ALGEBRA III (Doble grado Informática-Matemáticas)

1. Preliminares sobre extensiones de cuerpos y raíces de polinomios.

1.1. Sobre extensiones de cuerpos.

(1) Recordemos que por un **cuerpo** K entendemos un anillo conmutativo, no trivial (es decir, con $|K| \geq 2$ o, equivalentemente, donde $1 \neq 0$), en el cual todo elemento no nulo tiene un inverso para el producto. Así, por ejemplo, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, o $\mathbb{Z}_p$ para $p \geq 2$ un primo de $\mathbb{Z}$, son cuerpos bien conocidos.

(2) Dado un cuerpo K, por una **extensión de K entendemos un otro cuerpo E que contiene a K como subcuerpo**, esto es, tal que $K \subseteq E$ como conjunto y sucede que K tiene el mismo 0, el mismo 1, y los cálculos de sumas y productos (y entonces también de opuestos e inversos) se realizan en K como en E. Usualmente representamos la situación de dos formas: escribimos

$$K \leq E$$

cuando queremos enfatizar que "*K es un subcuerpo de E*", y escribimos

$$E/K,$$

expresión que leemos "*E sobre K*", cuando queremos enfatizar que "*E es un cuerpo extensión del cuerpo K*". Significan lo mismo, así que

$$K \leq E \Longleftrightarrow E/K.$$

(3) **Los homomorfismos entre cuerpos son monomorfismos**. Esto es, si K y E son cuerpos, cada aplicación $\sigma : K \to E$ preservando 0 y 1, sumas, y productos (y entonces opuestos e inversos) es inyectiva: Si suponemos que $\sigma(a) = \sigma(b)$ con $a \neq b$, tendríamos por un lado que $a - b \neq 0$, y existiría su inverso $(a-b)^{-1}$, y por otro que $\sigma(a - b) = \sigma(a) - \sigma(b) = 0$. Pero entonces, en el cuerpo E,

$$1 = \sigma(1) = \sigma\big((a-b)(a-b)^{-1}\big) = \sigma(a-b)\sigma(a-b)^{-1} = 0 \cdot \sigma(a-b)^{-1} = 0$$

lo que no puede ocurrir. Debido a esta propiedad, es usual referirse a un homomorfismo de cuerpos $\sigma : K \to E$ como a una **inmersión de K en E**, ya que este homomorfismo establece un isomorfismo de cuerpos entre K y el subcuerpo de E imagen del homomorfismo:

$$K \cong \sigma(K) = \{\sigma(a),\ a \in K\} \leq E, \quad a \mapsto \sigma(a)\,.$$

(4) **Cuando una inmersión $\sigma : K \to E$ es dada y bien conocida, es usual tratarla como una inclusión** (asumiendo de común acuerdo un abuso de lenguaje), identificando cada elemento a de K con su imagen $\sigma(a)$ en E, y K con el subcuerpo de E imagen de σ. De manera asumimos que $K \leq E$ es un subcuerpo (y E/K una extensión).

Un ejemplo típico de esta asunción es la inmersión

$$\sigma : \mathbb{Q} \to \mathbb{R},$$

del cuerpo de los números racionales en el cuerpo de los números reales, definida por $\sigma(\frac{a}{b}) = ab^{-1}$. Está bien definida, pues

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc \Rightarrow ab^{-1} = cd^{-1}$$

y es ciertamente una inmersión, pues

$$\sigma\Big(\frac{a}{b}+\frac{c}{d}\Big)=\sigma\Big(\frac{ad+cb}{bd}\Big)=(ad+cb)(bd)^{-1}=(ad+cb)b^{-1}d^{-1}$$
$$=adb^{-1}d^{-1}+cbb^{-1}d^{-1}=ab^{-1}+cd^{-1}=\sigma\Big(\frac{a}{b}\Big)+\sigma\Big(\frac{c}{d}\Big),$$
$$\sigma\Big(\frac{a}{b}\frac{c}{d}\Big)=\sigma\Big(\frac{ac}{bd}\Big)=(ac)(bd)^{-1}=acb^{-1}d^{-1}=\sigma\Big(\frac{a}{b}\Big)\sigma\Big(\frac{c}{d}\Big),$$

y claramente $\sigma(\frac{0}{1})=0$ y $\sigma(\frac{1}{1})=1$. Esta inmersión $\sigma:\mathbb{Q}\to\mathbb{R}$ nos es familiar y bien conocida, y es mediante ella que identificamos cada número racional con un número real y vemos a $\mathbb{Q}$ como un subcuerpo de $\mathbb{R}$ y a $\mathbb{R}$ como una extensión de $\mathbb{Q}$.

