{[0]_{10}, [6]_{10}, [2]_{10}, [8]_{10}, [4]_{10}\} = P$.
$K = Kerf = \{[0]_{20}, [5]_{20}, [10]_{20}, [15]_{20}\} \to$ ideal de $\mathbb{Z}_{20}$ porque es el nucleo de un homomorfismo.
Quien es $\mathbb{Z}_{20}/K$?

$$[0]_{20} + K = K$$
$$[1]_{20} + K = \{[1]_{20}, [6]_{20}, [11]_{20}, [16]_{20}\}$$
$$[2]_{20} + K = \{[2]_{20}, [7]_{20}, [12]_{20}, [17]_{20}\}$$
$$[3]_{20} + K = \{[3]_{20}, [8]_{20}, [13]_{20}, [18]_{20}\}$$
$$[4]_{20} + K = \{[4]_{20}, [9]_{20}, [14]_{20}, [19]_{20}\}$$

$\mathbb{Z}_{20}/K = \{[0]_{20} + K, [1]_{20} + K, [2]_{20} + K, [3]_{20} + K, [4]_{20} + K\}$
Quien es la $\overline{f}$ del primer teorema de isomorfia que hace que en $\mathbb{Z}_{20}/K \cong P$?

$$\overline{f}\colon \mathbb{Z}_{20}/K \longrightarrow P$$
$$[a]_{20} + K \longmapsto \overline{f}([a]_{20} + K) = f(a)$$



El primer teorema de isomorfia me dice que $\overline{f}$ es isomorfismo de anillos.
Por tanto, tenemos que $\mathbb{Z}_{20} = \mathbb{Z}/\mathbb{Z}_{20}$, $K = \frac{5}{Z}/20/Z$ y $\mathbb{Z}_{20}/K = (\mathbb{Z}/\mathbb{Z}_{20})/5\mathbb{Z}/20\mathbb{Z}$.
Aplicando el tercer teorema de isomorfia, $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$.

Ejemplo 1.2.4. Usar el Primer Teorema de Isomorfia para demostrar que $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.
$I = (x) = \{xp(x) \mid p(x) \in \mathbb{Z}\}$ (polinomios con term. indep. 0).
Tengo el cociente $A/I = \mathbb{Z}[x]/(x)$.

Ejemplo: $5+7x+9x^3+(x)=5+(x)$ porque $5+7x+9x^3-5=7x+9x^3\in I=(x)$.
Otra forma de visualizarlo $5+7x+9x^3+(x)=5+(x)+\underbrace{(7x+9x^3)+(x)}_{\substack{0+(x)\\ \text{porque } 7x+9x^3\in(x)}}$.

En general, $a_0+a_1x+a_2\cdot x^2+\cdots+(x)=a_0+(x)$.
$\mathbb{Z}[x]/(x)=\{a+(x)\mid a\in\mathbb{Z}\}$.
Vamos a demostrar que $\mathbb{Z}[x]/(x)\cong\mathbb{Z}$ usando el primer teorema de isomorfia.

$$\begin{aligned} f\colon \mathbb{Z}[x] &\longrightarrow \mathbb{Z}\\ a_0+a_1x+a_2x^2+\cdots &\longmapsto a_0\end{aligned}$$

Es f homomorfismo de anillos?

$$\begin{aligned} f(a_0+a_1x+cdots+b_0+b_1x+\cdots)=f(a_0+b_0+(a_1+b_1)x+\cdots)=a_0+b_0=\\ =f(a_0+a_1x+\cdots)+f(b_0+b_1x+\cdots)\end{aligned}$$

$$\begin{aligned} f((a_0+a_1x+\cdots)(b_0+b_1x+\cdots))=f(a_0b_0+\text{ terminos de grado }\geq 1)=\\ =a_0b_0=f(a_0+a_1x+\cdots)\cdot f(b_0+b_1x+\cdots)\end{aligned}$$

Aplicando el primer teorema de isomorfia, $\mathbb{Z}[x]/Kerf\cong Imf$.
f es suprayectiva porque dado $a\in\mathbb{Z}$ tiene preimagen.
$f(p(x)+a)=a\Rightarrow Imf=\mathbb{Z}$.
$Kerf=\{p(x)\mid f(p(x))=0\}=\{a_0+a_1x+a_2x^2+\cdots\mid a_0=0\}=\{a_1x+a_2x^2\}=(x)=I\Rightarrow\mathbb{Z}[x]/(x)\cong\mathbb{Z}$.
Quien es $\overline{f}$?

$$\begin{aligned} \overline{f}\colon \mathbb{Z}[x]/(x) &\longrightarrow \mathbb{Z}\\ a_0+(x) &\longmapsto \overline{f}(a_0+(x))=f(a_0+a_1x+\cdots)=a_0\end{aligned}$$

Teorema 1.2.2 — Segundo teorema de isomorfia. Sean I,J ideales de un anillo A. Entonces:

1. $I\cap J$ es un ideal de I.
2. J es ideal de $I+J$.
3. Los anillos $I/(I\cap J)$ y $(I+J)/J$ son isomorfos.

Proof.

Ejercicio. ■

Teorema 1.2.3 — Tercer teorema de isomorfia. Sean I,K ideales de un anillo A tales

que $I \subseteq K$. Entonces $(A/I)/(K/I)$ y A/K son anillos isomorfos.

Proof.

Ejercicio. ■

§1.2.4 Ideales primos y maximales

Definición 1.2.4. Sea A un anillo conmutativo y P un ideal de A. Decimos que P es ideal primo de A si cumple:

- $P \neq A$
- $\forall a, b \in A \ (ab \in P \Rightarrow a \in P \vee b \in P)$

Proposición 1.2.10. En $\mathbb{Z}$, dado $n \geq 2$, se cumple

$$n\mathbb{Z} \text{ es ideal primo} \Leftrightarrow n \text{ es numero primo}$$

Proof.

"$\Leftarrow$" Quiero ver que $n\mathbb{Z}$ es ideal primo de $\mathbb{Z}$ (sabemos que $n\mathbb{Z}$ es ideal).
$n \geq 2 \Rightarrow n\mathbb{Z} \neq \mathbb{Z}$.
Supongamos que $a \cdot b \in n\mathbb{Z} \Rightarrow n|a \cdot b$. Como n es primo, por el lema de Euclides se cumple que $n|a$ o $n|b \Rightarrow a \in n\mathbb{Z}$ o $b \in n\mathbb{Z}$.
"$\Rightarrow$" Por contrarreciproco, voy a demostrar que, si n es compuesto, entonces $n\mathbb{Z}$ no es ideal primo.
Como n es compuesto, $\exists d_1, d_2 \in \mathbb{N}$, $2 \leq d_1, d_2 \leq n-1$ tales que $n = d_1 \cdot d_2$.
Luego $n = d_1 \cdot d_2 \in n\mathbb{Z}$ pero $d_1 \notin n\mathbb{Z}$ y $d_2 \notin n\mathbb{Z}$ porque $2 \leq d_1, d_2 \leq n-1$. Luego $n\mathbb{Z}$ no es primo. ■

Proposición 1.2.11. Sean A un a.c.c.u. y $P \neq A$ un ideal de A. Se cumple

$$P \text{ es ideal primo} \Leftrightarrow A/P \text{ es dominio de integridad}$$

Proof.

"$\Rightarrow$" Por reduccion al absurdo, supongamos que A/P no es dominio de integridad. Entonces, $\exists (a+P), (b+P) \in A/P$ que son divisores de cero, es decir, $\underbrace{(a+P)}_{\neq 0+P}\underbrace{(b+P)}_{\neq 0+P} = 0+P \Rightarrow$ $ab + P = 0 + P \Rightarrow a \cdot b \in P \Rightarrow a \in P \vee b \in P$. Por tanto, o bien $a + P = 0 + P$ o bien

$b+P=0+P$, pero esto es una contradiccion.
"$\Leftarrow$" Supongamos que A/P es dominio de integridad. Quiero demostrar que P es primo. Supongamos que $a\cdot b\in P \Rightarrow a\cdot b+P=0+P \Rightarrow (a+P)(b+P)=0+P$. Como A/P es D.I., o bien $a+P=0+P$ o bien $b+P=0+P \Rightarrow a\in P \vee b\in P$. ■

Ejemplo 1.2.5. Forma alternativa de demostrar la proposicion 1.2.11:

$$n\mathbb{Z} \text{ primo} \Leftrightarrow \mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n \text{ es D.I.} \overset{\text{Tema 1}}{\Leftrightarrow} n \text{ primo}$$

Definición 1.2.5. Sea A un a.c.c.u. y M un ideal de A. Decimos que M es ideal maximal de A si cumple:

- $M\neq A$
- M es un elemento maximal con respecto a la relacion de contenido entre los ideales distintos de A, es decir, $\forall J$ ideal de A tal que $M\subseteq J$ se tiene que $J=M$ o $J=A$.

Proposición 1.2.12. Sean A un a.c.c.u. y $M\neq A$ un ideal de A. Se cumple

$$M \text{ es ideal maximal} \Leftrightarrow A/M \text{ es cuerpo}$$

Proof.

"$\Rightarrow$" Supongamos que M es ideal maximal. Quiero demostrar que A/M es un cuerpo, es decir, $\forall a+M\in A/M$ con $a+M\neq 0+M$, $a+M$ tiene que ser invertible.
Por otro lado, $a\notin M$ porque $a+M\neq 0+M$.
Construyo $J=M+(a)$. Sabemos (ejercicios) que J es ideal de A. Ademas, $M\subseteq J$ y $a\in(a)\Rightarrow a\in J\Rightarrow J\neq M$.
Como M es maximal, la unica opcion es $J=A$.
Tambien, $1\in J=M+(a)\Rightarrow \exists m\in M, \exists r\in A \mid 1=m+r\cdot a$. Tomo clase modulo M:

$$1+M=\underbrace{(m+M)}_{=0+M}+(ra+M)\Rightarrow 1+M=(r+M)(a+M)\Rightarrow a+M \text{ invertible .}$$

"$\Leftarrow$" Veamos que si A/M es un cuerpo, entonces M es maximal.
Sea J ideal de A con $M\subseteq J$ pero $M\neq J$. Tengo que demostrar que $J=A$.
Como $J\neq M\Rightarrow \exists a\in A$ tal que $a\in J$ pero $a\notin M$. Como $a\notin M\Rightarrow a+M\neq 0+M$ en A/M.
Al ser A/M un cuerpo, $\exists b+M$ tal que $(a+M)(b+M)=1+M\Rightarrow (a\cdot b)+M=1+M\Rightarrow a\cdot$

$b-1 \in M \Rightarrow \exists m \in M$ tal que $ab-1=m \Rightarrow 1=\underbrace{\underbrace{a}_{\in J}b}_{\in J}+\underbrace{(-m)}_{\in M\subseteq J} \in J \Rightarrow 1 \in J \overset{(ej)}{\Rightarrow} J=A.$ ■

Ejemplo 1.2.6. En $\mathbb{Z}$, $2\mathbb{Z}$ es maximal. Por que?
$\mathbb{Z}/2\mathbb{Z}=\mathbb{Z}_2$ que es un cuerpo (por ser 2 primo). Por la proposicion 1.2.12, $2\mathbb{Z}$ es maximal en $\mathbb{Z}$.
En general, si tengo $n \geq 2$, $n\mathbb{Z}$ es maximal $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$ es cuerpo $\Leftrightarrow n$ es primo.

Corolario 1.2.3. Sean A un a.c.c.u. e I un ideal de A. Se cumple

$$I \text{ ideal maximal} \Rightarrow I \text{ ideal primo}$$

Proof.

Si un ideal I es maximal, por la proposicion 1.2.12, A/I es cuerpo $\Rightarrow A/I$ es dominio de integridad. Por la proposicion 1.2.11, I es primo. ■

Observación 1.2.5. El reciproco del resultado anterior no es cierto.

Ejemplo 1.2.7.

1. $\{0\}$ es primo en $\mathbb{Z}$ pero no maximal.
2. (x) es primo en $\mathbb{Z}[x]$ pero no maximal.

   Vimos que $\mathbb{Z}[X]/(x) \cong \mathbb{Z} \Rightarrow (x)$ es primo en $\mathbb{Z}[x]$ pero (x) no es maximal en $\mathbb{Z}[x]$ (aplicando 1.2.11 y 1.2.12).

   $p(x)q(x) \in (x) \Rightarrow p(x)q(x)=a_1x+a_2x^2+\cdots$. Luego uno de los dos no tiene termino independiente $\Rightarrow p(x) \in (x) \vee q(x) \in (x) \Rightarrow (x)$ es primo.

   Por que no es maximal? Sea $J=\{2a+xp(x)\}$. Se cumple que $(x) \subset J \subset \mathbb{Z}[x]$.

§1.3 Anillos de polinomios

§1.3.1 Generalidades y teorema de la division

Definición 1.3.1 — Polinomio. Sea A un anillo. Un polinomio en una variable x con coeficientes en A es una expresion formal del tipo

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = \sum_{i=0}^{n} a_ix^i$$

donde $n \in \mathbb{N} \cup \{0\}$ y cada $a_i \in A$.

$A[x]$ denota el conjunto de todos los polinomios en la variable x con coeficientes en el anillo A.

Definición 1.3.2 — Suma y producto de polinomios. Sean $p, q \in A[x]$ de la forma $p(x) = \sum_{i=0}^{m} a_ix^i$ y $q(x) = \sum_{i=0}^{n} b_ix^i$. Se define la suma de p y q como otro polinomio

$$(p+q)(x) = \sum_{i=0}^{max(m,n)} c_ix^i$$

donde cada $c_i = a_i + b_i$ (considerando coeficientes igual a cero si no estan definidos).
Se define el producto de p y q como otro polinomio

$$(p \cdot q)(x) = \sum_{i=0}^{m+n} d_ix^i$$

donde cada $d_i = \sum_{j=0}^{i} a_jb_{i-j}$ (considerando coeficientes igual a cero si no estan definidos).

Proposición 1.3.1. Sea A un anillo. Entonces $(A[x], +, \cdot)$ es un anillo. Ademas:
A conmutativo $\Rightarrow A[x]$ conmutativo.
A unitario $\Rightarrow A[x]$ unitario.

Definición 1.3.3. Sea $p(x) = \sum_{i=0}^{n} a_ix^i \in A[x]$ con $a_n \neq 0$. Decimos que:

- a_n es el coeficiente director de p.

  Notacion: $a_n := cd(p)$

- n es el grado de p.
  Notacion: $n \coloneqq gr(p)$
- Si $a_n = 1$ decimos que p es monico

Si $p(x) = 0$ se define $gr(p) \coloneqq -\infty$ y p no tiene coeficiente director.

Proposición 1.3.2. Sean $p, q \in A[x]$. Se cumple:

$$gr(p \cdot q) \leq gr(p) + gr(q)$$

Proof.

Porque la potencia mas alta que puede salir es la suma de los grados. ■

Ejemplo 1.3.1. En $\mathbb{Z}_6[x]$,
$p(x) = 3x^2 + 2$ (grado 3), $q(x) = 2x^2 + x + 1$ (grado 2).
Multiplicando, $p(x)q(x) = 6x^5 + 3x^4 + 3x^3 + 4x^2 + 2x + 1$ (grado 4).
En general no tengo que $gr(p \cdot q) =$ suma de los grados.

