Magma

Es un par $(A, \cdot)$ donde A es un conjunto y $\cdot$ operación binaria interna en A.

$\cdot : A \times A \longrightarrow A$
$(a,b) \longmapsto a \cdot b$

Semigrupo

sea $(A, \cdot)$ un magma, decimos que es un semigrupo si $\cdot$ es asociativa.

Subsemigrupo

Sea $(A, \cdot)$ un semigrupo, con $X \subseteq A$
X subsemigrupo si $\cdot|_X$ es una operación binaria interna.

Monoide

Sea $(A, \cdot)$ un semigrupo, decimos que es un monoide si $\cdot$ tiene elemento neutro

Submonoide

Sea $(A, \cdot)$ un monoide, con $X \subseteq A$
X submonoide si $\cdot$ tiene elemento neutro y coincide.

Grupo

Sea $(G, \cdot)$ monoide, decimos que es un grupo si $\cdot$ tiene el simétrico, esto es,
$\forall g \in G \ \exists! h \in G : g \cdot h = h \cdot g = e$

Subgrupo

Sea un grupo $(G, \cdot)$, $H \subseteq G$ es subgrupo si:
•) $e \in H$
•) $\forall h, h' \in H$, $hh' \in H$ esto es, $\forall a, b \in H$, $ab^{-1} \in H$
•) $\forall h \in H$, $h^{-1} \in H$

$\left\{ \begin{array}{l} (g^{-1})^{-1} = g \\ (ab)^{-1} = b^{-1} a^{-1} \end{array} \right.$

Anillo

$(A,+,\cdot)$ es un conjunto de dos operaciones binarias internas para ser anillo debe verificar:

1) $(A,+)$ grupo abeliano
2) $(A,\cdot)$ monoide
3) $\forall a,b,c \in A$
$a\cdot(b+c) = a\cdot b + ac$
$(a+b)c = ac + bc$

- $A \neq \{0\} \Rightarrow 0 \neq 1$
- $\forall a \in A,\ 0\cdot a = a\cdot 0 = 0$
- $\forall a,b \in A, (-ab) = (-a)b = a(-b)$
- $\forall a,b \in A,\ (-a)(-b) = ab$

Subanillo

$(A,+,\cdot)$ y $B \subseteq A$ es un subanillo si $\cdot$ y $+$ son operaciones internas en B y $i: B \hookrightarrow A$ es un morfismo de anillos, esto es,

$$\forall x,y \in B \quad \begin{cases} x-y \in B \\ xy \in B \\ 1 \in B \end{cases}$$

Ideal

$I \subset A$, siendo A un anillo.

- Si $1 \in I \Rightarrow I = A$
- Si A cuerpo $\Rightarrow \nexists$ ideales propios
- $aR_I b \Leftrightarrow a-b \in I$

1) $(I,+)$ es un subgrupo de $(A,+)$
- $e \in I$
- $\forall h,h' \in I,\ h+h' \in I$, esto es, $a-b \in I \quad \forall a,b \in I$
- $\forall h \in I,\ -h \in I$

2) $\left.\begin{matrix} a \in A \\ i \in I \end{matrix}\right\} ai \in I$ (ideal por la izquierda)

Relaciones de equivalencia

Sea $R \subset X \times X$ una relación binaria en X,

x está relacionado con y, xRy si

- R reflexiva, esto es, $\forall x \in X \quad xRx$
- R simétrica, esto es, $xRy \Rightarrow yRx$
- R transitiva, esto es, $xRy \wedge yRz \Rightarrow xRz$

Si verifica esto se dice que R es una relación de equivalencia. $[x] = \{y \in X : yRx\}$

$\bigcup_{x \in X} [x]_R = X$ partición (quitando repetidos)