Veamos otro ejemplo típico en el que usualmente consideramos una cierta inmersión como una inclusión. Supongamos K cualquier cuerpo y $p\in K[x]$ un polinomio de grado ≥ 1 irreducible. Sea

$$K[x]/_p=\{\overline{f}\mid f\in K[x]\},$$

el *cuerpo de clases de congruencias módulo p* (también llamado el *cuerpo de restos módulo p*) donde, recordamos,

$$\begin{aligned}\overline{f}=\overline{g}&\Leftrightarrow f\equiv g \mod p\\ &\Leftrightarrow p\mid f-g\\ &\Leftrightarrow f \text{ y } g \text{ dan el mismo resto al dividirlos por } p,\end{aligned}$$

las operaciones de suma y producto de clases de congruencias son

$$\overline{f}+\overline{g}=\overline{f+g},\ \ \overline{f}\ \overline{g}=\overline{fg},$$

y el zero y el uno son $\overline{0}$ y $\overline{1}$, respectivamente. Puesto que p es irreducible en el Dominio Euclídeo $K[x]$, conocemos que $K[x]/_p$ es un cuerpo: Si $\overline{f}\neq\overline{0}$, será $p\nmid f$ y $mcd(p,f)=1$. Tendremos coeficientes de Bezout $u,v\in K[x]$ tal que $1=fu+pv$, de donde $\overline{1}=\overline{f}\ \overline{u}$, lo que nos asegura que existe $\overline{f}^{\,-1}=\overline{u}$. La asignación $a\mapsto\overline{a}$ nos determina una inmersión estandard

$$K\to K[x]/_p,$$

que miraremos usualmente como una inclusión, considerando a K como un subcuerpo del cuerpo de clases de congruencias módulo p.

Un caso particular es familiar: Tomemos $K=\mathbb{R}$ y $p=x^2+1$, que es irreducible en $\mathbb{R}[x]$ (no tiene raíces). Tenemos, como antes la "inclusión" $\mathbb{R}\leq\mathbb{R}[x]/_{x^2+1}$, después de identificar cada número real a con su clase $\overline{a}$ en $\mathbb{R}[x]/_{x^2+1}$. Analicemos un poco este cuerpo de restos, llamando $i=\overline{x}$. Sea $f\in\mathbb{R}[x]$ cualquier polinomio, sabemos que existen polinomio únicos $q,r\in\mathbb{R}[x]$ tal que $f=(x^2+1)q+r$, donde $gr(r)\leq 1$. Será $r=a+bx$, para ciertos $a,b\in\mathbb{R}$, y tendremos que

$$\overline{f}=\overline{r}=\overline{a}+\overline{b}\,\overline{x}=a+bi.$$

Así que todo elemento de $\mathbb{R}[x]/_{x^2+1}$ se expresa en la forma $a+bi$ para ciertos números reales a y b. Además, de forma única: Supongamos que $a+bi=a'+b'i$. Tendremos que $\overline{a}+\overline{b}\,\overline{x}=\overline{a'}+\overline{b'}\,\overline{x}$, o sea $\overline{a+bx}=\overline{a'+b'x}$. Pero esto significa que x^2+1 divide a $a-a'+(b-b')x$, lo que no es posible si ese último es distinto de

cero, ya que un polinomio no nulo de grado uno no puede ser múltiplo de uno de grado dos. Así que $a - a' = 0$, $b - b' = 0$, y $a = a'$ y $b = b'$.

Observar ahora que

$$i^2 = \overline{x}^{\,2} = \overline{x^2} = \overline{-1} = -1$$

y que

$$\begin{aligned}(a + bi) + (a' + b'i) &= a + a' + (b + b')i,\\ (a + bi)\,(a' + b'i) &= aa' + (ab' + ba')i + bb'i^2 = aa' + (ab' + ba')i - bb'\\ &= aa' - bb' + (ab' + ba')i.\end{aligned}$$

De manera que $\mathbb{R}[x]/_{x^2+1} = \mathbb{C}$, el cuerpo de los números complejos, y la inmersión $\mathbb{R} \to \mathbb{C}$, $a \mapsto a = \overline{a}$, es la ordinaria con que se ve $\mathbb{R}$ como un subcuerpo del cuerpo $\mathbb{C}$ de los complejos.