Proposición 1.3.3 — Formula del grado. Sean A un DI y $p, q \in A[x]$. Se cumple:

$$gr(p \cdot q) = gr(p) + gr(q)$$

Proof.

Si A es un DI $\Rightarrow \underbrace{cd(p \cdot q)}_{\neq 0 (\text{DI})} = \underbrace{cd(p)}_{\Leftarrow \neq 0} \cdot \underbrace{cd(q)}_{\neq 0} \Rightarrow gr(p \cdot q) = gr(p) + gr(q)$. ■

Corolario 1.3.1. A es DI $\Rightarrow A[x]$ es DI.

Proof.

Supongamos que A es DI.
Sean $p(x) \neq 0, q(x) \neq 0$ (ambos tienen coeficiente director $\neq 0$).
Entonces $(p \cdot q)(x)$ tiene coeficiente director distinto de cero $\Rightarrow (p \cdot q)(x) \neq 0$.
Luego $A[x]$ es DI.

■

Teorema 1.3.1 — Teorema de la division. Sean K un cuerpo y $f, g \in K[x]$ con $g \neq 0$. Entonces $\exists q, r \in K[x]$ tales que:

- $f = g \cdot q + r$
- $gr(r) < gr(g)$.

Ademas q y r son los unicos polinomios que cumplen simultaneamente las dos propiedades anteriores.

Ejemplo 1.3.2. Division en $\mathbb{Q}[x]$:

$$x^3 + 7x^2 - 2x + 1 = (2x^2 + 3) \cdot (\frac{1}{2}x + \frac{7}{2}) + (\frac{7}{2}x - \frac{19}{2})$$

Otro ejemplo: $x^2 + 1 = 2 \cdot (\frac{1}{2}x^2 + 1) + 0$.
Se cumple que $\underbrace{gr(\text{resto})}_{-\infty} < \underbrace{gr(\text{divisor})}_{0}$

§1.3.2 Divisibilidad en $K[x]$

Definición 1.3.4 — Divisor y multiplo. Sean K un cuerpo y $f, g \in K[x]$. Decimos que f divide a g si $\exists p \in K[x]$ tal que $g = p \cdot f$.
Decimos tambien que f es divisor de g y que g es multiplo de f.
Notacion: $f|g$.

Proposición 1.3.4.

- $f|g \Rightarrow \forall c \in K \setminus \{0\}\ cf|g$
- $g \neq 0, f|g \Rightarrow gr(f) \leq gr(g)$

Proof.

- Si $f|g \Rightarrow \exists p(x) \in K[x] \mid g(x) = f(x) \cdot p(x)$. Como K es cuerpo, dado $c \neq 0, \exists c^{-1} \in K$. Luego $g(x) = (cf(x)) \cdot (c^{-1}p(x)) = f(x) \cdot p(x) \Rightarrow cf(x)|g(x)$.
- Sea $g(x) \neq 0$ y $f(x)|g(x) \Rightarrow \exists p(x) \in K[x] \mid g(x) = p(x) \cdot f(x)$. Por la formula de los grados, $gr(g) = gr(p) + gr(f)$ (porque los coeficientes estan en K que es cuerpo y, por tanto, DI).

  Sabemos que $gr(p) \geq 0$ porque la unica opcion de que no pasara esto seria con $p(x) = 0 \Rightarrow g(x) = 0$. Esto seria una contradiccion.

  Luego $gr(g) = gr(p) + gr(f) \geq 0 + gr(f) = gr(f)$.

■

Definición 1.3.5 — Maximo comun divisor. Sean $f, g \in K[x]$. Decimos que p es un maximo comun divisor de f y g si p es un polinomio monico, divisor comun de f y g de grado maximo.

Ejemplo 1.3.3. En $\mathbb{R}[x]$,
$f(x) = x^3 - x = x(x^2 - 1) = x(x+1)(x-1)$
$g(x) = x^2 + 2x + 1 = (x+1)^2$
Vemos que $x+1$ es un divisor comun y polinomio monico.

Proposición 1.3.5 — Unicidad. El maximo comun divisor de dos polinomios es unico.

Asimismo, el maximo comun divisor de f y g se denota por $mcd(f, g)$.

Proposición 1.3.6 — Identidad de Bezout. Sean K un cuerpo y $f, g \in K[x]$. Entonces $\exists u, v \in K[x]$ tales que

$$mcd(f, g) = uf + vg$$

Observación 1.3.1. El algoritmo de Euclides y su extension para calcular identidades de Bezout funcionan en $K[x]$.
$x^3 - x = (x^2 + 2x + 1) \cdot (x - 2) + (2x + 2) \Rightarrow x^2 + 2x + 1 = (2x + 2) \cdot (\frac{1}{2}x + \frac{1}{2}) + 0.$
El mcd es el ultimo resto antes de tener resto 0 (ajustado con una constante para que sea monico).
Entonces $mcd(f, g) = \frac{1}{2}(2x + 2) = x + 1$.
Ahora puedo usar los cocientes para encontrar una identidad de Bezout entre f y g.

$$2x+2 = (x^3-x)-(x^2+2x+1)(x-2) \Rightarrow \underbrace{x+1}_{mcd(f,g)} = \underbrace{\frac{1}{2}}_{u(x)} \underbrace{(x^3-x)}_{f(x)} + \underbrace{(-\frac{1}{2})(x-2)}_{v(x)} \underbrace{(x^2+2x+1)}_{g(x)}$$

§1.3.3 Polinomios irreducibles en $K[x]$

Proposición 1.3.7. Sean K un cuerpo y $p(x) \in K[x]$

$$p(x) \text{ es invertible en } K[x] \Leftrightarrow p(x) \in K \setminus \{0\}$$

Proof.

"$\Leftarrow$" Sea $p(x) = c \neq 0$ polinomio constante. Como K es un cuerpo $\Rightarrow \exists c^{-1} \in K$. Luego

$c \cdot c^{-1} = 1 \Rightarrow p(x) = c$ es invertible.
"$\Rightarrow$" Supongamos $p(x)$ invertible $\Rightarrow \exists q(x) \in K[x]$ tal que $p(x) \cdot q(x) = 1$.
Por la formula de los grados, $gr(p) + gr(q) = gr(1) = 0$.
La unica opcion es $gr(p) = gr(q) = 0 \Rightarrow p(x)$ y $q(x)$ son constantes. ■

Observación 1.3.2. No es cierto en general, si los coeficientes no estan en un DI. Veamos un contraejemplo en $\mathbb{Z}_4[x]$.
$(2x+1)(2x+1) = 4x^2 + 2x + 2x + 1 = 4x^2 + 4x + 1 = 1 \Rightarrow 2x+1$ es invertible en $\mathbb{Z}_4[x]$.

Definición 1.3.6 — Polinomios asociados. Sean $p(x), q(x) \in K[x]$. Decimos que $p(x)$ es asociado de $q(x)$ si $\exists c \neq 0 \in K$ tal que $p(x) = cq(x)$ (es decir, si existe un elemento invertible que pasa de uno a otro).

Definición 1.3.7 — Polinomio irreducible. Sea $p(x) \in K[x]$ un polinomio no constante. Decimos que p es irreducible si sus unicos divisores son constantes y asociados de p. En caso contrario decimos que p es reducible.

Observación 1.3.3. Para definir polinomios irreducibles no puedo decir que solo tiene 2 divisores.
x^2+1 tiene infinitos divisores: $x^2+1, 2(x^2+1), 7(x^2+1), \ldots, 1, -3, \pi, \ldots$ porque $x^2+1 = (7)(\frac{1}{7}(x^2+1))$.
Estos divisores estan siempre. Si son los unicos, decimos que el polinomio es irreducible.

Proposición 1.3.8. Sea $p \in K[x]$ un polinomio de grado 1. Entonces p es irreducible.

Proof.

Supongamos que $f(x)$ es divisor de $p(x) \Rightarrow \exists g(x) \in K[x] \mid p(x) = f(x) \cdot g(x)$.
La formula de los grados nos dice que $gr(p) = gr(f) + gr(p)$, pero $gr(p) = 1$. Luego hay dos opciones:

- $gr(f) = 0 \Rightarrow f$ constante
- $gr(f) = 1 \Rightarrow gr(g) = 0 \Rightarrow g(x) = c$ constante
  $p(x) = cf(x) \Rightarrow f(x) = c^{-1}p(x) \Rightarrow f(x)$ es asociado de $p(x)$.

Luego p es irreducible (porque sus unicos divisores son constantes y asociados). ■

Proposición 1.3.9. Sea $p(x) \in K[x]$ no constante

$$p(x) \text{ es reducible} \Leftrightarrow \exists q(x), r(x) \in K[x] \mid p(x) = q(x)r(x) \text{ con } gr(q), gr(r) < gr(p)$$

Proof.

"$\Rightarrow$" $p(x)$ es reducible $\Rightarrow$ $\exists q(x)$ divisor de $p(x)$ que no es ni constante ni asociado de $p(x) \Rightarrow \exists r(x) \mid p(x) = q(x) \cdot r(x)$.
Falta demostrar que $gr(q), gr(r) < gr(p)$. Por reduccion al absurdo, supongo que $gr(q) = gr(p) \Rightarrow gr(p) = \underbrace{gr(q)}_{=gr(p)} + gr(r) \Rightarrow gr(r) = 0 \Rightarrow r(x) = c$ constante $\Rightarrow q(x) = c^{-1}p(x) \Rightarrow$ $q(x)$ es asociado de $p(x)$. Esto es una contradiccion porque habiamos dicho que $q(x)$ no era asociado.
Supongamos que $gr(r) = gr(p) \Rightarrow gr(p) = gr(q) + \underbrace{gr(r)}_{=gr(p)} \Rightarrow gr(q) = 0 \Rightarrow q(x) = c$ constante.
"$\Leftarrow$" Supongamos que $f(x) = g(x) \cdot h(x)$ con $gr(q), gr(r) < gr(p) \Rightarrow g(x)$ y $h(x)$ no pueden ser constantes y no pueden ser asociados de $f(x)$.
Como $f(x) = g(x)h(x)$, $g(x)$ divide a $f(x)$ asi que $f(x)$ es reducible. ■

Proposición 1.3.10.

1. Si $p(x)$ irreducible cumple $p(x)|a(x)b(x)$ entonces $p(x)|a(x)$ o $p(x)|b(x)$.
2. Si $p(x)$ divide a $\prod_{i=1}^{n} f_i(x)$ entonces $\exists i$ tal que $p(x)|f_i(x)$.

Teorema 1.3.2 — Factorizacion unica. Se dice que $K[x]$ es un dominio de factorizacion unica (DFU) si todo $f(x) \in K[x]$ es producto de polinomios irreducibles.
Ademas, si $f(x) = p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x)$, entonces $r = s$ y los factores se pueden reordenar de manera que cada f_j sea asociado de q_j.

§1.3.4 Raices de un polinomio

Definición 1.3.8. Si A es un a.c.c.u. y sea $p(x) \in A[x]$, definimos la funcion inducida por $p(x)$ (o funcion evaluacion de $p(x)$) de la siguiente forma:

$$\begin{aligned} p\colon A &\longrightarrow A \\ b &\longmapsto p(b) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 \end{aligned}$$

Definición 1.3.9. Dado $p(x) \in A[x]$, decimos que b es una raiz de b si $p(b) = 0$.

Teorema 1.3.3 — Teorema del resto. Sean K un cuerpo, $p(x) \in K[x]$ y $b \in K$. El resto de dividir $p(x)$ entre $g(x) = x - b$ es $p(b)$.

Proof.

Como $gr(r(x)) < 1$, $r(x)$ es una constante y la denotamos r.
Por el algoritmo de la division $p(x) = (x - b) \cdot q(x) + r$.
Evaluando en b: $p(b) = (b - b) \cdot q(b) + r$, es decir, $r = p(a)$. ■

Corolario 1.3.2 — Teorema del factor lineal. Sean $p(x) \in K[x]$ y $b \in K$,

$$p(b) = 0 \Leftrightarrow (x - b) | p \text{ (b es una raiz de } p(x))$$

Proof.

El resto de dividir $p(x)$ entre $x - b$ da cero $\overset{\text{T. resto}}{\Leftrightarrow}$ $p(b) = 0 \Leftrightarrow b$ es una raiz. ■

Corolario 1.3.3. Sea $f(x) \in K[x]$ de grado $n \geq 1$. Entonces f tiene, como mucho, n raices.

Proof.

Lo demostraremos por induccion.
Para $n = 1$, $f(x) = a_1 x + a_0 \Rightarrow$ la raiz es $\dfrac{-a_0}{a_1}$. Luego se cumple para el caso base.
Supongamos que es cierto para n y veamos que tambien lo es para $n + 1$.
Sea $f(x)$ con $gr(f(x)) = n + 1$.

- Si no tiene raices, ya estaria.
- Si tiene raices, sea $a \in K$ una de las raices.

$$f(x) = (x - a) \cdot h(x)$$

Veamos que $\{$ raices de $f(x)\} = \{a\} \cup \{$raices de $h(x)\}$.

$\subseteq]$ Sea c una raiz de $f(x)$ que no sea a. Como sabemos que $f(x) = (x - a)h(x)$, evaluando en c, $u = f(c) = \underbrace{(c - a)}_{\neq 0} \cdot h(c) \Rightarrow h(c) = 0$, por lo que c es raiz de h.

$\supseteq]$ Claramente a es una raiz de $f(x)$ porque lo estamos suponiendo.

Si b es raiz de $h(x)$ $(h(b)=0) \Rightarrow f(b)=(b-a)\cdot \underbrace{h(b)}_{=0}=0$. Luego b es raiz de $f(x)$.

Aplicamos la hipotesis de induccion a $h(x)$, que tiene grado n. $h(x)$ tiene, como mucho, n raices (que son raices de $f(x)$).

Ademas, tenemos que a es una raiz de $f(x) \Rightarrow f(x)$ tiene como mucho $n+1$ raices.

■

Corolario 1.3.4. Sean $p \in K[x]$ con $gr(p) \geq 2$.

1. p irreducible $\Rightarrow p$ no tiene raices en K.
2. p no tiene raices en K y $gr(p) \in \{2,3\} \Rightarrow p$ irreducible

Observación 1.3.4.

1. Los polinomios irreducibles no tienen raices.
2. Si $f(x)$ tiene grado 2 o 3 y no tiene raices, entonces $f(x)$ es irreducible.

Corolario 1.3.5. Sean K un cuerpo infinito y $f, g \in K[x]$.

$$f(x)=g(x) \Leftrightarrow f \text{ y } g \text{ inducen la misma funcion en } K$$

Proof.

"$\Rightarrow$" Obvio.
"$\Leftarrow$" Consideremos $h(x)=f(x)-g(x)$ un polinomio de cierto grado $m<\infty$.
Tenemos que $\forall a \in K$, $h(a)=f(a)-g(a)=0$. Es decir, todos los numeros de K (infinitos) son raices de $h(x)$. Por el corolario 1.3.3, $h(x)$ es el polinomio 0, es decir, $f(x)=g(x)$. ■

§1.3.5 Criterios de irreducibilidad

§1.3.5.1 Polinomios en $\mathbb{C}[x]$

Teorema 1.3.4 — Teorema fundamental del Algebra. Sea $p \in \mathbb{C}[x]$ no constante. Entonces p tiene una raiz en $\mathbb{C}$.

Proof.