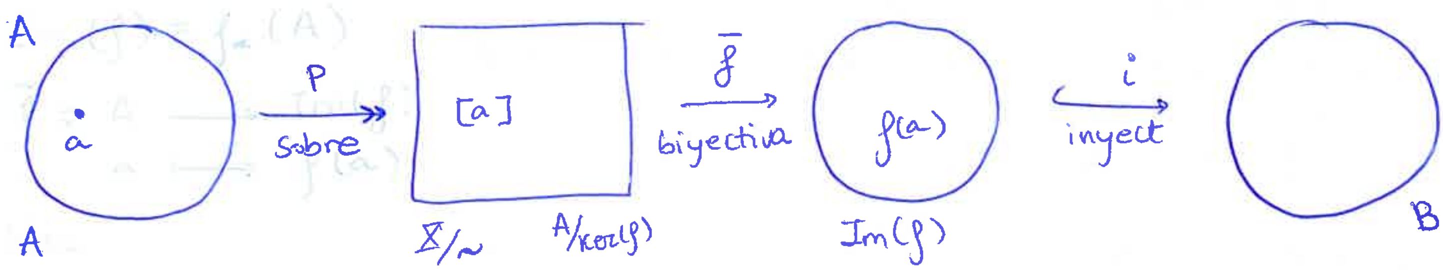
El conjunto de clases de equivalencia con respecto a una relación se denomina conjunto cociente

$X/R = \{ [x]_R : x \in X \}$ es el conj. cociente de X sobre R.

Descomposición canonica de una aplicación.

(Primer teorema de isomorfía)

Sean A, B conjuntos y $f: A \to B$ app



$f = i \circ \bar{f} \circ p$

lo que nos dice este primer teorema de isomorfía es que existe isomorfía entre $X/\sim$ y $Im(f)$, esto es,

$X/\sim \;\cong\; Im(f)$

Congruencia

Es una relación de equivalencia que es compatible con la operación, esto es,

$$aRb \Rightarrow \begin{cases} ca\ R\ cb \\ ac\ R\ bc \end{cases}$$

Homomorfismos o morfismos

Sean $(A, \cdot)$, $(B, *)$ semigrupos

$f: A \to B$ es morfismo de semigrupos si:

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

f es morfismo de monoides si además verifica:

$f(e_A) = e_B$

f es morfismo de grupos si además verifica:

$f(a^{-1}) = f(a)^{-1}$

Sean A, B anillos y $f: A \to B$

f es morfismo de anillos si:

- $f(a+b) = f(a) + f(b) \quad \forall a, b \in A$
- $f(a \cdot b) = f(a) \cdot f(b) \quad \forall a, b \in A$
- $f(1) = 1$

Recordemos que:

- f monomorfismo $\Leftrightarrow \ker(f) = \{0\}$
- f epimorfismo $\Leftrightarrow \operatorname{Im}(f) = B$
- f isomorfismo $\Leftrightarrow$ verifica las dos prop anteriores

Unidades

Sea $(A,+,\cdot)$ anillo

$a \in A$ es una <u>unidad</u> si $\exists b \in A: ab = ba = 1$

Además b es único y se denota por a^{-1}.

$\mathcal{U}(A) = \{a \in A : a \text{ unidad}\}$ $(\mathcal{U}(A), \cdot)$ grupo.

Si $\forall a \in A \setminus \{0\}$ es unidad $\Rightarrow$ A <u>anillo de división</u>

- Anillo división + conmutatividad = Cuerpo

Divisores de cero

Sea $(A,+,\cdot)$ un anillo conmutativo,

$a \in A$ es <u>divisor de cero</u> si $\exists b \in A \setminus \{0\}: ab = 0$

Si A no tiene divisores de cero $\neq \{0\}$ lo denominaremos <u>dominio de integridad</u>

- los dom. integridad son cancelativos
- Cuerpo $\Rightarrow$ dom. integridad
  "$\Leftarrow$" solo si es finito

Si $a,b \in \mathbb{R}$, $ab = 0$

$aa^{-1}b = 0 \Leftrightarrow b = 0$

$abb^{-1} = 0 \Leftrightarrow a = 0$

Características

Sea $(A,+,\cdot)$ anillo

Si $\exists n > 0$ con $n1 = 0$

$\operatorname{car}(A) = \min\{k \in \mathbb{N}^* : k1 = 0\}$

Número de veces que hay que sumar el el. neutro del producto hasta conseguir el el. neutro de la suma.

segundo teorema de isomorfía

Sea A anillo, $B \subseteq A$, $I \trianglelefteq A$ ideal.

1) $B + I \subseteq A$ subanillo
2) $I \trianglelefteq B + I$
3) $B \cap I \trianglelefteq B$
4) $\dfrac{B}{B \cap I} \cong \dfrac{B+I}{I}$

Un el. <u>NO</u> puede ser unidad y div de 0 al mismo tiempo

Suponemos a. div. 0 y unidad.

