Capítulo 5

Polinomios.

Este capítulo trata sobre los polinomios con coeficientes en un cuerpo K. Hasta ahora mencionamos en la materia varios ejemplos de cuerpos: el cuerpo de los números racionales $\mathbb{Q}$, el cuerpo de los números reales $\mathbb{R}$, el cuerpo de los números complejos $\mathbb{C}$, los cuerpos finitos $\mathbb{Z}/p\mathbb{Z}$, para p un número primo, aunque nunca introdujimos la definición formal. A continuación definimos la noción de cuerpo y hacemos un repaso exhaustivo del cuerpo de los números complejos.

5.1. El cuerpo de los números complejos $\mathbb{C}$.

5.1.1. Cuerpos.

Definición 5.1.1. (Cuerpo.)

Sea K un conjunto, y sean $+, \cdot : K \times K \to K$ dos operaciones en K (usualmente la suma y el producto). Se dice que $(K, +, \cdot)$ es un *cuerpo* si

- $+$ y $\cdot$ son operaciones asociativas y conmutativas. Es decir $\forall\, x, y, z \in K$ se tiene $(x+y)+z = x+(y+z)$ y $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (asociatividad) y $\forall\, x, y \in K$ se tiene $x+y = y+x$ y $x \cdot y = y \cdot x$.
- Existe un elemento neutro para la suma, que se nota 0_K, es decir $\forall\, x \in K$ se tiene $x + 0_K = x$, y un elemento neutro para el producto, que se nota 1_K, es decir $\forall\, x \in K$ se tiene $x \cdot 1_K = x$.
- Cualquiera sea $x \in K$, x tiene un inverso aditivo, u opuesto, que se nota $-x$, es decir $x + (-x) = 0_K$, y cualquiera sea $x \in K$, $x \neq 0$, x tiene un inverso multiplicativo que se nota x^{-1}, es decir $x \cdot x^{-1} = 1_K$.
- La operación $\cdot$ es distributiva sobre $+$, es decir $\forall\, x, y, z \in K$ se tiene $x \cdot (y+z) = x \cdot y + x \cdot z$.

Estas propiedades implican en particular que $0 \cdot x = 0$, $\forall\, x \in K$, pues $0 = 0 + 0 \Rightarrow 0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$, y por lo tanto sumando de cada lado $-0 \cdot x$ se obtiene $0 \cdot x = 0$.

También se deduce que $\forall\, x, y \in K$ no nulos, vale que $x \cdot y \neq 0$ pues si fuera $x \cdot y = 0$ con $x \neq 0$ entonces, como existe x^{-1}, se tendría $y = x^{-1} \cdot x \cdot y = x^{-1} \cdot 0 = 0$.

En particular, cuando K es un cuerpo, notando $K^\times := K - \{0\}$, se tiene que $\cdot : K^\times \times K^\times \to K^\times$, y tanto $(K, +)$ como $(K^\times, \cdot)$ son grupos abelianos.

La información siguiente es en su mayoría extraída de Wikipedia.

Lo números naturales ya eran conocidos desde el principio de los tiempos, pero claro, no se podía "restar". Los números racionales positivos, las fracciones positivas, (que permiten "dividir") ya eran utilizadas de alguna manera por los Egipcios alrededor del año 1000 AC, y luego también por los griegos. Los números negativos aparecieron por primera vez en un libro de matemática de la Dinastía Han en China (202 AC-202 DC), y también en un manuscrito indio escrito en algún momento entre los años 200 AC y 400 DC. Matemáticos indios $\sim$ 700 AC y griegos $\sim$ 500 AC ya reconocían el concepto de irracionalidad (en particular con $\sqrt{2}$). Durante el Medioevo los árabes ya trataban a los números irracionales como entidades algebraicas, y asociaron los conceptos de números y magnitudes.

En el Siglo XVI apareció la notación decimal de los números reales, pero fue recién en 1871 cuando Georg Cantor realizó la descripción rigurosa de los números reales, uno de los avances matemáticos más importantes del Siglo XIX, mostrando en particular que hay muchos más números irracionales que racionales.

5.1.2. Números complejos: generalidades.

Con respecto a los números complejos, la primera referencia conocida a raíces cuadradas de números negativos proviene del trabajo de los matemáticos griegos, como Herón de Alejandría en el Siglo I AC, como resultado de una imposible sección de una pirámide.

Los complejos se hicieron más patentes en el Siglo XVI, cuando la búsqueda de fórmulas que dieran las raíces exactas de los polinomios de grado 3 fueron encontradas por matemáticos italianos como Scipione del Ferro (1465-1526), Niccolo Fontana Tartaglia (1499-1557) y Gerolamo Cardano (1501-1576): aunque sólo estaban interesados en las raíces reales de este tipo de ecuaciones, se encontraban con la necesidad de lidiar con raíces de números negativos. Las reglas para la suma, resta, producto y división fueron desarrolladas por el matemático italiano Rafael Bombelli (1526-1572). El término imaginario para estas cantidades (y real para los números reales) fue acuñado por Descartes en el Siglo XVII. Muchos matemáticos contribuyeron al desarrollo completo de los números complejos.

Lo que todos sabemos es que no existe ningún número real r que satisface $r^2 = -1$, dado que el cuadrado de un número real siempre es un número real ≥ 0. Luego se introduce una cantidad *imaginaria* i, que no pertenece a $\mathbb{R}$, que satisface $i^2 = -1$. Se "agrega" esa cantidad al cuerpo de los números reales, construyendo el "menor" conjunto que contiene a $\mathbb{R}$ y a i, y donde se puede sumar y multiplicar (respetando la distributividad): a este conjunto lo llamamos el conjunto de los números *complejos* $\mathbb{C}$.

Al estar $a, b \in \mathbb{R} \subset \mathbb{C}$ e $i \in \mathbb{C}$, tiene que estar $b \cdot i \in \mathbb{C}$, y luego también $a + b \cdot i \in \mathbb{C}$. O sea


del Ferro


Tartaglia


Cardano


Bombelli

$\{z = a + b \cdot i;\ a, b \in \mathbb{R}\} \subset \mathbb{C}$.

Pero observemos que dados $a + b \cdot i, c + d \cdot i \in \mathbb{C}$, con $a, b, c, d \in \mathbb{R}$, entonces si operamos respetando la distributividad,

- $(a + b \cdot i) + (c + d \cdot i) = (a + c) + (b + d) \cdot i$.
- $(a + b \cdot i) \cdot (c + d \cdot i) = ac + ad \cdot i + bc \cdot i + bd \cdot i^2 = (ac - bd) + (ad + bc) \cdot i$.

O sea la suma y el producto de estos números tienen la misma forma: un número real + otro número real multiplicado por i. Es decir, el menor conjunto donde tiene sentido sumar y multiplicar números de la forma $a + b \cdot i$ con $a, b \in \mathbb{R}$ es el conjunto

$$\mathbb{C} = \{z = a + b \cdot i;\ a, b \in \mathbb{R}\},$$

donde si $z = a + b \cdot i$, $\omega = c + d \cdot i \in \mathbb{C}$ con $a, b, c, d \in \mathbb{R}$, entonces $z = \omega \Leftrightarrow a = c$ y $b = d$.

Teorema 5.1.2. (El cuerpo de los números complejos.)

$(\mathbb{C}, +, \cdot)$ *es un cuerpo.*

Demostración.

- La operación $+$ es conmutativa y es asociativa pues lo es sobre los números reales. Además $0 = 0 + 0 \cdot i \in \mathbb{C}$ es el elemento neutro para la suma, y el opuesto aditivo de $z = a + b \cdot i$, con $a, b \in \mathbb{R}$, es $-z = -a - b \cdot i \in \mathbb{C}$.
- Se puede verificar que la operación $\cdot$ es conmutativa y asociativa también. El elemento $1 = 1 + 0 \cdot i \in \mathbb{C}$ es el elemento neutro para el producto, y para todo $z = a + b \cdot i \neq 0$, con $a, b \in \mathbb{R}$, se tiene que existe

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} \cdot i \ \in \ \mathbb{C},$$

  pues si $z \neq 0$, $a^2 + b^2 > 0$, por lo tanto es un denominador permitido, y es fácil verificar que $(a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i\right) = \frac{a^2 - (-b^2)}{a^2 + b^2} + \frac{\big(a(-b) + ba\big)}{a^2 + b^2} = 1 + 0\, i = 1$.
- La operación $\cdot$ es distributiva sobre $+$ pues lo es en $\mathbb{R}$: sean $z = a + b\, i$, $\omega = c + d\, i$ y $\omega' = c' + d' i$, con $a, b, c, d, c', d' \in \mathbb{R}$, entonces

$$\begin{aligned} z\cdot(\omega+\omega') &= (a+b\,i)\cdot\big((c+d\,i)+(c'+d'i)\big) \\ &= (a+b\,i)\cdot\big((c+c')+(d+d')i\big) \\ &= \big(a(c+c')-b(d+d')\big)+\big(a(d+d')+b(c+c')\big)i \\ &= ac+ac'-bd-bd'+(ad+ad'+bc+bc')i \\ &= \big((ac-bd)+(ad+bc)\,i\big)+\big((ac'-bd')+(ad'+bc')\,i\big) \\ &= (a+b\,i)(c+d\,i)+(a+b\,i)(c'+d'i) \;=\; z\cdot\omega+z\cdot\omega'. \end{aligned}$$

□

Por lo tanto el cuerpo $\mathbb{C}$ es un cuerpo que "contiene" al cuerpo de los números reales $\mathbb{R}$: $\forall\, a\in\mathbb{R}\,,\ a=a+0\cdot i\in\mathbb{C}$.

Se gana al extender de esa forma el cuerpo $\mathbb{R}$ que la ecuación $X^2+1=0$ tiene solución en $\mathbb{C}$, y probaremos más adelante que todas las ecuaciones cuadráticas $z\,X^2+\omega\,X+u=0$ con $z,\omega,u\in\mathbb{C}$, z,ω no ambos nulos, tienen solución en $\mathbb{C}$. En realidad veremos sin demostración un resultado mucho más general: que todas las ecuaciones de cualquier grado con coeficientes complejos tienen solución en $\mathbb{C}$ (éste es el renombrado Teorema Fundamental del Álgebra).

Se pierde que en $\mathbb{C}$ no se puede establecer ningún orden $\geq$ como tienen los números reales: no hay ninguna forma de establecer un orden completo $\geq$ en $\mathbb{C}$ (es decir una relación reflexiva, antisimétrica y transitiva, que satisface además $z\geq\omega$ o $\omega\geq z$, $\forall\, z,\omega\in\mathbb{C}$) que respete la suma ($z\geq z'\Rightarrow z+\omega\geq z'+\omega$, $\forall\,\omega\in\mathbb{C}$) y el producto por no negativos ($z\geq 0$ y $\omega\geq 0\ \Rightarrow\ z\,\omega\geq 0$): pues si $i\geq 0$ entonces $i^2=-1\geq 0$ implica $0=-1+1\geq 0+1=1$, pero por otro lado, $1=(-1)^2\geq 0^2=0$. Es decir $0\geq 1$ y $1\geq 0$. Por la antisimetría, eso tendría que implicar $0=1$, contradicción. Un razonamiento análogo prueba que no puede ser $0\geq i$.

<u>*Ejemplos:*</u>

- $i^2=-1,\ i^3=-i,\ i^4=1$ y en general,

$$i^{4n}=1,\ i^{4n+1}=1,\ i^{4n+2}=-1,\ i^{4n+3}=-i,\qquad \forall\, n\in\mathbb{N}_0.$$

- Para todo $a,b\in\mathbb{R}$, $(a+b\,i)^2=a^2-b^2+2\,a\,b\,i$ y $(a+b\,i)\cdot(a-b\,i)=a^2+b^2\in\mathbb{R}_{\geq 0}$.

Definición 5.1.3. (Forma binomial, parte real, parte imaginaria, conjugado, módulo.)

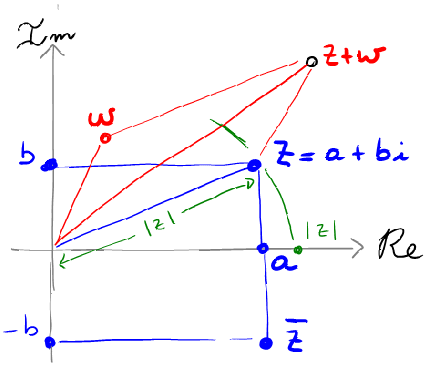
- Dado $z\in\mathbb{C}$, la forma $z=a+b\cdot i$ con $a,b\in\mathbb{R}$ se llama la *forma binomial* de z, su parte real es $\Re e(z):=a\in\mathbb{R}$ y su parte imaginaria es $\Im m(z):=b\in\mathbb{R}$.

- Dado $z=a+b\,i$ con $a,b\in\mathbb{R}$, el *conjugado* de z es $\overline{z}:=a-b\,i\in\mathbb{C}$, y el *módulo* de z es $|z|=\sqrt{a^2+b^2}\ \in\ \mathbb{R}_{\geq 0}$. Observemos que $|z|=0\Leftrightarrow z=0$, y que si $z\neq 0$, entonces $|z|\in\mathbb{R}_{>0}$.

Se representa z y esas cantidades en el *plano complejo*, así como la operación suma, que se hace con la regla del paralelogramo. Se nota que por el Teorema de Pitágoras, $|z| = \operatorname{dist}(z,0)$, es decir $|z| \geq 0$ mide la distancia del número complejo z al origen 0.

Además se tiene las siguientes relaciones entre $\overline{z}$ y $|z|$:

$$z \cdot \overline{z} = |z|^2, \quad \forall\, z \in \mathbb{C} \qquad \text{y} \qquad z^{-1} = \frac{\overline{z}}{|z|^2}, \quad \forall\, z \in \mathbb{C}^{\times}.$$



Proposición 5.1.4. (Propiedades del conjugado y del módulo.)

Para todo $z \in \mathbb{C}$, se tiene

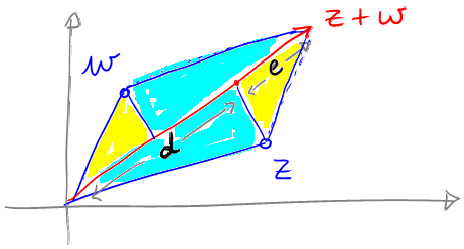
- $\overline{\overline{z}} = z$,
- $z = \overline{z} \iff z \in \mathbb{R}$,
- $z + \overline{z} = 2\,\Re e(z)$, $z - \overline{z} = 2\,\Im m(z)\, i$,
- $|\Re e(z)| \leq |z|$ *e* $|\Im m(z) \leq |z|$.

Además, para todo $z, \omega \in \mathbb{C}$, se tiene

- $\overline{z + \omega} = \overline{z} + \overline{\omega}$.
- $\overline{z \cdot \omega} = \overline{z} \cdot \overline{\omega}$.
- *Si* $z \neq 0$, $\overline{z^{-1}} = \overline{z}^{-1}$.
- *Si* $z \neq 0$, $\overline{z^k} = \overline{z}^k$, $\forall\, k \in \mathbb{Z}$.
- $|z + \omega| \leq |z| + |\omega|$.
- $|z \cdot \omega| = |z| \cdot |\omega|$
- *Si* $z \neq 0$, $|z^{-1}| = |z|^{-1}$.
- *Si* $z \neq 0$, $|z^k| = |z|^k$, $\forall\, k \in \mathbb{Z}$.

La propiedad $|z + \omega| \leq |z| + |\omega|$ se llama la *desigualdad triangular* y se puede comprobar geométricamente:

$$d \leq |z|, \; e \leq |\omega| \implies |z + \omega| = d + e \leq |z| + |\omega|.$$



Lo notorio es que cuando se construye $\mathbb{C}$ agregándole a $\mathbb{R}$ la raíz cuadrada i de -1, se consigue que en $\mathbb{C}$ todos los números complejos tengan raíces cuadradas, y no solo -1 o los números reales negativos b, cuyas raíces cuadradas son $\pm\sqrt{|b|}\, i$.

Proposición 5.1.5. (Raíces cuadradas de números complejos.)

Sea $z \in \mathbb{C}$. Entonces existe $\omega \in \mathbb{C}$ tal que $\omega^2 = (-\omega)^2 = z$. Si $z \neq 0$, entonces z tiene exactamente dos raíces cuadradas distintas, que son ω y $-\omega$.

Hagamos un ejemplo antes de hacer la demostración.

<u>*Ejemplo:*</u> Calcular las raíces cuadradas complejas de $z = 3 - 4\,i$.

Planteemos $\omega^2 = z$ donde $\omega = x + y\,i \in \mathbb{C}$ con $x, y \in \mathbb{R}$ a determinar. Esto implica $|\omega^2| = |z|$, es decir $|\omega|^2 = |z|$ también. Por lo tanto, de $\omega^2 = 3-4\,i$ y $|\omega|^2 = |3-4\,i| = \sqrt{25} = 5$, obtenemos las ecuaciones:

$$\begin{cases} x^2 - y^2 + 2xy\,i = 3 - 4\,i \\ x^2 + y^2 = 5 \end{cases} \iff \begin{cases} x^2 - y^2 = 3 \\ 2xy = -4 \\ x^2 + y^2 = 5. \end{cases}$$

De la primer y tercer ecuación deducimos

$$2x^2 = 5+3 = 8 \quad \text{y} \quad 2y^2 = 5-3 = 2 \implies x = \pm\sqrt{\frac{8}{2}} = \pm\sqrt{4} = \pm 2 \ \text{ e } \ y = \pm\sqrt{\frac{2}{2}} = \pm\sqrt{1} = \pm 1.$$

O sea que en principio tenemos 4 posibilidades, eligiendo x e y positivos y/o negativos. Pero la segunda condición nos dice que $x\,y = -2$, el producto es negativo, por lo tanto si se toma $x = 2$ se debe tomar $y = -1$ y si se toma $x = -2$ se debe tomar $y = 1$: los candidatos a raíces cuadradas son entonces

$$\omega = 2 - i \quad \text{y} \quad \omega' = -\omega = -2 + i.$$

Efectivamente, es inmediato verificar que $\omega^2 = (-\omega)^2 = (4-1) + 2(-2)\,i = 3 - 4\,i$.

Demostración. (de la Proposición 5.1.5.)

Sea $z = a + b\,i \in \mathbb{C}$, con $a, b \in \mathbb{R}$, y planteemos $\omega^2 = z$ donde $\omega = x + y\,i \in \mathbb{C}$ con $x, y \in \mathbb{R}$ a determinar.

Si $z = 0$, entonces $\omega = 0$.

