Universidad de Cantabria

Facultad de Ciencias

ANTOLOGÍA DE DEMOSTRACIONES DEL TEOREMA FUNDAMENTAL DEL ÁLGEBRA

(Anthology of proofs of the Fundamental Theorem of Algebra)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Luis Aller Vicario

Director: Jesús Javier Jiménez Garrido

Febrero - 2025

Resumen

El objetivo principal del trabajo consiste en elaborar un recopilatorio compacto, lógico y coherente de las distintas demostraciones del Teorema Fundamental del Álgebra, que establece que todo polinomio complejo no constante tiene una raíz compleja. Las pruebas se exponen de menor a mayor complejidad según los prerrequisitos necesarios para comprenderlas. Se presentarán y se compararán las pruebas procedentes de las diferentes ramas de las matemáticas, entre ellas: el cálculo diferencial, el álgebra, la topología, la topología algebraica, la variable compleja y la geometría diferencial.

Palabras clave: Teorema Fundamental del Álgebra, polinomio, números complejos, números reales, axioma del supremo, raíz.

Abstract

The main goal of this work is to elaborate a compact, logical and coherent compilation of the different proofs of the Fundamental Theorem of Algebra, which states that every non constant complex polynomial has a complex root. The demonstrations are presented in increasing order of difficulty, based on the previous requirements needed to understand them. We will present and compare those proofs from the different mathematical branches, amongst them: differential calculus, algebra, topology, algebraic topology, complex analysis and differential geometry.

Key words: Fundamental Theorem of Algebra, polynomial, complex numbers, real numbers, least upper bound axiom, root.

Índice general

Introducción

El teorema que establece que todo polinomio complejo no constante ha de tener una raíz compleja, es un teorema que despertó el interés de muchos matemáticos a lo largo de la historia. Evidentemente, este teorema no siempre fue enunciado así, varios matemáticos conjeturaron e intentaron probar versiones menos maduras del mismo. Entre ellos están: Girard en el S. XVII, d'Alembert, Euler, Lagrange y Laplace en el S. XVIII. Dicho teorema es por supuesto el conocido como Teorema Fundamental del Álgebra (TFA). Sin embargo, no fue hasta 1799 cuando Gauss dio la que es considerada la primera prueba válida de la historia del TFA en su tesis doctoral con tan solo 22 años. Aunque la prueba tenía un hueco, fue posteriormente resuelto en 1920 por Ostrowski [35]. Otros matemáticos dieron demostraciones alternativas a partir de entonces, entre otros: Argand, quien dio la primera prueba completa sin huecos, Cauchy, Weierstrass, etc. Incluso el propio Gauss realizó tres pruebas más, la última siendo muy parecida a la primera. Según se dice en *Numbers* [18], en el año 1907 se hizo una revisión de casi cien pruebas clásicas del TFA. Desde ese momento hasta la actualidad han seguido publicándose nuevas pruebas.

Pese a su nombre, no se trata de un teorema fundamental del álgebra moderna y no pueden existir pruebas puramente algebraicas del mismo dado que su veracidad reside en la estructura del conjunto de los números reales. En concreto, cualquier demostración hace uso de alguna consecuencia más o menos directa del axioma del supremo, que no es un concepto algebraico. Como menciona B. Cipra en su artículo [13], E. Artin y O. Schrier con su teoría sobre los cuerpos real cerrados, mostraron que la noción de continuidad es esencial para cualquier prueba del TFA y así se verá reflejado en las pruebas de este trabajo.