$a \cdot b = 0$ porque a es div. 0.

unidad $\Rightarrow \exists a^{-1}$

$0 = a^{-1} \cdot 0 = a^{-1} \cdot a \cdot b = 1 \cdot b = b$

pero esto es contradicción ya que si se multiplica por 0 no es div. 0.

Tercer teorema de isomorfía

sea A anillo, $I \trianglelefteq A$, $J \trianglelefteq A$, $J \subseteq I$

A/I, A/J anillos.

① $I/J = \{ i + J : i \in I \} \trianglelefteq A/J$

② $$\frac{A/J}{I/J} \cong \frac{A}{I}$$

Algunas definiciones

Sea A conmutativo

- $I \trianglelefteq A$ es <u>principal</u> si $\exists a \in A$ $I = aA$. (Lo escribiremos $I = (a)$).
- $I \trianglelefteq A$ es <u>primo</u> si $\forall a, b \in A$, si $ab \in I \Rightarrow \begin{cases} a \in I \\ \vee \\ b \in I \end{cases}$
- $I \trianglelefteq A$ es <u>maximal</u> si $\nexists$ $J \trianglelefteq A$ con $I \subsetneq J \subsetneq A$

Caracterización:

$I \trianglelefteq A$ es primo $\Leftrightarrow$ A/I es dom integridad $\Rightarrow$ conmutativo

$I \trianglelefteq A$ es maximal $\Leftrightarrow$ A/I es un cuerpo

- Todo maximal es primo.

Factorización

A dom. integridad.

$a, b \in A$ a divide a b, esto es,

$a | b$ si $\exists$ $c \in A$: $b = ac$

- sean $a, b \in A$ son <u>asociados</u> si $a|b$ y $b|a$

Además, si a, b son asociados $a = ub$, $u \in \mathcal{U}(A)$

- $N(a+bi) = a^2 + b^2$

• Sea A anillo, a es irreducible (o átomo) si siempre que $a = bc$ con $b, c \in A \Rightarrow \begin{cases} b \in \mathcal{U}(A) \\ \vee \\ c \in \mathcal{U}(A) \end{cases}$

• Sea $a \neq 0$, $a \in A \setminus \mathcal{U}(A)$ es primo si siempre que $a | bc$, con $b, c \in A \Rightarrow \begin{cases} a|b \\ \vee \\ a|c \end{cases}$

• Todo primo es irreducible.

Máximo común divisor

Dados $a, b \in A$, decimos que d es m.c.d de a y b

1) $d|a$ y $d|b$
2) Si $c \in A$ verifica que $c|a$ y $c|b \Rightarrow c|d$

Si d, d' son mcd de a y b, d y d' son asociados

Propiedades

1) $(a,b) = (b,a)$
2) $((a,b),c) = (a,(b,c))$
3) $(ac, bc) = (a,b)c$
4) (a,b) asociado de $a \Leftrightarrow a|b$
5) $(a,0) = a$

Mínimo común múltiplo.

$a, b \in A$ dom integridad. Decimos que m es un m.c.m si

1) $a|m$ y $b|m$
2) Si $\exists c$ con $a|c$ y $b|c \Rightarrow m|c$

Dos m.c.m son dos elementos asociados.

Propiedades

1) $[a,b] = [b,a]$
2) $[[a,b],c] = [a,[b,c]]$
3) $[ac, bc] = [a,b]c$
4) $[a,b]$ es asociado a $b \Leftrightarrow a|b$
5) $[m,1] = m$

Otras prop

$a, b \in A$. dom. integridad.

1) $[a,b] = 0 \iff a = 0 \lor b = 0$

2) Si $\exists\ [a,b]$ y no nulo $\Rightarrow (a,b) = \dfrac{ab}{[a,b]}$

~~Recordemos~~: de factorización única.