Gauss, 1789. Demostracion compleja. ■

Corolario 1.3.6. Todo polinomio de grado n factoriza como producto de n polinomios de grado 1.

Proof.

Sea $f(x)$ de grado $n \geq 2$.
Buscamos $a_1 \in \mathbb{C}$ raiz de $f(x)$. Entonces, $f(x) = (x - a_1) \cdot f_1(x) = (x - a_1)(x - a_2)f_2(x) = (x - a_1)(x - a_2) \cdots (x - a_{n-1}) \cdot$ factor de grado 1. ■

Corolario 1.3.7. Sea $p \in \mathbb{C}[x]$ no constante. Entonces p es irreducible si y solo si $gr(p) = 1$.

§1.3.5.2 Polinomios en $\mathbb{R}[x]$

Definición 1.3.10. Dado un $z = a + bi \in \mathbb{C}$, se define su conjugado $\overline{z}$ como $\overline{z} = a - bi$

Observación 1.3.5. Dados $z_1, z_2 \in \mathbb{C}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.
Luego $\overline{(z)^n} = (\overline{z})^n$

Proposición 1.3.11. Sea $p(x) \in \mathbb{R}[x]$ y $z = a + bi$ una raiz de p en $\mathbb{C}$. Entonces $\overline{z} = a - bi$ es tambien raiz de p en $\mathbb{C}$ con la misma multiplicidad que z.

Proof.

Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$.
Sea $z \in \mathbb{C}$ raiz de $f(x)$. Entonces, $f(z) = 0$, es decir, $a_n z^n + \cdots + a_1 z + a_0 = 0$.
Tomamos conjugados en los dos lados de la igualdad $\Rightarrow \overline{a_n z^n + \cdots + a_1 z + a_0} = \overline{0} = 0$.
Asi, nos queda $a_n(\overline{z})^n + a_{n-1}(\overline{z})^{n-1} + \cdots + a_1\overline{z} + a_0$ (usando que $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{R}$). Luego tenemos que $f(\overline{z}) = 0$, es decir, $\overline{z}$ es raiz de $f(x)$. ■

Teorema 1.3.5. Sea $f(x) \in \mathbb{R}[x]$ no constante. Entonces

$$f(x) \text{ es irreducible} \Leftrightarrow \begin{cases} gr(p) = 1 \\ \text{o bien} \\ gr(p) = 2 \text{ y } p(x) = ax^2 + bx + c \\ \quad \text{con } b^2 - 4ac < 0 \end{cases}$$

Proof.

"⇐" Obvia.
"⇒" No la hacemos. ■

Corolario 1.3.8. Sea $p \in \mathbb{R}[x]$ no constante. Entonces p factoriza en producto de factores irreducibles de grados 1 y 2.

Corolario 1.3.9. Si $f(x) \in \mathbb{R}[x]$ de grado impar, al menos tiene una raiz real.

§1.3.5.3 Polinomios en $\mathbb{Q}[x]$

Observación 1.3.6. Lo mejor es "quitar denominadores" y suponer que $p(x) \in \mathbb{Z}[x]$. Ejemplo: $\frac{1}{2}x^2 + \frac{3}{2}x + \frac{7}{2} = \frac{1}{2}(x^2 + 3x + 7)$

Definición 1.3.11. Decimos que un numero racional $x = \frac{r}{s}$ esta en forma reducida si $mcd(r, s) = 1$.

Teorema 1.3.6. Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$.

$$\text{Un racional } \frac{r}{s} \text{ (en forma reducida) es raiz de } f(x) \Rightarrow r|a_0, s|a_n$$

Proof.

Supongamos que $\frac{r}{s}$ es raiz de $f(x)$.

$$0 = a_n(\frac{r}{s})^n + \cdots + a_1\frac{r}{s} + a_0 \overset{\cdot s^n}{\Rightarrow} 0 = a_n r^n + a_{n-1}r^{n-1}s + a_1 r s^{n-1} + a_0 \cdot s^n \Rightarrow -a_0 s^n = \\ = r(a_n r^{n-1} + a_{n-1}r^{n-2}s + \cdots + a_1 s^{n-1})$$

Por tanto, $r| - a_0 \cdot s^n \Rightarrow r|a_0$.
Ademas, $-a_n r^n = s(\cdots) \Rightarrow s| - a_n r^n \Rightarrow s|a_n$. ■

Ejemplo 1.3.4. El polinomio $x^4 - 5x^2 + 1$ tiene alguna raiz en $\mathbb{Q}$?
$\{\text{candidatos a raices}\} = \{\frac{r}{s} \mid r|1, s|1\} = \{\pm 1\}$.
Tomo $\lambda = 1$, $1^4 - 5 \cdot 1^2 + 1 \neq 0$.

Tomo $\lambda = -1$, $(-1)^4 - 5 \cdot (-1)^2 + 1 \neq 0$.
Por tanto, este polinomio no tiene raices racionales, es decir, no tiene factores de grado 1.
Demostrar que tampoco tiene factores de grado 2: Por reduccion al absurdo, supongamos que $x^4 - 5x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ $a, b, c, d \in \mathbb{Z}$.
$(x^2+ax+b)(x^2+cx+d) = x^4 + \underbrace{(a+c)x^3}_{0} + \underbrace{(d+b+ac)x^2}_{-5} + \underbrace{(ad+bc)x}_{0} + \underbrace{bd}_{1}$. Esto acaba en una contradiccion.

Lema 1.3.1 — Lema de Gauss. Dado $p(x) \in \mathbb{Z}[x]$. Si $p(x)$ es irreducible en $\mathbb{Z}[x]$, entonces $p(x)$ es irreducible en $\mathbb{Q}[x]$.

Teorema 1.3.7 — Criterio de Eisenstein. Sea $p(x) = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$ no constante con $a_n \neq 0$.
Si $\exists p \in \mathbb{N}$ primo tal que:

- $p | a_0, a_1, \ldots, a_{n-1}$
- $p \nmid a_n$
- $p^2 \nmid a_0$

entonces $p(x)$ es irreducible en $\mathbb{Q}[x]$.

Proof.

En el libro de Hungerford. ■

Ejemplo 1.3.5. Ejemplo: $x^4 + 2x^2 + 2x + 2$. Tomando $p = 2$, vemos que es irreducible.

Teorema 1.3.8 — Criterio modular. Sea $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ no constante con $a_n \neq 0$.
Si $\exists q \in \mathbb{N}$ primo tal que:

- $q \nmid a_n$ (es decir, el grado no varia).
- $\overline{p}(x) := \sum_{i=0}^{n} [a_i]_q x^i$ es irreducible en $\mathbb{Z}_q[x]$

entonces $p(x)$ es irreducible en $\mathbb{Q}[x]$.

Proof.

En el libro de Hungerford. ■

Ejemplo 1.3.6. Sea $p(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$. Pensamos este polinomio en $\mathbb{Z}_2$: $\overline{p}(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$.
$\overline{p}(0) = 1 \neq 0$ y $\overline{p}(1) = 1 \neq 0 \Rightarrow$ no tiene factores de grado 1.
En caso de ser reducible, tendria que descomponerse en dos factores irreducibles, siendo uno de grado 2 y otro de grado 3.
Como son los irreducibles en $\mathbb{Z}_2[x]$ de grado 2? $x^2 + ax + b \Rightarrow g(0)$ tiene que ser distinto de cero $\Rightarrow g(0) = b = 1$. Tambien $g(1) = 1 + a + b \neq 0 \Rightarrow a = 1$.
Vamos a ver dividir $x^5 + x^4 + 1$ entre $x^2 + x + 1$. Nos da resto 1. Por tanto no tiene factores de grado 2. Hemos llegado a que $x^5 + x^4 + 1$ es irreducible en $\mathbb{Z}_2[x]$. Aplicando el criterio modular, $x^5 + 8x^4 + 3x^2 + 4x + 7$ es irreducible en $\mathbb{Q}[x]$.

§1.3.6 Cuerpos finitos

Teorema 1.3.9. Sean K un cuerpo, $p(x) \in K[x]$ no constante e $I = (p(x))$ el ideal principal generado por $p(x)$. Las siguientes afirmaciones son equivalentes:

1. $p(x)$ es irreducible
2. $K[x]/I$ es un dominio de integridad
3. $K[x]/I$ es un cuerpo

Proof.

- 3) $\Rightarrow$ 2) Obvio (tema 1).
- 1) $\Rightarrow$ 3) Vamos a ver que $I = (p(x))$ es un ideal maximal de $K[x]$. Supongamos que $\exists M$ ideal de $K[x]$ tal que $I \subsetneq M \subseteq K[x]$. Por tanto, $\exists q(x) \in M$ pero $q(x) \notin I$.

  Como $p(x)$ es irreducible, $mcd(p(x), q(x)) = 1$. Por el teorema de existencia de identidades de Bezout, $\exists a(x), b(x)$ tal que $1 = \underbrace{a(x)\underbrace{p(x)}_{\in M}}_{\in M} + \underbrace{b(x)\underbrace{q(x)}_{M}}_{\in M} \in M \Rightarrow K[x] \subseteq M$.

  Luego I es maximal. Por el teorema, $K[x]/I$ es un cuerpo
- 2) $\Rightarrow$ 1) Supongamos que $K[x]/(p(x))$ es dominio de integridad y veamos que $p(x)$ es irreducible.

  Por reduccion al absurdo, supongamos que $p(x) = q_1(x) \cdot q_2(x)$ con $gr(q_1), gr(q_2) < gr(p)$.

$$\left.\begin{array}{l} 0 \neq q(x) + I \\ 0 \neq q_2(x) + I \end{array}\right\} \Rightarrow \underbrace{(q_1(x) + I)}_{\neq 0}\underbrace{(q_2(x) + I)}_{\neq 0} = p(x) + I = 0$$

Esto es una contradiccion porque es dominio de integridad. Luego $p(x)$ es irreducible. ■

Ejemplo 1.3.7. Sea $p(x) - x^2 + x + 1 \leftarrow$ irreducible en $\mathbb{Z}_2[x]$.

$$\mathbb{Z}_2[x]/(p(x)) \leftarrow \text{ cuerpo de 4 elementos.}$$

Todos los restos de dividir $a_1x + a_0$ entre $p(x)$ son $\{[0], [1], [x], [1] + [x]\}$.

Teorema 1.3.10. Sea $p(x)$ irreducible en $\mathbb{Z}_p[x]$. Entonces $\mathbb{Z}_p[x]/(p(x))$ es un cuerpo finito con p^n-elementos donde $n = gr(p(x))$.

§1.4 Mas ejemplos de anillos. DFU, DIP y DE.

§1.4.1 Cuerpo de fracciones de un anillo

Proposición 1.4.1. Sea A un dominio de integridad. Consideramos el conjunto

$$S = \{(a, b)/a, b \in A, b \neq 0_A\}$$

junto con la relacion $(a, b) \sim (c, d)$ si y solo si $ad = bc$. Esta relacion es de equivalencia.

Proposición 1.4.2. Consideramos el conjunto cociente $K = S/\sim$. Para la clase de equivalencia de un elemento, utilizaremos la notacion

$$[(a, b)]_\sim = \frac{a}{b}$$

Definimos en K las siguientes dos operaciones:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \; \forall \frac{a}{b}, \frac{c}{d} \in S/\sim$$

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ad}{bc} \forall \frac{a}{b}, \frac{c}{d} \in S/\sim$$

Estas operaciones estan bien definidas (no dependen de la eleccion de representantes).

Proposición 1.4.3. K dotado de las dos operaciones anteriores es un cuerpo.
El conjunto K recibe el nombre de **cuerpo de fracciones** de A. Se denota $K = cdf(A)$.

Ademas, existe un monomorfismo de anillos unitarios $\varphi\colon A \to cdf(A),\ a \mapsto \frac{a}{1}$. Mas aun, si A es un cuerpo entonces φ es un isomorfismo: $A \cong cdf(A)$.

Ejemplo 1.4.1.

- Si $A = \mathbb{Z}$, entonces $cdf(A) = \mathbb{Q}$.
- Si $A = K[x]$ (sirve con que K sea DI), $cdf(A) = \{\underbrace{\frac{p(x)}{q(x)}}_{\text{(clases)}} / p(x), q(x) \in A, q(x) \neq 0\}$.

  En este caso $cdf(A) = K(x)$.

§1.4.2 Los anillos $A[b]$, $K(b)$

Vamos a ver otros dominios de integridad de los que podemos hallar su cuerpo de fracciones.

Proposición 1.4.4. Sea B un a.c.c.u., A un subanillo de B, $b \in B$ y la funcion

$$\begin{aligned} f_b\colon A[x] &\longrightarrow B \\ p(x) &\longmapsto f_b(p(x)) = p(b) \end{aligned}$$

Entonces f_b es un homomorfismo de anillos.

Definición 1.4.1. $A[b] \coloneqq im(f_b) = \{p(b) \mid p \in A[x]\}$

Corolario 1.4.1. $A[b]$ es un subanillo de B.

Ejemplo 1.4.2.

- $\mathbb{R}[i] = \{p(i) \mid p(x) \in \mathbb{R}[x]\} \overset{i^2=-1}{=} \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$.
  Por ejemplo, $3x^3 + x^2 + x + 2 = p(x) \to p(i) = -3i - 1 + i + 2 = -2i + 1 \in \mathbb{R}[i]$.
  Ademas, se tiene que $x^2 + 1$ es el polinomio minimo de i.
- $\mathbb{Z}[\sqrt{2}] = \{p(\sqrt{2}) \mid p \in \mathbb{Z}[x]\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$.
  $\mathbb{Z}[x] \Rightarrow p(x) = (x^2 - 2)q(x) + \underbrace{r(x)}_{a+bx}$.
  Al evaluarlo en $\sqrt{2}, p(\sqrt{2}) = ((\sqrt{2})^2 - 2)q(x) + r(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2}$.
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$.
- $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$. El polinomio minimo es $x^3 - 2$.
- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ (enteros de Gauss).

Definición 1.4.2. Sea K un cuerpo.

$$K(x) \coloneqq cdf(K[x]) = \{\frac{p(x)}{q(x)} \mid p, q \in K[x], q \neq 0\}$$

Definición 1.4.3. Sean L otro cuerpo tal que $K \subseteq L$ y $b \in L$.

$$K(b) \coloneqq cdf(K[b]) = \left\{\frac{p(b)}{q(b)} \mid p, q \in K[x], q(b) \neq 0\right\}$$

Observación 1.4.1. Si $K[b]$ es cuerpo, entonces $K[b] = K(b)$.
Por ejemplo $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

§1.4.3 DFU, DIP, DE

Definición 1.4.4. Sea A un anillo con unidad.

$$A^* \coloneqq \{a \in A \mid a \text{ es invertible}\}$$

Definición 1.4.5 — Elemento irreducible. Sea $a \in A \setminus A^*, a \neq 0$. Decimos que a es irreducible si sus unicos divisores son elementos invertibles y asociados de a. En caso contrario decimos que a es reducible.

Definición 1.4.6 — DFU. Sean A un DI. Decimos que A es dominio de factorizacion unica (DFU) si todo elemento $a \in A \setminus A^*, a \neq 0$, factoriza como producto de elementos irreducibles de manera unica (salvo reordenacion y asociados).

Ejemplo 1.4.3.

- $K[x]$ es un DFU.
- $\mathbb{Z}$ es un DFU (teorema fundamental de la aritmetica).