En esta memoria se han detallado una veintena de demostraciones del TFA, con el objetivo de crear un texto compacto que siga un cierto orden lógico y coherente para entender y plasmar las demostraciones elegidas, de menor a mayor dificultad según los conocimientos adquiridos durante el Grado y desde distintas ramas de las matemáticas. Además de los criterios técnicos, las demostraciones elegidas para formar parte de este escrito, son a juicio del autor, las más elegantes, ilustrativas y claras que se han encontrado tras la búsqueda bibliográfica. A lo largo del trabajo, se mencionan algunas demostraciones que han quedado fuera de su estudio en profundidad, unas debido a su similitud con las pruebas propuestas, y otras por su extensión y mayor complejidad. Cada capítulo está dedicado a las demostraciones que usan como principales argumentos los resultados de un mismo área de las matemáticas: álgebra, análisis, topología, topología algebraica y geometría diferencial. Dentro de cada capítulo, las demostraciones también están ordenadas de menor a mayor complejidad según los prerrequisitos necesarios para comprenderlas.

Dar una prueba completa y detallada del TFA que incluya la demostración de todos los resultados previos que se usen, excedería las limitaciones de extensión de la memoria. Por este motivo, cada capítulo comienza con un resumen de los resultados que se van a usar para probar el TFA. Se ha tratado de elaborar los resúmenes de tal modo que el lector acudiendo a las referencias señaladas pueda, si lo desea, reconstruir la demostración del TFA desde cero. Principalmente se han omitido las pruebas de los resultados clásicos que forman parte de los contenidos de las asignaturas del Grado. Destacamos también que en algunas secciones en lugar de probar que todo polinomio complejo no constante tiene una raíz compleja, se ha probado un enunciado equivalente que por simplicidad también se ha denominado TFA.

A continuación describimos brevemente la estructura de la memoria. En el primer capítulo, se dan dos pruebas basadas en el Teorema de Weierstrass y en la nulidad del módulo mínimo de un polinomio empleando la existencia de las raíces $k-$ésimas de los números complejos. En el segundo capítulo, damos tres pruebas basadas en Álgebra: la primera con álgebra lineal y teoría del endomorfismo; en la segunda se usa teoría de cuerpos y polinomios simétricos y en la tercera teoría de Galois. En el tercer capítulo, se dan cuatro pruebas: la primera inspirada en la primera prueba de Gauss; la segunda, utilizando los multiplicadores de Lagrange y las ecuaciones de Cauchy-Riemann; la tercera utilizando el Teorema de la Función Implícita y la conexión de $\mathbb{C}$ menos un conjunto finito de puntos. La cuarta es similar pero emplea el Teorema de la Función Inversa en lugar del Teorema de la Función Implícita. En el cuarto capítulo, veremos tres pruebas: la primera mediante el número de rotación de un lazo; la segunda con la teoría del grado de aplicaciones continuas entre $\mathbb{S}^1$ y $\mathbb{S}^1$ y la tercera con la versión de topología algebraica del Teorema de Rouché. En el quinto capítulo, se dan siete pruebas: la primera aplicando el Teorema Integral de Cauchy; la segunda aplicando el Teorema de Liouville y la tercera una versión de la anterior aplicando el Teorema del Valor Medio Integral; la cuarta emplea el Principio del Mínimo; la quinta usa el Principio del Argumento; la sexta se basa en el Teorema de Rouché y la séptima el Pequeño Teorema de Picard. En el sexto capítulo, se da una prueba con dos variantes, ambas basadas estudiando la curvatura de Gauss de la esfera para una métrica construida a partir de un polinomio.

El libro *The Fundamental Theorem of Algebra* [19] ha servido de esqueleto para elaborar este trabajo.

Notación: A lo largo de la memoria se ha tratado de emplear una notación unificada y, en consecuencia, esta notación en ocasiones difiere de la empleada habitualmente en el área correspondiente. Denotaremos por $\mathbb{N} = \{0, 1, 2, \dots\}$ el conjunto de los números naturales, $\mathbb{Z}$ el conjunto de los números enteros, $\mathbb{Q}$ el conjunto de los números racionales, $\mathbb{R}$ el conjunto de los números reales, $\mathbb{C}$ el conjunto de los números complejos y

$$\mathbb{S}^n = \{x \in \mathbb{R}^n : |x| = 1\}.$$

Dado (X, d) un espacio métrico, $x_0 \in X$ y r un número real positivo, escribimos

$$\begin{aligned} B(x_0, r) &= \{x \in X : d(x, x_0) < r\}, \\ \overline{B}(x_0, r) &= \{x \in X : d(x, x_0) \leq r\}, \\ \partial B(x_0, r) &= \{x \in X : d(x, x_0) = r\}. \end{aligned}$$