1.2. Sobre raíces de polinomios y su multiplicidad.

(1) Dada una extensión E/K, recordemos que para cada $\alpha \in E$ hay un homomorfismo de anillos $K[x] \to E$, llamado el **homomorfismo de evaluación en** α, que asigna a cada polinomio $f = \sum_i a_i x^i \in K[x]$, el elemento $f(\alpha) = \sum_i a_i \alpha^i \in E$. Un elemento $\alpha \in E$ tal que $f(\alpha) = 0$ es llamado **una raíz de** f **en** E. Notemos que $K[x] \leq E[x]$ como subanillo, por tanto $f \in E[x]$ y, por el Teorema de Ruffini, el que α sea una raíz de f en E es equivalente a que $(x - \alpha)|f$ en el anillo $E[x]$; esto es, $(x - \alpha)$ es uno de los irreducibles que aparecen en la factorización de f en producto de irreducibles en el anillo $E[x]$. Si en dicha factorización en $E[x]$ aparece el irreducible $x - \alpha$ con exponente m, esto es, si $(x - \alpha)^m$ es la maxima potencia de $x - \alpha$ que divide a f en $E[x]$, decimos que α es una **raíz de** f **en** E **de multiplicidad** m. Decimos que α es una **raíz simple** si es de multiplicidad 1, y que es **raíz múltiple** si es de multiplicidad ≥ 2.

(2) El **criterio del polinomio derivado** es un útil recurso para conocer la inexistencia de raíces múltiples de un polinomio en cuerpos extensión.

Si $f = \sum_i a_i x^i \in K[x]$ es un polinomio con coeficientes es un cuerpo K, se define su **derivado** como el polinomio

$$f' = \sum_i i a_i x^{i-1} = a_1 + 2a_2 x + \cdots \in K[x]\ ^{1}.$$

El cálculo de polinomios derivados tiene las mismas propiedades básicas que las propias del cálculo diferencial:

$$(f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

La primera igualdad es inmediata desde la propia definición. Para la segunda, supongamos ahora que tenemos los polinomios $f = \sum_i a_i x^i$ y $g = \sum_j b_j x^j$. Entonces $fg = \sum_{i,j} a_i b_j x^{i+j}$,

$(fg)' = \left(\sum_{i,j} a_i b_j x^{i+j}\right)' = \sum_{i,j} \left(a_i b_j x^{i+j}\right)' = \sum_{i,j} (i + j) a_i b_j x^{i+j-1}$,

[1] El producto na, de enteros $n \geq 0$ por elementos a de un anillo es el usual: Si $n = 0$, entonces $0a = 0$. Si $n > 0$, entonces $na = a + \overset{n}{\cdots} + a$, la suma reiterada de ese elemento a consigo mismo n veces.

y, finalmente,

$$f'g + fg' = \Big(\sum_i i a_i x^{i-1}\Big)\Big(\sum_j b_j x^j\Big) + \Big(\sum_i a_i x^i\Big)\Big(\sum_j j b_j x^{j-1}\Big)$$
$$= \sum_{i,j} i a_i b_j x^{i+j-1} + \sum_{i,j} j a_i b_j x^{i+j-1} = \sum_{i,j} (i+j) a_i b_j x^{i+j-1} = (fg)'.$$

Por ejemplo,

$$\Big((x-a)^2\Big)' = (x-a)'(x-a) + (x-a)(x-a)' = (x-a) + (x-a) = 2(x-a).$$

Proposición 1.1. *(i) Si $f \in K[x]$ es tal que $mcd(f, f') = 1$ en $K[x]$, entonces todas las raíces de f en cualquier cuerpo extensión de K son simples.*

(ii) Si $f \in K[x]$ es irreducible y $f' \neq 0$, todas las raíces de f en cualquier cuerpo extensión de K son simples.

Demostración.(*i*) Supongamos E/K es una extensión y que α es raíz múltiple de f en E. En el anillo $E[x]$, será $f = (x-\alpha)^2 g$ para un cierto $g \in E[x]$. Pero entonces $f' = 2(x-\alpha)g + (x-\alpha)^2 g'$ y vemos que $f'(\alpha) = 0$. Pero, por el Teorema de Bezout, existen polinomios $u, v \in K[x]$ tal que $1 = fu + f'v$, y evaluando en α, resulta que

$$1 = f(\alpha)u(\alpha) + f'(\alpha)v(\alpha) = 0u(\alpha) + 0v(\alpha) = 0,$$

lo que no es posible.