Definición 1.4.7 — DIP. Sea A un DI. Decimos que A es dominio de ideales principales (DIP) si todo ideal de A es principal, es decir, $\forall I$ ideal de A existe $a \in A$ tal que $I = (a)$.

Ejemplo 1.4.4.

- $\mathbb{Z}$ es DIP. Todos los ideales de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$ para algun $m \in \mathbb{Z}$.
- $\mathbb{Z}[x]$ no es DIP.
- $K[x]$ es DIP.

Definición 1.4.8 — DE. Sea A un DI. Decimos que A es **dominio euclideo** (DE) si existe una funcion, llamada **norma**, $\delta\colon A \setminus \{0_A\} \to \mathbb{N} \cup \{0\}$ tal que

1. $\forall a, b \in A \setminus \{0_A\}$ se tiene que $\delta(a) \leq \delta(ab)$
2. $\forall a, b \in A, b \neq 0_A$, $\exists q, r \in A$ tales que $a = bq + r$ y r cumple que $\delta(r) < \delta(b)$ o bien $r = 0_A$.

Ejemplo 1.4.5.

- $K[x]$ es un DE con $\delta =$ grado.
- $\mathbb{Z}$ con $\delta =$ "valor absoluto" tambien es DE.

Teorema 1.4.1. A DE $\Rightarrow$ A DIP $\Rightarrow$ A DFU $\Rightarrow$ A DI

Ejemplo 1.4.6. Contraejemplos a los reciprocos:

- $\mathbb{Z}[\sqrt{-5}]$ es DI pero no DFU.
- $\mathbb{Z}[x]$ es DFU pero no DIP.
- $\mathbb{Z}\left[\dfrac{n + \sqrt{-19}}{2}\right]$

2 Grupos

§2.0.1 Definiciones básicas

Definición 2.0.1 — Grupo. Un grupo es un par $(G, \otimes)$ donde:

- G es un conjunto no vacio
- $\otimes: G \times G \to G$ es una operacion interna

que cumplen:

1. Asociativa: $\forall a, b, c \in G \ (a \otimes b) \otimes c = a \otimes (b \otimes c)$
2. Existencia de neutro: $\exists e_G \in G \mid \forall a \in G \ a \otimes e_G = e_G \otimes a = a$
3. Existencia de inversos: $\forall a \in G \ \exists b \in G \mid a \otimes b = b \otimes a = e_G$

Definición 2.0.2. Un grupo $(G, \otimes)$ es abeliano o conmutativo si la operacion $\otimes$ es conmutativa, es decir, $\forall a, b \in G \ a \otimes b = b \otimes a$.

Proposición 2.0.1.

1. Sean G un conjunto y $\otimes$ una opreacion en G con elemento neutro e_G. Se cumple que e_G es el unico elemento de G con la propiedad que define al neutro.
2. Sea $(G, \otimes)$ un grupo. Se cumplen las propiedades de cancelacion:

$$\forall a, b, c \in G \qquad a \otimes b = a \otimes c \Rightarrow b = c$$
$$b \otimes a = c \otimes a \Rightarrow b = c$$

3. En un grupo, el inverso de cualquier elemento es unico.

Proof.

1. Supongamos que $\exists e_1, e_2$ que tienen la propiedad de neutro. Entonces $e_1 = e_1 \otimes e_2 = e_2 \Rightarrow e_1 = e_2$.
2. Como $a \in G$ tiene inverso, multiplicando por el inverso en ambos lados se obtiene el resultado (trivial).

3. Sea $a \in G$ y supongamos que $\exists b_1, b_2$ que actuan como inversos de a. Entonces $b_1 = b_1 \otimes e = b_1 \otimes (a \otimes b_2) = (b_1 \otimes a) \otimes b_2 = e \otimes b_2 = b_2$.

■

En el caso en el que G sea conmutativo, $\otimes$ se suele denotar $+$, al elemento neutro se le denota 0 y el inverso de cada elemento $a \in G$ se llama opuesto y se denota $-a$.
En general, la operacion interna en el grupo se denota como $\cdot$ o simplemente por yuxtaposicion $a \cdot b = ab = a \otimes b$, y a^{-1} denota el inverso de $a \in G$.

Definición 2.0.3. El orden de un grupo G es su numero de elementos, es decir, $|G|$.
Notacion: $ord(G)$.

Ejemplo 2.0.1.

- $(A, +, \cdot)$ es un anillo $\Rightarrow (A, +)$ es un grupo abeliano.
- $(A, +, \cdot)$ es un anillo $\Rightarrow (A^*, \cdot)$ es un grupo, con $A^* = \{\text{elementos invertibles de A}\}$
- En particular, $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ con p primo.
  $\mathbb{Z}_6^* = \{1, 5\} = \{m \in \mathbb{Z}_6 \mid mcd(m, 6) = 1\}$
  $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$
- $(\mathcal{M}_{m\times n}(K), +)$ es un abeliano.
- Se denomina grupo general lineal a $GL_n = (\{A \in \mathcal{M}_n(K) \mid det(A) \neq 0\}, \cdot)$.
- Se denomina grupo especial lineal a $SL_n = (\{A \in \mathcal{M}(K) \mid det(A) = 1\}, \cdot)$ (contenido en el anterior).

Proposición 2.0.2. Sean G un grupo y $a \in G$. Las funciones $f_a \colon G \to G$ y $g_a \colon G \to G$ definidas como $f_a(x) \coloneqq ax$ y $g_a(x) \coloneqq xa$ son biyectivas.

Definición 2.0.4 — Funcion phi de Euler. La funcion $\varphi \colon \mathbb{N} \setminus \{1\} \to \mathbb{N}$ definida como $\varphi(n) \coloneqq ord(\mathbb{Z}_n^*)$ recibe el nombre de funcion phi de Euler.

Proposición 2.0.3.

1. p es primo $\Rightarrow \varphi(p) = p - 1$
2. p es primo y $k \geq 2 \Rightarrow \varphi(p^k) = (p - 1)p^{k-1}$
3. $m, n \geq 2$ tales que $mcd(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

Definición 2.0.5. Sea $(G, \cdot)$ un grupo y $\varnothing \neq H \subseteq G$. Decimos que H es subgrupo de G si:

1. $\forall r, s \in H \quad r \cdot s \in H$
2. $(H, \cdot|_{H\times H})$ cumple la definicion de grupo.

Proposición 2.0.4 — Caracterizacion 1 de subgrupo. Sea $(G, \cdot)$ un grupo y $H \subseteq G$. H es subgrupo de G si y solo si se cumplen:

1. $e_g \in H$
2. $\forall r \in H \quad r^{-1} \in H$
3. $\forall r, s \in H \quad r \cdot s \in H$

Proposición 2.0.5 — Caracterizacion 2 de subgrupo. Sea $(G, \cdot)$ un grupo y $H \subseteq G$. H es subgrupo de G si y solo si se cumplen:

- $e_g \in H$
- $\forall r, s \in H \quad r \cdot s^{-1} \in H$

Definición 2.0.6. Sean $(G_1, \otimes_1)$ y $(G_2, \otimes_2)$ dos grupos. En el conjunto $G_1 \times G_2$ se define la operacion

$$(x_1, x_2) \otimes (y_1, y_2) \coloneqq (x_1 \otimes_1 y_1, x_2 \otimes_2 y_2) \in G_1 \times G_2$$

Proposición 2.0.6. $(G_1 \times G_2, \otimes)$ es un grupo.

Definición 2.0.7. Sea $(G, \cdot)$ un grupo y $a \in G$ podemos definir:

$$L_a \colon G \longrightarrow G \qquad R_a \colon G \longrightarrow G$$
$$x \longmapsto ax \qquad\qquad x \longmapsto xa$$

Ademas, L_a y R_a son biyectivas.

Definición 2.0.8 — Homomorfismo. Sean $(G_1, \otimes_1)$ y $(G_2, \otimes_2)$ dos grupos y $f\colon G_1 \to G_2$ una funcion. Decimos que f es homomorfismo de grupos si cumple:

$$\forall x, y \in G_1 \quad f(x \otimes_1 y) = f(x) \otimes_2 f(y)$$

Observación 2.0.1. En general, L_a y R_a no son homomorfismos de grupos.

Definición 2.0.9 — Monomorfismo, epimorfismo, isomorfismo, automorfismo. Sean G_1 y G_2 dos grupos y $f\colon G_1 \to G_2$ una funcion.
Decimos que f es un monomorfismo de grupos si f es un homomorfismo inyectivo ($G_1 \hookrightarrow G_2$), epimorfismo si f es un homomorfismo suprayectivo ($G_1 \twoheadrightarrow G_2$), isomorfismo si f es un homomorfismo biyectivo, y automorfismo si f es un isomorfismo tal que $G_1 = G_2$.

Definición 2.0.10 — Grupos isomorfos. Sean G_1 y G_2 dos grupos. Decimos que G_1 y G_2 son grupos isomorfos si existe algun isomorfismo $f\colon G_1 \to G_2$.
Notacion: $G_1 \cong G_2$.

Proposición 2.0.7. Sea $f\colon G_1 \to G_2$ un homomorfismo de grupos. Se cumple:

1. $f(e_1) = e_2$
2. $\forall a \in G_1 \; f(a^{-1}) = (f(a))^{-1}$

Proof. 1. $f(e_1) = f(e_1 \cdot_1 e_1) = f(e_1) \cdot_2 f(e_1) \overset{\text{Cancelacion}}{\Rightarrow} e_2 = f(e_1)$.

2. $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e_1) = e_2 \Rightarrow (f(a))^{-1} = f(a)$.
   Analogamente, $f(a^{-1}) \cdot f(a) = e_2$.

■

Proposición 2.0.8. Sean $f\colon G \to H$ y $g\colon H \to L$ homomorfismos de grupos. Entonces $g \circ f$ es un homomorfismo de grupos.

Proof.

Trivial. ■

Proposición 2.0.9. Sea $f\colon G \to H$ un isomorfismo de grupos. Se cumple:

1. f^{-1} es isomorfismo de grupos.
2. G abeliano $\Rightarrow H$ abeliano.

Proposición 2.0.10. La relacion de isomorfia de grupos es una relacion de de equivalencia.

Definición 2.0.11. Sea $f\colon G \to H$ un homomorfismo de grupos. Se definen el nucleo y la imagen de f como:

- $Kerf \coloneqq \{x \in G \mid f(x) = e_H\}$
- $Imf \coloneqq \{y \in H \mid \exists x \in G \mid \exists f(x) = y\}$

Proposición 2.0.11.

1. $Kerf$ es un subgrupo de G.
2. f es inyectiva $\Leftrightarrow Kerf = \{e_G\}$.
3. Imf es un subgrupo de H.
4. f es suprayectiva $\Leftrightarrow Imf = H$.

Proof.

- Veamos que $Kerf$ es cerrado para la operacion. Si $h_1, h_2 \in Kerf$, $h_1h_2 \in Kerf$?.

$$f(h_1h_2) \overset{\text{Homomorfismo}}{=} \underbrace{f(h_1)}_{e}\underbrace{f(h_2)}_{e} = e$$

Luego $h_1h_2 \in Kerf$.

Si $h \in H$, $f(h^{-1}) = (\underbrace{f(h)}_{e})^{-1} = e$. $Kerf$ es cerrado para opuestos.

■

§2.0.2 Orden de un elemento

Sean G un grupo, $a \in G$ y $k \in \mathbb{N}$, denotamos $a^k \coloneqq \underbrace{a \cdot a \cdots a}_{k \text{ veces}}$, $a^{-k} \coloneqq (a^{-1})^k$ y $a^0 \coloneqq e_G$.

Definición 2.0.12 — Orden de un elemento. Sean G un grupo y $a \in G$.

- Decimos que a es de orden finito si $\exists k \in \mathbb{N}$ tal que $a^k = e$. En ese caso definimos el

orden de a como:

$$ord(a) := \text{mín}\{k \in \mathbb{N} \mid a^k = e\}$$

- Decimos que a es de orden infinito si $\nexists k \in \mathbb{N}$ tal que $a^k = e$. En ese caso definimos el orden de a como:

$$ord(a) := \infty$$

Ejemplo 2.0.2. 1. $G = (\mathbb{Z}_3, +) \leftarrow$ grupo abeliano con neutro 0. En vez de escribir a^k, escribiremos $Ka = a + a + \cdots + a$ (k veces). Tenemos que $o(0) = 1$, $o(1) = 8$, $o(2) = 4$, $o(3) = 8$, $o(4) = 2$, $o(5) = 8$, $o(6) = 4$ y $o(7) = 8$.

2. En $G = (\mathbb{Z}_8^*, \cdot)$, $o(1) = 1$, $o(3) = 2$, $o(5) = 2$, $o(7) = 2$.
3. En $G = (\mathbb{Z}, +)$, $o(0) = 1$ y $\forall x \neq 0$ $o(1) = \infty$.
4. $G = (\mathbb{Z}_2 \times \mathbb{Z}_3, +)$, $o(1, 1) = 6$...

Proposición 2.0.12. Sean G un grupo y $a \in G$.

1. G finito $\Rightarrow \forall a \in G$ a es de orden finito.
2. $ord(a) = \infty \Rightarrow \{a^0, a^1, a^2, \ldots, a^k, \ldots\}$ esta formado por elementos distintos dos a dos.
3. Sean $k \in \mathbb{Z}$ y $n = ord(a)$. Entonces:

$$a^k = e \Leftrightarrow n|k$$

4. Sean $j, k \in \mathbb{Z}$ y $n = ord(a)$. Entonces:

$$a^j = a^k \Leftrightarrow j \equiv k \pmod{n}$$

5. Sea $n = ord(a)$ y supongamos que $n = td$. Entonces $ord(a^t) = d$.

Proof. 1. Supongamos que $|G| = n$ con $n \in \mathbb{N}$. Consideramos $a, a^2, a^3, \ldots, a^n, a^{n+1}$.

Como $|G| = n$, tiene que haber al menos 2 iguales en la lista anterior.

Sea $a^k = a^m$ con $k > m$. Multiplicando por $(a^m)^{-1}$ ($(a^m)^{-1} = a^{-1} \cdot a^{-1} \cdots a^{-1}$ (m veces)) en ambos lados, $a^k \cdot a^{-m} = a^m \cdot a^{-m} = e \Rightarrow a^{k-m} = e \Rightarrow ord(a) < \infty$.

2. Por reduccion al absurdo, supongamos que en la lista $a, a^2, \ldots, a^m, \ldots$ hay dos elementos a^k y a^m que son iguales.

Supongamos que $a^k = a^m$ con $k > m$. Multiplicando por $(a^m)^{-1}$, $a^{k-m} = a^k \cdot a^{-m} = e \Rightarrow ord(a) < \infty$.

3. Supongamos que $o(a) = n < \infty$.

   "$\Rightarrow$" Supongamos que $a^k = e$. Tengo que $k = n \cdot q + r \Rightarrow e = a^k = a^{nq+r} = (a^n)^q \cdot a^r = e^q a^r = a^r$. Hay dos casos: $r = 0$ o $n > r \neq 0$. Si $n > r \neq 0$, hay una contradiccion con que $o(a) = n$. Luego $r = 0$ y por tanto $n|k$.

   "$\Leftarrow$" $n|k$, es decir, $k = nq$. Entonces $a^k = a^{nq} = (a^n)^q = e$.