Luego podemos asumir $z \neq 0$. La condición $\omega^2 = z$ implica $|\omega^2| = |z|$, es decir $|\omega|^2 = |z|$ también. Por lo tanto, de $\omega^2 = z$ y $|\omega|^2 = |z|$ obtenemos las ecuaciones:

$$\begin{cases} x^2 - y^2 + 2xy\,i = a + b\,i \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases} \iff \begin{cases} x^2 - y^2 = a \\ 2xy = b \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases}$$

De la primer y tercer ecuación deducimos

$$2x^2 = \sqrt{a^2+b^2} + a \quad \text{y} \quad 2y^2 = \sqrt{a^2+b^2} - a.$$

Observemos que tanto $\sqrt{a^2+b^2} + a$ como $\sqrt{a^2+b^2} - a$ son números reales no negativos por la propiedad $|\Re e(z)| \leq |z|$ que dice que valen tanto $a \leq \sqrt{a^2+b^2}$ como $-a \leq \sqrt{a^2+b^2}$. Por lo tanto existen las raíces cuadradas reales

$$x = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \in \mathbb{R} \quad \text{e} \quad y = \pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \in \mathbb{R}.$$

Esto nos daría en principio 4 posibles candidatos para ω. Pero solo dos de ellas son en realidad candidatos: las dos que cumplen con la segunda condición $2xy = b$: si $b \geq 0$, hay que tomar

$$x = \sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\,, y = \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \quad \text{y} \quad x = -\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\,, y = -\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}},$$

mientras que si $b<0$, hay que tomar

$$x=\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\,,y=-\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\quad\text{y}\quad x=-\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\,,y=\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}.$$

Observemos que en ambos casos se obtiene $\omega=x+y\,i$ y $\omega'=-\omega$. Verifiquemos finalmente que estas dos candidatos a solución ω y $\omega'=-\omega$ son efectivamente raíces cuadradas de z cuando $z\neq 0$. Como claramente $(-\omega)^2=\omega^2$, alcanza con probarlo para

$$\omega=\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\,i$$

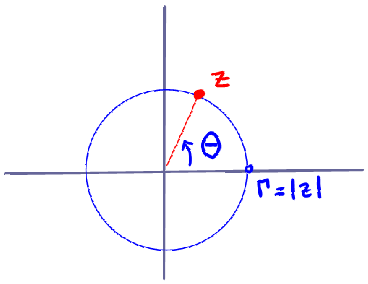
donde el $\pm$ es $+$ o $-$ dependiendo de si $b\geq 0$ o $b<0$.

$$\begin{aligned}\omega^2&=\Big(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\Big)^2\\&=\Big(\frac{a^2+b^2+a}{2}-\frac{a^2+b^2-a}{2}\Big)\pm 2\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\,i\\&=a\pm 2\sqrt{\frac{\sqrt{a^2+b^2}^{\,2}-a^2}{4}}\,i\;=\;a\pm\sqrt{b^2}\,i\;=\;a\pm|b|\,i\;=\;a+b\,i,\end{aligned}$$

pues si $b\geq 0$, $|b|=b$ y el signo en $\pm$ era $+$ mientras que si $b<0$, $|b|=-b$ pero el signo en $\pm$ era $-$. □

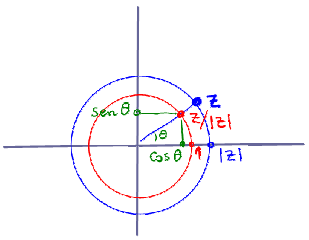
Más adelante veremos que no sólo se consigue que todo número complejo tiene raíces cuadradas de números complejos, sino también que todo número complejo tiene raíces n-ésimas, para todo $n\in\mathbb{N}$. Para ello introducimos la forma trigonométrica o polar de los números complejos.

5.1.3. Forma trigonométrica (o polar) de un número complejo no nulo.



Sea $z\in\mathbb{C}^\times$. Entonces z no solo está determinado por su parte real $\Re e(z)\in\mathbb{R}$ y su parte imaginaria $\Im m(z)\in\mathbb{R}$, pero también se lo puede determinar de otra forma por su módulo $r=|z|\in\mathbb{R}_{>0}$, que determina en qué circunferencia se encuentra z, y por un ángulo θ con respecto a (por ejemplo) el semieje real positivo, como lo muestra el dibujo.

Dado $z\in\mathbb{C}^\times$, $z/|z|$ pertenece a la circunferencia unidad, pues $\big|z/|z|\big|=|z|/|z|=1$, y por lo tanto sus coordenadas son de la forma $(\cos\theta,\operatorname{sen}\theta)$:



Luego,

$$z = r\,(\cos\theta + i\,\operatorname{sen}\theta),\ \text{ donde } r = |z| \text{ y } \theta \text{ es tal que } \cos\theta = \frac{\Re e(z)}{|z|} \text{ y } \operatorname{sen}\theta = \frac{\Im m(z)}{|z|}.$$

Vamos a adoptar para la expresión $\cos\theta + i\,\operatorname{sen}\theta$ la notación exponencial $e^{\theta i}$, que se denomina la *Fórmula de Euler* ya que él fue el primero en demostrar su validez:

$$e^{\theta i} = \cos\theta + i\,\operatorname{sen}\theta, \quad \forall\,\theta \in \mathbb{R}.$$

Por lo tanto

$$z = r\,e^{\theta i}, \quad \text{donde } r = |z| \in \mathbb{R}_{>0} \text{ y } \theta \in \mathbb{R} \text{ es tal que } \cos\theta = \frac{\Re e(z)}{|z|} \text{ y } \operatorname{sen}\theta = \frac{\Im m(z)}{|z|}.$$

El ángulo $\theta \in \mathbb{R}$ está por convención dado en radianes. Claramente, el ángulo no está determinado en forma única, ya que sabemos que $\cos\theta = \cos(\theta + 2k\pi)$ y $\operatorname{sen}\theta = \operatorname{sen}(\theta + 2k\pi)$, $\forall\,k \in \mathbb{Z}$. Así,

$$e^{\theta i} = e^{(\theta + 2k\pi)i}, \quad \forall\,k \in \mathbb{Z},$$

y más aún, para $r, s \in \mathbb{R}_{>0}$ y $\theta, \varphi \in \mathbb{R}$, se tiene

$$s\,e^{\varphi i} = r\,e^{\theta i} \iff \begin{cases} s = r \\ \varphi = \theta + 2k\pi \ \text{ para algún } k \in \mathbb{Z}. \end{cases}$$

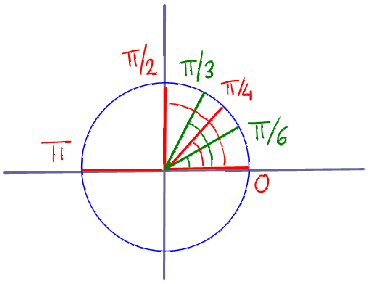
Si elegimos θ con $0 \le \theta < 2\pi$, entonces este ángulo está determinado en forma única y se denomina el *argumento de* z que se denota $\arg(z)$.

La *forma trigonométrica* o *polar* de $z \in \mathbb{C}^\times$ es

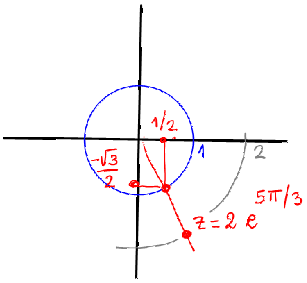
$$z = r\,(\cos\theta + i\,\operatorname{sen}\theta) \ = \ r\,e^{\theta i} \quad \text{con } r \in \mathbb{R}_{>0} \text{ y } 0 \le \theta < 2\pi.$$

Repasemos los ángulos típicos con sus coseno y seno:

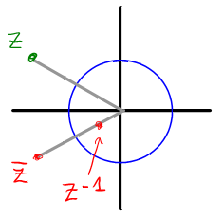
θ	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$	π
$\cos\theta$	1	$\sqrt{3}/2$	$\sqrt{2}/2$	$1/2$	0	-1
$\operatorname{sen}\theta$	0	$1/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	1	0



<u>*Ejemplo:*</u> Sea $z = 1 - \sqrt{3}\,i$. Entonces $z = r\,e^{i\theta}$ donde $r = |z| = \sqrt{1+3} = 2$ y $\theta \in \mathbb{R}$ es un ángulo tal que $\cos\theta = 1/2$, $\operatorname{sen}\theta = -\sqrt{3}/2$. Por lo tanto $\theta = -\pi/3$ o $\theta = \pi/3 + 2k\pi$, $k \in \mathbb{Z}$. Se tiene $\arg(z) = -\pi/3 + 2\pi = 5\pi/3$, y $z = 2\,e^{\frac{5\pi}{3}i}$ es la forma trigonométrica de z.



Observación 5.1.6. Sea $z = r\,(\cos\theta + i\,\operatorname{sen}\theta) = r\,e^{\theta i}$ con $r \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$. Entonces



- $\overline{z} = r\,\big(\cos(-\theta) + i\,\operatorname{sen}(-\theta)\big) = r\,e^{-\theta i}$,
- $z^{-1} = r^{-1}\,\big(\cos(-\theta) + i\,\operatorname{sen}(-\theta)\big) = r^{-1}\,e^{-\theta i}$.

Demostración. El segundo inciso es porque $z^{-1} = \dfrac{\overline{z}}{|z|^2}$ y $|z^{-1}| = |z|^{-1}$. Por lo tanto z^{-1} está en la misma semirrecta que $\overline{z}$ (ya que es un múltiplo de $\overline{z}$ que se obtiene al multiplicar $\overline{z}$ por el número real positivo $1/|z|^2$). Por lo tanto $\overline{z}$ y z^{-1} vienen definidos por el mismo ángulo $-\theta$. □

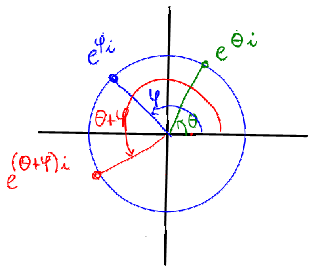
A continuación vamos a recordar la Fórmula de de Moivre, que debe su nombre al matemático francés Abraham de Moivre, 1667-1754.

Teorema 5.1.7. (Fórmula de de Moivre.)
Sean $z = r\,(\cos\theta + i\,\operatorname{sen}\theta) = r\,e^{\theta i}$ *y* $\omega = s(\cos\varphi + i\,\operatorname{sen}\varphi) = s\,e^{\varphi i}$ *con* $r, s \in \mathbb{R}_{>0}$ *y* $\theta, \varphi \in \mathbb{R}$. *Entonces*

$$z \cdot \omega = rs\,\big(\cos(\theta+\varphi) + i\,\operatorname{sen}(\theta+\varphi)\big) = rs\,e^{(\theta+\varphi)i}.$$

Es decir

$$r\,e^{\theta i} \cdot s\,e^{\varphi i} = rs\,e^{(\theta+\varphi)i}.$$



En particular,

$$\arg(z+\omega) = \arg(z) + \arg(\omega) - 2k\pi$$

con $k = 0$ *o* 1 *elegido de modo tal que* $0 \le \arg(z) + \arg(\omega) - 2k\pi < 2\pi$.

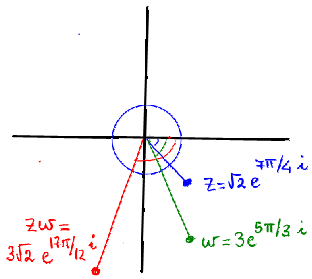
Demostración. Es una consecuencia muy simple de cómo es el producto de números complejos, y las fórmulas del coseno y seno de la suma de ángulos:

$$\begin{aligned} z \cdot \omega &= r\,(\cos\theta + i\,\operatorname{sen}\theta) \cdot s(\cos\varphi + i\,\operatorname{sen}\varphi) \\ &= rs\,\big((\cos\theta\cos\varphi - \operatorname{sen}\theta\operatorname{sen}\varphi) + i\,(\cos\theta\operatorname{sen}\varphi + \operatorname{sen}\theta\cos\varphi)\big) \\ &= rs\,\big((\cos(\theta+\varphi) + i\,(\operatorname{sen}(\theta+\varphi)\big). \end{aligned}$$

□

<u>*Ejemplo:*</u> Sean $z = \sqrt{2}\,e^{\frac{7\pi}{4}i}$ y $\omega = 3\,e^{\frac{5\pi}{3}i}$. Entonces

$$\begin{aligned} z \cdot \omega = \sqrt{2}\,e^{\frac{7\pi}{4}i} \cdot 3\,e^{\frac{5\pi}{3}i} &= 3\sqrt{2}\,e^{(\frac{7\pi}{4}+\frac{5\pi}{3})i} \\ = 3\sqrt{2}\,e^{\frac{41\pi}{12}i} &= 3\sqrt{2}\,e^{(\frac{41\pi}{12}-2\pi)i} = 3\sqrt{2}\,e^{\frac{17\pi}{12}i}. \end{aligned}$$



Por inducción en $n \in \mathbb{N}$ se puede deducir la fórmula para cualquier potencia n-ésima, $n \in \mathbb{Z}$.

Corolario 5.1.8. (Expresión trigonométrica de una potencia.)
Sean $z = r\,(\cos\theta + i\ \mathrm{sen}\,\theta) = r\,e^{\theta i}$ *y* $\omega = s(\cos\varphi + i\ \mathrm{sen}\,\varphi) = s\,e^{\varphi i}$ *con* $r, s \in \mathbb{R}_{>0}$ *y* $\theta, \varphi \in \mathbb{R}$. *Entonces*

- $\dfrac{z}{\omega} = \dfrac{r}{s}\big(\cos(\theta-\varphi) + i\ \mathrm{sen}(\theta-\varphi)\big) = \dfrac{r}{s}\,e^{(\theta-\varphi)i}$.
- $z^n = r^n\big(n\cos\theta) + i\ \mathrm{sen}(n\theta)\big) = r^n\,e^{n\theta i}$, *para todo* $n \in \mathbb{Z}$.

En particular,

$$\arg(z^n) = n\ \arg(z) - 2k\pi \ \textit{con}\ k \in \mathbb{Z}\ \textit{elegido de modo tal que}\ 0 \le n\ \arg(z) - 2k\pi < 2\pi.$$

<u>*Ejemplos:*</u>

- Calcular $\left(\dfrac{-1+i}{-2-2\sqrt{3}i}\right)^{10}$:

  Se tiene que $-1+i = \sqrt{2}\,e^{\theta i}$ con $\theta \in \mathbb{R}$ tal que $\cos\theta = -1/2$, $\mathrm{sen}\,\theta = 1/2$, o sea $-1+i = \sqrt{2}\,e^{\frac{3\pi}{4}i}$. Del mismo modo, $-2-2\sqrt{3}i = 4\,e^{\frac{4\pi}{3}i}$. Por lo tanto

$$\begin{aligned}\left(\frac{-1+i}{-2-2\sqrt{3}i}\right)^{10} &= \left(\frac{\sqrt{2}}{4}\right)^{10} e^{10\left(\frac{3\pi}{4}-\frac{4\pi}{3}\right)i} \;=\; \frac{2^5}{2^{20}}\,e^{\frac{-70\pi}{12}i}\\ &= 2^{-15}\ e^{(\frac{-70\pi}{12}+3\cdot 2\pi)i} \;=\; 2^{-15}\ e^{\frac{\pi}{6}i} \;=\; \frac{\sqrt{3}}{2^{16}} + \frac{1}{2^{16}}\,i.\end{aligned}$$

- Calcular todos los $n \in \mathbb{N}$ tales que $(1+i)^{2n} = (\sqrt{3}-i)^n$:

  Se tiene $1+i = \sqrt{2}\,e^{\frac{\pi}{4}i}$ y por lo tanto

$$(1+i)^{2n} = \sqrt{2}^{2n}\ e^{\frac{2n\pi}{4}i} = 2^n\ e^{\frac{n\pi}{2}i},$$

  y $\sqrt{3}-i = 2\,e^{\frac{-\pi}{6}i}$, y por lo tanto

$$(\sqrt{3}-i)^n = 2^n\ e^{\frac{-n\pi}{6}i}.$$

  Esto implica

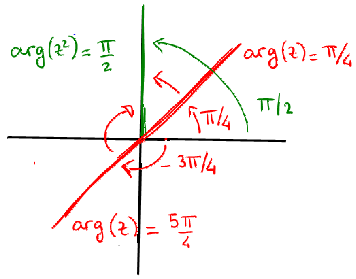
$$\begin{aligned}(1+i)^{2n} = (\sqrt{3}-i)^n \quad &\Longleftrightarrow \quad \frac{n\pi}{2} = \frac{-n\pi}{6} + 2k\pi \ \text{ para algún } \ k \in \mathbb{Z}\\ &\Longleftrightarrow \quad \frac{2n\pi}{3} = 2k\pi \ \text{ para algún } \ k \in \mathbb{Z}\\ &\Longleftrightarrow \quad 2n\pi = 6k\pi \ \text{ para algún } \ k \in \mathbb{Z}\\ &\Longleftrightarrow \quad 3 \mid n.\end{aligned}$$

- Determinar todos los $z \in \mathbb{C}$ tales que $\arg(z^2) = \dfrac{\pi}{2}$:

  Sea $z = r\,e^{\theta i}$ con $0 \le \theta < 2\pi$. Entonces $\arg(z^2) = 2\theta - 2k\pi$ con $k \in \mathbb{Z}$ de modo tal que $0 \le 2\theta - 2k\pi < 2\pi$. Se tiene

$$2\theta - 2k\pi = \frac{\pi}{2} \iff 2\theta = \frac{\pi}{2} + 2k\pi \iff \theta = \frac{\pi}{4} + k\pi.$$

  Para $k = 0$ se obtiene $\theta_0 = \dfrac{\pi}{4}$ y para $k = 1$ se obtiene $\theta_1 = 5\pi/4$. Luego los ángulos se van repitiendo:



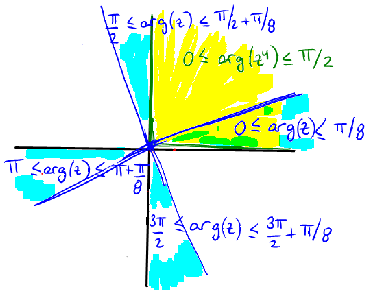
  - $k = 2j \;\Rightarrow\; \theta_k = \dfrac{\pi}{4} + 2j\pi$, i.e. $\theta_k = \theta_0 + 2j\pi$
  - $k = 2j+1 \;\Rightarrow\; \theta_k = \dfrac{5\pi}{4} + 2j\pi$, i.e. $\theta_k = \theta_1 + 2j\pi$.

- Determinar todos los $z \in \mathbb{C}$ tales que $0 \le \arg(z^4) \le \dfrac{\pi}{2}$:

  Sea $z = r\,e^{\theta i}$ con $0 \le \theta < 2\pi$. Entonces $\arg(z^4) = 4\theta - 2k\pi$ con $k \in \mathbb{Z}$ de modo tal que $0 \le 4\theta - 2k\pi < 2\pi$. Se tiene

$$0 \le 4\theta - 2k\pi \le \frac{\pi}{2} \iff \frac{k\pi}{2} \le \theta \le \frac{k\pi}{2} + \frac{\pi}{8}.$$

  - Para $k = 0$ se obtiene el sector $0 \le \theta \le \dfrac{\pi}{8}$.
  - Para $k = 1$ se obtiene el sector $\dfrac{\pi}{2} \le \theta \le \dfrac{\pi}{2} + \dfrac{\pi}{8}$.
  - Para $k = 2$ se obtiene el sector $\pi \le \theta \le \pi + \dfrac{\pi}{8}$.
  - Para $k = 3$ se obtiene el sector $\dfrac{3\pi}{2} \le \theta \le \dfrac{3\pi}{2} + \dfrac{\pi}{8}$.



5.1.4. Raíces n-ésimas de números complejos.

Sea $z \in \mathbb{C}^\times$. Hallar las raíces n-ésimas de z consiste en determinar los $\omega \in \mathbb{C}$ que satisfacen $\omega^n = z$. Hagamos primero un ejemplo.

<u>*Ejemplo:*</u> Las raíces sextas de $z = 1 + i$.