Capítulo 1

Pruebas basadas en el Teorema de Weierstrass

En este primer capítulo presentamos dos demostraciones del Teorema Fundamental del Álgebra (TFA) basadas en propiedades elementales de los números reales y complejos y en las propiedades de continuidad y derivabilidad básicas de las funciones polinomiales. A parte de estas propiedades elementales, ambas demostraciones hacen uso del Teorema de Weierstrass (Teorema 1.20), que recordamos que establece que toda función real continua sobre un espacio compacto alcanza su máximo y su mínimo.
Comenzaremos recordando la noción de polinomio con coeficientes en un anillo, presentaremos el cuerpo de los números reales y el cuerpo de los números complejos y concluimos los prerrequisitos con algunas propiedades básicas de las funciones continuas a valores reales. En la última sección se presentan las dos pruebas del TFA que se basan en demostrar que el mínimo del módulo de una función polinomial compleja debe ser cero.

1.1. Polinomios y funciones polinomiales

Para la elaboración de esta sección sobre polinomios hemos seguido como referencia principal el libro de S. Lang [29, Chapter II and IV].

Definición 1.1. *Sea $(A, +, \cdot)$ un anillo conmutativo. Una* ***sucesión de elementos de*** *A es una aplicación $a : \mathbb{N} \to A$. Denotaremos por $a_j := a(j)$ para todo $j \in \mathbb{N}$, en lugar de la notación funcional, representaremos la sucesión a por $(a_j)_{j=0}^{\infty}$ y el conjunto de todas las sucesiones de elementos de A se denota por $A^{\mathbb{N}}$.*

Empleando la noción anterior, podemos definir un polinomio con coeficientes en A como una sucesión de elementos de A que son cero de un lugar en adelante.

Definición 1.2. *Sea $(A, +, \cdot)$ un anillo conmutativo. Decimos que $(a_j)_{j=0}^{\infty} \in A^{\mathbb{N}}$ es un* ***polinomio con coeficientes en*** *A si existe $n \in \mathbb{N}$ tal que $a_j = 0$ para todo $j > n$. Lo denotaremos por*

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$

El conjunto de todos los polinomios con coeficientes en A se denota por $A[X]$. Sobre este conjunto se definen la ***suma*** *y el* ***producto de polinomios*** *del modo usual:*

$$+ : A[X] \times A[X] \to A[X] \qquad \cdot : A[X] \times A[X] \to A[X]$$

$$((a_j)_{j=0}^{\infty}, (b_j)_{j=0}^{\infty}) \to (a_j + b_j)_{j=0}^{\infty} \qquad ((a_j)_{j=0}^{\infty}, (b_j)_{j=0}^{\infty}) \to (c_j)_{j=0}^{\infty}$$

donde para cada $j \in \mathbb{N}$ se tiene que $c_j = \sum_{k=0}^{j} a_k b_{j-k}$.

Proposición 1.3. *Sea $(A, +, \cdot)$ un anillo conmutativo. Entonces se cumple que $(A[X], +, \cdot)$ es un anillo conmutativo.*

Podemos identificar A con el subanillo de los polinomios constantes y podemos definir el **grado de un polinomio**, no nulo, $p(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ como

$$\mathrm{gr}(p(X)) = \text{máx}\{j \in \mathbb{N} : a_j \neq 0\}.$$

Dado un polinomio le podemos asociar una función polinomial.