4. "$\Rightarrow$" Supongamos que $a^i = a^j$ y que $i > j$. Multiplicamos por a^{-j} y nos queda $\underbrace{a^i \cdot a^{-j}}_{a^{i-j}} = a^j \cdot a^{-j} = e \Rightarrow n|i-j \Leftrightarrow i \equiv j \pmod{n}$.

   "$\Leftarrow$" Supongamos que $i \equiv j \pmod{n}$, es decir, $i - j$ es multiplo de n: $\exists k \in \mathbb{Z} \mid i - j = n \cdot k$ $(i = j + nk)$. Nos queda

   $$a^i = a^{j+nk} = a^j \cdot (\underbrace{a^n}_{e})^k = a^j$$

5. Queremos ver que $ord(a^2) = d$. Hay que ver que $(a^t)^d = e$ (a) y que $\nexists d' < d$ tal que $(a^t)^d = e$ (b).

   En primer lugar, $(a^t)^d = a^{td} = a^n = e$ (a).

   (b) Por reduccion al absurdo, supongamos que $\exists d' < d$ tal que $(a^t)^d = e$. Entonces tendriamos que $n' = td' < td = n$. Esto no puede ser porque entonces existiria $n' < n$ tal que $a^{n'} = e$ y es una contradiccion con que $ord(a) = n$.

■

§2.0.3 Grupos ciclicos

Definición 2.0.13. Decimos que un grupo G es ciclico si $\exists a \in G$ tal que $G = \{a^k \mid k \in \mathbb{Z}\}$. En ese caso decimos tambien que a es un generador de G.
Notacion: $G = \langle a \rangle$.

Observación 2.0.2. Un grupo ciclico puede tener varios generadores distintos.

Observación 2.0.3. Los grupos ciclicos siempre son abelianos. Dados $a^k, a^j \in G$,

$$a^k \cdot a^j = a^{k+j} = a^{j+k} = a^j \cdot a^k$$

Proposición 2.0.13. Sean G un grupo ciclico y a un generador de G. Entonces:

- Si $ord(a) = \infty \Rightarrow G \cong \mathbb{Z}$

Es mas, la siguiente funcion es un isomorfismo

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow G \\ k &\longmapsto a^k \end{aligned}$$

- Si $ord(a) = n \Rightarrow G \cong \mathbb{Z}_n$

  Es mas, la siguiente funcion es un isomorfismo

$$\begin{aligned} f\colon \mathbb{Z}_n &\longrightarrow G \\ [k]_n &\longmapsto a^k \end{aligned}$$

Proof.

- Veamos que f es homomorfismo de grupos:

$$f(n+m) = a^{n+m} = a^n \cdot a^m = f(n) \cdot f(m)$$

  Tambien es inyectivo por el apartado 2 de la proposicion 2.0.12.

  Es suprayectiva por la definicion de grupo ciclico (todo elemento es de la forma a^k asi que $f(k) = a^k$).

  Luego f es isomorfismo.

- Supongamos que $ord(a) = n < \infty$.

  Definimos $f\colon \mathbb{Z}_n \to G, [k] \mapsto a^k$. Veamos si esta bien definida: si $k' \in [k]_n \Rightarrow k' \equiv_n k \overset{4) \text{ de } 2.0.12}{\Rightarrow} a^k = a^{k'} = f([k])$.

  Es homomorfismo de grupos ya que $f([k] + [j]) = f([k+j]) = a^{k+j} = a^k \cdot a^j = f([k]) \cdot f([j])$.

  f es inyectiva porque si $a^k = a^j \overset{4) \text{ de } 2.0.12}{\Rightarrow} k \equiv_n j \Leftrightarrow [k] = [j]$.

  Como el grupo es ciclico, todo elemento es de la forma a^k, una preimagen es $[k]_n$ ya que $f(k) \coloneqq a^k$. Por tanto es suprayectiva.

■

Proposición 2.0.14 — Subgrupo ciclico generado por un elemento. Sean G un grupo y $b \in G$.

$$\langle b \rangle \coloneqq \{b^k \mid k \in \mathbb{Z}\} \text{ es un subgrupo de } G$$

§2.0.4 Grupos de permutaciones

Definición 2.0.14. Sea $T \neq \varnothing, G = \{f\colon T \to T \mid f \text{ es biyectiva}\}$ y $\circ$ el simbolo que denota la composicion de funciones.
Entonces $(G, \circ)$ es un grupo ya que la composicion es una operacion interna en G, es

asociativa, tiene elemento neutro ($id\colon T \to T$) y $\forall f \in G, \exists f^{-1} \in G \mid f \circ f^{-1} = id$. Ademas, $(G, \circ)$ recibe el nombre de grupos de permutaciones de G.

Definición 2.0.15 — Grupo de permutaciones de n elementos. Sea $T_n = \{1, 2, \dots, n\}$ el conjunto formado por los primeros n numeros naturales. Definimos:

$$S_n \coloneqq \{\sigma\colon T_n \to T_n \mid \sigma \text{ es biyectiva}\}$$

$(S_n, \circ)$ recibe el nombre de grupo de permutaciones de n elementos o grupo simetrico.

Proposición 2.0.15. $|S_n| = n!$

Dado $\sigma \in S_n$ usaremos la siguiente notacion matricial para referirnos a σ:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Ejemplo 2.0.3.

$$\sigma = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 2\ 1\ 3\ 5\ 4 \end{pmatrix} \in S_5$$

Un caso particular de permutacion viene dado por los ciclos.

Definición 2.0.16. Sea $k \in \mathbb{N}$, $k \geq 2$. Decimos que una permutacion $\sigma \in S_n$ es un k-ciclo si $\exists a_1, a_2, \dots, a_k \in T_n$ tal que:

- $\forall i \in \{1, \dots, k-1\}\ \sigma(a_i) = a_{i+1}$
- $\sigma(a_n) = a_1$
- $\forall a \notin \{a_1, \dots, a_k\} \quad \sigma(a) = a$

$$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} \dots \xrightarrow{\sigma} i_k \xrightarrow{\sigma} i_1$$

Dado $\sigma \in S_n$ un k-ciclo, usaremos la siguiente notacion para referirnos a σ :

$$\sigma = \left(a_1 \dots a_k\right)$$

Ejemplo 2.0.4. $\sigma = \begin{pmatrix} 2 & 5 & 1 \end{pmatrix} \in S_5 \equiv \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} \qquad ord(\sigma) = 3$

Definición 2.0.17. Se dice que un ciclo es una trasposicion si tiene longitud 2.

Definición 2.0.18. Dados dos ciclos $\sigma, \tau \in S_n$, $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}$ y $\tau = \begin{pmatrix} b_1 & b_2 & \cdots & b_m \end{pmatrix}$, decimos que σ y τ son disjuntos si

$$\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_m\} = \varnothing$$

Ejemplo 2.0.5.

- $\begin{pmatrix} 2 & 5 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 4 \end{pmatrix}$ son disjuntos.
- $\begin{pmatrix} 2 & 5 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 3 \end{pmatrix}$ son disjuntos.

Observación 2.0.4. Los ciclos disjuntos conmutan.

Usualmente omitiremos el simbolo de composicion y escribiremos simplemente las permutaciones una despues de otra:

$$\sigma\tau \coloneqq \sigma \circ \tau$$

Proposición 2.0.16. Toda permutacion $\sigma \in S_n$ se puede escribir como composicion de ciclos disjuntos.

Proof.

Sea $\sigma \in S_n$. Sea i_1 tal que $i_1 \neq \sigma(i_1) = i_2, i_2 \neq \sigma(i_2) = i_3, i_3 \neq \sigma(i_3), i_4 \neq \sigma(i_4), \ldots$. Sea i_k el primero que cumple que $\sigma(i_k) \in \{i_1, i_2, \ldots, i_{k-1}\}$.
Veamos que $\sigma(i_k) = i_1$. Por reduccion al absurdo, supongamos que $\sigma(i_k) = i_j$ con $j > 1$. Entonces $\sigma(i_k) = i_j = \sigma(i_{j-1})$. Esto es imposible porque σ es biyectiva. Luego $\sigma(i_k) = i_1$.
Sea $b \in \{1, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$ tal que $\sigma(b) \neq b$: $b_1 = b, b_2 = \sigma(b_1), \ldots, b_s = \sigma(b_{s-1}), \sigma(b_s) = b_1$.
Repetimos el proceso hasta descomponer todo σ y nos queda que $\sigma = (i_1 i_2 \cdots i_k)(b_1 \cdots b_s)$ ■

Ejemplo 2.0.6. 1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 3 & 1 & 8 & 7 & 4 & 5 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 6 & 7 & 4 \end{pmatrix} \begin{pmatrix} 5 & 8 \end{pmatrix}$

2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 2 & 4 & 6 & 3 & 8 \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 & 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 7 \end{pmatrix} \begin{pmatrix} 6 & 8 \end{pmatrix}$

Ejemplo 2.0.7. Composicion a la derecha:
$\begin{pmatrix} 2 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 5 & 2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$

Lema 2.0.1. Todo ciclo se escribe como producto de trasposiciones (no necesariamente disjuntas).

Proof.
$\begin{pmatrix} i_1 & i_2 & \cdots & i_k \end{pmatrix} = \begin{pmatrix} i_1 & i_k \end{pmatrix} \begin{pmatrix} i_i & i_{k-1} \end{pmatrix} \begin{pmatrix} i_1 & i_{k-2} \end{pmatrix} \cdots \begin{pmatrix} i_1 & i_2 \end{pmatrix}$ ■

Corolario 2.0.1. Toda permutacion se escribe como producto de trasposiciones.

Proof.
Trivial. ■

Definición 2.0.19. Decimos que una permutacion es:

- par si se escribe como un numero par de trasposiciones
- impar si se escribe como un numero impar de trasposiciones

$$\begin{aligned} s\colon S_n &\longrightarrow \mathbb{Z}_2 \\ \sigma &\longmapsto 0 \text{ si es par} \\ \sigma &\longmapsto 1 \text{ si es impar} \end{aligned}$$

Observación 2.0.5. La descomposicion con trasposiciones no es unica.

Lema 2.0.2. La identidad no se puede poner como un numero impar de trasposiciones.

Proof.
Hungerford, pg 222. ■

Teorema 2.0.1. Una permutacion no puede ser par e impar a la vez.

Proof.

Sea σ una permutacion tal que $\sigma = \tau_1\tau_2\cdots\tau_m = \mu_1\mu_2\cdots\mu_n$ con cada τ_i y μ_i una trasposicion y m par y n impar. Entonces

$$id = \sigma\sigma^{-1} = (\tau_1\tau_2\cdots\tau_m)\cdot(\mu_1\mu_2\cdots\mu_n)^{-1} = \tau_1\tau_2\cdots\tau_m\cdot\mu_n\cdots\mu_1$$

Hemos escrito id como producto de $m+n$ trasposiciones. Pero esto es imposible porque $m+n$ es impar y sabemos que la identidad solo se puede poner como un numero par de trasposiciones.
Por tanto, una permutacion no puede ser par e impar a la vez. ■

Definición 2.0.20. Se denomina signatura o signo de una permutacion a la funcion

$$\begin{aligned} f\colon S_n &\longrightarrow \mathbb{Z}_2 \\ \sigma &\longmapsto f(\sigma) = \begin{cases} 0 \text{ si } \sigma \text{ es par} \\ 1 \text{ si } \sigma \text{ es impar} \end{cases} \end{aligned}$$

Proposición 2.0.17. Sea $A_n \coloneqq \{\sigma \in S_n \mid \sigma \text{ es par}\}$. Se cumple que A_n es un subgrupo de S_n. A_n recibe el nombre de grupo alternado de grado n.

Proposición 2.0.18. $|A_n| = \dfrac{n!}{2}$

§2.0.5 Grupo diedrico

Definición 2.0.21 — Grupo diedrico. Sea $n \geq 3$. Definimos el grupo diedral o grupo diedrico de grado n como el conjunto D_n formado por los movimientos del plano que dejan invariante un poligono regular de n lados.

Proposición 2.0.19.

- D_n con la composicion de aplicaciones es un grupo.
- $|D_n| = 2n$
- $D_n = \{id, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau_1, \tau_2, \ldots, \tau_n\}$ donde σ es el giro de angulo $2\pi/n$ en sentido

positivo (antihorario) y $\tau_1, \ldots, \tau_n$ son simetrias respecto de los n ejes que pasan por el centro del poligono.

- Ademas:
  - La identidad y los giros preservan la orientacion
  - Las simetrias invierten la orientacion.

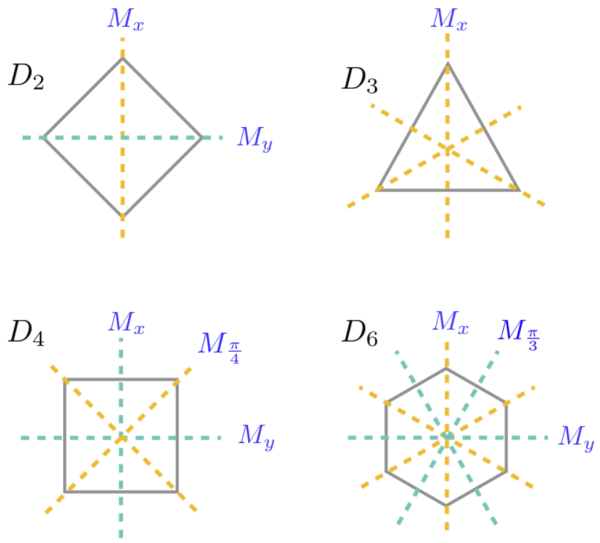
Ejemplo 2.0.8.

- $D_3 = \{1, \sigma, \sigma^2, \tau_1, \tau_2, \tau_3\}$

  Composicion simetria y giro: $\sigma\tau_1 : 1 \to 3, 2 \to 2, 3 \to 1 = \tau_3$.

  $\sigma = \tau_1\tau_2 : 1 \to 2, 2 \to 3, 3 \to 1$.

- $D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau_1, \tau_2, \tau_3, \tau_4\}$



Observación 2.0.6. Otra forma de escribir $D_n = \langle \sigma, \tau \mid o(\sigma) = n, o(\tau) = 2, \tau\sigma\tau = \sigma^{-1} \rangle$ (grupo dado por generadores y relaciones).

Observación 2.0.7. D_n puede verse como un subgrupo de S_n, numerando los vertices del poligono regular del 1 al n e identificando cada movimiento con la permutacion que induce en el conjunto de los vertices.

Ejemplo 2.0.9.

- $D_3 \leq S_3$:

$$D_3 = \{1, \underbrace{(123)}_{\sigma}, \underbrace{(132)}_{\sigma^2}, \underbrace{(12)}_{\tau_1}, \underbrace{(23)}_{\tau_2}, \underbrace{(13)}_{\tau_3}\}$$

- $D_4 \leq S_4$:

$$D_4 = \{1, \underbrace{(1234)}_{\sigma}, \underbrace{(13)(24)}_{\sigma^2}, \underbrace{(1432)}_{\sigma^3}, \underbrace{(24)}_{\tau_1}, \underbrace{(12)(34)}_{\tau_2}, \underbrace{(13)}_{\tau_3}, \underbrace{(14)(23)}_{\tau_4}\}$$

§2.1 Subgrupos normales y grupos cociente

§2.1.1 Definiciones basicas

Definición 2.1.1 — Congruencia modulo un subgrupo. Sean G un grupo y H un subgrupo de G (notacion: $H < G$).
Se dice que dos elementos $a, b \in G$ son congruentes por la izquierda modulo H si

$$a^{-1} \cdot b \in H$$

Notacion: $a \equiv_i b \pmod{H}$
Se dice que dos elementos $a, b \in G$ son congruentes por la derecha modulo H si

$$b \cdot a^{-1} \in H$$

Notacion: $a \equiv_d b \pmod{H}$

Observación 2.1.1. Si G es abeliano, las dos definiciones anteriores coinciden.