(*ii*) Como $\mathrm{gr}(f') < \mathrm{gr}(f)$, y f es irreducible, necesariamente $mcd(f, f') = 1$. □

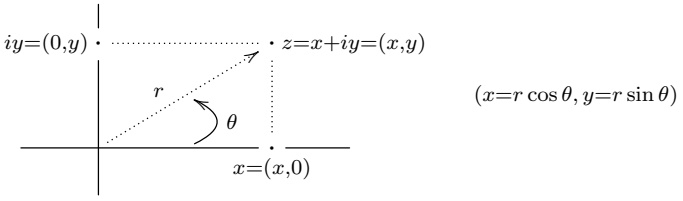
Notar que el polinomio derivado de un polinomio puede ser cero: Si $f = x^2 + 1 \in \mathbb{Z}_2[x]$, entonces $f' = 2x = x + x = (1+1)x = 0x = 0$.

1.3. Raíces n-ésimas de números complejos.

Para todo lo que sigue, es útil el pensar en los puntos del plano como la representación geométrica de los números complejos, así que vamos a identificar cada punto del plano Euclídeo $\mathbb{R}^2$ de coordenadas cartesianas (x, y) con el número complejo $z = x+iy$. Además, sobre todo a efectos de multiplicación, es cómodo usar la expresión de los complejos no nulos, es decir, los del grupo multiplicativo $\mathbb{C}^\times$, en su forma polar

$$z = re^{i\theta}$$

donde $r = |z| = \sqrt{x^2+y^2}$ es el módulo del complejo que coincide con longitud del segmento de extremos 0 y z, $\theta \in \mathbb{R}$ es la amplitud en radianes del ángulo desde el eje de abscisas a la recta que pasa por 0 y z, y $e^{i\theta} = \cos\theta + i\sin\theta$, que es justo el complejo en que la semi-recta que pasa por 0 y z corta a la circunferencia $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$:



$$z = x + iy = r\cos\theta + i\, r\sin\theta = r(\cos\theta + i\sin\theta) = re^{i\theta}.$$

Si $z' = r'e^{i\theta'}$ es otro complejo no nulo, entonces

$$\begin{aligned} zz' = rr'e^{i\theta}e^{i\theta'} &= rr'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') \\ &= rr'\big(\cos\theta\cos\theta' - \sin\theta\sin\theta' + i(\sin\theta\cos\theta' + \cos\theta\sin\theta')\big) \\ &= rr'\big(\cos(\theta+\theta') + i\sin(\theta+\theta')\big) \\ &= rr'e^{i(\theta+\theta')}. \end{aligned}$$

En particular, calculamos las potencias z^n, $n \geq 1$, de un complejo $z = re^{i\theta}$ por la simple fórmula

$$z^n = r^n e^{in\theta}.$$

Si $0 \neq z \in \mathbb{C}$ es cualquier complejo no nulo, para cualquier natural $n \geq 1$, las raíces complejas del polinomio $x^n - z$, esto es, los números complejos x tales que $x^n = z$, son llamadas las **raíces n-ésimas del número** z (cuadradas si $n = 2$, cúbicas si $n = 3$, etc.). Para realizar una descripción de las mismas, procedemos como sigue:

Si $0 < r \in \mathbb{R}$ es un número real positivo, la gráfica de la función real de variable real $y = x^n$ corta exactamente una vez a la recta $y = r$ en el intervalo $(0, +\infty)$, lo que significa que el polinomio $x^n - r$ tiene exactamente una raíz que es real y positiva. Usaremos para ella la notación

$$\sqrt[n]{r}.$$

Las reglas básicas que rigen la extracción de raíces n-ésimas de números reales positivos son las bien familiares: $\sqrt[n]{r}\,\sqrt[n]{r'} = \sqrt[n]{rr'}$, $(\sqrt[n]{r})^m = \sqrt[n]{r^m}$, $\sqrt[m]{\sqrt[n]{r}} = \sqrt[mn]{r}$. Pero hay que manejar los radicales con precaución, pues no todo cálculo con estos se puede hacer en base al uso formal de esas propiedades. Por ejemplo: $\sqrt{5+2\sqrt{6}} = \sqrt{2}+\sqrt{3}$, ya que $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$.