$(\ker(f), +)$ subgrupo $(A, +)$

$(\operatorname{Im}(f), +, \cdot)$ subanillo de B

$\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

$[0] = \{0, 3, 6, 9, \dots\} = 0 + 3\mathbb{Z}$

$[1] = \{1, 4, 7, 10, \dots\} = 1 + 3\mathbb{Z}$

$[2] = \{2, 5, 8, 11, \dots\} = 2 + 3\mathbb{Z}$

Dominios de factorización única. (única < salvo excepción / salvo asociado)

A dom. integridad decimos que es de factorización única si $a = p_1 \cdots p_n = q_1 \cdots q_n$ con $p_1, \dots, p_n, q_1, \dots, q_n$ irreducibles de A. Entonces:

1) $n = m$

2) $\exists\ \sigma \in S_n$: p_i asociado a $q_{\sigma(i)}$ $\forall i$.

• En los dominios de factorización única todo irreducible es primo. El recíproco es cierto en un dom. integridad.

$\boxed{\text{Cuerpo} \Rightarrow \text{DFU}}$

CARACTERIZACIÓN DE DFU

A un dom. integridad. ELSA:

1) A es DFU

2) Todo elemento factoriza como producto de irreducibles y además todo irreducible es primo.

3) Todo elemento factoriza como producto de irreducibles y cualesquiera dos elementos tienen m.c.d. y mcm

CARACTERIZACIÓN DE DIVISIBILIDAD EN DFU

Sea A un DFU y $a, b \in A$.

$a = u p_1^{e_1} \cdots p_k^{e_k}$ $\quad u, v \in \mathcal{U}(A)$ $\quad p_i$ irreducibles $\quad e_i \in \mathbb{N}$

$b = v p_1^{f_1} \cdots p_k^{f_k}$

Entonces $a | b \iff e_i \leq f_i \quad \forall i$

Además:

$\text{mcd}(a,b) = p_1^{x_1} \cdots p_k^{x_k} \quad x_i = \min(e_i, f_i)$

$\text{mcm}(a,b) = p_1^{y_1} \cdots p_k^{y_k} \quad y_i = \max(e_i, f_i)$

- a y b es asociado al mcm y al mcd.
- ab es asociado al mcm y al mcd.
- Todo par de elementos en DFU tiene mcm y mcd.

Dominios de ideales principales

Sea D un dom. integridad, se dice dom de ideales principales, si todo ideal $I \trianglelefteq D$ es principal, esto es, $\exists\, d_I \in D$ con $(d_I) = I$

$$(d_I) = d_I D$$

- Si D es DIP $\Rightarrow$ Toda cadena ascendente de ideales es estacionaria.

Denotemos (a) a los múltiplos de a.

$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots \quad \exists k : (a_k) = (a_{k+1}) = \cdots$

- $(a) \subseteq (b) \iff a \in (b) \iff a = b \cdot c$ para algun $c \in D$ $\iff b | a$

- Sea D un DIP, $a \in D$, $a \neq 0$, $a \neq$ unidad, entonces $\exists p_1, \ldots, p_k$ irreducibles con $a = p_1 \cdots p_k$
- Sea D un DIP y $a, b \in D \Rightarrow \exists (a,b)$

Estas últimas dos propiedades nos dan:

- DIP $\Rightarrow$ DFU
- Identidad de Bezóut:

Sea D un DIP con $a, b \in D \Rightarrow \exists\, u, v \in D$: $(a,b) = ua + vb$

- Se dice que $a, b \in D$ son primos relativos si $(a,b) = 1$.

$d = ax + by$ tiene solución $\Leftrightarrow (a,b) \mid d$.

Algoritmo extendido de euclides

Versión cutre del algoritmo de euclides (Tablita).

$(a,b) = (a, b-a) = (a, a-b)$

Ejemplo del algoritmo:

queremos calcular $(33, 10) = 33u + 10v$

c	r	u	v
	33	1	0
	10	0	1
3	3	1	-3
3	1	-3	10
3	0		

$1 = (-3)33 + 10 \cdot 10$

Con la tablita obtenemos x_0 e y_0. Para conseguir todas las posibles soluciones, debemos calcularlas de la siguiente manera:

$c = ax_0 + by_0$; $\quad x = x_0 + k\dfrac{b}{(a,b)} \qquad k \in \mathbb{Z}$

$$y = y_0 - k\frac{a}{(a,b)}$$

En un ejemplo de la siguiente forma: $2 = 1 \cdot 22 - 2 \cdot 10$

$\times 6 \quad 12 = 10(-12) + 22(6)$

$x_0 = -12 \quad y_0 = 6$

$$x = -12 + k\frac{22}{2} = -12 + 11k$$

$$y = 6 - k\frac{10}{2} = 6 - 5k$$

Función tociente de Euler

$\mathcal{U}(\mathbb{Z}_m) = \{ a : (a,m)=1 , 1 \leq a \leq m-1 \}$

$\# \mathcal{U}(\mathbb{Z}_m) = \phi(m)$ es la función tociente de Euler

Ej: $\mathbb{Z}_6$, $\mathcal{U}(\mathbb{Z}_6) = \{1,5\} = \{1,-1\}$.