Proposición 2.1.1. Las dos relaciones de la Definicion 2.1.1 son relaciones de equivalencia.

Proof. 1. Reflexiva: $a \equiv_i a \pmod{H}$?
Si porque $a^{-1} \cdot a = e \in H$

2. Simetrica: $a \equiv_i b \pmod{H} \Rightarrow b \equiv_i a \pmod{H}$?
Por hipotesis: $a^{-1} \cdot b \in H \overset{H \leq G}{\Rightarrow} b^{-1}(a^{-1})^{-1} = b^{-1}a = (a^{-1}b)^{-1} \in H$ es decir $b \equiv_i a \pmod{H}$

3. Transitiva: $a \equiv_i b \pmod{H}, b \equiv_i c \pmod{H} \Rightarrow a \equiv_i c \pmod{H}$?
Como $H \leq G$, $(a^{-1}b)(b^{-1}c) \in H$ y $(a^{-1}b)(b^{-1}c) = a^{-1}bb^{-1}c = a^{-1}c \in H \Rightarrow a \equiv_i c \pmod{H}$.

Analogamente, se prueba que $\equiv_d$ es una relacion de equivalencia. ■

Las clases de equivalencia de estas relaciones (clases laterales o cogrupos) son:

$$[a]_{i,H} = \{b \in G \mid a \equiv_i b \pmod{H}\}$$

$$[a]_{d,H} = \{b \in G \mid a \equiv_d b \pmod{H}\}$$

Proposición 2.1.2.

$$[a]_{i,H} = \{a \cdot h \mid h \in H\} \coloneqq aH \text{ (clase por la izquierda)}$$

$$[a]_{d,H} = \{h \cdot a \mid h \in H\} \coloneqq Ha \text{ (clase por la derecha)}$$

Proof.

Lo demostraremos por doble contenido.
"$\subseteq$" Sea $b \in G$ tal que $a^{-1} \cdot b \in H$, es decir, $\exists h \in H$ tal que $a^{-1} \cdot b = h \Rightarrow b = a \cdot h \in \{a \cdot h \mid h \in H\} = aH$
"$\supseteq$" Sea $\underbrace{ah}_{b} \in aH$. Entonces $a^{-1}b = a^{-1}ab = eh = h \in H$.
Por tanto, $ah \in \{b \in G \mid a^{-1}b \in H\}$.
La demostracion para la relacion de equivalencia por la derecha es analoga. ■

Ejemplo 2.1.1. Sea $G = D_4 = \{1, \underbrace{(1234)}_{\sigma}, \underbrace{(13)(24)}_{\sigma^2}, \underbrace{(1432)}_{\sigma^3}, \underbrace{(24)}_{\tau_1}, \underbrace{(12)(34)}_{\tau_2}, \underbrace{(13)}_{\tau_3}, \underbrace{(14)(23)}_{\tau_4}\}$.
Consideramos $H = \{id, (24)\} \leq G$ (subgrupo abeliano).
Vamos a coger σH y $\sigma^3 H$. Tenemos $\sigma H = \{\sigma h \mid h \in H\} = \{\sigma, \sigma\tau_1\} = \{(1234), (14)(23)\}$ y $\sigma^3 H = \{\sigma^3 h \mid h \in H\} = \{\sigma^3, \sigma^3\tau_3\} = \{(1432), (12)(34)\}$.
Nos inventamos la operacion: $\sigma H \cdot \sigma^3 H = \sigma\sigma^3 H = H = \{1, (13)\}$.
Si escogemos otro representante, $\sigma\tau_3 H \cdot \sigma^3 H = \sigma\tau_3\sigma^3 H = \tau_1 H = \{(24), (24)(13)\} \neq \{1, (13)\}$. Esto no es posible.
Para corregir este problema, vamos a imponer que $aH = Ha \; \forall a \in G$.

Definición 2.1.2 — Subgrupo normal. Sean $H < G$. Decimos que H es normal en G si $\forall a \in G$ se tiene que $aH = Ha$.
Notacion: $H \lhd G$.

Teorema 2.1.1. Sea $H \leq G$. Las siguientes afirmaciones son equivalentes:

1. H es normal en G.
2. $\forall a \in G$, $a^{-1}Ha = H$
3. $\forall a \in G$, $a^{-1}Ha \subseteq H$
4. $\forall a \in G$, $\forall h \in H$, $a^{-1}ha \in H$

Proof.

1) $\Rightarrow$ 2) Por hipotesis, H es un subgrupo normal de G, asi que $\forall a \in G\ aH = Ha$, es decir, $\{ah \mid h \in H\} = \{ha \mid h \in H\}$. Multiplicando por la izquierda por a^{-1} cada uno de los elementos de estos conjuntos, $\{a^{-1}ah \mid h \in H\} = \{a^{-1}ha \mid h \in H\} \Rightarrow \{h \mid h \in H\} = H = a^{-1}Ha$.

2) $\Rightarrow$ 3) Obvio.

3) $\Rightarrow$ 4) Obvio.

4) $\Rightarrow$ 1) Queremos ver que $aH = Ha\ \forall a \in G$. Por doble contenido,
$\supseteq$) Sea $ha \in Ha$. Multiplicamos por la izquierda por a^{-1} y tenemos $\underbrace{a^{-1}ha}_{\in H (5)} = h_1 \in H$. Luego $ha = a\underbrace{a^{-1}ha}_{h_1} = ah_1 \in aH$.
$\subseteq$) Tomamos $ah \in aH$. Sabemos que si tomamos $b = a^{-1}$, el apartado 5) nos dice que $b^{-1}hb \in H$, es decir, $(a^{-1})^{-1}ha^{-1} = aha^{-1}$. Luego $\exists h_2 \in H$ tal que $aha^{-1} = h_2 \in H$.
Por tanto, $ah = aha^{-1}a = \underbrace{aha^{-1}}_{h_2} \cdot a = h_2 a \in Ha$. ■

Definición 2.1.3. Si G es abeliano, todo subgrupo de G es normal.

Proposición 2.1.3 — Subgrupo normal $\Rightarrow$ producto bien definido. Sean $H \lhd G$. Sean $a, b, c, d \in G$ tales que $a_1H = a_2H$ y $b_1H = b_2H$. Entonces se tiene

$$a_1b_1H = a_2b_2H$$

Proof.

Veamos si este producto esta bien definido, es decir, que $abH = cdH$.

$$(a_2b_2)^{-1} \cdot a_1b_1 = b_2^{-1}\underbrace{a_2^{-1}a_1}_{\in H} \cdot b_1 = b_2^{-1} \cdot \underbrace{h_1 \cdot b_1}_{Hb_1 = b_1H} \overset{h_1b_1 = b_1h_2}{=} b_2^{-1}b_1h_2 \in H$$

Es decir, $a_1b_1 \equiv_I a_2b_2 \Rightarrow a_1b_1H = a_2b_2H$ ■

Definición 2.1.4. Sean $H \lhd G$. Denotamos el cociente de G bajo cualquiera de las relaciones de la definicion 2.1.1 (ambas coinciden) como

$$G/H := \{aH \mid a \in G\}$$

Proposición 2.1.4 — Grupo cociente. Sean $H \lhd G$. Definimos en el cociente G/H la operacion $(aH)\cdot(bH) := abH$. El conjunto G/H con esta operacion es un grupo.

Lema 2.1.1. Si $f\colon G \to H$ es un isomorfismo entonces $\forall a \in G, o(a) = o(f(a))$.

Proof.

Si $o(a) = n < \infty$, se cumple que $o(f(a)) = n$?
Sabemos que $(f(a))^n = \underbrace{f(a)\cdot f(a)\cdots f(a)}_{n \text{ veces}} \overset{\text{Hom}}{=} f(a\cdot a\cdots a) = f(a^n) = f(e_G) = e_H$.
Entonces supongamos que $\exists m < n$ tal que $(f(a))^m = e \Rightarrow e = (f(a))^m = \underbrace{f(a)\cdots f(a)}_{} = f(a^m) \Rightarrow f^{-1}(e) = f^{-1}\cdot f(a^m) = a^m$. Esto es una contradiccion porque $m < n$ y $o(a) = n$.
Si $o(a) = \infty$, por reduccion al absurdo supongamos que $o(f(a)) \neq \infty$. Entonces $e_H = (f(a))^m \overset{\text{Hom}}{\Rightarrow} e_H = f(a^m) \Rightarrow f^{-1}(e_H) = f^{-1}(f(a^m)) \Rightarrow e_G = a^m \Rightarrow o(a) \leq m$. Contradiccion con que $a = \infty$. ■

§2.1.2 Indice de un subgrupo y Teorema de Lagrange

Proposición 2.1.5. Sea G un grupo y H un subgrupo de G, podemos definir una biyeccion

$$\begin{aligned} f\colon G/\cong_i &\longrightarrow G/\cong_d \\ aH &\longmapsto f(aH) = Ha^{-1} \end{aligned}$$

Proof.

Veamos que f esta bien definida. Supongamos que $aH = bH$, es decir, $a \equiv_i b \Rightarrow a^{-1}b \in H \Rightarrow b\cdot a^{-1} \in H \overset{def}{\Leftrightarrow} b^{-1} \equiv_d a^{-1} \pmod H$, es decir, $Hb^{-1} = Ha^{-1}$.
Veamos que f es inyectiva. Suponer que $Ha^{-1} = Hb^{-1}$, es decir, $a^{-1} \equiv_d b^{-1} \pmod H \Leftrightarrow a^{-1}(b^{-1})^{-1} = a^{-1}b \Rightarrow a \equiv b \pmod H$, es decir, $aH = bH$.
Tambien es suprayectiva. Si tomamos Hb en $G/\cong_d$, $f(b^{-1}H) = Hb$. ■

Definición 2.1.5. Sean $H < G$. Se define el indice de H en G como el cardinal del conjunto formado por las clases por la izquierda modulo H (que, por la proposicion anterior, coincide con el cardinal del conjunto formado por las clases por la izquierda modulo H). Se denota como $[G\colon H]$.

Observación 2.1.2. Si H es normal en G, es trivial que los indices por la izquierda y por la derecha coinciden y se puede definir el indice. Pero la proposicion 5 demuestra que,

aunque H no sea normal en G, el indice esta bien definido.

Teorema 2.1.2 — de Lagrange. Sean G un grupo finito y $H < G$. Se cumple que

$$|G| = [G\colon H] \cdot |H|.$$

En particular notese que $|H|$ divide a $|G|$. Ademas, si $H \trianglelefteq G$, entonces $|G/H| = \dfrac{|G|}{|H|}$.

Proof.

Suponemos que $H = \{h_1, h_2, \ldots, h_n\} \leftarrow n$ elementos. Vemos que $aH = \{ah_1, ah_2, \ldots, ah_n\}$, con todos los elementos distintos dos a dos por la propiedad de cancelacion. Es decir, $|aH| = |H|$.
Como $\equiv_i$ es una relacion de equivalencia, G es la union disjunta de las clases de equivalencia a la izquierda. Por tanto, $|G| = \underbrace{|H| + \cdots + |H|}_{[G\colon H] \text{ veces}} = [G\colon H] \cdot |H|$.

■

Corolario 2.1.1. Sea G un grupo finito:

1. $\forall a \in G$, $o(a)$ divide a $|G|$
2. $\forall a \in G$, $a^{|G|} = e$
3. Si $H \triangleleft G$, entonces
$$|G/H| = \frac{|G|}{|H|}$$

Proof.

1. Si tomamos $H = \langle a \rangle$ (subgrupo ciclico generado por a), $|H| = o(a)$. Por el teorema de Lagrange, $o(a)$ divide a $|G|$.
2. Sabemos que $o(a)$ divide a $|G|$. Por tanto, $a^{|G|} = a^{o(a)\cdot m} = (\underbrace{a^{o(a)}}_{e})^m = e$.
3. Obvio.

■

Corolario 2.1.2 — Teorema de Euler. $\forall a \in \mathbb{Z}_n^*$, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Proof.

Llamamos $G = \mathbb{Z}_n^*$. Sabemos que $|G| = \varphi(n)$. Por el apartado 2 del corolario anterior, $a^{\varphi(n)} = 1_{\mathbb{Z}_n^*} \Leftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$ ■

Observación 2.1.3. El pequeño teorema de Fermat es otro corolario importante.

§2.1.2.1 Ejemplos de aplicacion del teorema de Lagrange

Ejemplo 2.1.2.

- Dado un primo p, hallar todos los grupos de orden p (salvo isomorfismo).

  Sea G un grupo con $|G| = p$. Si $a \in G$, $o(a) = 1 \vee o(a) = p$ (porque $o(a)$ divide a $|G|$). Sabemos que si $o(a) = 1$, $a = e$.

  Si $o(a) = p$, $\langle a \rangle = \{\underbrace{a, a^2, \ldots, a^{o(a)}}_{p \text{ elem}}\} = G$.

  Vamos a intentar definir un homomorfismo entre G y $\mathbb{Z}_p$.

$$\begin{aligned} f\colon (G, \cdot) &\longrightarrow (\mathbb{Z}_p, +) \\ a^k &\longmapsto [k]_p \end{aligned}$$

  - Homomorfismo:
$$f(a^k \cdot a^l) = f(a^{k+l})$$
    Si $k + l \leq p$, $f(a^{k+l}) = k + l = f(a^k) + f(a^l)$. Si $k + l > p$, por el teorema de la division $\exists q, r \in \mathbb{Z}$ tal que $k + l = pq + r$. Luego $f(a^{k+l}) = f(a^{pq+r}) = f(a^r) = [r]_n = [k + l] = [k] + [l] = f(a^k) + f(a^l)$.
  - Inyectiva:
$$Ker f = \{a^k \mid k \leq p \mid f(a^k) = 0\} = \{a^p\} = \{e\}$$
    Por tanto, es inyectiva.
  - Es suprayectiva por construccion: $k \in \mathbb{Z}_p, a^k$ cumple $f(a^k) = k$.

  Por lo tanto, $G \cong \mathbb{Z}_p$.

- Hallar todos los grupos de tamaño 4. Sea $|G| = 4$. Dado un $a \in G$, $o(a) = 1 \vee o(a) = 2 \vee o(a) = 4$. Si en G tenemos algun elemento a con $o(a) = 4$, $\langle a \rangle = \{a, a^2, a^3, a^4\} = G$ y $G \cong \mathbb{Z}_4$ (igual que antes para p). En caso contrario, todos los elementos salvo el neutro tienen orden 2. Sea $G = \{e, a, b, c\}$.

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Podemos definir

$$\begin{aligned} f\colon G &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \\ e &\longmapsto (0,0) \\ a &\longmapsto (1,0) \\ b &\longmapsto (0,1) \\ c &\longmapsto (1,1) \end{aligned}$$

Comprobar que es isomorfismo.