Definición 1.4. *Sea $p(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ con A un subanillo de un anillo conmutativo B. La **función polinomial** asociada a $p(X)$, $F_p : B \to B$, está definida para cada $x \in B$ por*

$$F_p(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

En general, dos polinomios diferentes pueden definir la misma función polinomial, por ejemplo, en $\mathbb{Z}/2\mathbb{Z}[X]$ $p(X) = X^2 + X$ y $q(X) = 0$ definen la misma función polinomial sobre $\mathbb{Z}/2\mathbb{Z}$. Sin embargo, si el cuerpo sobre el que se definen es infinito, podemos relacionar de manera biunívoca polinomios y funciones polinomiales.

Teorema 1.5. *Sea $(\mathbb{K}, +, \cdot)$ un cuerpo infinito. Dados $p(X), q(X) \in \mathbb{K}[X]$ tales que $F_p = F_q$ entonces $p(X) = q(X)$.*

Concluimos recordando la noción de raíz de un polinomio.

Definición 1.6. *Sean $p(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ con A un subanillo de un anillo conmutativo B y $b \in B$. Decimos que b es **raíz** de $p(X)$ si $F_p(b) = 0$.*

Los polinomios que consideraremos en esta memoria tendrán coeficientes reales o complejos, luego por el Teorema 1.5 podemos identificar un polinomio con su función polinomial asociada. Abusando de la notación representaremos polinomio y función polinomial con la misma letra, escribiendo la variable en mayúsculas en el primer caso y en minúsculas en el segundo para diferenciarlos si fuera necesario.

1.2. El cuerpo de los números reales

Existen diversas construcciones equivalentes de los números reales a partir de los números racionales: mediante números decimales, sucesiones de Cauchy o mediante el método de las cortaduras de Dedekind, etc. Estos procedimientos no son muy complicados, pero sí muy laboriosos, y su presentación detallada alargaría en exceso la longitud de esta memoria. La construcción mediante cortaduras de Dedekind se puede consultar en el libro de W. Rudin [38] que se ha empleado para escribir el resumen de esta sección.

Definición 1.7. *Se llama **recta real** o **conjunto de los números reales** a todo conjunto $\mathbb{R}$ no vacío provisto de dos operaciones $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ y $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ y una relación de orden que cumple:*

1. *$(\mathbb{R}, +, \cdot)$ es un cuerpo.*
2. *$(\mathbb{R}, \leq)$ es un conjunto totalmente ordenado.*
3. *La relación de orden es compatible con la estructura algebraica:*

- *Si* $a, b, c \in \mathbb{R}$ *y* $a \leq b$*, entonces* $a + c \leq b + c$.
- *Si* $a, b, c \in \mathbb{R}$, $a \leq b$ *y* $0 \leq c$*, entonces* $a \cdot c \leq b \cdot c$.
- *Axioma del supremo: Todo subconjunto no vacío de* $\mathbb{R}$ *y acotado superiormente tiene extremo superior en* $\mathbb{R}$.

Cabe destacar que todas las pruebas del TFA se apoyan, directa o indirectamente en el axioma del supremo, que garantiza que el conjunto de los números reales es Dedekind completo. Esto significa que si consideráramos las cortaduras de Dedekind del conjunto de los números reales obtendríamos de nuevo la recta real. De hecho, se puede probar que dos cuerpos ordenados que verifican el axioma del supremo son isomorfos.

Teorema 1.8. *La recta real existe y es única salvo isomorfismos.*

Haciendo uso de estos axiomas, y en particular del axioma del supremo, se pueden probar todas las propiedades básicas tanto aritméticas como de la estructura de orden que tienen los números reales y que emplearemos a lo largo de la memoria. Asimismo, se puede definir el valor absoluto de un número real y se pueden probar las propiedades de la topología usual en $\mathbb{R}$ y $\mathbb{R}^n$. Por su relevancia para los desarrollos de este capítulo destacamos las siguientes:

Proposición 1.9. *Sea* E *un subconjunto de* $\mathbb{R}$ *no vacío y acotado superiormente. Si* $y = \sup E$*, entonces* $y \in \overline{E}$*. Por tanto, si* E *es cerrado,* $y \in E$*. Análogamente se tiene el mismo resultado para el extremo inferior de los conjuntos acotados inferiormente.*

Por otro lado, los conjuntos compactos de $\mathbb{R}^n$ admiten una caracterización sencilla gracias al Teorema de Heine-Borel.