Queremos determinar los $\omega \in \mathbb{C}$ tales que $\omega^6 = 1 + i$. Como comparar potencias es más facil con la forma trigonométrica, planteemos $\omega = r\,e^{\theta i}$ con $r \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$, y comparemos $\omega^6 = r^6\,e^{6\theta i}$ con $1 + i = \sqrt{2}\,e^{\frac{\pi}{4}i}$:

$$r^6\,e^{6\theta i} = \sqrt{2}\,e^{\frac{\pi}{4}i} \iff \begin{cases} r^6 = \sqrt{2} \\ 6\theta = \dfrac{\pi}{4} + 2k\pi \quad \text{para algún } k \in \mathbb{Z}. \end{cases}$$

O sea,

$$r = \sqrt{2}^{1/6} = 2^{1/12} \quad \text{y} \quad \theta = \frac{\pi}{24} + \frac{2k\pi}{6} \quad \text{para algún} \quad k \in \mathbb{Z},$$

Es decir

$$\omega = 2^{1/12}\, e^{(\frac{\pi}{24} + \frac{2k\pi}{6})i} \quad \text{para algún} \quad k \in \mathbb{Z}.$$

Observemos que si $\ell = 6j + k$ con $0 \le k < 6$, entonces

$$\frac{2\ell\pi}{6} = \frac{2(6j+k)\pi}{6} = \frac{2k\pi}{6} + 2j\pi,$$

y por lo tanto

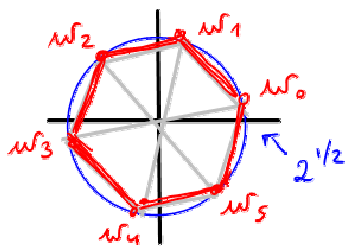
$$\theta_\ell := \frac{\pi}{24} + \frac{2\ell\pi}{6} = \frac{\pi}{24} + \frac{2k\pi}{6} + 2j\pi =: \theta_k + 2j\pi.$$

Se deduce que

$$\omega_\ell = 2^{1/12}\, e^{\theta_\ell i} = 2^{1/12}\, e^{\theta_k i} = \omega_k.$$

Para $k = 0, 1, \ldots, 5$, se obtienen los 6 ángulos, y luego las 6 soluciones

$$\begin{aligned}
\theta_0 &= \frac{\pi}{24} + \frac{2\cdot 0\pi}{6} = \frac{\pi}{24} &&\Longrightarrow \quad \omega_0 = 2^{1/12}\, e^{\frac{\pi}{24} i}\\
\theta_1 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{9\pi}{24} &&\Longrightarrow \quad \omega_1 = 2^{1/12}\, e^{\frac{9\pi}{24} i}\\
\theta_2 &= \frac{\pi}{24} + \frac{2\cdot 2\pi}{6} = \frac{17\pi}{24} &&\Longrightarrow \quad \omega_2 = 2^{1/12}\, e^{\frac{17\pi}{24} i}\\
\theta_3 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{25\pi}{24} &&\Longrightarrow \quad \omega_3 = 2^{1/12}\, e^{\frac{25\pi}{24} i}\\
\theta_4 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{33\pi}{24} &&\Longrightarrow \quad \omega_4 = 2^{1/12}\, e^{\frac{33\pi}{24} i}\\
\theta_5 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{41\pi}{24} &&\Longrightarrow \quad \omega_5 = 2^{1/12}\, e^{\frac{41\pi}{24} i},
\end{aligned}$$



que son todas distintas pues $0 \le \theta_k < 2\pi$ son todos argumentos distintos.

Teorema 5.1.9. (Las raíces n-ésimas de $z \in \mathbb{C}^\times$.)

Sea $n \in \mathbb{N}$ y sea $z = s\, e^{\varphi i} \in \mathbb{C}^\times$, con $s \in \mathbb{R}_{>0}$ y $0 \le \varphi < 2\pi$. Entonces z tiene n raíces n-ésimas $\omega_0, \ldots, \omega_{n-1} \in \mathbb{C}$, donde

$$\omega_k = s^{1/n}\, e^{\theta_k i} \quad \textit{donde} \quad \theta_k = \frac{\varphi + 2k\pi}{n} \quad \textit{para } 0 \le k \le n-1.$$

Demostración. La prueba es igual que en el ejemplo. Tenemos que determinar los $\omega \in \mathbb{C}$ tales que $\omega^n = z$. Planteemos $\omega = r\, e^{\theta i}$ con $r \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$, y comparemos $\omega^n = r^n\, e^{n\theta i}$ con $z = s\, e^{\varphi i}$:

$$\begin{aligned}
r^n\, e^{n\theta i} = s\, e^{\varphi i} \quad &\Longleftrightarrow \quad \begin{cases} r^n = s \\ n\,\theta = \varphi + 2k\pi \quad \text{para algún} \quad k \in \mathbb{Z} \end{cases}\\
&\Longleftrightarrow \quad \begin{cases} r = s^{1/n} \\ \theta = \dfrac{\varphi + 2k\pi}{n} \quad \text{para algún} \quad k \in \mathbb{Z}. \end{cases}
\end{aligned}$$

Es decir

$$\omega = s^{1/n}\, e^{\frac{\varphi+2k\pi}{n}i} \quad \text{para algún} \quad k \in \mathbb{Z}.$$

Observemos que si $\ell = jn + k$ con $0 \le k < n$, entonces

$$\theta_\ell := \frac{\varphi + 2\ell\pi}{n} = \frac{\varphi + 2(jn+k)\pi}{n} = \frac{\varphi + 2k\pi}{n} + 2j\pi =: \theta_k + 2j\pi,$$

y por lo tanto

$$\omega_\ell = s^{1/n}\, e^{\theta_\ell i} = s^{1/n}\, e^{\theta_k i} = \omega_k.$$

Pero más aún, para $0 \le k < n$, $\theta_k = \dfrac{\varphi + 2k\pi}{n}$ son todos distintos y satisfacen $0 \le \theta_k < 2\pi$ pues $0 \le \varphi < 2\pi$ y $0 \le k \le n-1$ implica

$$0 \le \frac{\varphi + 2k\pi}{n} < \frac{2\pi + 2(n-1)\pi}{n} = \frac{2n\pi}{n} = 2\pi.$$

Por lo tanto son todos argumentos distintos, es decir $\omega_k \ne \omega_{k'}$ para $0 \le k \ne k' < n$. Se obtienen por lo tanto las n raíces distintas

$$\omega_k = s^{1/n}\, e^{\theta_k i} \quad \text{donde} \quad \theta_k = \frac{\varphi + 2k\pi}{n} \quad \text{para } 0 \le k \le n-1.$$

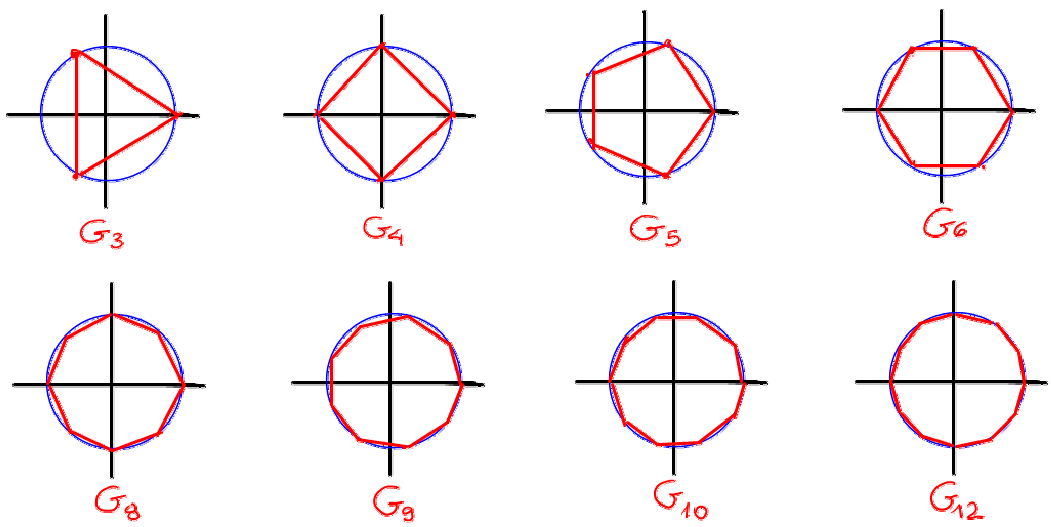
□

5.1.5. El grupo G_n de raíces n-ésimas de la unidad.

Cuando $z = 1$, el polinomio de la sección anterior es el polinomio $X^n - 1$. Sus raíces $\omega_0, \ldots, \omega_{n-1}$ satisfacen todas $\omega_k^n = 1$ para $0 \le k \le n-1$: se denominan las *raíces n-ésimas de la unidad.* Se tiene

$$\omega_k = e^{\frac{2k\pi}{n}i}, \quad 0 \le k \le n-1.$$

En particular, todas las raíces están sobre la circunferencia unidad, $\omega_0 = 1$ y las demás se obtienen dividiendo el ángulo 2π por n, o sea forman un n-ágono regular en la circunferencia unidad, empezando por el 1, como lo muestran las figuras para los valores de $n = 3$, $n = 4$, $n = 5$, $n = 6$, $n = 8$, $n = 9$, $n = 10$ y $n = 12$.



A continuación, estudiamos más en detalle el comportamiento del conjunto de raíces n-ésimas de la unidad para un $n \in \mathbb{N}$ fijo.

Definición 5.1.10. (El conjunto G_n.)

Sea $n \in \mathbb{N}$. El conjunto G_n es el conjunto de raíces n-ésimas de la unidad, es decir

$$G_n := \{\omega \in \mathbb{C} : \omega^n = 1\} \ = \ \{\omega_k = e^{\frac{2\,k\,\pi}{n} i},\ 0 \leq k \leq n-1\} \ \subseteq \ \mathbb{C}.$$

El conjunto G_n tiene n elementos distintos en $\mathbb{C}$ que forman un n-ágono regular en la circunferencia unidad del plano complejo, empezando desde el 1. Por ejemplo,

$$G_1 = \{e^0\} = \{1\},\ G_2 = \{e^0, e^\pi\} = \{1, -1\},\ G_3 = \{e^{\frac{2k\pi}{3} i}, 0 \leq k \leq 2\} = \{1, -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i\}$$
$$G_4 = \{e^{\frac{2k\pi}{4} i}, 0 \leq k \leq 3\} = \{\pm 1, \pm i\},\ G_5 = \{e^{\frac{2k\pi}{5} i}, 0 \leq k \leq 4\}$$
$$G_6 = \{e^{\frac{2k\pi}{6} i}, 0 \leq k \leq 5\} = \{\pm 1, \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2} i\},\ G_8 = \{e^{\frac{2k\pi}{8} i}, 0 \leq k \leq 7\} = \{\pm 1, \pm i, \pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2} i\}.$$

En particular, si $n \neq m$, $G_n \neq G_m$ pues G_n tiene n elementos y G_m tiene m elementos.

Podemos conjeturar de los dibujos un montón de propiedades, que se pueden demostrar incluso sin conocer la forma particular de los elementos de G_n, pero solamente usando la definición: que $\omega \in G_n \Leftrightarrow \omega^n = 1$.

Proposición 5.1.11. ($(G_n, \cdot)$ es un grupo abeliano.)

Sea $n \in \mathbb{N}$.

1. *$\forall\, \omega, z \in G_n$ se tiene que $\omega \cdot z \in G_n$.*
2. *$1 \in G_n$.*
3. *$\forall\, \omega \in G_n$, existe $\omega^{-1} \in G_n$.*

Estas tres propiedades muestran que G_n es un grupo abeliano dentro del grupo multiplicativo $(\mathbb{C}^\times, \cdot)$: es un subconjunto de $\mathbb{C}$ cerrado para la operación producto, el producto es claramente asociativo y conmutativo (pues es el producto de $\mathbb{C}$ que lo es), el elemento neutro 1 de $\mathbb{C}$ pertenece a ese subconjunto, y además cada elemento de G_n tiene inverso en G_n.

Demostración.

1. $\omega, z \in G_n$ si y solo si por definición $\omega^n = 1$ y $z^n = 1$. Por lo tanto $(\omega \cdot z)^n = \omega^n \cdot z^n = 1 \cdot 1 = 1$ también. O sea $\omega \cdot z \in G_n$.
2. $1 \in G_n$ pues $1^n = 1$.
3. Dado $\omega \in G_n$, como $\omega \in \mathbb{C}$ y $\omega \neq 0$ (pues $0^n \neq 1$), se tiene que ω tiene un inverso $\omega^{-1} \in \mathbb{C}$. Alcanza con probar que ese inverso pertenece a G_n. Pero $(\omega^{-1})^n = (\omega^n)^{-1} = 1^{-1} = 1$ también, y por lo tanto $\omega^{-1} \in G_n$.

$\square$

También se pueden inferir las propiedades siguientes de los elementos de G_n, del estudio de los ejemplos anteriores.

Proposición 5.1.12. (Más propiedades de G_n.)

Sea $n \in \mathbb{N}$.

1. $\omega \in G_n \;\Rightarrow\; |\omega| = 1$.
2. $\forall\, \omega \in G_n,\ \omega^{-1} = \overline{\omega}$.
3. $-1 \in G_n \;\Leftrightarrow\; n$ *es par.*
4. *Sea $m \in \mathbb{Z}$ tal que $n \mid m$. Entonces $\omega^m = 1$.*
5. *Sean $m, m' \in \mathbb{Z}$ tales que $m \equiv m' \pmod{n}$, entonces $\omega^m = \omega^{m'}$.*
   En particular $\omega^m = \omega^{r_n(m)}$.
6. $\forall\, \omega \in G_n,\ \omega^{-1} = \overline{\omega} = \omega^{n-1}$.

Demostración.

1. Esto ya lo sabemos porque ya conocemos la forma particular de los elementos de G_n, pero se puede probar directamente de la definición: $\omega^n = 1 \;\Rightarrow\; 1 = |\omega^n| = |\omega|^n$, y por lo tanto $|\omega| = 1$.
2. $\omega^{-1} = \dfrac{\overline{\omega}}{|\omega|}$ pero $|\omega| = 1$.
3. $(-1)^n = 1 \;\Leftrightarrow\; n$ es par.
4. Si $n \mid m$, entonces $m = kn$ y por lo tanto $\omega^m = \omega^{kn} = (\omega^n)^k = 1^k = 1$.
5. Sea $k \in \mathbb{Z}$ tal que $m = k\,n + m'$. Entonces $\omega^m = \omega^{kn+m'} = (\omega^n)^k \cdot \omega^{m'} = 1^k \cdot \omega^{m'} = \omega^{m'}$.
6. Es una consecuencia del inciso anterior, dado que $-1 \equiv n - 1 \pmod{n}$.

$\square$

<u>*Ejemplo:*</u> Para cada $\omega \in G_5$, calcular $\omega^{103} + \omega^{27} + \omega^{-4} + \overline{\omega}$:

Por la Proposición 5.1.12 (5,6), se tiene

$$\omega^{103} + \omega^{27} + \omega^{-4} + \overline{\omega} = \omega^3 + \omega^2 + \omega + \omega^4 = \begin{cases} -1 & \text{si } \omega \neq 1 \\ 4 & \text{si } \omega = 1. \end{cases}$$

ya que

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 = \sum_{i=0}^{4} \omega^i = \begin{cases} \dfrac{\omega^5 - 1}{\omega - 1} = \dfrac{1-1}{\omega - 1} = 0 & \text{si } \omega \neq 1 \\ 5 & \text{si } \omega = 1. \end{cases}$$

por la fórmula de la serie geométrica.

También se pueden comparar distintos G_n.

Proposición 5.1.13. **($G_n \cap G_m = G_{(n:m)}$).**

Sean $n, m \in \mathbb{N}$.

1. $n \mid m \Rightarrow G_n \subset G_m$.
2. $G_n \cap G_m = G_{(n:m)}$.
3. $G_n \subset G_m \Leftrightarrow n \mid m$.

Demostración. 1. $n \mid m \Rightarrow m = k\,n$ para algún $k \in \mathbb{Z}$. Por lo tanto, si $\omega \in G_n$, $\omega^m = \omega^{kn} = (\omega^n)^k = 1^k = 1$, o sea $\omega \in G_m$.

2. Como $(n : m) \mid n$ y $(n : m) \mid m$, $G_{(n:m)} \subset G_n$ y $G_{(n:m)} \subset G_m$ por el inciso anterior, y por lo tanto $G_{(n:m)} \subset G_n \cap G_m$.

   Falta probar la otra inclusión: se sabe que existen $s, t \in \mathbb{Z}$ tales que $(n : m) = sn + tm$, por lo tanto $\omega^{(n:m)} = \omega^{sn+tm} = (\omega^n)^s \cdot (\omega^m)^t$. Si $\omega \in G_n \cap G_m$, entonces $\omega^n = \omega^m = 1$ y por lo tanto, $\omega^{(n:m)} = 1^s \cdot 1^t = 1$, es decir $\omega \in G_{(n:m)}$ también.

3. Ya sabemos que vale $(\Leftarrow)$ por el inciso 1. Probemos $(\Rightarrow)$:

   $G_n \subset G_m \Rightarrow G_n \cap G_m = G_n$. Pero por el inciso anterior, se sabe que $G_n \cap G_m = G_{(n:m)}$. Por lo tanto $G_n = G_{(n:m)}$. Esto implica $n = (n : m)$ (pues hemos visto que distintos G_n tienen distina cantidad de elementos) y por lo tanto $n \mid m$ como se quería probar.

□

Saquemos ahora provecho de la forma particular de los elementos de G_n:

$$G_n := \{\omega_k = e^{\frac{2\,k\,\pi}{n} i},\ 0 \le k \le n-1.\}$$

Proposición 5.1.14. **(G_n es un grupo cíclico.)**

Sea $n \in \mathbb{N}$. *Existe* $\omega \in G_n$ *tal que*

$$G_n = \{\omega^0, \omega^1, \omega^2, \ldots, , \omega^{n-1}\} = \{\omega^k,\ 0 \le k \le n-1\}.$$

Demostración. Se puede tomar por ejemplo $\omega := \omega_1 = e^{\frac{2\,\pi}{n} i}$, ya que sabemos por la fórmula de de Moivre que

$$\omega_1^k = \left(e^{\frac{2\,\pi}{n} i}\right)^k = e^{k\frac{2\,\pi}{n} i} = e^{\frac{2k\,\pi}{n} i} = \omega_k, \quad 0 \le k \le n-1.$$

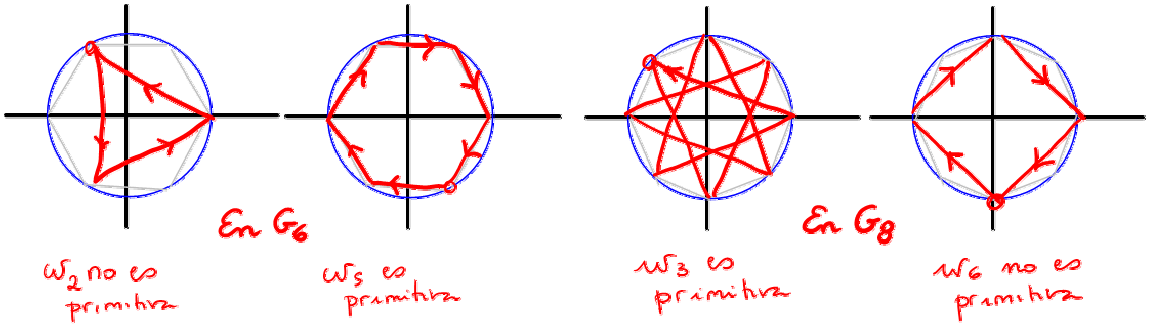
Pero ω_1 no es la única elección posible en esta demostración, por ejemplo también podríamos haber tomado $\omega_{n-1} = \overline{\omega_1}$ pues $\overline{\omega_1}^k = \overline{\omega_1^k} = \overline{\omega_k} = \omega_{n-k}$ para $0 \le k \le n-1$, es decir $\omega_{n-1}^k = \omega_{n-k}$ para $0 \le k \le n-1$. Esto motiva la definición siguiente. □

Definición 5.1.15. **(Raíz n-ésima primitiva de la unidad.)**

Sea $n \in \mathbb{N}$. Se dice que $\omega \in \mathbb{C}$ es una raíz n*-ésima primitiva* de la unidad si

$$G_n = \{\omega^k,\ 0 \le k \le n-1\}.$$

Ejemplo:



Observación 5.1.16. Observemos que la definición de raíz primitiva de orden n de la unidad implica en particular que $\omega^k = \omega^j$ para $0 \leq k, j \leq n-1$ implica que $k = j$, pues ya sabemos que G_n tiene n elementos distintos, luego no pueden coincidir dos potencias distintas de ω en el rango $0 \leq k, j \leq n-1$.

Proposición 5.1.17. (Caracterización de las raíces n-ésimas primitivas de la unidad.)