Si ahora $0 \neq z = re^{i\theta} = r(cos\,\theta + i\,sen\,\theta)$ es cualquier complejo no nulo expresado en su forma polar, entonces los n complejos

$$\sqrt[n]{r}e^{i\frac{\theta+2k\pi}{n}} = \sqrt[n]{r}\Big(cos\tfrac{\theta+2k\pi}{n} + i\,sen\tfrac{\theta+2k\pi}{n}\Big), \quad k = 0, \ldots, n-1.$$

son todos ellos raices n-ésimas de z, y por tanto las n-raíces de z (no puede haber más raíces de $x^n - a$). Destacamos entre ellas la raíz que se obtiene cuando $k = 0$, para la que reservamos la notación $\sqrt[n]{z}$, esto es

$$\sqrt[n]{z} = \sqrt[n]{r}\,e^{i\frac{\theta}{n}} = \sqrt[n]{r}\,\big(cos\tfrac{\theta}{n} + i\,sen\tfrac{\theta}{n}\big)\,.$$

Así, por ejemplo,

- $\sqrt[n]{1} = 1$.
- $\sqrt[n]{-1} = cos\frac{\pi}{n} + i\,sen\frac{\pi}{n}$, ya que $-1 = e^{i\pi} = cos\,\pi + i\,sen\,\pi$. Particularmente,

  $$\sqrt{-1} = i, \quad \sqrt[3]{-1} = \tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}, \quad \sqrt[4]{-1} = \tfrac{\sqrt{2}}{2} + i\tfrac{\sqrt{2}}{2}, \quad \ldots$$

  (notar, por ejemplo, que $\sqrt[3]{-1} \neq -1$)
- $\sqrt[2]{i} = \cos\frac{\pi}{4} + i\,sen\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, ya que $i = e^{i\frac{\pi}{2}} = cos\,\frac{\pi}{2} + i\,sen\,\frac{\pi}{2}$.
- $\sqrt[3]{i} = \cos\frac{\pi}{6} + i\,sen\frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i\,.$
- $\sqrt{-2} = \sqrt{2}\cos\frac{\pi}{2} + i\,sen\,\frac{\pi}{2} = i\sqrt{2}$, ya que $-2 = 2\,e^{i\pi} = 2(cos\,\pi + i\,sen\,\pi)$.

En términos de $\sqrt[n]{z}$, las n raíces de $z = e^{i\theta}$ se pueden expresar entonces como $\sqrt[n]{z}\, e^{\frac{2k\pi i}{n}}$, con $0 \leq k \leq n-1$. Por ejemplo, las dos raíces cuadradas de la unidad son 1, -1; las tres raíces cúbicas de la unidad son 1, $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$, y las 4 raíces cuartas de la unidad son 1, i, -1, $-i$.

1.4. **El Teorema Fundamental del Álgebra.**

Si $f \in K[x]$ es un polinomio, decimos que este **descompone totalmente en una extensión** E/K, si en el anillo $E[x]$ el polinomio factoriza como producto de irreducibles de grado uno, esto es, en la forma

$$f = a(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r}.$$

para ciertos $\alpha_i \in E$ con $\alpha_i \neq \alpha_j$ si $i \neq j$, y ciertos enteros $m_i \geq 1$. Es decir, si f tiene todos sus raíces en E.

Un cuerpo K se dice **algebraicamente cerrado** si todo polinomio con coeficientes en K descompone totalmente en K.

Proposición 1.2. *Las siguientes propiedades sobre un cuerpo K son equivalentes:*

(1) *K es algebraicamente cerrado.*
(2) *Todo polinomio de $K[x]$ de grado ≥ 1 tiene una raíz en K.*

Demostración. Es claro que (1) $\Rightarrow$ (2). Para el reciproco, supongamos que $f \in K[x]$ es de grado $n \geq 1$, y hagamos inducción en n. Si $n = 1$, será $f = a_0 + a_1 x$, con $a_1 \neq 0$, y por tanto también $f = a_1\big(x - (-a_0 a_1^{-1})\big)$. Para el caso general $n > 1$, sabemos que existe un $\alpha \in K$ tal que $f(\alpha) = 0$. Por Ruffini, tendremos que $f = (x - \alpha)g$ para un cierto $g \in K[x]$ de grado $n - 1$, y el resultado se deduce de aplicar la hipótesis de inducción a g. □