- Hallar todos los subgrupos de S_3.

  $|S_3| = 3! = 3 \cdot 2 = 6$ y $S_3 = \{id, (12), (13), (23), (123), (132)\}$.

  Sea $\sigma \in S_3$, $o(\sigma) \in \{1,2,3\}$. $o(\sigma) \neq 6$ porque entonces $\underbrace{\langle\sigma\rangle}_{S_3} \cong \mathbb{Z}_6$ pero $S_3 \not\cong \mathbb{Z}_6$ porque $\mathbb{Z}_6$ es conmutativo y S_3 no.

  Si $o(\sigma) = 1, \langle\sigma\rangle = \{id\}$. Si $o(\sigma) = 2$, $\langle(12)\rangle = \{id, (12)\} = H_1$, $\langle(13)\rangle = \{id, (13)\} = H_2$, $\langle(23)\rangle = \{id, (23)\} = H_3$. Si $o(\sigma) = 3$, $\langle(123)\rangle = \{id, (123), (132)\} = H_4$. Estos son los conjuntos no triviales de S_3.

Proposición 2.1.6. Sean $H \leq G$ tales que $[G\colon H] = 2$. Entonces H es normal en G.

Proof.

Supongamos que $[G\colon H] = 2$. Entonces $\{H, aH\}$ (2 clases) o $\{H, Ha\}$ (2 clases).
$G = H \underset{disjunta}{\cup} aH$, $aH = \{x \in G \mid x \notin H\}$ y $G = H \underset{disjunta}{\cup} Ha$, $Ha = \{x \in G \mid x \notin H\}$.
Por tanto, $aH = Ha$ y H es normal. ■

§2.1.3 Teoremas de isomorfia

Proposición 2.1.7. Sea $f\colon G_1 \to G_2$ un homomorfismo de grupos. Se cumple que $Kerf \trianglelefteq G_1$.

Proof.

Sea $H = Kerf$. Sabemos que $Kerf$ es un subgrupo de G_1. Nos falta ver que $H \trianglelefteq G_1 \Rightarrow \forall a \in G_1, \forall h \in H,\ a^{-1}ha \in H$?

$$f(a^{-1}ha) = \underbrace{f(a^{-1})}_{(f(a))^{-1}} \underbrace{f(h)}_{e} f(a) = e$$

■

Teorema 2.1.3 — Primer teorema de isomorfia. Sea $f\colon G_1 \to G_2$ un homomorfismo de grupos. Entonces la siguiente funcion es un isomorfismo de grupos:

$$\begin{aligned} \overline{f}\colon G_1/Kerf &\longrightarrow Imf \\ aKerf &\longmapsto \overline{f}(aKerf) = f(a) \end{aligned}$$

Proof.

En primer lugar, veamos que $\overline{f}$ esta bien definida. Si $aKerf = bKerf$, $f(a) = f(b)$?
Como $aKerf = bKerf$, $a^{-1}b \in Kerf \Rightarrow \underbrace{f(a^{-1}b)}_{e} \overset{\text{Hom.}}{=} f(a^{-1})f(b) = (f(a))^{-1} \cdot f(b)$.
Despejando, tenemos que $f(a) = f(b)$.
Veamos que f es homomorfismo: $\overline{f}((aKerf)(bKerf)) = \overline{f}(abKerf) = f(ab) \overset{\text{Hom.}}{=} f(a) \cdot f(b) = \overline{f}(aKerf) \cdot \overline{f}(bKerf)$.
Ademas, se cumple que es inyectiva. Si $f(a) = f(b)$, es lo mismo que $e = f(a)^{-1} \cdot f(b) \Rightarrow e = f(a^{-1}) \cdot f(b) \overset{\text{Hom}}{=} f(a^{-1}b)$, es decir, $a^{-1}b \in Kerf \Rightarrow a \equiv_i b \pmod{Kerf} \Rightarrow aKerf = bKerf$.
Por ultimo, $\overline{f}$ es suprayectiva por construccion.
Luego $\overline{f}$ es un isomorfismo de grupos. ■

Corolario 2.1.3.

$$|A_n| = \frac{n!}{2}$$

Proof.

Definimos la funcion

$$\begin{aligned} f\colon S_n &\longrightarrow \mathbb{Z}_2 \\ \sigma &\longmapsto f(\sigma) = \begin{cases} 0 \text{ si } \sigma \text{ es par} \\ 1 \text{ si } \sigma \text{ es impar} \end{cases} \end{aligned}$$

Sabemos que f es un homomorfismo de grupos suprayectivo. Ademas, $Kerf = A_n$. Por tanto, aplicando el primer teorema de isomorfia, $S_n/A_n \cong \mathbb{Z}_2$. Como $|\mathbb{Z}_2| = 2$, $|S_n/A_n| = 2$ y aplicando el teorema de Lagrange $|S_n| = 2 \cdot |A_n| \Rightarrow |A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$. ■

Teorema 2.1.4 — Segundo teorema de isomorfia. Sean G un grupo, $H \leq G$ y $N \trianglelefteq G$. Entonces:

1. $HN \coloneqq \{hn \mid h \in H, n \in N\}$ es un subgrupo de G.
2. $N \triangleleft HN$ y $H \cap N \triangleleft H$.
3. $HN/N \cong H/H \cap N$.

Proof. 1. Tenemos que ver que HN es un subgrupo de G. Si $h_1n_1, h_2n_2 \in HN$, como $N \trianglelefteq G, \exists n_3 = h_2^{-1}n_1h_2 \in N \Rightarrow h_2n_3 = n_1h_2$. Por tanto, $h_1n_1h_2n_2 = h_1h_2n_3n_2 \in HN$. Luego es cerrado para el producto. Equivalentemente, $n_1h_2 \in Nh_2 = h_2N \Rightarrow \exists n_3$ tal que $n_1h_2 = h_2n_3 \Rightarrow h_1n_1h_2n_2 = h_1h_2n_3n_2$.

Si $hn \in HN$, $(hn)^{-1} = n^{-1}h^{-1} \overset{\exists n_4 \in N}{=} h^{-1}n_4 \in HN$. Luego es cerrado para opuestos.

2. Veamos que $N \triangleleft HN$. Si $\forall x \in G\ xN = Nx$, entonces $\forall x \in HN$, $xN = Nx$ (porque $HN \subseteq G$).

3. Vamos a definir

$$\begin{aligned} f\colon H &\longrightarrow G/N \\ h &\longmapsto f(h) = hN \end{aligned}$$

f es homomorfismo de grupos: Dados $h_1, h_2 \in H$, $f(h_1h_2) = h_1h_2N = (h_1N)(h_2N) = f(h_1) \cdot f(h_2)$.

Por otro lado, $Kerf = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N \trianglelefteq H$ (porque $Kerf$ es normal). Asi queda demostrada la segunda parte de 2).

$Imf = \{f(h) \mid h \in H\} = \{hN \mid h \in H\} \overset{*}{=} \{hN \mid h \in HN\}$.

(*) $\subseteq$) $hN = \underbrace{h}_{\in H}\underbrace{e}_{\in N}N \in \{hN \mid h \in HN\}$.

$\supseteq$) $hnN = hN \cdot nN = hN \in \{hN \mid h \in H\}$

Por el primer teorema de isomorfia

$$\overline{f}\colon H/Kerf \longrightarrow Imf$$

es un isomorfismo. Por tanto, $H/H \cap N \cong HN/N$.

■

Teorema 2.1.5 — Tercer teorema de isomorfia. Sean G un grupo y $K, H \triangleleft G$ tales que $K \subseteq H$. Entonces:

1. $K \triangleleft H$.
2. $(H/K) \triangleleft (G/K)$.
3. $((G/K)/(H/K)) \cong (G/H)$.

Proof. 1. Como K es subgrupo normal de G, $\forall x \in G$ se tiene que $xK = Kx$. Por tanto, en particular $\forall x \in H$, $xK = Kx$. Luego $K \trianglelefteq H$.

2. Se obtiene como consecuencia de la demostracion de 3).

3. Vamos a definir
$$f\colon G/K \longrightarrow G/H$$
$$xK \longmapsto f(xK) = xH$$
Veamos si esta bien definida, es decir, si dados $x, y \in G$ $xK = yK$ entonces $xH = yH$. Como $xK = yK \Rightarrow x^{-1}y \in K \subseteq H$. Por este contenido, $x \equiv_y \pmod{H}$. Luego tenemos que $xH = yH$.

Veamos si es homomorfismo de grupos. Dados $xK, yK \in G/K$, $f((xK)(yK)) = f(xyK) = xyH = (xH)(yH) = f(xK)f(yK)$.

Hallamos el nucleo de f. $Kerf = \{xK \mid f(xK) = 1_{G/H}\} = \{xK \mid xH = H\} = \{xK \mid x \in H\} = H/K$. Como $Kerf$ es subgrupo normal de G/K, tenemos que $(H/K) \triangleleft (G/K)$ (2).

Por construccion, f es suprayectiva. Luego $Imf = G/H$.

Por el primer teorema de isomorfia,
$$\overline{f}\colon (G/K)/Kerf \longrightarrow Imf$$
$$xK \cdot Kerf \longmapsto \overline{f}(xK) = f(xK) = xH$$
Luego $(G/K)/(H/K) \cong G/H$.

■

§2.2 Mas sobre grupos

§2.2.1 Centro, centralizador y normalizador

Definición 2.2.1 — Centro de un grupo. Sea G un grupo. Se define el centro de G como el conjunto
$$Z(G) \coloneqq \{x \in G \mid \forall g \in G\ gx = xg\}$$

Proposición 2.2.1.
- $Z(G)$ es subgrupo normal de G.
- G es abeliano si y solo si $G = Z(G)$.

Proof.
- Veremos dentro de un rato que $Z(G) = Ker(\hat{\varphi})$ donde $\hat{\varphi}$ es un homomorfismo de grupos, y por tanto $Z(G) \leq G$.
- Trivial.

■

Ejemplo 2.2.1. 1. $G = S_3 = \{id, (123), (132), (13), (23), (12)\}$.

$\sigma = (12) \in Z(G)$? $(12)(13) = (132)$, $(13)(12) = (123)$. Luego $(12) \notin Z(G)$. Analogamente, $(13) \notin Z(G)$.

$\mu = (123) \in Z(G)$? $(123)(12) = (123)$, $(12)(123) = (23) \Rightarrow \mu \notin Z(G)$. De modo analogo, $(132) \notin Z(G)$ (es su cuadrado).

Luego, en este ejemplo, $Z(G) = \{id\}$.

2. $G = D_4 = \{id, (1234), (13)(24), (1432), (24), (12)(34), (13), (14)(23)\}$.

   $\sigma = (1234) \in Z(G)$? $(1234)(24) = (12)(34)$, $(24)(1234) = (14)(23)$. Como son distintos, $\sigma \notin Z(G)$. De la misma manera $(1432) \notin Z(G)$.

   $\sigma^2 = (13)(24) \in Z(G)$? $(13)(24)(12)(34) = (14)(32)$, $(12)(34)(13)(24) = (14)(32) \Rightarrow$ conmutan. Probamos con $(14)(23) \Rightarrow (13)(24)(14)(23) = (12)(34)$, $(14)(23)(13)(24) = (12)(34)$. Ademas, conmuta con σ^n por ser potencias y con τ_1 porque se tachan los (24).

   $\tau_2 = (12)(34) \in Z(G)$? $(12)(34)(24) = (1234)$ y $(24)(12)(34) = (1432)$. Luego $\tau_2 \notin Z(G)$.

   Por el teorema de Lagrange, $Z(G)$ no puede tener 3 elementos. Descartamos τ_4.

   Por tanto, $Z(G) = \{id, (13)(24)\}$.

3. $G = \{A \in \mathcal{M}_2(\mathbb{R}) \mid |A| \neq 0\}$.

   $AB = BA \quad \forall B \Rightarrow A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \ \lambda \neq 0.$

   Para n, $GL_n = \{A \in \mathcal{M}_n(\mathbb{R}) \mid |A| \neq 0\}$. Se tiene que $Z(GL_n) = \{\lambda I_n \mid \lambda \neq 0\}$.

Definición 2.2.2 — Centralizador de un conjunto en un grupo. Sean G un grupo y H un subgrupo de G. Se define el centralizador de H en G como el conjunto

$$C_G(H) \coloneqq \{x \in G \mid \forall h \in H \quad xh = hx\} = \{x \in G \mid \forall h \in H \quad xhx^{-1} = h\}$$

Definición 2.2.3 — Normalizador de un conjunto en un grupo. Sean G un grupo y H un subgrupo de G. Se define el normalizador de H en G como el conjunto

$$N_G(H) \coloneqq \{x \in G \mid xH = Hx\} = \{x \in G \mid xHx^{-1} = H\}$$

§2.2.2 Acciones de grupos

Definición 2.2.4 — Accion de un grupo sobre un conjunto. Sean G un grupo y X un

conjunto no vacio. Una accion (por la izquierda) de G sobre X es una aplicacion

$$\begin{aligned} \phi\colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto \phi(g, x) = g \cdot x \end{aligned}$$

que cumple:

1. Si e es el neutro de G, entonces $g \cdot x = x$
2. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \quad \forall g_1, g_2 \in G,\ \forall x \in X.$

Usamos la notacion $\cdot$ para la accion. Si queremos denotar que estamos operando dos elementos del grupo ponemos uno a continuacion del otro, sin nada en medio.

Proposición 2.2.2. Dada una accion $\varphi\colon G \times X \to X$, podemos definir un homomorfismo asociado

$$\begin{aligned} \hat{\phi}\colon G &\longrightarrow S(X) = \{\sigma\colon X \to X \mid \sigma \text{ biyectiva}\} \\ g &\longmapsto \phi_g \end{aligned}$$

con

$$\begin{aligned} \phi_g\colon X &\longrightarrow X \\ x &\longmapsto \phi_g(x) = g \cdot x \end{aligned}$$

Proof.

Veamos que $\hat{\phi}$ esta bien definida y que es homomorfismo de grupos:

- Bien definida: $\phi_g\colon X \to X$ es una biyeccion de X?
  - Inyectiva: si $g \cdot x_1 = g \cdot x_2$ entonces $g^{-1}(g \cdot x_1) = g^{-1}(g \cdot x_2) \overset{2)}{\Rightarrow} (g^{-1} \cdot g) \cdot x_1 = (g^{-1} \cdot g) \cdot x_2 \overset{1)}{\Rightarrow} e \cdot x_1 = e \cdot x_2 \Rightarrow x_1 = x_2$.
  - Suprayectiva: si $y \in X$, $\exists x \in X$ tal que $g \cdot x = y \Rightarrow x = g^{-1}y$?

$$y = g \cdot \underbrace{(g^{-1} \cdot y)}_{\in X} = \phi_g(g^{-1} \cdot y) = y$$

- Homomorfismo: $g_1, g_2 \in G$
  - $\hat{\phi}(g_1 \cdot g_2) = \begin{aligned} \phi_{g_1 \cdot g_2}\colon X &\to X \\ x_2 &\mapsto (g_1 g_2) \cdot x \end{aligned}$
  - $\begin{aligned} \hat{\phi}(g_1) \cdot \hat{\phi}(g_2)\colon X &\to X \\ x &\mapsto g_1(g_2 x) \end{aligned}$ (composicion)

■

Definición 2.2.5. Una accion es fiel si $Ker\hat{\phi} = \{e\}$.