$\mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$

$a \longmapsto (a \bmod 2, a \bmod 3)$ isomorfismo de anillos.

El teorema chino de los restos nos dice que esta app es biyectiva.

$\mathcal{U}(\mathbb{Z}_6) \cong \mathcal{U}(\mathbb{Z}_2) \times \mathcal{U}(\mathbb{Z}_3)$

$1 \longmapsto (1,1)$

$5 \longmapsto (1,-1)$

$\left. \begin{array}{l} x \equiv 1 \bmod 2 \\ x \equiv -1 \bmod 3 \end{array} \right\}$

$\phi(6) = \phi(2) \cdot \phi(3)$

$(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ ¿$\exists x \in \mathbb{Z}_6$ con $f(x) = (a,b)$?

$\left. \begin{array}{l} x \equiv a \bmod 2 \\ x \equiv b \text{ mo } 3 \end{array} \right\}$

El teorema chino de los ~~restos~~ restos nos dice que es biyectiva la aplicación, esto es, nos dice que existe solución y por tanto es sobreyectiva y además que la solución es única nos dice que es inyectiva.

Así, si $m = m_1 \cdot m_2$ con $(m_1, m_2) = 1$, entonces:

$\phi(m) = \phi(m_1)\, \phi(m_2)$.

En resumen:

$\mathcal{U}(\mathbb{Z}_m) \cong \mathcal{U}(\mathbb{Z}_{m_1}) \times \mathcal{U}(\mathbb{Z}_{m_2})$ si $m = m_1 \times m_2$ y $(m_1, m_2) = 1$

$\phi(m) = \phi(m_1)\, \phi(m_2)$ es la función tociente.

En general, $m = p_1^{e_1} \cdots p_k^{e_k}$ $p_i \neq p_j$ $i \neq j$ irreducibles

$\phi(m) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k})$

Notación de congruencias

Sea D un DIP, $d \in D$.

$a \equiv b \mod d \iff [a] = [b]$ en $\frac{D}{(d)} \iff a-b \in (d) \iff d \mid (a-b)$

- $ax \equiv b \mod c$ tiene solución si $c \mid (ax-b) \iff ax-b = cy$ para algún y. $\iff b = ax - cy$

Ejemplo: $3x+5 \equiv 6 \mod 7$.

$3x \equiv 6-5 = 1 \mod 7$, $3x \equiv 1 \mod 7$

$\underbrace{5 \cdot 3}_{1} x \equiv 5 \mod 7$, $x \equiv 5 \mod 7 \iff x = 5 + 7k$, $k \in \mathbb{Z}$

- Sea $\left.\begin{array}{l} x \equiv a \mod n \\ x \equiv b \mod m \end{array}\right\}$ tiene solución $\iff (n,m) \mid b-a \iff a \equiv b \mod (n,m)$

Ejemplo: $\left.\begin{array}{l} x \equiv 3 \mod 4 \\ x \equiv 5 \mod 7 \end{array}\right\}$ $x = 3 + t4$, $t \in \mathbb{Z}$

$3 + t4 \equiv 5 \mod 7$

$4t \equiv 2 \mod 7$

aquí he multiplicado por el inverso de 4 en mod 7, pero para poder hacer este paso en un caso general debemos hacer la tablita (alg. ext. Euclides)

$t \equiv 4 \mod 7 \iff t = 4 + 7k$

sustituimos t

$x = 3 + 4(4+7k) = 19 + 28k$

- Caso general:

$\left.\begin{array}{l} x \equiv a_1 \mod m_1 \\ \vdots \\ x \equiv a_r \mod m_r \end{array}\right\}$ tiene sol $\iff \forall i,j \in \{1, \dots, r\}$ $a_i \equiv a_j \mod (m_i, m_j)$ y es la única solución $\mod [m_1, \dots, m_r]$