Teorema 1.3 (Teorema de Gauss)**.** *El cuerpo $\mathbb{C}$ es algebraicamente cerrado.*

Demostración. El cuerpo $\mathbb{C}$ es un espacio vectorial real de dimensión 2, con base $\{1, i\}$, que es métrico con norma el valor absoluto, esto es donde la distancia entre dos complejos a y b es dada por $d(a, b) = |a - b|$. Tiene entonces la topología asociada a dicha métrica, donde una base de entornos abiertos de cualquier punto está formada por las bolas abiertas $B(a, r) = \{z \in \mathbb{C} \mid |z - a| < r\}$, con $0 < r \in \mathbb{R}$. Usaremos el Teorema de Weierstass: *Una función continua $f : \mathbb{C} \to \mathbb{R}$ siempre alcanza su mínimo (y su máximo) en cualquier subconjunto cerrado y acotado de $\mathbb{C}$, particularmente en cualquier bola cerrada $B[a, r] = \{z \in \mathbb{C} \mid |z - a| \leq r\}$.* Usaremos también algunas desigualdades básicas entre módulos, como que $|a| - |b| \leq |a + b| \leq |a| + |b|$.

Sea $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{C}[x]$ un polinomio de grado $n \geq 1$ ($a_n \neq 0$). Se trata de probar que existe un complejo $z \in \mathbb{C}$ tal que $f(z) = 0$. Para ello, comenzamos considerando la función continua $\mathbb{C} \to \mathbb{R}$ definida por $z \mapsto |f(z)|$, y vamos a probar, por inducción en el grado n, el número real $|f(z)|$ se hace más grande que cualquier número real positivo k fuera de cierta bola cerrada $B[0, r]$; es decir vamos a probar que

"Para cada número real $k \geq 0$, existe un real $r \geq 0$ tal que $|z| > r \Rightarrow |f(z)| > k$."

En efecto, escribamos f como

$$f = a_0 + xg, \quad \text{donde } g = a_1 + a_2 x + \cdots + a_n x^{n-1},$$

de manera que, para cualquier $z \in \mathbb{C}$,

$$|f(z)| = |zg(z) + a_0| \geq |z| \cdot |g(z)| - |a_0|.$$

Si $n = 1$, $g = a_1$ es constante y podemos tomar $r = \frac{k+|a_0|}{|a_1|}$, pues si $|z| > r$, entonces

$$|f(z)| \geq |z| \cdot |a_1| - |a_0| > \frac{k + |a_0|}{|a_1|}|a_1| - a_0 = k.$$

Para el caso general $n > 1$, la hipótesis de inducción aplicada al polinomio g y al número real $k' = k + |a_0|$ nos asegura la existencia de un real $r' > 0$ tal que $|g(z)| > k + |a_0|$ siempre que $|z| > r'$. Pero entonces, tomando $r = \text{máx}\{r', 1\}$, para cualquier $z \in \mathbb{C}$ con $|z| > r$, tenemos que $|f(z)| \geq |z| \cdot |g(z)| - |a_0| > 1 \cdot (k + |a_0|) - |a_0| = k$.

En particular, para el caso $k = |a_0|$, concluimos que existe un real $r \geq 0$ tal que $|f(z)| > |a_0|$ siempre que $|z| > r$. Ahora, aplicando el Teorema Weierstrass a la función continua $\mathbb{C} \to \mathbb{R}$ definida por $z \mapsto |f(z)|$, podemos asegurar que existe un $z_0 \in B[0, r]$ tal que $|f(z_0)| \leq |f(z)|$ para todo $z \in B[0, r]$. Pero la misma desigualdad se verifica automáticamente para los $z \notin B[0, r]$, pues si $|z| > r$ entonces $f(z) > |a_0| = |f(0)| \geq |f(z_0)|$. Concluimos así que

"*Existe un* $z_0 \in \mathbb{C}$ *tal que* $|f(z_0)| \leq |f(z)|$*para todo* $z \in \mathbb{C}$".