Sea $n \in \mathbb{N}$, y sea $\omega \in \mathbb{C}$. Entonces ω es una raíz n-ésima primitiva de la unidad si y solo si

$$\forall\, m \in \mathbb{Z}, \quad \omega^m = 1 \iff n \mid m.$$

Demostración. ($\Rightarrow$) Sea ω una raíz n-ésima primitiva de la unidad. Queremos probar que $\omega^m = 1 \Leftrightarrow n \mid m$.

Como ω es raíz n-ésima de la unidad, sabemos por la Proposición 5.1.12(4) que si $n \mid m$, entonces $\omega^n = 1$.

Queremos probar la recíproca, que si $\omega^m = 1$ entonces $n \mid m$. Pero por la Proposición 5.1.12(5), $\omega^m = \omega^{r_n(m)}$. Luego $\omega^m = 1$ implica $\omega^{r_n(m)} = 1 = \omega^0$, lo que implica por la Observación anterior que $r_n(m) = 0$, o sea $n \mid m$.

($\Leftarrow$) Queremos probar que si ω satisface $\omega^m = 1 \Leftrightarrow n \mid m$, entonces $G_n = \{\omega^k,\ 0 \leq k \leq n-1\}$.

Pero $\omega^m = 1 \Leftrightarrow n \mid m$ implica $\omega^n = 1$ y $\omega^k \neq 1$ para $1 \leq k \leq n-1$. Por lo tanto $\omega \in G_n$, lo que implica que $\omega^k \in G_n,\ 0 \leq k \leq n-1$. Así $\{\omega^k,\ 0 \leq k \leq n-1\} \subset G_n$.

Pero además $\omega^k \neq \omega^j$ para todo $0 \leq k < j \leq n-1$, pues si para $0 \leq k < j \leq n$ se tuviera $\omega^k = \omega^j$, entonces $\omega^{j-k} = 1$ con $1 \leq j-k \leq n-1$, lo que es una contradicción con $\omega^k \neq 1$ para $1 \leq k \leq n-1$. Por lo tanto $\#\{\omega^k;\ 0 \leq k \leq n-1\} = n = \#\, G_n$ implica que $\{\omega^k,\ 0 \leq k \leq n-1\} = G_n$. $\square$

Corolario 5.1.18. (Raíces primitivas y potencias.)

Sean $n, k \in \mathbb{N}$ y sea $\omega \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Entonces ω^k es una raíz n-ésima primitiva de la unidad si y solamente si $(n : k) = 1$.

Demostración. ($\Leftarrow$) Alcanza con probar, según la proposición anterior, que $(\omega^k)^m = 1 \Leftrightarrow n \mid m$, sabiendo que cualquiera sea el exponente j, $\omega^j = 1 \Leftrightarrow n \mid j$. Pero

$$1 = (\omega^k)^m = \omega^{km} \iff n \mid k\,m \underset{(n:k)=1}{\iff} n \mid m,$$

como se quería probar.

($\Rightarrow$) Lo demostramos por la contrarecíproca: Supongamos que $(n:k) = d \neq 1$. Entonces

$$(\omega^k)^{\frac{n}{d}} = (\omega)^{\frac{kn}{d}} = (\omega^n)^{\frac{k}{d}} = 1^{\frac{k}{d}} = 1$$

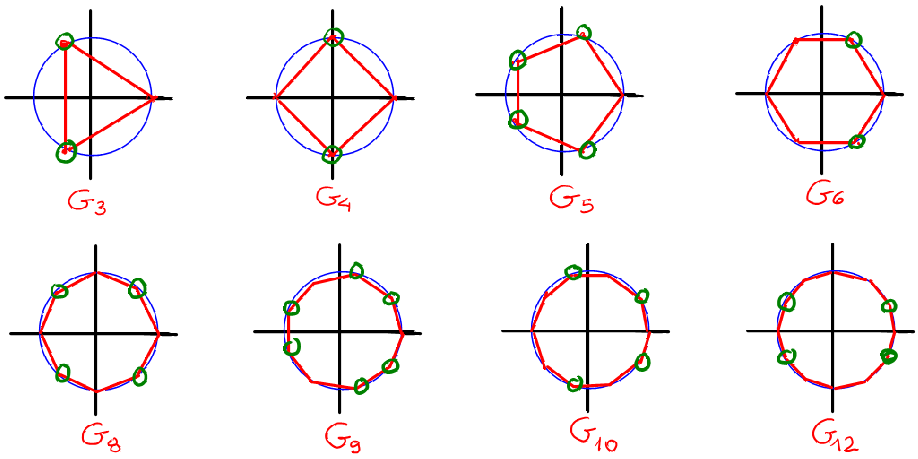
y por lo tanto ω^k no es una raíz n-ésima primitiva de la unidad, pues $n \nmid \dfrac{n}{d}$ y se contradice la Proposición 5.1.17. $\square$

Corolario 5.1.19. (Las raíces primitivas en G_n.)

Sea $n \in \mathbb{N}$, y sea $\omega_k = e^{\frac{2k\pi}{n}i}$, $0 \leq k \leq n-1$. Entonces ω_k es raíz n-ésima primitiva de la unidad si y solamente si $(n:k) = 1$.

Demostración. Pues sabemos que ω_1 es raíz n-ésima primitiva de la unidad y $\omega_k = (\omega_1)^k$. $\square$

En los ejemplos siguientes, las raíces primitivas están marcadas con un círculo verde:



Corolario 5.1.20. (Las raíces primitivas en G_p.)

Sea p un primo. Entonces cualquiera sea k, $1 \leq k \leq p-1$, se tiene que $\omega_k = e^{\frac{2k\pi}{p}i}$ es ráiz p-ésima primitiva de la unidad. Es decir $\forall\, \omega \in G_p$, $\omega \neq 1$, se tiene que ω es una raíz p-ésima primitiva de la unidad.

<u>*Ejemplo:*</u> Sea ω una raíz primitiva de la unidad de orden 15.

- Probar que ω^3 es una raíz primitiva de la unidad de orden 5: Se tiene $(\omega^3)^5 = \omega^{15} = 1$, por lo tanto ω^3 es una raíz de la unidad de orden 5. Pero $\omega \neq 1$ pues ω es *primitiva* de orden 15, por lo tanto $\omega^3 \in G_5 - \{1\}$ implica que ω^3 es primitiva de orden 5, pues 5 es primo, y todas las raíces de la unidad de orden 5 salvo el 1 son primitivas.

- Calcular $\omega^{159} + \overline{\omega}^{27} - \omega^{27} + \omega^6 + 2\omega^{-3}$:

  Se tiene

$$\omega^{159}+\overline{\omega}^{27}-\omega^{27}+\omega^6+2\omega^{-3} = \omega^9+\omega^3-\omega^{12}+\omega^6+2\omega^{12} = \sum_{k=1}^{4}(\omega^3)^k = \frac{(\omega^3)^5-1}{\omega^3-1}-(\omega^3)^0 = -1,$$

  pues $\omega^3 \neq 1$ al ser ω *primitiva* de orden 15.

Terminemos este capítulo con una propiedad general de las raíces de la unidad.

Proposición 5.1.21. (Suma y producto de los elementos de G_n.)
Sea $n \in \mathbb{N}$. Entonces

$$\sum_{\omega \in G_n} \omega = 0 \qquad y \qquad \prod_{\omega \in G_n} \omega = \begin{cases} 1 & si \quad n \text{ es impar}, \\ -1 & si \quad n \text{ es par}. \end{cases}$$

Demostración. Sabemos que G^n es un grupo cíclico, es decir existe $\omega \in G^n$ tal que $G_n = \{w^0, w^1, \ldots, w^{n-1}\}$. Por lo tanto,

$$\sum_{\omega \in G_n} \omega = \sum_{k=0}^{n-1} \omega^k = \frac{\omega^n - 1}{\omega - 1} = \frac{1-1}{\omega - 1} = 0,$$

por la suma geométrica, ya que $\omega \neq 1$, y porque $\omega^n = 1$.

Con respecto al producto, en G_n sabemos que cada vez que está ω también está $\omega^{-1} = \overline{\omega} \neq \omega$ si $\omega \neq \pm 1$. Por lo tanto, cuando n es impar (caso en que $-1 \notin G_n$), las raíces de la unidad vienen de a pares inversos, cuyo producto da 1, además de la raíz 1, y por lo tanto el producto da 1. Cuando n es par (caso en que $-1 \in G_n$), las raíces de la unidad vienen de a pares inversos, cuyo producto da 1, además de las raíces 1 y -1, y por lo tanto el producto da -1. □

5.2. El anillo de polinomios $K[X]$: generalidades.

Sea K un cuerpo, por ejemplo $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}/p\mathbb{Z}$, donde p es un número primo (positivo). Se dice que f es un *polinomio con coeficientes en* K si f es de la forma

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i,$$

para algún $n \in \mathbb{N}_0$, donde X es una indeterminada sobre K y $a_i \in K$ para $0 \leq i \leq n$. Los elementos $a_i \in K$ se llaman los *coeficientes* de f. Se conviene que dos polinomios son iguales si y solo si coinciden todos sus coeficientes, es decir si $f = \sum_{i=0}^{n} a_i X^i$ y $g = \sum_{i=0}^{n} b_i X^i$, entonces $f = g \Leftrightarrow a_i = b_i$, $0 \leq i \leq n$.

El conjunto de todos los polinomios f con coeficientes en K se nota $K[X]$.

Si f no es el polinomio nulo, es decir $f \neq 0$, entonces se puede escribir para algún $n \in \mathbb{N}_0$ en la forma

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{con} \quad a_n \neq 0.$$

En ese caso n es el *grado* de f y se nota $\mathrm{gr}(f)$, a_n es el *coeficiente principal* de f y lo notaremos aquí $\mathrm{cp}(f)$, y a_0 se denomina el *coeficiente constante* o *término independiente* de f. El polinomio nulo no tiene grado. Cuando el coeficiente principal de f es igual a 1, se dice que el polinomio es *mónico*. Notemos que para todo $f \in K[X] - \{0\}$, se tiene $\mathrm{gr}(f) \in \mathbb{N}_0$.

5.2.1. Operaciones en $K[X]$.

Las operaciones $+$ y $\cdot$ del cuerpo K se trasladan al conjunto $K[X]$ en forma natural, se suma coeficiente a coeficiente y se multiplica aplicando la distributividad:

- Si $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{m} b_i X^i \in K[X]$, entonces
$$f + g = \sum_{i=o}^{n} (a_i + b_i) X^i \in K[X].$$
- Si $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j \in K[X]$, entonces
$$f \cdot g = \sum_{k=0}^{n+m} c_k X^k \in K[X] \quad \text{donde } c_k = \sum_{i+j=k} a_i b_j.$$

<u>*Ejemplos:*</u>

- Sean $f = 5X^4 - 2X^3 + 3X^2 - X + 1$ y $g = 3X^3 - X^2 + X - 3$. Entonces
$$f+g = 5X^4+X^3+2X^2-2 \quad \text{y} \quad f \cdot g = 15X^7-11X^6+16X^5-23X^4+13X^3-11X^2+4X-3.$$
- En este caso, $\mathrm{gr}(f+g) = 4 = \text{máx}\{\mathrm{gr}(f), \mathrm{gr}(g)\}$, y $\mathrm{gr}(f \cdot g) = 7 = \mathrm{gr}(f) + \mathrm{gr}(g)$, más aún, $\mathrm{cp}(f \cdot g) = 15 = 5 \cdot 3 = \mathrm{cp}(f) \cdot \mathrm{cp}(g)$.
- Sean $f = 2X^3 + 3X - 1$, $g = -2X^3 + 2X^2 - 1$ y $h = -3X^3 - 2$. Entonces $f + g = 2X^2 + 3X - 2$ y $f + h = -X^3 + 3X - 3$. En este caso $\mathrm{gr}(f+g) = 2 < \text{máx}\{\mathrm{gr}(f), \mathrm{gr}(g)\}$ pues los dos polinomios tienen el mismo grado y se cancelaron los coeficientes principales, pero $\mathrm{gr}(f+h) = 3 = \text{máx}\{\mathrm{gr}(f), \mathrm{gr}(g)\}$ pues por más que los dos polinomios tienen mismo grado, no se cancelaron los coeficientes principales.

Observación 5.2.1. (Grado de la suma y del producto.)

Sea K un cuerpo y sean $f, g \in K[X]$ *no nulos*. Entonces

- Si $f + g \neq 0$, entonces $\mathrm{gr}(f+g) \leq \text{máx}\{\mathrm{gr}(f), \mathrm{gr}(g)\}$. Más precisamente,
  $\mathrm{gr}(f+g) = \text{máx}\{\mathrm{gr}(f), \mathrm{gr}(g)\}$ si $\mathrm{gr}(f) \neq \mathrm{gr}(g)$ o $\mathrm{gr}(f) = \mathrm{gr}(g)$ pero $\mathrm{cp}(f) + \mathrm{cp}(g) \neq 0$.
  $\mathrm{gr}(f+g) < \text{máx}\{\mathrm{gr}(f), \mathrm{gr}(g)\}$ si $\mathrm{gr}(f) = \mathrm{gr}(g)$ y $\mathrm{cp}(f) + \mathrm{cp}(g) = 0$.

- $\mathrm{cp}(f \cdot g) = \mathrm{cp}(f) \cdot \mathrm{cp}(g)$. En particular, $f \cdot g \neq 0$ y $\mathrm{gr}(f \cdot g) = \mathrm{gr}(f) + \mathrm{gr}(g)$.

<u>*Ejemplo:*</u> Calcular el coeficiente principal, el coeficiente constante y el que acompaña a X de

$$f = (X^3 + 2)^{10}(2X + 3)^5$$

- El coeficiente principal de f se obtiene multiplicando los coeficientes principales de los factores:
$$\mathrm{cp}(f) = \mathrm{cp}(X^3 + 2)^{10}\mathrm{cp}(2X + 3)^5 = 1^{10} \cdot 2^5 = 2^5.$$

- El coeficiente constante de f se obtiene multiplicando los coeficientes constantes de los factores, en este caso:
$$2^{10} \cdot 3^5.$$

- ¿Cómo se obtiene el coeficiente que acompaña a X en este producto? La única forma es eligiendo el coeficiente constante en $(X^3+2)^{10}$, esto es 2^{10}, y calculando en $(2X+3)^5$ el coeficiente que acompaña a X, es decir eligiendo en uno de los 5 paréntesis de $(2X+3)^5$ una vez el $2X$ y 4 veces el 3, esto es $\binom{5}{1}2 \cdot 3^4 = 5 \cdot 2 \cdot 3^4$. El resultado es entonces:
$$2^{10} \cdot 5 \cdot 2 \cdot 3^4 = 2^{11} \cdot 3^4 \cdot 5.$$

Teorema 5.2.2. (El anillo $(K[X], +, \cdot)$.)

Sea K un cuerpo. Entonces, $(K[X], +, \cdot)$ es un anillo conmutativo*(al igual que $\mathbb{Z}$). Más aún, al igual que en $\mathbb{Z}$, si se multiplican dos elementos no nulos, el resultado es no nulo, o dicho de otra manera:*
$$\forall\, f, g \in K[X], \quad f \cdot g = 0 \implies f = 0 \ o \ \ g = 0.$$
(Esto se llama ser un dominio íntegro*.)*

Demostración. Las propiedades conmutativa y asociativo de las operaciones $+$ y $\cdot$ son consecuencia de las definiciones de las operaciones y del hecho que valen las mismas propiedades en K. El elemento neutro para la suma es el polinomio 0, y el opuesto aditivo de $f = \sum_{i=o}^{n} a_i X^i$ es $-f = sum_{i=0}^{n}(-a_i)X^i$. El elemento neutro para el producto es el polinimio 1. Pero en ese caso no todo $f \neq 0$ tiene inverso multiplicativo, como veremos a continuación.

La segunda afirmación es una consecuencia de la observación anterior: si f y g son no nulos, entonces fg es no nulo. □

Como consecuencia de la observación sobre el grado del producto se deduce inmediatamente quiénes son los polinomios en $K[X]$ que tienen inverso multiplicativo.

Observación 5.2.3. (Inversibles de $K[X]$.)

Sea K un cuerpo. Entonces $f \in K[X]$ es inversible si y solo si $f \in K^\times$. O sea los elementos inversibles de $K[X]$ son los polinomios de grado 0.

Demostración.

- ($\Rightarrow$) Sea $f \in K[X]$ inversible. Por lo tanto $f \neq 0$ y existe $g \in K[X]$ tal que $f \cdot g = 1$. Esto implica que $g \neq 0$ también y $\mathrm{gr}(1) = \mathrm{gr}(f \cdot g)$, es decir $0 = \mathrm{gr}(f) + \mathrm{gr}(g)$. Como $\mathrm{gr}(f), \mathrm{gr}(g) \in \mathbb{N}_0$, la única posibilidad es $\mathrm{gr}(f) = 0 = \mathrm{gr}(g)$ y por lo tanto $f, g \in K$, y no nulos.
- ($\Leftarrow$) Sea $f \in K - \{0\}$. Entonces, como K es un cuerpo, f es inversible y existe $g \in K - \{0\}$ tal que $f \cdot g = 1$, es decir f es inversible.

□

5.3. Divisibilidad, Algoritmo de División y MCD en $K[X]$.

Por lo que vimos en la sección anterior, $K[X]$ es un anillo conmutativo (más bien un dominio íntegro) que, al igual que $\mathbb{Z}$, no es un cuerpo ya que no todo elemento no nulo es inversible: sabemos que los únicos polinomios inversibles son los polinomios constantes (no nulo). Tiene sentido entonces estudiar la *divisibilidad* así como hicimos en $\mathbb{Z}$. En esta sección haremos todo un paralelismo con la teoría desarrollada en $\mathbb{Z}$.

Definición 5.3.1. (Divisibilidad.)

Sean $f, g \in K[X]$ con $h \neq 0$. Se dice que g *divide a* f, y se nota $g \mid f$, si existe un polinomio $q \in K[X]$ tal que $f = q \cdot g$. O sea:

$$g \mid f \iff \exists\, q \in K[X] \,:\, f = q \cdot g.$$

En caso contrario, se dice que g no divide a f, y se nota $g \nmid f$.

Propiedades 5.3.2. (Propiedades de la divisibilidad.)

- Todo polinomio $g \neq 0$ satisface que $g \mid 0$ pues $0 = 0 \cdot g$ (aquí $q = 0$).
- $g \mid f \Leftrightarrow c\,g \mid f$, $\forall\, c \in K^\times$ (pues $f = q \cdot g \Leftrightarrow f = (c^{-1}q) \cdot (c\,g)$).

  De la misma manera $g \mid f \Leftrightarrow g \mid d\,f, \forall\, d \in K^\times$.

  Se concluye que si $f, g \in K[X]$ son no nulos,

  $$g \mid f \iff c\,g \mid d\,f,\ \forall\, c, d \in K^\times \iff \frac{g}{\mathrm{cp}(g)} \mid \frac{f}{\mathrm{cp}(f)}.$$

  Es decir la divisibilidad no depende de constantes no nulas (que son los elementos inversibles de K), y por lo tanto todo polinomio tiene infinitos divisores. Pero todo divisor g de f tiene un divisor mónico asociado, que es $g/\mathrm{cp}(g)$.
- Sean $f, g \in K[X]$ no nulos tales que $g \mid f$ y $\mathrm{gr}(g) = \mathrm{gr}(f)$. Entonces $g = c\,f$ para algún $c \in K^\times$ (pues $f = q\,g$ con $q \neq 0$ y $\mathrm{gr}(g) = \mathrm{gr}(f) \Rightarrow \mathrm{gr}(q) = 0,$, i.e. $q = c \in K^\times$).
- $g \mid f$ y $f \mid g \Leftrightarrow f = c\,g$ para algún $c \in K^\times$ (pues tienen el mismo grado).

- Para todo $f \in K[X]$, $f \notin K$, se tiene $c \mid f$ y $c\,f \mid f$, $\forall\, c \in K^\times$.

  Así, todo f en esas condiciones tiene esas dos categorías distintas de divisores asegurados (los de grado 0 y los de su mismo grado).