- Teorema Chino de los restos:

$\left.\begin{array}{l} x \equiv a_1 \mod m_1 \\ \vdots \\ x \equiv a_r \mod m_r \end{array}\right\}$ $(m_i, m_j) = 1$ $\forall i \neq j$

Tiene sol única $\mod [m_1, \dots, m_r]$

Recordemos: $ax \equiv b \mod c$ tiene solución si $b \mid (c,a)$

$p^e - p^{e-1} = \phi(p^e)$; $\phi(p) = p-1$ Esto cuando es primo relativo.

Teorema de Euler.

Sea m entero positivo, $a \in \mathbb{Z}$ con $(a,m)=1$, entonces:

$a^{\phi(m)} \equiv 1 \mod m.$

Decimos que la <u>lambda de Krambeicker</u> $\lambda(m)$ es el valor más pequeño que verifica esa condición.

Teorema pequeño de Fermat.

Sea p primo positivo y $1 \leq a \leq p-1$

$a^{p-1} \equiv 1 \mod p$; $a^p \equiv a \mod p$ $\forall a.$

Dominios Euclídeos

D es un dom. euclídeo si $\exists d : D \setminus \{0\} \longrightarrow \mathbb{N}$

(1) $\forall a, b \in D^*$ $d(ab) \geq d(a)$

(2) $\forall a \in D$ y $b \in D^*$ $\exists c, r \in D$ con $a = bc + r$ y $\begin{cases} r = 0 \\ d(r) < d(b \end{cases}$

<u>Propiedades de d</u>

$b, a \in D^*$

① $d(1) \leq d(a)$

② Si $b \in \mathcal{U}(D)$, $d(ab) = d(a)$

③ Si $b \notin \mathcal{U}(D)$, $d(ab) > d(a)$

Ejemplo: $\mathbb{Z}$ $d = |\cdot|$ $\begin{array}{r|l} 7 & 3 \\ \hline 1 & 2 \end{array}$ $7 = 3 \cdot 2 + 1$ $0 \leq |1| < 3$ 1)

$7 = 3 \cdot 3 - 2$ $0 \leq |-2| < |3|$ 2)

1) resto por defecto

2) resto por exceso.

- $d(b) = d(1) \iff b \in \mathcal{U}(D)$
- $d(ab) > d(a)$ y $d(ab) > d(b)$
- $DE \Rightarrow DIP \Rightarrow DFU$

Pasos para reducir un polinomio

Paso 1

Mirar el polinomio
Si tengo coeficientes que no sean enteros quitamos denominadores

Paso 2

Aquí el polinomio debe estar en $\mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$, ya que hemos quitado denominadores.
Debemos calcular su contenido, esto es, mcd (coef).

Si $c(f) \neq \pm 1 \Rightarrow f(x)$ reducible en $\mathbb{Z}$ pero en $\mathbb{Q}$ No lo se.

- Si nos lo piden en $\mathbb{Z}$ y $c(f) = \pm 1 \Rightarrow$ siguiente paso
- Si nos lo piden en $\mathbb{Z}$ y $c(f) \neq \pm 1 \Rightarrow$ reducible.

Si nos lo piden en $\mathbb{Q}$, aplicamos la fórmula

$$c(f)\, f' = f$$

y pasamos al tema 3 con f'.

Por tanto, solo pasamos al paso 3 si nos lo piden en $\mathbb{Z}$ y $c(f) = \pm 1$ o nos lo piden en $\mathbb{Q}$ y en este caso pasamos con f'.

Paso 3

$f \in \mathbb{Z}[x]$, f primitivo.

Miramos a ver si podemos aplicar Eiseinstein, teniendo en cuenta que esto solo podemos aplicarlo en $\mathbb{Z}$.
Además vamos a utilizar una proposición que nos dice que un pol es irred en $\mathbb{Z}[x] \Leftrightarrow$ irred en $\mathbb{Q}[x]$

Por tanto vamos a trabajar en $\mathbb{Z}$.

Podemos aplicar Eiseinstein cuando el valor que queremos extraer como factor común divide a todos los coeficientes menos al lider, y ese valor al cuadrado No divide al término independiente.