Es claro que f tiene una raíz en $\mathbb{C}$ si y solo si el polinomio $f(x + z_0)$, que resulta de sustituir x por $x + z_0$ en f tiene una raíz, y este tiene la ventaja notacional de que la función $z \mapsto |f(z + z_0)|$ tiene un mínimo absoluto en el 0. Por tanto, sustituyendo f por $f(x + z_0)$, podemos seguir trabajando con f pero suponiendo que $z_0 = 0$. Esto es, asumimos en lo que sigue que

$$|f(z)| \geq |f(0)| = |a_0| \text{ } \textit{para todo } z \in \mathbb{C}.$$

Si $a_0 = 0$ hemos terminado, pues sería $f(0) = 0$ y f tiene una raíz. Vemos a continuación que suponer $a_0 \neq 0$ nos lleva a una contradicción:

Supuesto $a_0 \neq 0$, si sustituimos f por $\frac{1}{a_0}f$, la función $z \mapsto |\frac{1}{a_0}f(z)|$ también tiene a 0 como mínimo absoluto, así que podemos suponer que $a_0 = 1$, de manera que

$$|f(z)| \geq 1 \text{ } \textit{para todo } z \in \mathbb{C}$$

y, excluyendo los primeros términos de coeficiente nulo, podemos escribir

$$f = 1 + a_m x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n, \qquad \text{con } a_m \neq 0.$$

entonces, sustituyendo x por $\sqrt[m]{-a_m^{-1}}x$, obtenemos el polinomio $f(\sqrt[m]{-a_m^{-1}}x) = 1 - x^m +$ términos de grado mayor que m, es decir,

$$f(\sqrt[m]{-a_m^{-1}}x) = 1 - x^m + x^m g,$$

donde $g \in \mathbb{C}[x]$ es un cierto polinomio con $g(0) = 0$ (pues todos sus términos son de grado ≥ 1). Finalizamos demostrando la existencia de un número real t tal que $f(\sqrt[m]{-a_m^{-1}}t) < 1$ (lo que es imposible pues $f(z) \geq 1$ para todo $z \in \mathbb{C}$): Consideremos la función $\mathbb{R} \to \mathbb{R}$ definida por $t \mapsto |g(t)|$. Su límite en $t = 0$ es $g(0) = 0$ (por continuidad), luego seguro que existe un número real t en el intervalo $(0, 1)$ tal que $|g(t)| < 1$ (tomando $\epsilon = 1$ en la formulación usual de límite, existe un $\delta > 0$ tal que $g(t) < 1$ siempre que $|t| < \delta$,

pues tomemos cualquier $t \in (0,1) \cap (-\delta, \delta)$). Entonces, tanto t^m como $1 - t^m$ están en el intervalo $(0,1)$ y tenemos que

$$|f(\sqrt[m]{-a_m^{-1}}t)| = |1 - t^m + t^m g(t)| \leq |1 - t^m| + |t^m g(t)| < 1 - t^m + t^m \cdot 1 = 1,$$

lo que concluye la demostración. □

1.5. **Sobre existencia de extensiones donde los polinomios tienen todas sus raíces.**

Si $K \leq \mathbb{C}$ es un cuerpo de números, cualquier $f \in K[x]$ descompone totalmente en $\mathbb{C}$, ya que este es algebraicamente cerrado. Para el caso general, tenemos la siguiente hecho.

Proposición 1.4. *Sea K un cuerpo. Dado cualquier polinomio $f \in K[x]$ de grado ≥ 1, existe un cuerpo E extensión de K en el cual f descompone totalmente.*

Demostración. Hagamos inducción sobre el grado del polinomio en cuestión, $f = \sum_i a_i x^i$. Si el grado es 1, basta tomar $E = K$, pues $a_1 x + a_0 = a_1(x - \frac{-a_0}{a_1})$. Supongamos $\mathrm{gr}(f) \geq 2$, y escojamos $p \in K[x]$ un irreducible tal que $p|f$. Sea $E = K[x]/_p$ el cuerpo extensión de K de classes de congruencias de polinomios en $K[x]$ módulo p, y llamemos $\alpha = \overline{x} \in E$. Entonces,

$$f(\alpha) = \textstyle\sum_i a_i \alpha^i = \sum_i a_i \overline{x}^i = \overline{\sum_i a_i x^i} = \overline{f} = 0,$$

y α es una raíz de f en E. Pongamos $f = (x - \alpha)g$, para un cierto $g \in E[x]$. Como g es de grado menor que el de f, existirá un cuerpo extension F/E en el cual g descompone totalmente. Claramente entonces f descompone totalmente en F. □