  Hay polinomios que tienen únicamente esos divisores, y otros que tienen más. Esto motiva la separación de los polinomios en $K[X]$ no constantes en dos categorías, la de polinomios *irreducibles* y la de los polinomios *reducibles* :

Definición 5.3.3. (Polinomios irreducibles y reducibles.)

Sea $f \in K[X]$.

- Se dice que f es *irreducible* en $K[X]$ cuando $f \notin K$ y los únicos divisores de f son de la forma $g = c$ o $g = c\,f$ para algún $c \in K^\times$. O sea f tiene únicamente dos divisores mónicos (distintos), que son 1 y $f/\mathrm{cp}(f)$.
- Se dice que f es *reducible* en $K[X]$ cuando $f \notin K$ y f tiene algún divisor $g \in K[X]$ con $g \neq c$ y $g \neq c\,f$, $\forall\, c \in K^\times$, es decir f tiene algún divisor $g \in K[X]$ (no nulo por definición) con $0 < \mathrm{gr}(g) < \mathrm{gr}(f)$.

En particular, todo polinomio de grado 1 en $K[X]$ es irreducible.

Pero no solo ellos, dependiendo del cuerpo K: por ejemplo el polinomio $X^2 + 1 \in \mathbb{R}[X]$ es irreducible en $\mathbb{R}[X]$, pues si fuera reducible, tendría un divisor mónico de grado 1 (grado intermedio), y luego se tendría $X^2+1 = (X+a)\,(X+b)$ con $a, b \in \mathbb{R}$, lo que implica $a+b = 0$, i.e. $b = -a$ y $a\,b = 1$, i.e. $-a^2 = 1$, lo que es imposible para $a \in \mathbb{R}$. Pero es reducible en $\mathbb{C}[X]$ ya que $X^2 + 1 = (x - i)(x + i)$, i.e. $X - i \mid X^2 + 1$ en $\mathbb{C}[X]$.

Y el polinomio $X^2 - 2 \in \mathbb{Q}[X]$ es irreducible en $\mathbb{Q}[X]$, pues si fuera reducible, tendría un divisor mónico de grado 1, y luego se tendría $X^2 - 2 = (X + a)\,(X + b)$ con $a, b \in \mathbb{Q}$, lo que implica $a+b = 0$, i.e. $b = -a$ y $a\,b = -2$, i.e. $a^2 = 2$, lo que es imposible para $a \in \mathbb{Q}$. Pero es reducible en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$ ya que $X^2 + 2 = (x - \sqrt{2})(x + \sqrt{2})$, i.e. $X - \sqrt{2} \mid X^2 - 2$ en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$.

La divisibilidad de polinomios cumple exactamente las mismas propiedades que la divisibilidad de números enteros. Repasar esas propiedades.

Continuamos entonces el paralelismo con $\mathbb{Z}$ para $K[X]$:

Teorema 5.3.4. (Algoritmo de división.)

Dados $f, g \in K[X]$ no nulos, existen únicos $q, r \in K[X]$ que satisfacen

$$f = q \cdot g + r \quad \textit{con} \quad r = 0 \quad \textit{o} \quad \deg(r) < \deg(g).$$

Se dice que q es el *cociente* y r es el *resto* de la división de f por g, que notaremos $r_g(f)$.

<u>*Ejemplo:*</u> Sean $f = X^5 + X^4 - 3X^3 + 4X^2 + 2X$ y $g = X^4 + 3X^3 - X^2 - 6X - 2$, entonces

$$f = (X - 2)g + r \quad \text{con } r = 4X^3 + 8X^2 - 8X - 4.$$

Demostración. ▪ *Existencia de q y r :*

La demostración es calcada del caso $\mathbb{Z}$. Dados $f, g \in K[X]$ no nulos, consideramos el conjunto

$$A = \{f - \tilde{q}\, g;\ \tilde{q} \in K[X]\} \ \subset\ K[X],$$

que es claramente un conjunto $\neq \{0\}$ pues por ejemplo $f \in A$ tomando $\tilde{q} = 0$. Si $0 \notin A$, elijamos un polinomio $r \in A$ de grado mínimo, y si $0 \in A$, elijamos $r = 0$. Es decir

$$\exists\, q \in K[X] \ \text{ tal que } \quad r = f - q\, g \quad \text{ y } \quad r = 0 \ \text{ o } \ \mathrm{gr}(r) \leq \mathrm{gr}(\tilde{r}),\ \forall\, \tilde{r} \in A.$$

Por lo tanto, $f = q\, g + r$ y se afirma que si $r \neq 0$, entonces $\mathrm{gr}(r) < \mathrm{gr}(g)$. Pues si fuera $\mathrm{gr}(r) \geq \mathrm{gr}(g)$, puedo considerar el polinomio

$$\tilde{r} = r - \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\, g = f - q\, g - \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\, g = f - \Big(q + \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\Big)\, g \ \in\ A.$$

Es fácil verificar que los dos sumandos tienen el mismo grado, y en esta resta, se cancela el coeficiente principal de r. Por lo tanto $\mathrm{gr}(\tilde{r}) < \tilde{r}$, lo que contradice el hecho que r tenía grado mínimo en A.

▪ *Unicidad de g y r :*

Supongamos que existen $q_1, r_1, q_2, r_2 \in K[X]$ con $r_1 = 0$ o $\mathrm{gr}(r_1) < \mathrm{gr}(g)$ y $r_2 = 0$ o $\mathrm{gr}(r_2) < \mathrm{gr}(g)$ tales que

$$f = q_1\, g + r_1 = q_2\, g + r_2.$$

Entonces $(q_1 - q_2)\, g = r_2 - r_1$ implica $g \mid r_2 - r_1$. Pero si $r_2 - r_1 \neq 0$, se tiene que $\mathrm{gr}(r_2 - r_1) < \text{máx}\{\mathrm{gr}(r_2), \mathrm{gr}(r_1)\} < \mathrm{gr}(g)$, luego no puede ser divisible por g. Por lo tanto $r_2 - r_1 = 0$, i.e. $r_1 = r_2$ de lo que se deduce que $q_1 = q_2$ pues $(q_1 - q_2)\, g = 0$ con $g \neq 0$ implica $q_1 - q_2 = 0$.

□

Definición 5.3.5. (Máximo Común Divisor.)

Sean $f,\, g \in K[X]$ no ambos nulos. El *máximo común divisor* entre f y g, que se nota $(f : g)$, es el polinomio mónico de mayor grado que divide simultáneamente a f y a g.

Observación 5.3.6. No es obvio en este caso que este polinomio es único, de hecho es una consecuencia de las propiedades siguientes que se cumplen para un polinomio mónico de mayor grado que es divisor común de f y g, y de los resultados que se deducen de esas propiedades.

- $(f : 0) = f/\mathrm{cp}(f)$, $\forall\, f \in K[X]$ no nulo.
- Sean $f, g \in K[X]$ con g no nulo. Si $f = q \cdot g + r$ para $q, r \in K[X]$, entonces $(f : g) = (g : r)$.

<u>*Ejemplos:*</u> Sean $f,\, g \in K[X]$, $g \neq 0$. Entonces :

- Sea $c \in K^{\times}$, $(c : g) = 1$

- Si $g \mid f$, entonces $(f : g) = \frac{g}{\mathrm{cp}(g)}$.

A continuación deducimos el Algoritmo de Euclides, que al igual que en el caso $\mathbb{Z}$, permite calculer el máximo común divisor entre dos polinomios (y es para polinomios arbitrarios la única forma de calcular el máximo común divisor de hecho).

Teorema 5.3.7. (Algoritmo de Euclides.)

Sean $f, g \in K[X]$ no nulos. Entonces $(f : g)$ es el último resto r_k no nulo (dividido por su coeficiente principal para volverlo mónico) que aparece en la sucesión de divisiones siguiente:

$$\begin{array}{lcll} f & = & q_1\, g + r_1 & \textit{con} \quad \mathrm{gr}(r_1) < \mathrm{gr}(g) \\ g & = & q_2\, r_1 + r_2 & \textit{con} \quad \mathrm{gr}(r_2) < \mathrm{gr}(r_1) \\ r_1 & = & q_3\, r_2 + r_3 & \textit{con} \quad \mathrm{gr}(r_1) < \mathrm{gr}(g) \\ & \vdots & & \\ r_{k-2} & = & q_k\, r_{k-1} + r_k & \textit{con} \quad \mathrm{gr}(r_k) < \mathrm{gr}(r_{k-1}) \\ r_{k-1} & = & q_{k+1}\, r_k & \end{array}$$

(pues resulta $(f : g) = (g : r_1) = (r_1 : r_2) = \cdots = (r_{k-2} : r_{k-1}) = (r_{k-1} : r_k) = \frac{r_k}{\mathrm{cp}(r_k)}$, ya que $r_k \mid r_{k-1}$).

Luego, despejando en el Teorema r_k de la anteúltima igualdad, y volviendo hacia arriba despejando paso a paso r_{k-1}, $r_{k-2}, \ldots,$ r_2, r_1 en las igualdades anteriores, se logra escribir r_k en la forma $r_k = s'f + t'g$. Finalmente, dividiendo toda la expresión por la constante $\mathrm{cp}(r_k)$, se obtienen $s, t \in K[X]$ tales que $(f : g) = sf + tg$.

<u>*Ejemplo:*</u> Sean $f = X^5 + X^4 - 3X^3 + 4X^2 + 2X$ y $g = X^4 + 3X^3 - X^2 - 6X - 2$. Se tiene :

$$\begin{array}{lcll} f & = & (X-2)g + r_1 & \text{con} \quad r_1 = 4X^3 + 8X^2 - 8X - 4 \\ g & = & (\frac{1}{4}X + \frac{1}{4})r_1 + r_2 & \text{con} \quad r_2 = -X^2 - 3X - 1 \\ r_1 & = & (-4X + 4)r_2 & \end{array}$$

Luego $(f : g) = \frac{r_2}{\mathrm{cp}(r_2)} = X^2 + 3X + 1$ y

$$\begin{array}{lcl} r_2 & = & g - (\frac{1}{4}X + \frac{1}{4})r_1 \\ & = & g - (\frac{1}{4}X + \frac{1}{4})(f - (X-2)g) \\ & = & -(\frac{1}{4}X + \frac{1}{4})f + [1 + (\frac{1}{4}X + \frac{1}{4})(X-2)]g \\ & = & -(\frac{1}{4}X + \frac{1}{4})f + (\frac{1}{4}X^2 - \frac{1}{4}X + \frac{1}{2})g \end{array}$$

Así : $(f : g) = -r_2 = (\frac{1}{4}X + \frac{1}{4})f - (\frac{1}{4}X^2 - \frac{1}{4}X + \frac{1}{2})g$.

Corolario 5.3.8. (Mcd y combinación polinomial.)

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g es el (único) polinomio mónico $h \in K[X]$ que satisface simultáneamente las dos condiciones siguientes :

- *$h \mid f$ y $h \mid g$,*
- *Existen $s, t \in K[X]$ tales que $h = sf + tg$.*

También se puede deducir, como en el caso de los enteros, la propiedad siguiente que relaciona el máximo común divisor con los divisores comunes mediante divisibilidad.

Corolario 5.3.9. (Mcd y divisores comunes.)

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g es el (único) polinomio mónico $h \in K[X]$ que satisface simultáneamente las dos condiciones siguientes :

- $h \mid f$ *y* $h \mid g$,
- *Si* $\tilde{h} \in K[X]$ *satisface que* $\tilde{h} \mid f$ *y* $\tilde{h} \mid g$, *entonces* $\tilde{h} \mid h$.

Definición 5.3.10. (Polinomios coprimos)

Sean $f, g \in K[X]$ no ambos nulos. Se dice que son *coprimos* si satisfacen $(f : g) = 1$, es decir si ningún polinomio de grado ≥ 1 divide simultáneamente a f y a g , o equivalentemente si existen polinomios s, $t \in K[X]$ tales que $1 = sf + tg$.

Proposición 5.3.11. (Divisibilidad con coprimalidad.)

Sean f, g, $h \in K[X]$, entonces:

1. *Si g y h son* coprimos, *entonces* $g \mid f$ *y* $h \mid f \iff g\,h \mid f$
2. *Si g y h son* coprimos, *entonces* $g \mid h\,f \iff g \mid f$.

Demostración. $(g : h) = 1 \Longrightarrow \exists\, s, t \in K[X]$ tales que $1 = sg + th$. Luego $f = sgf + thf$.

1. $(\Leftarrow)$ vale siempre.

   $(\Rightarrow)$ Por la escritura arriba, f es divisible por $g\,h$ pues cada sumando lo es ($h \mid f$ en el primer sumando y $g \mid f$ en el segundo).

2. $(\Rightarrow)$ vale siempre.

   $(\Leftarrow)$ g divide a cada sumando, por lo tanto g divide a f .

□

5.4. El Teorema Fundamental de la Aritmética para Polinomios.

Observación 5.4.1. (Primalidad de los polinomios irreducibles.)

Sean f un polinomio *irreducible* en $K[X]$. Entonces

- Para todo $g \in K[X]$, $(f : g) = \frac{f}{\mathrm{cp}(f)}$ si $f \mid g$ y $(f : g) = 1$ si $f \not\mid g$.
- Para todo $g, h \in K[X]$, $f \mid g\,h \Longrightarrow f \mid g$ o $f \mid h$.

Teorema 5.4.2. (Teorema Fundamental de la Aritmética para polinomios.)
Sea K un cuerpo, y sea $f \in K[X]$ un polinomio no constante. Entonces existen únicos polinomios irreducibles mónicos distintos $g_1, \ldots, g_r$ *en* $K[X]$ *tales que*

$$f = c\, {g_1}^{m_1} \ldots {g_r}^{m_r} \quad \text{donde} \quad c \in K \setminus \{0\} \text{ y } m_1, \ldots, m_r \in \mathbb{N}$$

(La unicidad de los factores irreducibles g_i es salvo el orden de los factores.)
La constante c resulta ser el coeficiente principal de f.

<u>*Ejemplo:*</u> El polinomio $(X^2+1)(X^2-2)$ está factorizado en factores irreducibles en $\mathbb{Q}[X]$ (pues ambos factores son irreducibles) pero su factorización en $\mathbb{R}[X]$ es $(X^2+1)(X-\sqrt{2})(X+\sqrt{2})$ y su factorización en $\mathbb{C}[X]$ es $(X+i)(X-i)(X+\sqrt{2}i)(X-\sqrt{2}i)$. Notemos que en $\mathbb{Q}[X]$ el polinomio $(X^2+1)(X^2-2)$ es reducible, pues $X^2+1 \mid f$ en $\mathbb{Q}[X]$ pero sin embargo no tiene raíces en $\mathbb{Q}$. Pero de todos modos como veremos en lo que sigue la búsqueda de raíces de f ayuda para la factorización.

5.5. Evaluación y Raíces.

Sea $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$ un polinomio, entonces f define en forma natural una función

$$f : K \to K, \quad f(x) = a_n x^n + \cdots + a_1 x + a_0$$

que se llama la función *evaluación.*

Esta función evaluación cumple las dos propiedades siguientes para todo $f, g \in K[X]$:

$$\big(f+g\big)(x) = f(x) + g(x) \quad \text{y} \quad \big(f \cdot g\big)(x) = f(x) \cdot g(x), \quad \forall\, x \in K.$$

En particular, si $f = q\,g + r$ con $q, r \in K[X]$, entonces $f(x) = q(x)\,g(x) + r(x)$, $\forall\, x \in K$.

<u>*Ejemplos:*</u>

- Sea $f = X^2 + X - 2 \in \mathbb{Q}[X]$. Entonces $f(3) = 3^2 + 3 - 2 = 10$, $f(0) = -2$ y $f(1) = 1^2 + 1 - 2 = 0$.
- Sea $f = \sum_{i=0}^{n} a_i X_i \in K[X]$. Entonces $f(0) = a_0$ y $f(1) = \sum_{i=0}^{n} a_i$.
- Sea $f = c$ un polinomio constante en $K[X]$. Entonces $f(x) = c$, $\forall\, x \in K$.
- Determinar todos los polinomios $f \in \mathbb{R}[X]$ de grado ≤ 2 (o nulo) tales que $f(0) = 1$ y $f(1) = f(2)$:

  El polinomio f es de la forma $f = aX^2 + bX + c \in \mathbb{R}[X]$. Se tiene $f(0) = 1 \Leftrightarrow c = 1$ y $f(1) = f(2) \Leftrightarrow a + b + c = 4a + 2b + c$, es decir $3a + b = 0$. En definitiva, $b = -3a$ y $c = 1$, lo que implica que $f = aX^2 - 3aX + 1$, $a \in \mathbb{R}$.

- Sea $f \in \mathbb{Q}[X]$ tal que $f(0) = 1$ y $f(1) = f(2) = 3$. Calcular el resto de dividir f por $X(X-1)(X-2)$:

  El polinomio f se escribe por el Algoritmo de División como

  $$f = q \cdot X(X-1)(X-2) + r \quad \text{con} \quad r = 0 \quad \text{o} \quad \text{gr}(r) < 3, \quad \text{o sea} \quad r = aX^2 + bX + c \in \mathbb{Q}[X].$$

  Por lo tanto, dado que el polinomio $X(X-1)(X-2)$ se anula en 0, 1 y 2, si evaluamos en $x = 0$, $x = 1$ y $x = 2$ obtenemos $f(0) = r(0)$, $f(1) = r(1)$ y $f(2) = r(2)$. O sea $r(0) = 1$, $r(1) = r(2) = 3$. Por el inciso anterior, $r = aX^2 - 3aX + 1$, con $r(1) = a - 3a + 1 = 3$, es decir $-2a = 2$, o sea $a = -1$. Se concluye $r = -X^2 + 3X + 1$.

Definición 5.5.1. (Raíz de un polinomio.)

Sean $f \in K[X]$ un polinomio y $x \in K$. Si $f(x) = 0$, se dice que x es una *raíz* de f (en K).

Proposición 5.5.2. (Teorema del resto.)

Dados $f \in K[X]$ y $x \in K$, se tiene que $r_{X-x}(f) = f(x)$.

Demostración. Si dividimos al polinomio f por el polinomio $X - x \in K[X]$, obtenemos

$$f = q \cdot (X - x) + r \quad \text{con} \quad r = 0 \text{ o } \text{gr}(r) < gr(X - x) = 1, \quad \text{o sea } r = c \in K$$

es un polinomio constante. Evaluando la expresión en $x \in K$ se obtiene

$$f(x) = q(x)\,(x - x) + c = c$$

dado que evaluar el polinomio constante c en x da siempre c. □

Corolario 5.5.3. (Equivalencias de raíz.)

$$x \in K \text{ es raíz de } f \iff f(x) = 0 \iff X - x \mid f \iff f = (X - x)q \text{ para algún } q \in K[X].$$

Es decir, si $f \neq 0$, $X - x$ es un factor irreducible (mónico) en la descomposición en irreducibles de $f \in K[X]$.

Observación 5.5.4. Sean $f, g \in K[X]$ con $g \neq 0$ tal que $g \mid f$ en $K[X]$. Sea $x \in K$. Si x es raíz de g, entonces x es raíz de f también. (Pues $g \mid f$ implica existe $q \in K[X]$ tal que $f = q\,g$ y por lo tanto $f(x) = q(x)\,g(x) = q(x) \cdot 0 = 0$.)

<u>*Ejemplos:*</u>

- f constante: $f = c$ con $c \in K$.

  Entonces, o bien $c = 0$ y todo $x \in K$ es raíz de f, ó bien $c \neq 0$ y f no tiene ninguna raíz en K.

- f de grado 1: $f = aX + b$ con $a, b \in K$, $a \neq 0$. Como f tiene grado 1, es irreducible en $K[X]$. Se tiene que $x = -\frac{b}{a}$ es raíz de f y $f = a\big(X - (-\frac{b}{a})\big) = a(X - x)$ es la factorización del polinomio irreducible f en $K[X]$.