~~Si esto es así podemos sacar ese valor como factor común, por tanto~~, Este criterio solo nos dice si el polinomio es irreducible.

Paso 4

$f(x) \in \mathbb{Z}[x]$, f primitivo.

Vemos si tiene factores de grado 1, para aplicar Ruffinni.

probamos los divisores del término independiente.

Si encontramos algún divisor del térm.ind que verifique esto, sabemos que el polinomio es reducible.

Si no encontramos ninguno, podemos afirmar que no tiene ningún factor de grado 1, y pasamos al siguiente paso.

cuando coef lider $\neq 1$

otra forma de hacerlo es buscar los $ax+b \mid f(x)$ tales que $\begin{cases} a \mid \text{coef. lider} \\ b \mid \text{térm. ind} \end{cases}$ y $f(-\frac{b}{a}) = 0$

buscamos todos los posibles y si alguno es 0, es reducible, si no, no lo sabemos y pasamos al siguiente paso.

Paso 5

$f(x) \in \mathbb{Z}[x]$, f primitivo. f no tiene fact de grado 1.

Miramos el grado.

- Si $gr = 2 \Rightarrow$ aplicamos $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- Si $gr \leq 3 \Rightarrow$ No damos el paso **5**. (Lo habríamos encontrad
- Si $gr > 3 \Rightarrow$ Aplicamos reducción módulo p.

La teoría nos dice que $f_p = f \mod p$.

Si $gr(f) = gr(f_p)$ y tiene un factor de grado r

$\Downarrow$

f_p tiene un factor de grado r.

Pero para la práctica No vamos a usar este resultado, sino su contrarrecíproco, esto es,

f_p No tiene fact grado r $\Rightarrow$ f tampoco.

P NO PUEDE SER DIVISOR DEL COEF. LIDE

p va a ser usualmente 2, 3 o como mucho 5.

La idea es obtener f_2 del polinomio, y ver si tiene factores lineales. Si los tiene no obtenemos información alguna, en cambio si No los tiene podemos afirmar que f tampoco los tiene.

Paso 6

Aquí llegamos si lo anterior no nos dice nada y en el paso 5 hemos probado con 2, 3 y 5, y no nos dice nada. Pero es bastante raro tener que llegar aquí

Aquí lo más probable es que sea reducible, así que vamos a estudiar/buscar un factor. Como sabemos que No tiene factores de grado 1, buscamos factores de grado 2.

$$g \mid f \Rightarrow g(a) \mid f(a)$$

se trata básicamente en elegir 3 valores, tomemos sus imágenes por f.
por ej 0, 1, −1. Calculamos

$f(0) = 2$
$f(1) = 6$ ← Supongamos que son esos valores
$f(-1) = 2$

Posibilidades: (divisores de la imagen)

$\pm 1 \quad \pm 2$
$\pm 1 \quad \pm 2 \quad \pm 3 \quad \pm 6$
$\pm 1 \quad \pm 2$

Ahora buscamos condiciones de g de manera que

$$f = g \cdot h \Rightarrow \begin{cases} f_2 = g_2 h_2 \\ f_3 = g_3 h_3 \end{cases}$$

Supongamos
$f_2 = x(x+1)^2(x^2+x+1)$
$f_3 = (x-1)^2(x^3-x-1)$
$f_5 = (x^2+x+1)(x^3+4x+2)$

$$g_2 = \begin{cases} (x+1)^2 \\ (x^2+x+1) \\ (x^2+x) = x(x+1) \end{cases}$$

Aquí hay muchas posibilidades.

$g_3 = (x-1)^2$
$g(0) = 1 \mod 3$
$g(1) = 0 \mod 3$
$g(-1) = 1 \mod 3$

← Estas son condiciones que debe cumplir g.

Posibilidades

$\Rightarrow$
$f(0) = \pm 1 \quad \pm 2$
$f(1) = \pm 3 \quad \pm 6$
$f(-1) = \pm 1 \quad \pm 2$

Así nos quedan 16 posibilidades.

La idea por tanto de este paso es ir reduciendo las posibilidades, encontrar ese g y ver por tanto que el polinomio es reducible.

Una vez calculado g, calculamos h dividiendo y aplicamos de nuevo los pasos a h.