Ejemplo 2.2.2. 1. Si σ es un grupo y $x = \sigma$, podemos definir

$$\begin{aligned} \varphi\colon X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x = gxg^{-1} \end{aligned}$$

Es accion?

- $e \cdot x = exe^{-1} = x \quad \forall x \in X = G$
- $g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x g_2^{-1}) = g_1(g_2 x g_2^{-1})g_1^{-1} = (g_1 g_2)x(g_1 g_2)^{-1} = (g_1 g_2) \cdot x$

Si es una accion.

Veamos su homomorfismo asociado.

$$\begin{aligned} \hat{\varphi}\colon G &\longrightarrow Biy(x) \\ g &\longmapsto \hat{\varphi}(g) = \varphi_g\colon X \to X, x \mapsto gxg^{-1} \end{aligned}$$

$Ker\hat{\varphi} = \{g \in G \mid \varphi_g = id\} = \{y \in G \mid gxg^{-1} = x \ \forall x \in X = G\} = \{g \in G \mid gx = xg \ \forall x \in G\} = Z(G)$ y $Ker\hat{\varphi} \trianglelefteq G \Rightarrow Z(G) \trianglelefteq G$ (resultado que faltaba por probar).

2. G grupo, $X = \{H \text{ tal que } H \leq G\}$.

$$\begin{aligned} \varphi\colon G \times X &\longrightarrow X \\ (g, H) &\longmapsto \varphi((g, H)) = gHg^{-1} \end{aligned}$$

- Bien definida? gHg^{-1} es subgrupo de G?

  Cerrado para el producto: sean gh_1g^{-1}, $gh_2g^{-1} \in K \Rightarrow (gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in K$.

  Contiene inversos: $ghg^{-1} \in K$, $(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in K$.

Veamos que es accion (accion por conjugacion sobre el conjunto de los subgrupos):

a) $e \cdot H = eHe^{-1} = H \ \forall H \in X$

b) $g_1 \cdot (g_2 \cdot H) = g_1(g_2 H g_2^{-1})g_1^{-1} = g_1 g_2 H (g_1 g_2)^{-1}$.

Defino

$$\begin{aligned} \hat{\varphi}\colon G &\longrightarrow Biy(X) \\ g &\longmapsto \varphi_g\colon X \to X, H \mapsto gHg^{-1} \end{aligned}$$

$Ker\hat{\varphi} = \{g \in G \mid \varphi_g = id\} = \{g \in G \mid gHg^{-1} = H \quad \forall H \in X\} = \{g \in G \mid gH = Hg \quad \forall H \in X\} = \bigcap_{H \in X} N(H)$

3. Sea G un grupo y $X = G$.

- Accion por traslacion a la izquierda.

$$\begin{aligned}\varphi\colon G \times X &\longrightarrow X\\ (g,x) &\longmapsto \varphi(g,x) = gx\end{aligned}$$

  Ver que es accion y comprobar que es fiel.

- Accion por traslacion a la derecha.

$$\begin{aligned}\varphi\colon G \times X &\longrightarrow X\\ (g,x) &\longmapsto \varphi((g,x)) = xg^{-1}\end{aligned}$$

  Ver que es accion y comprobar que es fiel.

Definición 2.2.6. Si $\varphi\colon G \times X \to X$ es una accion en X podemos definir la siguiente relacion:

$$x \equiv_\varphi y \Leftrightarrow \exists g \in G \text{ tal que } \varphi(g,x) = y$$

Proposición 2.2.3. La relacion $\equiv_\varphi$ es una relacion de equivalencia en X.

Proof.

Veamos que cumple las propiedades de relacion de equivalencia:

1. Reflexiva: $x \equiv_\varphi x$ porque $e \cdot x = x$
2. Simetrica: si $x \equiv_\varphi y$, $\exists g \in G$ con $g \cdot x = y$, es decir, $\varphi_g(x) = y$. Como φ_g es biyectiva, $g^{-1} \cdot y = x \Rightarrow y \equiv_\varphi x$.
3. Transitiva: si $x \equiv_\varphi y$, $y \equiv_\varphi z \Rightarrow \exists g_1 \in G \mid g_1 \cdot x = y$, $\exists g_2 \in G \mid g_2 \cdot y = z$ $(y = g_2^{-1} \cdot z) \Rightarrow g_1 \cdot x = g_2^{-1} \cdot z \Rightarrow g_2 \cdot g_1 \cdot x = g_2 \cdot g_2^{-1} \cdot z \Rightarrow g_2 g_1 \cdot x = z \Rightarrow x \equiv_\varphi z$.

■

Definición 2.2.7. Dado $x \in X$, se llama orbita de x bajo la accion de φ al conjunto:

$$orb(x) := \{y \in X \mid x \equiv_\varphi y\} = \{y \in X \mid \exists g \in G \text{ tal que } g \cdot x = y\}.$$

Notese que las orbitas son las clases de equivalencia de la relacion $\equiv_\varphi$ y forman, por tanto, una particion de X.

Definición 2.2.8. Una accion es transitiva si solo hay una orbita

$$orb(X) = X, \text{ es decir, } \forall x, y \in X \quad \exists g \in G \text{ tal que } g \cdot x = y$$

Definición 2.2.9. Sean $x \in B$ y φ una accion. Se define el estabilizador de x como el conjunto

$$S_x = \{g \in G \mid g \cdot x = x\}$$

Una notacion alternativa para el estabilizador es $Stab_G(x)$. Notese que el estabilizador de x esta formado por los elementos de G que dejan fijo x cuando actuan sobre el.

Proposición 2.2.4. $\forall x \in B$, S_x es un subgrupo de G.

Proof.

Veamos que $S_x \leq G$.

- Si $g_1, g_2 \in Stab_G(x)$, $g_1 g_2 \in Stab_G(x)$?

$$(g_1 g_2) \cdot x \overset{2)}{=} g_1 \cdot (g_2 \cdot x) \overset{g_2 \in S(x)}{=} g_1 \cdot x \overset{g_1 \in S(x)}{=} x \Rightarrow g_1 g_2 \in Stab_G(x)$$

- Si $g \in Stab_G(x)$, $g^{-1} \in Stab_G(x)$?

$$g^{-1} \cdot x \overset{g \cdot x = x}{=} g^{-1} \cdot (g \cdot x) \overset{2)}{=} \underbrace{(g^{-1} g)}_{e} \cdot x \overset{1)}{=} x, \text{ es decir, } g^{-1} \in Stab_G(x)$$

■

Sea

$$\begin{aligned} \hat{\varphi} \colon G &\longrightarrow Biy(x) \\ g &\longmapsto \hat{\varphi}(g) = \varphi_g \end{aligned}$$

Vamos a calcular $Ker\hat{\varphi}$:

$$Ker\hat{\varphi} = \{g \in G \mid \varphi_g = id\} = \{g \in G \mid g \cdot x = x \quad \forall x \in X\} = \bigcap_{x \in X} Stab_G(x)$$

Ejemplo 2.2.3. Si φ es la accion por conjugacion $X = G$

$$\begin{aligned} \varphi \colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto \varphi((g, x)) = gxg^{-1} \end{aligned}$$

Para $x \in X = G$, $Stab_G(x) = \{g \in G \mid g \times x = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(\{x\}) \leq G$. Como consecuencia de esto, hemos obtenido que el centralizador es un subgrupo.

$$Ker\hat{\varphi} = \bigcap_{x \in X} Stab_G(x) = \bigcap_{x \in X} C_G(\{x\}) = \{g \in G \mid gx = xg \quad \forall x \in X\} = Z(G)$$

Teorema 2.2.1 — de la orbita. Sea φ una accion de un grupo G sobre un conjunto X. Consideramos $H = Stab_G(x) \leq G$.
Consideramos $\{g \cdot Stab_G(x) \mid g \in G\}$ (conjunto de clases a la izquierda respecto de la relacion ser congruente a izquierda modulo H). Podemos definir una biyeccion entre $\{gStab_G(x) \mid g \in G\}$ y $orb(x)$ dada por

$$\begin{aligned} f\colon \{gStab_G(x) \mid g \in G\} &\longrightarrow orb(x) \\ gStab_G(x) &\longmapsto g \cdot x \end{aligned}$$

En particular $[G : Stab_G(x)] = |orb(x)|$.

Proof.

Vamos a ver que f es una biyeccion. En primer lugar, veamos que esta bien definida: si $g_1Stab_G(x) = g_2Stab_G(x)$, entonces $g_1^{-1}g_2 \in Stab_G(x) \Rightarrow (g_1^{-1}g_2)\cdot x = x \Rightarrow g_1\cdot((g_1^{-1}g_2)\cdot x) = g_1 \cdot x \Rightarrow (g_1g_1^{-1}g_2)\cdot x = g_1 \cdot x \Rightarrow g_2 \cdot x = g_1 \cdot x$. Por lo tanto, $f(g_1Stab_G(x)) = f(g_2Stab_G(x))$.
Veamos que es inyectiva. Si $f(g_1Stab_G(x)) = f(g_2Stab_G(x)) \Rightarrow g_1\cdot x = g_2\cdot x \Rightarrow g_1^{-1}\cdot(g_2\cdot x) = g_1^{-1}\cdot(g_2\cdot x) \Rightarrow (g_1^{-1}g_1)\cdot x = (g_1^{-1}g_2)\cdot x \Rightarrow x = (g_1^{-1}g_2)\cdot x$. Luego $g_1^{-1}g_2 \in Stab_G(x) \Rightarrow g_1 \equiv_i g_2$ (mód $Stab_G(x)$) $\Rightarrow g_1Stab_G(x) = g_2Stab_G(x)$.
Nos falta ver que es suprayectiva. Sea $y \in orb(x)$, es decir, $\exists g \in G$ tal que $g \cdot x = y$. Entonces $f(gStab_G(x)) = y$ porque, por definicion, $g \cdot x = y$.
Por tanto, $[G : Stab_G(x)] = |orb(x)|$. ■

Observación 2.2.1. En el caso de que G sea un grupo finito, el teorema anterior nos da la relacion:

$$|orb(x)| = \frac{|G|}{|S_x|}$$

por el teorema de Lagrange.

§2.2.3 Clasificacion de grupos

Definición 2.2.10 — Conjunto generador. Sean G un grupo y $\varnothing \neq S \subseteq G$. Decimos que S es un conjunto generador de G si todo elemento de G se puede escribir como producto finito (que puede ser de un solo factor) de elementos de S y de inversos de elementos de S.

Definición 2.2.11 — Grupo finitamente generado. Decimos que un grupo G es finitamente generado si existe un conjunto S finito y generador de G.

Observación 2.2.2. Si G es finito, es obvio que G es finitamente generado y se puede tomar como conjunto generador al propio G.

Observación 2.2.3.

- Si G es ciclico y $G = \langle a \rangle$, $S = \{a\}$ es el conjunto generador de G.
- D_n tiene como conjunto generador $\{\sigma, \tau\}$ donde σ es el giro de angulo $2\pi/n$ en sentido positivo y τ es una simetria cualquiera.
- S_n esta generado por el conjunto de las trasposiciones: $S = \{(ab) \mid a, b \in \{1, \dots, n\}\}$ es un conjunto generador de S_n porque todo $\sigma \in S_n$ se escribe como producto de trasposiciones.
- Si $G = \mathbb{Z} \times \mathbb{Z} \times \cdots \times Z = \mathbb{Z}^m$, $S = \{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 0, 1)\}$ es un conjunto generador de $\mathbb{Z}^m$.

Los dos siguientes teoremas proporcionan una clasificacion de los grupos abelianos finitamente generados. Ambas clasificaciones son equivalentes, simplemente cambia la presentacion de los grupos.

Teorema 2.2.2 — Descomposicion en factores invariantes. Sea G un grupo abeliano finitamente generado con $|G| \geq 2$. Entonces existen m (rango de la parte libre), $k_1, \dots, k_n \in \mathbb{N} \cup \{0\}$ (factores invariantes de G) tales que

- $\forall j \in \{1, \dots, n\} \quad k_j \geq 2$
- $\forall j \in \{1, \dots, n-1\} \quad k_j | k_{j+1}$
- $G \cong \underbrace{\mathbb{Z}^m}_{\substack{\text{parte} \\ \text{libre}}} \times \underbrace{\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n}}_{\text{parte de torsion}}$

donde

- $\mathbb{Z}^0$ se interpreta como que no aparece este factor.
- Se incluye el caso en el que solo aparece un factor de tipo $\mathbb{Z}^m$.

Ademas los numeros $m, k_1, k_2, \dots, k_n$ son unicos cumpliendo estas condiciones.

Ejemplo 2.2.4.

- Descomposicion de todos los grupos abelianos de orden 36.

  $m = 0$ porque son grupos finitos. Posibilidades para los factores invariantes:

- $k = 36 \to G \cong \mathbb{Z}_{36}$.
- $k_1 = 2, k_2 = 18 \to G \cong \mathbb{Z}_2 \times \mathbb{Z}_{18}$
- $k_1 = 3, k_2 = 12 \to G \cong \mathbb{Z}_3 \times \mathbb{Z}_{12}$
- $k_1 = 6, k_2 = 6 \to G \cong \mathbb{Z}_6 \times \mathbb{Z}_6$

Estos son los 4 grupos (salvo isomorfismo) que podemos tener con las condiciones de ser abeliano y tener orden 36.

Teorema 2.2.3 — Descomposicion en factores primarios. Sea G un grupo abeliano finitamente generado con $|G| \geq 2$. Entonces existen m (rango de la parte libre), $q_1, q_2, \ldots, q_t \in \mathbb{N} \cup \{0\}$ tales que

- $\forall j \in \{1, \ldots, t\} \quad q_j$ es una potencia de un numero primo (se llaman divisores elementales o factores primarios).
- $G \cong \underbrace{\mathbb{Z}^m}_{\substack{\text{parte} \\ \text{libre}}} \times \underbrace{\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n}}_{\text{parte de torsion}}$

donde Ademas los numeros $m, q_1, \ldots, q_t$ son unicos cumpliendo estas condiciones (salvo el orden de los q_j).

Ejemplo 2.2.5. Descomposicion de todos los grupos abelianos de orden 36 (en funcion de sus divisores elementales).
Posibilidades para los divisores elementales:

- $2^2, 3^2 \to G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \cong \mathbb{Z}_{36}$
- $2, 2, 3^2 \to G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_{18}$
- $2, 2, 3, 3, \to G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$
- $2^2, 3, 3 \to G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \times \mathbb{Z}_6$

Vamos a ver cuales son todos los grupos de orden menor o igual que 8. Para ello, introduciremos un grupo de orden 8 que aun no conocemos.

Definición 2.2.12. Consideremos el conjunto $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ donde

- $i^2 = j^2 = k^2 = -1$.
- $ij = k$, $jk = i$, $ki = j$.

Q_8 es un grupo llamado grupo de los cuaternios (o cuaterniones). Ademas, Q_8 no es abeliano y $Z(Q_8) = \{1, -1\}$.

A continuacion se enumeran todos los grupos (salvo isomorfismo) de un orden dado. En la

primera linea aparecen los abelianos y en la segunda, si hay, los no abelianos:

Orden	Grupos
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$ S_3
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8, \mathbb{Z}_2\times\mathbb{Z}_4, \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ D_4, Q_8

Cuadro 1. Grupos de orden menor o igual que 8.