- f de grado 2: $f = aX^2 + bX + c$ con $a, b, c \in K$, $a \neq 0$.

  Como f tiene grado 2, es reducible si y solo si tiene un factor en $K[X]$ de grado 1, que podemos asumir mónico de la forma $X - x$ con $x \in K$. Así que en este caso f es reducible en $K[X]$ si y solo si f tiene una raíz $x \in K$.

  Asumimos en lo que sigue que $1 + 1 \neq 0$ en K, es decir $2 \neq 0 \in K$ (por ejemplo si $K \neq \mathbb{Z}/p\mathbb{Z}$ con p primo, entonces $p \neq 2$) para que tenga sentido dividir por 2 en la cuenta que hacemos a continuación.

  Luego

$$f = a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right) = a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) = a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right)$$

  Se define el *discriminante* de f como $\Delta = \Delta(f) := b^2 - 4ac \in K$.

  Si existe $\omega \in K$ tal que $\omega^2 = \Delta$, se tiene que :

$$f = a\left(\left(X + \frac{b}{2a}\right)^2 - \left(\frac{\omega}{2a}\right)^2\right) = a\left(X - \frac{-b + \omega}{2a}\right)\left(X - \frac{-b - \omega}{2a}\right)$$

  y por lo tanto, dado que K es un cuerpo, $f(x) = 0 \Leftrightarrow x - \frac{-b+\omega}{2a} = 0$ o $x - \frac{-b-\omega}{2a} = 0$. Es decir, se obtienen las 2 raíces (a lo mejor la misma repetida si $\omega = 0$):

$$x_{\pm} = \frac{-b \pm \omega}{2a}.$$

  Lo que probamos hasta ahora es que si $\Delta \in K$ es un cuadrado en K, entonces el polinomio cuadrático $f = aX^2 + bX + c$ tiene (al menos) una raíz en K. Podemos probar la recíproca también: que si f tiene una raíz en K, entonces Δ es un cuadrado en K:

  En efecto, si $f = aX^2 + bX + c$ tiene una raíz $x_1 \in K$, $X - x_1 \mid K$ y el cociente, que tiene grado 1, se puede escribir en la forma $a(X - x_2)$. Por lo tanto

$$f = a(X - x_1)(X - x_2) = aX^2 - a(x_1 + x_2)X + ax_1x_2.$$

  Igualando coeficiente a coeficiente, resulta que $b = -a(x_1 + x_2)$ y $c = ax_1x_2$. Por lo tanto,

$$\Delta = b^2 - 4ac = a^2(x_1 + x_2)^2 - 4a^2x_1x_2 = a^2(x_1^2 + x_2^2 - 2x_1x_2) = \big(a(x_1 - x_2)\big)^2 = \omega^2$$

  donde $\omega = a(x_1 - x_2) \in K$: Δ resulta ser un cuadrado en K!

Hemos probado el siguiente resultado:

Proposición 5.5.5. (Polinomios cuadráticos en $K[X]$.)

Sea K un cuerpo y sea $f = aX^2 + bX + c \in K[X]$, con $a \neq 0$, un polinomio cuadrático. Entonces f es reducible en $K[X]$ si y solo si f tiene una raíz en K.

Si $2 \neq 0$ en K, f es reducible en $K[X]$ (o equivalentemente tiene raíz en K) si y solo si $\Delta = b^2 - 4ac$ es un cuadrado en K. En ese caso, sea $\omega \in K$ tal que $\omega^2 = \Delta$. Entonces las raíces de f en K son

$$x_\pm = \frac{-b \pm \omega}{2a}$$

(donde si $\Delta = 0$, $x_+ = x_-$), y $f = a(X - x_+)(X - x_-)$ es la factorización de f en $K[X]$.

<u>*Ejemplos:*</u> Sea $f = aX^2 + bX + c \in K[X]$, con $a \neq 0$, un polinomio cuadrático.

- Cuando $K = \mathbb{C}$, vimos en la Proposición 5.1.5 que siempre existe $\omega \in \mathbb{C}$ tal que $\omega^2 = \Delta \in \mathbb{C}$ (pues todo número complejo tiene raíz cuadrada), luego todo polinomio de grado 2 es reducible en $\mathbb{C}[X]$, o equivalentemente tiene dos raíces en $\mathbb{C}$ (que pueden ser distintas o la misma repetida dos veces cuando $\Delta = 0$).

  Por ejemplo si $f = X^2 - iX + (-1 + i)$, entonces $\Delta = 3 - 4i = \omega^2$ con $\omega = 2 - i$. Se obtiene
  $$x_+ = \frac{i + (2 - i)}{2} = 1 \quad \text{y} \quad x_- = \frac{i - (2 - i)}{2} = -1 + i.$$
  La factorización de f en $\mathbb{C}[X]$ es $f = (X - x_+)(X - x_-) = (X - 1)(X - (-1 + i))$.

- Cuando $K = \mathbb{R}$, existe $\omega \in \mathbb{R}$ tal que $\omega^2 = \sqrt{\Delta}$ si y sólo si $\Delta \geq 0$. Por lo tanto, f es reducible en $\mathbb{R}[X]$ si y solo si $\Delta \geq 0$. Existen luego polinomios de grado 2 irreducibles en $\mathbb{R}[X]$ (o equivalentemente en este caso sin raíces reales), como por ejemplo los polinomios de la forma $X^2 + c$ con $c > 0$.

- Cuando $K = \mathbb{Q}$, f es reducible en $\mathbb{Q}[X]$ (o tiene raíz en $\mathbb{Q}$) si y solo si Δ es un cuadrado en $\mathbb{Q}$. Existen luego polinomios de grado 2 irreducibles en $\mathbb{Q}[X]$ (o equivalentemente en este caso sin raíces racionales), como por ejemplo los polinomios de la forma $X^2 + c$ con $c > 0$, o también $X^2 - 2$.

- Cuando $K = \mathbb{Z}/p\mathbb{Z}$ con p primo $\neq 2$, f puede ser reducible o no según si Δ es un cuadrado o no en $\mathbb{Z}/p\mathbb{Z}$. Por ejemplo el polinomio $f = X^2 + \overline{2}X + \overline{5}$ es irreducible en $\mathbb{Z}/7\mathbb{Z}$ pues $\Delta = \overline{2}^2 - 4 \cdot \overline{5} = \overline{4 - 20} = \overline{-16} = \overline{5}$ no es un cuadrado en $\mathbb{Z}/7\mathbb{Z}$, mientras que el polinomio $X^2 + X + \overline{1}$ es reducible pues $\Delta = \overline{1}^2 - 4 \cdot \overline{1} = \overline{-3} = \overline{4} = \overline{2}^2$ es un cuadrado en $\mathbb{Z}/7\mathbb{Z}$ (aquí $\omega = \overline{2}$): se tiene
  $$x_+ = \frac{-\overline{1} + \overline{2}}{2} = \frac{\overline{1}}{2} = \overline{4} \quad \text{y} \quad x_- = \frac{-\overline{1} - \overline{2}}{2} = \frac{\overline{-3}}{2} = \frac{\overline{4}}{2} = \overline{2},$$
  y por lo tanto $f = (X - x_+)(X - x_-) = (X - \overline{4})(X - \overline{2})$ es la factorización de f en $\mathbb{Z}/7\mathbb{Z}$.

- Cuando $K = \mathbb{Z}/2\mathbb{Z}$, hay pocos polinomios de grado 2, que son $f_1 = X^2$, $f_2 = X^2 + \overline{1}$, $f_3 = X^2 + X$ y $f_4 = X^2 + X + \overline{1}$. Se puede ver que los tres primeros son reducibles (por ejemplo $f_2 = (X - \overline{1})^2$) mientras que el último no lo es, pues ni $\overline{0}$ ni $\overline{1}$ son raíces de f_4. (Sin embargo $\Delta = \overline{1} - 4 \cdot \overline{1} = \overline{1}$ es un cuadrado en $\mathbb{Z}/2\mathbb{Z}$.)

Proposición 5.5.6. (Raíz común y Mcd.)

Sean $f, g \in K[X]$ *no ambos nulos y sea* $x \in K$ *. Entonces*

$$f(x) = 0 \;\; y \;\; g(x) = 0 \iff (f : g)(x) = 0.$$

Demostración.

- ($\Rightarrow$) Se sabe que existen $s, t \in K[X]$ tales que $(f : g) = s\,f + t\,g$. Por lo tanto $(f : g)(x) = s(x)f(x) + t(x)g(x) = 0$ si $f(x) = g(x) = 0$.
- ($\Leftarrow$) Como $(f : g) \mid f$ y $(f : g) \mid g$ en $K[X]$, si $(f : g)(x) = 0$, entonces $f(x) = 0$ y $g(x) = 0$.

□

5.5.1. Multiplicidad de las raíces.

Vimos en los ejemplos anteriores que a veces una raíz puede aparecer "repetida". Por ejemplo si consideramos el polinomio

$$f = 10(X-1)^2(X+1)(X-2)^3$$

tenemos que la raíz 1 "aparece" dos veces, la raíz -1 una sola, y la raíz 2 tres veces. Esto sugiere la noción de multiplicidad de una raíz de un polinomio.

Definición 5.5.7. (Multiplicidad de una raíz).

Sea $f \in K[X]$ *no nulo.*

- Sea $m \in \mathbb{N}_0$. Se dice que $x \in K$ es una *raíz de multiplicidad* m *de* f si $(X-x)^m \mid f$ y $(X-x)^{m+1} \nmid f$, o lo que equivalente, existe $q \in K[X]$ tal que

  $$f = (X-x)^m\, q \;\; \text{con} \;\; q(x) \neq 0.$$

  Notamos aquí $\operatorname{mult}(x; f) = m$.
- Se dice que $x \in K$ es una *raíz simple de* f cuando $\operatorname{mult}(x; f) = 1$, es decir $X - x \mid f$ pero $(X-x)^2 \nmid f$, o lo que es equivalente $f = (X-x)\,q$ con $q(x) \neq 0$.
- Se dice que $x \in K$ es una *raíz múltiple de* f cuando $\operatorname{mult}(x; f) > 1$, es decir $(X-x)^2 \mid f$.
- Se dice que $x \in K$ es una *raíz doble de* f cuando $\operatorname{mult}(x; f) = 2$ y que es una *raíz triple de* f cuando $\operatorname{mult}(x; f) = 3$.

Está claro de la definición que dado un polinomio $f \in K[X]$ *no nulo* y $x \in K$ una raíz de f, su multiplicidad m siempre está acotada por el grado del polinomio: $\operatorname{mult}(x; f) \leq \operatorname{gr}(f)$.

<u>*Ejemplos:*</u>

- En el ejemplo $f = 10(X-1)^2(X+1)(X-2)^3$, 1 es raíz doble de f, -1 es simple y 3 es triple.

- $\mathrm{mult}(x; f) = 0$ si y solo si x no es raíz de f.

Se recuerda que si $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$ entonces

$$f' = n\, a_n X^{n-1} + (n-1)\, a_{n-1} X^{n-2} + \cdots + a_1 \in K[X]$$

es la *derivada* de f, que satisface:

- $(f+g)' = f' + g'$ y $(fg)' = f'g + fg'$, $\forall\, f, g \in K[X]$.
- $(g \circ f)' = g'(f) f'$, $\forall\, f, g \in K[X]$. En particular $\big((X-x)^k\big)' = k(X-x)^{k-1}$.
- $f'' = (f')'$ y en general $f^{(m)} = (f')^{(m-1)}$, $\forall\, m \in \mathbb{N}$.

Observemos que si x es raíz múltiple de f, es decir $f = (X-x)^2 q$ para algún $q \in K[X]$, entonces $f' = 2(X-x)q + (X-x)^2 q' = (X-x)\big(2\,q + (X-x)\,q'\big)$. Por lo tanto $f'(x) = 0$ también. O sea no sólo vale que $f(x) = 0$ pero también $f'(x) = 0$. Esto es la base de la siguiente proposición que relaciona la multiplicidad con las derivadas de f.

Proposición 5.5.8. (Raíz múltiple y derivada.)
Sea $f \in K[X]$ y sea $x \in K$. Entonces

- *x es raíz múltiple de f si y solo si $f(x) = 0$ y $f'(x) = 0$.*
- *x es raíz simple de f si y solo si $f(x) = 0$ y $f'(x) \neq 0$.*

Demostración. Alcanza con probar el primer inciso, ya que el segundo es decir que x es raíz de f pero no múltiple.

Sabemos que $x \in K$ es raíz de f si y solo si $f = (X-x)\,q$ para algún $q \in K[X]$. Derivando, $f' = q + (X-x)q'$ satisface $f'(x) = q(x)$. En particular $f'(x) = 0 \Leftrightarrow q(x) = 0$.

Por lo tanto,

$$f(x) = 0 \text{ y } f'(x) = 0 \implies (X-x)^2 \mid f.$$

La recíproca fue observada antes de enunciar la proposición: si $(X-x)^2 \mid f$, entonces $f(x) = f'(x) = 0$. □

<u>*Ejemplos:*</u>

- Probar que el polinomio $2X^{15} + 7X^7 + 2X^3 + 1$ no tiene raíces múltiples reales.

  Supongamos que sí: Sea $x \in \mathbb{R}$ tal que $f(x) = f'(x) = 0$. En particular, dado que $f' = 30X^{14} + 49X^6 + 6X^2$, se tendría $0 = f'(x) = 30x^{14} + 49x^6 + 6x^2$. Lo que implica que $x = 0$ dado que todos los exponentes en f' son pares (luego $\forall\, x \in \mathbb{R}$, $f'(x) \geq 0$ y $f'(x) = 0 \Leftrightarrow x = 0$.) Pero claramente $f(0) = 1 \neq 0$.

- Hallar para qué valores de $a \in \mathbb{C}$ el polinomio $f = X^8 - 2X^4 + a$ tiene raíces múltiples en $\mathbb{C}$.

  Sea $x \in \mathbb{C}$ una raíz múltiple. Equivalentemente, $f(x) = f'(x) = 0$. Es decir, dado que $f' = 8X^7 - 8X^3$, $8x^7 - 8x^3 = 8x^3(x^4 - 1) = 0$. O sea $x = 0$ o $x^4 = 1$.

  - $f(0) = 0 \Leftrightarrow a = 0$: en ese caso $f = X^8 - 2X^4 = X^4(X^4 - 2)$, o sea f tiene la raíz 0 con multiplicidad 4.
  - Si $x^4 = 1$, entonces
  $$f(x) = x^8 - 2x^4 + a = (x^4)^2 - 2x^4 + a = 1 - 2 \cdot 1 + a = -1 + a$$
  implica que $f(x) = 0 \Leftrightarrow a = 1$. Por lo tanto $f = X^8 - 2X^4 + 1 = (X^4 - 1)^2$ tiene claramente la raíz 1 que es múltiple.

Se puede ser más explícito cuando se trabaja sobre $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ (pero atención, el argumento no es válido para los cuerpos finitos $\mathbb{Z}/p\mathbb{Z}$).

Proposición 5.5.9. (Multiplicidad en f y multiplicidad en f'.)

Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \in \mathbb{N}$. Entonces

$$\operatorname{mult}(x; f) = m \quad \Longleftrightarrow \quad f(x) = 0 \ \text{ y } \ \operatorname{mult}(x; f') = m - 1.$$

Demostración.

($\Rightarrow$)

$$\begin{aligned}
\operatorname{mult}(x; f) = m \ &\Longleftrightarrow \ \exists\, q \in K[X] \ \text{ tal que } \ f = (X - x)^m\, q \text{ con } q(x) \neq 0 \\
&\Longrightarrow \ f' = m(X - x)^{m-1} q + (X - x)^m q' = (X - x)^{m-1}\big(m\, q + (X - x)\, q'\big) \\
&\Longrightarrow \ f' = (X - x)^{m-1} h \ \text{ donde } \ h = m\, q + (X - x)\, q' \in K[X] \\
&\qquad\qquad \text{es tal que } \ h(x) = m\, q(x) \neq 0 \ \text{ pues } \ q(x) \neq 0.
\end{aligned}$$

Por lo tanto, $f(x) = 0$ y $\operatorname{mult}(x; f') = m - 1$.

(Este argumento no es válido en un cuerpo finito $\mathbb{Z}/p\mathbb{Z}$ si $p \mid m$ pues en ese caso $h(x) = 0$.)

($\Leftarrow$) Queremos probar que si $f(x) = 0$ y $\operatorname{mult}(x; f') = m - 1$, entonces $\operatorname{mult}(x; f) = m$. Como $f(x) = 0$, x es raíz de f con cierta multiplicidad $k \geq 1$ (y queremos probar que en realidad $k = m$). Por lo tanto por la implicación que acabamos de probar, $\operatorname{mult}(x; f') = k - 1$. Pero por hipótesis, $\operatorname{mult}(x; f') = m - 1$, de lo cual se deduce $k - 1 = m - 1$ y por lo tanto $k = m$ como se quería probar. $\square$

Proposición 5.5.10. (Raíz de multiplicidad m y derivadas hasta orden m.)

Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \in \mathbb{N}$. Entonces

$$\operatorname{mult}(x; f) = m \quad \Longleftrightarrow \quad \begin{cases} f(x) & = & 0 \\ f'(x) & = & 0 \\ & \vdots & \\ f^{(m-1)}(x) & = & 0 \\ f^{(m)}(x) & = & 0. \end{cases}$$

Demostración. Por inducción en $m \in \mathbb{N}$:

$$p(m): \quad \text{Dado } g \in K[X],\ x \in K \text{ es t.q. } \operatorname{mult}(x;g) = m \iff \begin{cases} g(x) & = & 0 \\ g'(x) & = & 0 \\ & \vdots & \\ g^{(m-1)}(x) & = & 0 \\ g^{(m)}(x) & = & 0. \end{cases}$$

- Caso base, $m = 1$: $p(1)$ es V? Sí pues $\operatorname{mult}(x;g) = 1 \Leftrightarrow g(x) = 0$ y $g'(x) \neq 0$ por la Proposicíón 5.5.8.

- Paso inductivo, $p(k)$ V $\to$ $p(k+1)$ V:

  Por la Proposición 5.5.9, $\operatorname{mult}(x,f) = k+1 \Leftrightarrow f(x) = 0$ y $\operatorname{mult}(x,f') = k$.

  Por HI, para $g = f'$ se tiene que

  $$f'(x) = 0, (f')'(x) = 0, \ldots, (f')^{(k-1)}(x) = 0 \text{ y } (f')^{(k)}(x) \neq 0,$$

  es decir

  $$f'(x) = 0, f''(x) = 0, \ldots, f^{(k)}(x) = 0 \text{ y } f^{(k+1)}(x) \neq 0.$$

  Así concluimos

  $$\operatorname{mult}(x,f) = k+1 \Leftrightarrow f(x) = 0, f'(x) = 0, \ldots, f^{(k)}(x) = 0 \text{ y } f^{(k+1)}(x) \neq 0.$$

  Hemos probado el paso inductivo.

Por lo tanto $p(m)$ es Verdadera para todo $m \in \mathbb{N}$. □

5.5.2. Cantidad de raíces en K.

Así como vimos en los ejemplos que –dado K un cuerpo– un polinomio $f \in K[X]$ no nulo de grado 0 no tiene raíces en K, de grado 1 siempre tiene una raíz en K y de grado 2 tiene a lo sumo dos raíces en K, vamos a ver que un polinomio $f \in K[X]$ no nulo no puede tener más raíces en el cuerpo K, aún contadas con su multiplicidad, que su grado.

Proposición 5.5.11. (Raíces de f y factores.)

Sea $f \in K[X]$ no nulo.

- *Sean $x_1, x_2 \in K$ raíces* distintas *de f tales que* $\operatorname{mult}(x_1;f) = m_1$ *y* $\operatorname{mult}(x_2;f) = m_2$. *Entonces* $(X - x_1)^{m_1}(X - x_2)^{m_2} \mid f$.

- *Sean* $x_1, \ldots, x_r \in K$ *raíces* distintas *de* f *tales que*

$$\mathrm{mult}(x_1; f) = m_1, \ldots, \mathrm{mult}(x_r; f) = m_r.$$

Entonces

$$(X - x_1)^{m_1} \cdots (X - x_r)^{m_r} \mid f.$$

Demostración.

- Esto es porque $(X - x_1)^{m_1}$ y $(X - x_2)^{m_2}$ son polinomios coprimos al ser potencias de polinomios irreducibles distintos. Luego,

$$(X - x_1)^{m_1} \mid f \ \text{ y } \ (X - x_2)^{m_2} \mid f \implies (X - x_1)^{m_1}(X - x_2)^{m_2} \mid f.$$

- Por inducción en la cantidad de raíces distintas.

□

En esas condiciones se tiene que si $f \neq 0$, $\mathrm{gr}\big((X - x_1)^{m_1} \cdots (X - x_r)^{m_r}\big) \leq \mathrm{gr}(f)$, es decir $m_1 + \cdots + m_r \leq \mathrm{gr}(f)$. Se obtuvo:

Proposición 5.5.12. (Cantidad de raíces en K.)

Sea K un cuerpo y sea $f \in K[X]$ un polinomio no nulo de grado n. Entonces f tiene a lo sumo n raíces en K contadas con multiplicidad.

5.6. Polinomios en $\mathbb{C}[X]$.

5.6.1. El Teorema Fundamental del Álgebra.

Vimos hasta ahora, en el ejemplo a continuación de la Proposición 5.5.5, que todo polinomio cuadrático $f = aX^2 + bX + c \in \mathbb{C}[X]$, con $a \neq 0$, tiene exactamente 2 raíces en $\mathbb{C}$ (contadas con multiplicidad), que son

$$z_\pm = \frac{-b \pm \omega}{2a} \quad \text{donde } \omega \in \mathbb{C} \text{ es tal que } \omega^2 = b^2 - 4ac,$$

y por lo tanto el polinomio f se factoriza en $\mathbb{C}[X]$ en la forma

$$f = (X - z_+)(X - z_-).$$

También podemos deducir inmediatamente del Teorema 5.1.9 que todo polinomio de la forma $X^n - z$ en $\mathbb{C}[X]$ tiene exactamente n raíces en $\mathbb{C}$ (contadas con multiplicidad):

- Si $z = 0$, el polinomio es X^n que tiene la raíz 0 con multiplicidad n.
- Si $z \neq 0$, determinar las raíces de $X^n - z$ equivale a hallar los $\omega \in \mathbb{C}$ tales que $\omega^n - z = 0$, es decir hallar los $\omega \in \mathbb{C}$ tales que $\omega^n = z$, o sea determinar las raíces n-ésimas de z. Y sabemos por el Teorema 5.1.9 que $z \neq 0$ tiene n raíces n-ésimas distintas en $\mathbb{C}$, que

son $\omega_0, \omega_1, \ldots, \omega_{n-1}$ descritas en el enunciado de ese teorema. Por lo tanto estas n raíces son simples (ya que el polinomio tiene a lo sumo n raíces contadas con multiplicidad), y el polinomio $X^n - z$ se factoriza en $\mathbb{C}[X]$ en la forma

$$X^n - z = (X - \omega_0) \cdots (X - \omega_{n-1}).$$

De hecho vale un resultado general al respecto, conocido como el Teorema Fundamental del Álgebra: todo polinomio no constante en $\mathbb{C}[X]$ tiene (al menos) una raíz en $\mathbb{C}$, o, lo que es equivalente aplicando divisiones sucesivas, todo polinomio de grado $n \geq 1$ en $\mathbb{C}[X]$ tiene exactamente n raíces contadas con multiplicidad! (Se dice que $\mathbb{C}$ es *algebraicamente cerrado.*)

Teorema 5.6.1. (Teorema Fundamental del Álgebra.)

Sea $f \in \mathbb{C}[X]$ un polinomio no constante. Entonces existe $z \in \mathbb{C}$ tal que $f(z) = 0$.

Equivalentemente, todo polinomio no constante en $\mathbb{C}[X]$ de grado n tiene exactamente n raíces contadas con multiplicidad en $\mathbb{C}$.

El Teorema Fundamental del Álgebra es equivalente a que los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1, de lo cual se deduce la factorización de polinomios en $\mathbb{C}[X]$.

Teorema 5.6.2. (Irreducibles y factorización en $\mathbb{C}[X]$.)

- *Sea $f \in \mathbb{C}[X]$. Entonces f es irreducible en $\mathbb{C}[X]$ si y solo si $\mathrm{gr}(f) = 1$, es decir $f = aX + b \in \mathbb{C}[X]$ con $a \neq 0$.*
- *Sea $f \in \mathbb{C}[X] - \mathbb{C}$. Entonces la factorización en irreducibles de f en $\mathbb{C}[X]$ es de la forma*

  $$f = c\,(X - z_1)^{m_1} \cdots (X - z_r)^{m_r}$$

  donde $z_1, \ldots, z_r \in \mathbb{C}$ son distintos, $m_1, \ldots, m_r \in \mathbb{N}$ y $c \in \mathbb{C}^\times$.

El Teorema Fundamental del Álgebra, que enunciamos en este curso sin demostración (se ven varias demostraciones en nuestra licenciatura en Matemática, pero hacen falta más herramientas que las que disponemos a este nivel) fue enunciado y demostrado en varias etapas a lo largo del tiempo, empezando con el matemático francés Albert Girard quién lo enunció en alguna forma en 1629. Una primera demostración, incompleta, fue esbozada por Jean le Rond D'Alembert en 1746. Aparecieron luego muchas demostraciones entre 1749 y 1795, pero con "agujeros" (argumentos no claros, que necesitan una demostración en sí mismo) ya que todas asumían que las raíces existen en "algún lado". Gauss también presentó una demostración con un agujero en 1799. En 1814, el librero y matemático amateur de origen suizo Jean-Robert Argand publicó la primer demostración completa, y luego Gauss presentó otra en 1816. Existen hoy en día numerosas demostraciones distintas de este teorema, aunque todas ellas usan algún ingrediente indispensable de la rama de la matemática que se suele llamar *Análisis*, la completitud de los números reales en una u otra forma (como por ejemplo el Teorema de Bolzano, que establece que toda función continua en $\mathbb{R}$ que toma un valor positivo y un valor negativo obligatoriamente toma el valor 0).

<u>*Ejemplos:*</u> (para información nomás)

- f de grado 3: (Scipione del Ferro 1515?, Tartaglia 1535, Cardano 1545.)

$$f = aX^3 + bX^2 + cX + d \ \in \mathbb{C}[X], \quad a \neq 0.$$

Haciendo el cambio de variables $Y = X - \dfrac{b}{3a}$, el problema se traduce en buscar las raíces del polinomio :

$$g = Y^3 + pY + q.$$

Buscando las soluciones de la forma $y = u + v$, con $u^3 + v^3 = -q$ y $u^3v^3 = -\dfrac{p^3}{27}$, se observa que u^3 y v^3 son las raíces del polinomio (*resolvente*):

$$Z^2 + qZ - \frac{p^3}{27}.$$

Por lo tanto hay 3 posibilidades para u y 3 posibilidades para v, o sea 6 posibilidades para $y = u + v$: las 3 raíces y del polinomio son 3 de entre esas 6 posibilidades, las 3 que son dadas por las elecciones de u y v que satisfacen $u\,v = -p/3$.

Pero puede ocurrir que calcular las raíces de un polinomio de esa forma puede dar una expresión muy engorrosa para algo mucho más sencillo! Por ejemplo la raíz $x = 1$ del polinomio $X^3 + X - 2$ aparece expresada en la forma

$$1 = \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{5}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{5}}}.$$

- f de grado 4: (Ludovico Ferrari, 1540?)

$$f = X^4 + pX^2 + qX + r.$$

Las 4 raíces son del tipo $\alpha = \frac{1}{2}(\pm u \pm v \pm \omega)$, donde $-u^2$, $-v^2$, $-\omega^2$ son las tres raíces del polinomio *resolvente*:

$$Z^3 - 2pZ^2 + (p^2 - 4r)Z + q^2.$$

La condición aquí para determinar las 4 raíces complejas entre las 8 posibles expresiones es $(\pm u)(\pm v)(\pm \omega) = -q$.

Hasta ahora se obtuvieron las raíces complejas de polinomios $f \in \mathbb{C}[X]$ de grado ≤ 4, por medio de fórmulas que se obtienen a partir de los coeficientes del polinomio f mediante las operaciones $+$, $-$, $\cdot$, $/$ y extracción de raíces cuadradas y cúbicas.

La pregunta natural es entonces : ¿Existirá para cada polinomio f de grado arbitrario una fórmula para las raíces que involucre los coeficientes de f y las operaciones $+$, $-$, $\cdot$, $/$ y extracción de raíces n-ésimas para algunos n adecuados?

Durante más de 200 años, muchos matemáticos buscaron esas fórmulas. Pero a principios del S. XIX el joven matemático noruego Niels Abel, 1802-1829, probó que sorprendentemente la respuesta es NO:

Teorema 5.6.3. (Abel, 1824?)

No existe ninguna fórmula que describa las raíces (complejas) de un polinomio general cualquiera $f \in \mathbb{C}[X]$ de grado ≥ 5 a partir de sus coeficientes y de las operaciones elementales $+$, $-$, $\cdot$, $/$ y extracciones de raíces n-ésimas.

El aún más joven matemático francés Evariste Galois, 1811-1832, caracterizó en 1832, según cuenta la historia la noche antes de morir a duelo, cuáles son los polinomios de grado ≥ 5 para los cuales existe tal fórmula (aunque no es facilmente deducible de los coeficientes del polinomio, sino que tiene que ver con cierto grupo asociado a él).

Esto es parte de la hoy llamada Teoría de Galois, que además de su importancia en matemática, constituye también la base matemática del funcionamiento de sistemas de navegación satelital como el GPS por ejemplo). Sus resultados fueron entendidos recién en 1846 por el matemático francés Joseph Liouville, 1809-1882.

Tanto Abel como Galois fueron los iniciadores de la Teoría de Grupos.

5.7. Polinomios en $\mathbb{R}[X]$.

Sabemos que un polinomio en $\mathbb{R}[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces contadas con multiplicidad. También sabemos que si $f \in \mathbb{R}[X]$ tiene grado ≥ 2 y tiene una raíz $x \in \mathbb{R}$, entonces f es reducible en $\mathbb{R}[X]$ pues $X - x \mid f$ ($X - x$ es un factor no trivial de f en $\mathbb{R}[X]$). Pero ser reducible en $\mathbb{R}[X]$ no implica tener raíz en $\mathbb{R}$: existen polinomios reducibles en $\mathbb{R}[X]$ de cualquier grado (par) que no tienen raíces reales, como por ejemplo el polinomio $(X^2+1)^n$, $\forall\, n \in \mathbb{N}$. Sin embargo no existen polinomios irreducibles en $\mathbb{R}[X]$ de cualquier grado. Es lo que estudiaremos a continuación, gracias al estudio ya realizado de los polinomios en $\mathbb{C}[X]$.

Primeramente volvamos a mencionar la consecuencia siguiente del famoso Teorema de Bolzano, probado en 1817 por el matemático bohemio Bernard Bolzano, 1781-1848.

Proposición 5.7.1. (Polinomios reales de grado impar.)

Sea $f \in \mathbb{R}[X]$ de grado impar. *Entonces f tiene al menos una raíz en $\mathbb{R}$.*

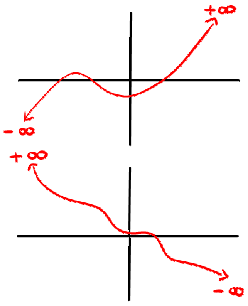
Demostración. Sea $f = a^n X^n + \cdots + a_0 \in \mathbb{R}[X]$, con n impar.

Si $a_n > 0$, entonces :

$$\lim_{x\to+\infty} f(x) = +\infty \quad \text{y} \quad \lim_{x\to-\infty} f(x) = -\infty :$$

Y si $a_n < 0$ se tiene :

$$\lim_{x\to+\infty} f(x) = -\infty \quad \text{y} \quad \lim_{x\to-\infty} f(x) = +\infty :$$



En ambos casos los signos son opuestos, y por lo tanto, por el Teorema de Bolzano (y dado que $f : \mathbb{R} \to \mathbb{R}$ define una función continua), debe existir $x \in \mathbb{R}$ tal que $f(x) = 0$. □

Pero se puede ser más explícito y precisar un poco más cuántas raíces reales puede tener f.

Proposición 5.7.2. (Raíces complejas conjugadas de polinomios reales.)
Sea $f \in \mathbb{R}[X]$, y sea $z \in \mathbb{C} \setminus \mathbb{R}$ un número complejo no real. Entonces

1. $f(z) = 0 \iff f(\overline{z}) = 0$.
2. *Para todo* $m \in \mathbb{N}$, $\operatorname{mult}(z; f) = m \iff \operatorname{mult}(\overline{z}; f) = m$.
3. $(X - z)(X - \overline{z})$ *es un polinomio irreducible de* $\mathbb{R}[X]$.
4. $f(z) = 0 \implies (X - z)(X - \overline{z}) \mid f$ *en* $\mathbb{R}[X]$.
5. $\operatorname{mult}(z; f) = m \implies \big((X - z)(X - \overline{z})\big)^m \mid f$ *en* $\mathbb{R}[X]$.

Demostración. 1. Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{R}[X]$. Entonces

$$\begin{aligned} f(z) = 0 &\iff a_n z^n + \cdots + a_1 z + a_0 = 0 \\ &\iff \overline{a_n z^n + \cdots + a_1 z + a_0} = 0 \\ &\iff \overline{a_n}\,\overline{z}^n + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0} = 0 \\ &\iff a_n \overline{z}^n + \cdots + a_1 \overline{z} + a_0 = 0 \quad \text{pues } a_0, \ldots, a_n \in \mathbb{R} \\ &\iff f(\overline{z}) = 0 \end{aligned}$$

2. Por la Proposición 5.5.10,

$$\operatorname{mult}(z; f) = m \iff f(z) = f'(z) = \cdots = f^{(m-1)}(z) = 0 \ \text{ y } \ f^{(m)}(z) \neq 0.$$

Pero $f', \ldots, f^{(m-1)}$, $f^{(m)}$ también son polinomios en $\mathbb{R}[X]$. Por lo tanto, por (1):

$$\begin{aligned} f(z) = \cdots = f^{(m-1)}(z) = 0, f^{(m)}(z) \neq 0 &\iff f(\overline{z}) = \cdots = f^{(m-1)}(\overline{z}) = 0, f^{(m)}(\overline{z}) \neq 0 \\ &\iff \operatorname{mult}(\overline{z}; f) = m. \end{aligned}$$

3. $(X-z)(X-\overline{z}) = X^2 - 2\,\Re e(z) + |z|^2 \in \mathbb{R}[X]$ pues sus coeficientes pertenecen a $\mathbb{R}$, y es irreducible por ser de grado 2 y no tener raíces reales.

4. $f(z) = 0 \Rightarrow f(\overline{z}) = 0$, por lo tanto $X - z \mid f$ y $X - \overline{z} \mid f$ en $\mathbb{C}[X]$. Luego, como son polinomios coprimos, su producto $(X-z)(X-\overline{z}) \mid f$ en $\mathbb{C}[X]$. Pero al ser $f \in \mathbb{R}[X]$ y $(X-z)(X-\overline{z}) \in \mathbb{R}[X]$, se concluye que $(X-z)(X-\overline{z}) \mid f$ en $\mathbb{R}[X]$.

5. Por inducción en $m \geq 1$. El caso base es el inciso anterior. Sea entonces $m > 1$ y sea $z \in \mathbb{C} - \mathbb{R}$ raíz de f de multiplicidad m. Entonces $(X-z)(X-\overline{z}) \mid f \in \mathbb{R}[X]$ y consideremos el cociente $q := \dfrac{f}{(X-z)(X-\overline{z})} \in \mathbb{R}[X]$. Se tiene que $\operatorname{mult}(z;q) = m-1$ y por lo tanto, por hipótesis inductiva, $\big((X-z)(X-\overline{z})\big)^{m-1} \mid q$ en $\mathbb{R}[X]$. Es decir, $\big((X-z)(X-\overline{z})\big)^{m} \mid f$ en $\mathbb{R}[X]$.

$\square$

La proposición anterior significa que las raíces complejas no reales de un polinomio real f vienen de a pares de complejos conjugados, o sea que un polinomio real f de grado n, que tiene exactamente n raíces complejas contadas con multiplicidad, tiene un número par de ellas que son complejas no reales, y el resto automáticamente tienen que ser (complejas) reales. Por ejemplo, un polinomio real de grado impar tiene un número impar de raíces reales. Más aún, existen algoritmos que calculan la cantidad exacta de raíces reales que tiene un polinomio en $\mathbb{R}[X]$ (como por ejemplo el Algoritmo de Sturm), pero no los vamos a ver aquí. Además permite caracterizar los polinomios irreducibles de $\mathbb{R}[X]$ y como es la factorización de polinomios en $\mathbb{R}[X]$.

Proposición 5.7.3. (Polinomios irreducibles en $\mathbb{R}[X]$.)

Los polinomios irreducibles en $\mathbb{R}[X]$ son exactamente los siguientes:

- *Los de grado 1, o sea de la forma $aX + b \in \mathbb{R}[X]$ con $a \neq 0$.*
- *Los de grado 2 con discriminante negativo, o sea de la forma*

$$aX^2 + bX + c \in \mathbb{R}[X] \quad \textit{con} \quad a \neq 0 \quad \textit{y} \quad \Delta := b^2 - 4ac < 0.$$

Demostración. Claramente los polinomios de grado 1 y los de grado 2 con discriminante negativo son irreducibles. Probemos que son los únicos.

- Si f tiene grado impar > 1, entonces tiene por lo menos una raíz real y por lo tanto es reducible.
- Si f es de grado 2, sabemos que es reducible si y solo si tiene discriminante ≥ 0.
- Si f tiene grado par ≥ 4, o bien tiene alguna raíz real, y en tal caso es reducible, o bien todas sus raíces son complejas no reales y vienen de a pares conjugados. Por lo tanto si z es una de esas raíces, el polinomio real $(X-z)(X-\overline{z})$ divide a f en $\mathbb{R}[X]$, y f resulta ser reducible.

$\square$

Teorema 5.7.4. (Factorización en $\mathbb{R}[X]$.)

Sea $f \in \mathbb{R}[X] - \mathbb{R}$. Entonces la factorización en irreducibles de f en $\mathbb{R}[X]$ es de la forma

$$f = c\,(X - x_1)^{m_1} \dots (X - x_r)^{m_r} (X^2 + b_1 X + c_1)^{n_1} \dots (X^2 + b_s X + c_s)^{n_s}$$

donde $c \in \mathbb{R}^\times$, $r, s \in \mathbb{N}_0$, $m_i, n_j \in \mathbb{N}$ para $1 \leq i \leq r, 1 \leq j \leq s$, $x_1, \dots, x_r \in \mathbb{R}$, $b_1, c_1, \dots, b_s, c_s \in \mathbb{R}$ y $\Delta_j := {b_j}^2 - 4c_j < 0$.

<u>*Ejemplo:*</u> Factorizar en $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio $f = X^4 - 2X^3 + X^2 - 4X - 2$ sabiendo que $\sqrt{2}\,i$ es raíz de f:

Como $f \in \mathbb{R}[X]$, por la Proposición 5.7.2, se tiene que $f(\sqrt{2}\,i) = 0 \Leftrightarrow f(-\sqrt{2}\,i) = 0$. Por lo tanto $(X - \sqrt{2}\,i)(X + \sqrt{2}\,i) = X^2 + 2 \mid f$. En efecto, $f = (X^2 + 2)(X^2 - 2X - 1)$. Las raíces de $X^2 - 2X - 1$ son reales: $1 + \sqrt{2}$ y $1 - \sqrt{2}$. Por lo tanto,

- $f = (X - \sqrt{2}\,i)(X + \sqrt{2}\,i)(X - (1 + \sqrt{2}))(X - (1 - \sqrt{2}))$ es la factorización de f en $\mathbb{C}[X]$
- $f = (X^2 + 2)(X - (1 + \sqrt{2}))(X - (1 - \sqrt{2}))$ es la factorización de f en $\mathbb{R}[X]$.

5.8. Polinomios en $\mathbb{Q}[X]$.

Sabemos que un polinomio en $\mathbb{Q}[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces contadas con multiplicidad. También sabemos que si $f \in \mathbb{Q}[X]$ tiene grado ≥ 2 y tiene una raíz $x \in \mathbb{Q}$, entonces f es reducible en $\mathbb{Q}[X]$ pues $X - x \mid f$ ($X - x$ es un factor no trivial de f en $\mathbb{Q}[X]$). Pero ser reducible en $\mathbb{Q}[X]$ no implica tener raíz en $\mathbb{Q}$: existen polinomios reducibles en $\mathbb{Q}[X]$ de cualquier grado que no tienen raíces racionales, como por ejemplo los polinomios $(X^2 - 2)^n$ y $(X^2 - 2)^n (X^3 - 2)$, $\forall\, n \in \mathbb{N}$.

Sin embargo la situación no es como en $\mathbb{R}[X]$ donde no existen polinomios irreducibles de cualquier grado: en $\mathbb{Q}[X]$ se puede probar que existen polinomios irreducibles de cualquier grado, como por ejemplo el polinomio $X^n - 2$, $\forall\, n \in \mathbb{N}$: no sólo el polinomio $X^n - 2$ no tiene raíces en $\mathbb{Q}$ para todo $n \geq 2$, pero más aún no tiene ningún factor en $\mathbb{Q}[X]$ de cualquier grado d, $1 \leq d \leq n - 1$. También se puede probar que para p primo, el polinomio $X^{p-1} + \dots + X + 1$ es irreducible en $\mathbb{Q}[X]$.

La situación parece desesperada. Pero al menos en $\mathbb{Q}$ existen algoritmos para encontrar (en forma exacta) todas las raíces racionales, y también para decidir si el polinomio es irreducible o no en $\mathbb{Q}[X]$, y en caso de ser reducible, determinar su factorización en irreducibles de $\mathbb{Q}[X]$.

5.8.1. Cálculo de raíces en $\mathbb{Q}$.

A pesar de que la situación en $\mathbb{Q}[X]$ parece mucho más complicada que en $\mathbb{C}[X]$, se puede encontrar todas las raíces racionales de un polinomio $f \in \mathbb{Q}[X]$ por medio de un algoritmo.

Este hecho es una consecuencia de que todo número entero $a \in \mathbb{Z} \setminus \{0\}$ tiene un número finito de divisores posibles, que se pueden calcular.

Sea $f = a_n X_n + \cdots + a_0 \in \mathbb{Q}[X]$. Entonces existe $c \in \mathbb{Z} \setminus \{0\}$ tal que $g = c\, f \in \mathbb{Z}[X]$, es decir g tiene todos sus coeficientes enteros (por ejemplo, eligiendo c como el mínimo común múltiplo de los denominadores de los coeficientes de f), y además las raíces de f claramente coinciden con las de g.

Por ejemplo, $f = \dfrac{3}{2}X^5 - \dfrac{1}{3}X^4 + X^2 - \dfrac{5}{4} \in \mathbb{Q}[X]$ y $g = 12\, f = 18X^5 - 4X^4 + 12X^2 - 15 \in \mathbb{Z}[X]$ tienen exactamente las mismas raíces.

Por consiguiente para encontrar las raíces racionales de un polinomio en $\mathbb{Q}[X]$, nos podemos restringir a estudiar cómo encontrar las raíces racionales de un polinomio en $\mathbb{Z}[X]$.

Lema 5.8.1. (Lema de Gauss.)

Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ *con* $a_n,\ a_0 \neq 0$. *Si* $\frac{\alpha}{\beta} \in \mathbb{Q}$ *es una raíz racional de* f, *con* α *y* β $\in \mathbb{Z}$ coprimos, *entonces* $\alpha \mid a_0$ *y* $\beta \mid a_n$.

Demostración.

$$\begin{aligned} f\left(\frac{\alpha}{\beta}\right) = 0 \quad &\Longleftrightarrow \quad a_n \left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \cdots + a_1\left(\frac{\alpha}{\beta}\right) + a_0 = 0 \\ &\Longleftrightarrow \quad \frac{a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n}{\beta^n} = 0 \\ &\Longleftrightarrow \quad a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0. \end{aligned}$$

Por lo tanto, $\alpha\left(a_n\alpha^{n-1} + \cdots + a_1\beta^{n-1}\right) = -a_0\beta^n$.

Esto implica $\alpha \mid -a_0\beta^n$ en $\mathbb{Z}$. Pero al ser α y β enteros coprimos, α es coprimo con β^n también, y por lo tanto $\alpha \mid a_0$.

De la misma manera, $\beta\left(a_{n-1}\alpha^{n-1} + \cdots + a_0\beta^{n-1}\right) = -a_n\alpha^n$ implica que $\beta \mid -a_n\alpha^n$ pero al ser coprimo con α, resulta $\beta \mid a_n$. □

Observación 5.8.2. (Algoritmo para calcular las raíces en $\mathbb{Q}$ de $f \in \mathbb{Z}[X]$.)

En las condiciones del teorema anterior, el Lema de Gauss implica que si se construye el conjunto (finito) $\mathcal{N}$ (por numerador) de los divisores positivos y negativos de a_0 y el conjunto $\mathcal{D}$ (por denominador) de los de a_n, las raíces del polinomio f se encuentran en el conjunto de todas las fracciones coprimas $\frac{\alpha}{\beta}$, eligiendo α en $\mathcal{N}$ y β en $\mathcal{D}$. Chequeando para cada fracción $\frac{\alpha}{\beta}$ así construída si $f(\frac{\alpha}{\beta}) = 0$, se obtienen todas las raíces racionales de f.

Simplemente hay que tener un poco de cuidado en que este procedimiento no aclara la multiplicidad de cada raíz.

<u>*Ejemplo:*</u> Hallar las raíces racionales del polinomio racional

$$f = X^8 + \frac{8}{3}X^7 + \frac{1}{3}X^6 - \frac{14}{3}X^5 - \frac{14}{3}X^4 - \frac{4}{3}X^3.$$

Limpiando los denominadores de f se obtiene el polinomio entero g con las mismas raíces:

$$g = 3X^8 + 8X^7 + X^6 - 14X^5 - 14X^4 - 4X^3 = X^3(3X^5 + 8X^4 + X^3 - 14X^2 - 14X - 4)$$

Claramente, $\mathrm{mult}(0; g) = 3$ (y por lo tanto $\mathrm{mult}(0; f) = 3$ también pues $g = 3\,f$), y las restantes raíces racionales de g (o f) son las de

$$h = 3X^5 + 8X^4 + X^3 - 14X^2 - 14X - 4.$$

Aquí, $a_0 = -4$ y $a_n = 3$.

Los divisores de a_0 son $\pm 1, \pm 2, \pm 4$ y los divisores de a_n son $\pm 1, \pm 3$, luego las raíces racionales se buscan en el conjunto :

$$\{\, \pm 1, \pm 2, \pm 4, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3} \,\}$$

Chequeando se obtiene que $h(-1) = 0$ y $h(-2/3) = 0$, y éstas son las únicas raíces racionales (distintas) de h.

Para conocer con qué multiplicidad son éstas raíces de h, se puede o bien dividir h por $(X + 1)(X + \frac{2}{3})$ y volver a evaluar el cociente en -1 y $-2/3$, o bien también se puede derivar h:

$h' = 15X^4 + 32X^3 + 3X^2 - 28X - 14$ y se tiene que $h'(-1) = 0$ mientras que $h'(-2/3) \neq 0$.

O sea -1 es raíz de multiplicidad ≥ 2 y $-2/3$ es raíz simple.

Volviendo a derivar h: $h'' = 60X^3 + 96X + 6X - 28$ y $h''(-1) \neq 0$.

Se concluye que -1 es raíz doble de h.

Finalmente la factorización de h en $\mathbb{Q}[X]$ es:

$$h = 3(X + 1)^2(X + \frac{2}{3})(X^2 - 2)$$

ya que $X^2 - 2$ es irreducible en $\mathbb{Q}[X]$.

Y dado que $f = \frac{1}{3}X^3\,h$, obtenemos la siguiente factorización de f en $\mathbb{Q}[X]$:

$$f = X^3(X + 1)^2(X + \frac{2}{3})(X^2 - 2).$$

Observación 5.8.3. El Lema de Gauss provee un algoritmo para calcular todas las raíces racionales de un polinomio racional, pero se ve claramente que éste es extremadamente costoso, pues hay que evaluar el polinomio de entrada en un gran número de fracciones $\dfrac{\alpha}{\beta}$ (la cantidad de fracciones está relacionada con la cantidad de divisores de a_0 y a_n).

5.8.2. Factorización en $\mathbb{Q}[X]$.

Una propiedad que puede ser útil para encontrar factores de grado 2 en $\mathbb{Q}[X]$ es cuando se sabe que el polinomio tiene una raíz de la forma $a + b\sqrt{m}$ con $m \in \mathbb{Q}$ tal que $\sqrt{m} \notin \mathbb{Q}$.

Proposición 5.8.4. (Raíces de la forma $a+b\sqrt{m}$ de polinomios racionales.)
Sea $m \in \mathbb{Q}$ tal que $\sqrt{m} \notin \mathbb{Q}$, y sean $a, b \in \mathbb{Q}$ con $b \neq 0$. Sea $f \in \mathbb{Q}[X]$. Entonces

1. $g := \big(X - (a+b\sqrt{m})\big)\big(X - (a-b\sqrt{m})\big)$ *es un polinomio irreducible de* $\mathbb{Q}[X]$,
2. $f(a+b\sqrt{m}) = 0 \implies g \mid f$ *en* $\mathbb{Q}[X]$,
3. $f(a+b\sqrt{m}) = 0 \iff f(a-b\sqrt{m}) = 0$,
4. *Para todo* $m \in \mathbb{N}$, $\operatorname{mult}(a+b\sqrt{m}; f) = m \iff \operatorname{mult}(a-b\sqrt{m}; f) = m$.

Demostración. 1. Haciendo la cuenta,

$$g := \big(X - (a+b\sqrt{m})\big)\big(X - (a-b\sqrt{m})\big) = X^2 - 2aX + a^2 - b^2 m \in \mathbb{Q}[X]$$

porque todos sus coeficientes pertenecen a $\mathbb{Q}$, y es irreducible por ser de grado 2 y no tener raíz en $\mathbb{Q}$.

2. Dividamos a $f \in \mathbb{Q}[X]$ por el polinomio $g \in \mathbb{Q}[X]$:

$$g = q\,g + r \quad \text{con} \quad r = 0 \quad \text{o} \quad \operatorname{gr}(r) < 2.$$

En todo caso se puede escribir en la forma $r = cX + d$ con $c, d \in \mathbb{Q}$. Ahora bien, como $a+b\sqrt{m}$ es raíz de f y de g, se obtiene que $a+b\sqrt{m}$ es raíz de r también. Es decir

$$\begin{aligned} 0 &= r(a+b\sqrt{m}) = c(a+b\sqrt{m}) + d = ca + d + cb\sqrt{m} \\ &\implies ca + d = -cb\sqrt{m}. \end{aligned}$$

Si fuera $c \neq 0$, como $b \neq 0$ se obtendría $\sqrt{m} = \dfrac{ca+d}{-cb} \in \mathbb{Q}$ lo que contradice la hipótesis $\sqrt{m} \notin \mathbb{Q}$. Por lo tanto $c = 0$, lo que implica también de la igualdad $0 = c(a+b\sqrt{m}) + d$ que $d = 0$. Se concluye que $r = cX + d$ es el polinomio nulo, y por lo tanto $g \mid f \in \mathbb{Q}[X]$.

3. Es una consecuencia directa del inciso anterior, ya que si $f(a+b\sqrt{m}) = 0$, entonces $g \mid f$ y por lo tanto $f(a-b\sqrt{m}) = 0$ también. La recíproca es análoga.

4. La misma multiplicidad se obtiene por inducción, aplicando la hipótesis inductiva al polinomio $f/g \in \mathbb{Q}[X]$ cuando $a+b\sqrt{m}$ es raíz de f.

□

<u>*Ejemplo:*</u> Factorizar en $\mathbb{C}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}[X]$ el polinomio $f = X^4 - X^3 - 2X^2 - 3X - 1$ sabiendo que tiene a $1-\sqrt{2}$ como raíz.

Como $f \in \mathbb{Q}[X]$ y $1-\sqrt{2}$ es raíz, también lo es $1+\sqrt{2}$ y f es divisible por el polinomio $g = \big(X - (1-\sqrt{2})\big)\big(X - (1+\sqrt{2})\big) = X^2 - 2X - 1$. En efecto, al hacer la división se obtiene

$$f = (X^2 - 2X - 1)(X^2 + X + 1).$$

Ahora bien, las raíces de X^2+X+1 son las raíces cúbicas primitivas de la unidad, $\dfrac{-1\pm\sqrt{3}i}{2}$, por lo tanto la factorización de f en $\mathbb{C}[X]$ es

$$f=\big(X-(1-\sqrt{2})\big)\big(X-(1+\sqrt{2})\big)\big(X-(\frac{-1+\sqrt{3}}{2})\big)\big(X-(\frac{-1-\sqrt{3}}{2})\big).$$

El polinomio X^2+X+1 es irreducible tanto en $\mathbb{R}[X]$ como en $\mathbb{Q}[X]$ al tener grado 2 y no tener raíces allí, y el polinomio X^2-2X-1 es irreducible en $\mathbb{Q}[X]$ al tener grado 2 y no tener raíces en $\mathbb{Q}$. Por lo tanto la factorización de f en $\mathbb{R}[X]$ es

$$f=\big(X-(1-\sqrt{2})\big)\big(X-(1+\sqrt{2})\big)\big(X^2+X+1\big)$$

y la factorización de f en $\mathbb{Q}[X]$ es

$$\big(X^2-2X-1\big)\big(X^2+X+1\big).$$

Con respecto a la factorización en general, en el caso de $\mathbb{Q}[X]$ no se puede decir nada más preciso que lo que ya dice el Teorema Fundamental de la Aritmética para polinomios:

Teorema 5.8.5. (Factorización en $\mathbb{Q}[X]$.)

Sea $f\in\mathbb{Q}[X]-\mathbb{Q}$. Entonces la factorización en irreducibles de f en $\mathbb{Q}[X]$ es de la forma

$$f=c\,g_1^{m_1}\dots g_r^{m_r}$$

donde $c\in\mathbb{Q}^\times$, $g_1,\dots,g_r$ son polinomios mónicos irreducibles distintos en $\mathbb{Q}[X]$ y $m_1,\dots,m_r\in\mathbb{N}$.

Notemos que cada factor irreducible $g_i\in\mathbb{Q}[X]$ cuando lo miremos como polinomio en $\mathbb{R}[X]$ o en $\mathbb{C}[X]$ va probablemente dejar de ser irreducible para factorizarse como polinomios de grado 1 o 2 en el caso de $\mathbb{R}$, o todos de grado 1 en el caso de $\mathbb{C}$. En ese sentido la factorización de f en $\mathbb{R}[X]$ "refina" la factorización de f en $\mathbb{Q}[X]$, y la de f en $\mathbb{C}[X]$ la refina aún más.

Por ejemplo el polinomio $f=X^4-2X^3+X^2-4X-2\in\mathbb{Q}[X]$ que consideramos arriba se factoriza en $\mathbb{Q}[X]$ en la forma

$$f=(X^2+2)(X^2-2X-1),$$

ya que ambos factores son irreducibles en $\mathbb{Q}[X]$ al no tener raíces en $\mathbb{Q}$ (por ser de grado 2).

Si bien no se sabe nada a priori sobre los factores irreducibles en $\mathbb{Q}[X]$ de un polinomio, en este caso existen algoritmos de factorización (exacta), contrariamente a lo que pasa en $\mathbb{C}[X]$ o $\mathbb{R}[X]$.

La historia de los algoritmos de factorización de polinomios en $\mathbb{Q}[X]$ comenzó con el astrónomo alemán Friedrich von Schubert en 1793, que presentó un algoritmo luego redescubierto por Leopold Kronecker en 1882 y y que se conoce hoy como el *Algoritmo de Kronecker*.


Zassenhaus


Berlekamp


A. Lenstra


H. Lenstra


Lovasz

Para factorizar un polinomio en $\mathbb{Q}[X]$, dado que las constantes no influyen, alcanza con considerar el polinomio en $\mathbb{Z}[X]$ obtenido limpiando los denominadores comunes. Y en realidad se puede probar más: se puede probar que el problema de la factorización en $\mathbb{Q}[X]$ se reduce a encontrar factores con coeficientes enteros.

El algoritmo de Kronecker se basa en ese hecho, y en evaluación e interpolación de polinomios. Es muy sencillo teóricamente, aunque terriblemente costoso de implementar computacionalmente. Pero tiene la importante característica de indicar que existen algoritmos, y por lo tanto se pueden buscar algoritmos que funcionen mejor... Hubo posteriormente grandes mejoras en cuanto a la velocidad de los algoritmos de factorización en $\mathbb{Q}[X]$.

El primero de ellos, debido a Hans Zassenhaus, en 1969, se basa esencialmente en un algoritmo de Elwyn Berlekamp para factorizar rápidamente polinomios en cuerpos finitos, 1967. El algoritmo requiere en promedio un número de operaciones del orden de $\mathrm{gr}(f)^c$, donde c es una constante calculada, aunque en el peor de los casos puede necesitar un número exponencial en $\mathrm{gr}(f)$ operaciones como en el algoritmo de Kronecker mencionado más arriba.

El primer algoritmo polinomial para factorizar polinomios en $\mathbb{Q}[X]$, conocido como algoritmo L^3, es debido a los hermanos holandeses Arjen Lenstra y Hendrik Lenstra y al húngaro László Lovász, en 1982. Establece exactamente lo siguiente :

Teorema 5.8.6. **(L^3.)**

Sea $f = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ un polinomio que satisface que sus coeficientes (enteros) no tienen ningún factor común no trivial en $\mathbb{Z}$. Sea H una cota superior para los módulos de los coeficientes $a_i \in \mathbb{Z}$. Entonces, se puede factorizar f en $\mathbb{Q}[X]$ realizando del orden de $n^{12} + n^9(\log_2 H)^3$ operaciones "bit"(es decir los números se representan en base 2, y se cuenta una operación cada vez que se suma,resta, multiplica o divide un bit "0"ó "1").

Este es el primer algoritmo *polinomial* que existe para factorizar en $\mathbb{Q}[X]$ polinomios racionales, donde polinomial significa que si el polinomio de entrada se mide a través de su grado n y del tamaño de sus coeficientes en representación binaria $\log_2 H$, la cantidad total de operaciones binarias que realiza el algoritmo está acotado por $(n \cdot \log_2 H)^c$ para algún $c \in \mathbb{N}$ calculado, y no del tipo 2^n como lo era hasta entonces.

El algoritmo utilizado hoy en día por la mayoría de los sistemas de álgebra computacional es un algoritmo más moderno, debido principalmente a Mark van Hoeij (que trabaja en él desde el 2002, y logró varias mejoras teóricas y prácticas): tiene la ventaja de ser polinomial en teoría y también eficiente en la práctica.

La descripción y la demostración de los algoritmos de Zassenhaus-Berlekamp, L^3 y van Hoeij

quedan fuera de nuestro alcance, y utilizan fundamentalmente en el primer caso la reducción a factorizar polinomios módulo p para p primo, en el segundo caso la teoría de látices o reticulados en $\mathbb{Z}^n$, y en el último una combinación de ambos.