Teorema 1.10. *Sea* $E \subseteq \mathbb{R}^n$*. Son equivalentes:*

1. E *es compacto.*
2. E *es cerrado y acotado.*

1.3. El cuerpo de los números complejos

Del mismo modo que ocurría con los números reales a partir de los racionales, existen varias construcciones equivalentes de los números complejos a partir de los números reales. En este trabajo construiremos los números complejos como pares ordenados de números reales dotados de una estructura algebraica apropiada.

Definición 1.11. *Un* ***número complejo*** *es un par* $z = (a, b)$ *con* $a, b \in \mathbb{R}$*,* a *se denomina la* ***parte real*** *de* z *y se denota por* $a = \Re(z)$ *y* b *se denomina la* ***parte imaginaria*** *de* z *y se denota* $b = \Im(z)$.
El ***conjunto de los números complejos*** *se denota por* $\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$ *y definimos la* ***suma*** *y el* ***producto de números complejos*** *para todos* $z = (a, b)$, $w = (c, d) \in \mathbb{C}$ *por*

1. $z + w = (a, b) + (c, d) := (a + c, b + d)$.
2. $z \cdot w = (a, b) \cdot (c, d) := (ac - bd, ad + bc)$.

Empleando que $(\mathbb{R}, +, \cdot)$ es un cuerpo, probamos que:

Teorema 1.12. $(\mathbb{C}, +, \cdot)$ *es un cuerpo.*

Observamos que cada número complejo $z = (a, b)$ se puede escribir como

$$(a, b) = (a, 0) + (b, 0) = (a, 0) + (b, 0)(0, 1),$$

denotando por $i = (0, 1)$ e identificando cada número real $a \in \mathbb{R}$ con $(a, 0)$, podemos expresar z como $a + bi$. De la manera habitual, definimos el conjugado de un número complejo, su módulo y un argumento de z.

Definición 1.13. *Sea* $z = a + bi \in \mathbb{C}$.

1. *El número complejo* $a - bi$ *se llama* ***conjugado*** *de* z *y se denota por* $\overline{z}$.
2. *El número real positivo* $\sqrt{a^2 + b^2}$, *se denomina* ***módulo*** *de* z *y se denota* $|z|$.
3. *Si* $z \in \mathbb{C}$, $z \neq 0$, *un* ***argumento*** *de* z *es un número real* θ *tal que*

$$\frac{z}{|z|} = (\cos(\theta) + i \operatorname{sen}(\theta)).$$

A partir de estas definiciones se pueden probar las propiedades elementales del módulo y la conjugación compleja que emplearemos a lo largo de la memoria aunque no detallaremos su demostración. De la misma forma, empleando el módulo podemos definir y probar las propiedades de la topología usual en $\mathbb{C}$.
Por otro lado, recordamos la definición de la exponencial y el logaritmo complejos.

Definición 1.14. *Sea* $z = a + bi \in \mathbb{C}$ *con* $a, b \in \mathbb{R}$. *Llamamos* ***exponencial compleja*** *del número* z *a*

$$e^z := e^a(\cos(b) + i \operatorname{sen}(b)).$$

Observamos que si $z \in \mathbb{C}$, $z \neq 0$, y si θ es un argumento de z podemos escribir $z = |z|e^{i\theta}$. Empleando las propiedades de la exponencial real y las propiedades de las funciones trigonométricas se pueden demostrar las propiedades de la exponencial compleja. En concreto, para cada $c \in \mathbb{R}$, la exponencial compleja establece una biyección entre

$$B_c = \{z \in \mathbb{C} : c \leq \Im(z) < c + 2\pi\}$$

y $\mathbb{C} \setminus \{0\}$. Como $E_c : B_c \to \mathbb{C} \setminus \{0\}$ es una biyección $E_c(z) = \exp(z)$ podemos considerar:

Definición 1.15. *La aplicación inversa de* E_c, $E_c^{-1} : \mathbb{C} \setminus \{0\} \to B_c$ *se llama* ***rama o determinación del logaritmo de rango*** B_c. *Cuando* $c = -\pi$, *se denomina rama principal.*

Un cálculo sencillo nos muestra que si $c \in \mathbb{R}$ y $z \in \mathbb{C} \setminus \{0\}$, entonces

$$\log_c(z) = \ln(|z|) + i \arg(z)$$

con $\arg(z)$ el único argumento de z en $[c, c + 2\pi)$.

Observación 1.16. *Se cumple que* $\Re(\log(z)) = \ln(|z|)$.

Un caso particular se obtiene cuando estudiamos las raíces n-ésimas de un número complejo.

Teorema 1.17 (Teorema de De Moivre's para raíces)**.** *Sea* $z \in \mathbb{C}, z \neq 0$, *entonces* z *tiene exactamente* n ***raíces n-ésimas*** *distintas. Si* $z = re^{i\theta}$, *las raíces están dadas por*

$$w_k = r^{1/n} e^{i\frac{\theta + 2\pi k}{n}}, \quad k \in \{0, 1, \ldots, n-1\}.$$

Observación 1.18. *Por el teorema anterior las raíces* $k-$*ésimas de un número complejo de módulo 1, tienen también módulo 1.*

1.4. Propiedades de continuidad y de crecimiento de las funciones polinomiales

Recordamos algunas propiedades clásicas que relacionan continuidad y compacidad, ver [38, Chapter 4].

Teorema 1.19. *Sean (X, d_X), (Y, d_Y) dos espacios métricos y $f : X \to Y$ una aplicación continua. Si X es compacto, entonces $f(X)$ es compacto.*

Empleando que los conjuntos compactos de $\mathbb{R}$ son exactamente los conjuntos cerrados y acotados, ver Teorema 1.10, y que en $\mathbb{R}$ un conjunto cerrado y acotado contiene a su extremo inferior y a su extremo superior Proposición 1.9, concluimos que toda función continua real sobre un compacto alcanza sus extremos:

Teorema 1.20 (Teorema de Weierstrass)**.** *Sea (X, d) un espacio métrico compacto y $f : X \to \mathbb{R}$ una función continua. Si escribimos*

$$M = \sup_{x \in X} f(x) \quad y \quad m = \inf_{x \in X} f(x)$$

entonces existen $p, q \in X$ tal que $f(p) = M$ y $f(q) = m$.

Observación 1.21. *Sea $p(Z) = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_0$ un polinomio real o complejo de grado $n > 0$. Sin pérdida de generalidad, podremos asumir siempre que sea necesario que el polinomio es mónico puesto que las raíces de $p(Z)$ y $p(Z)/a_n$ son las mismas debido a que $\mathbb{R}$ y $\mathbb{C}$ son cuerpos. Si fuera necesario supondremos que $a_0 \neq 0$, porque si el término independiente es igual a cero entonces 0 es raíz del polinomio.*

Proposición 1.22. *Sea $p(Z) \in \mathbb{C}[Z]$. Entonces la función polinomial asociada $p : \mathbb{C} \to \mathbb{C}$ es una función continua.*

Empleando las propiedades elementales de los números complejos, tenemos las siguientes estimaciones que nos indican el orden de crecimiento del módulo de un polinomio.

Lema 1.23 (Lema del crecimiento)**.** *Sea $p(Z) = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_0$ un polinomio complejo con $n > 0$. Entonces existe $R \geq 1$ tal que para todo $z \in \mathbb{C}$ con $|z| \geq R$ se tiene que*

$$\frac{1}{2}|a_n||z|^n \leq |p(z)| \leq 2|a_n||z|^n.$$

En particular, se tiene que $|p(z)| \to \infty$ cuando $|z| \to \infty$.

Las dos demostraciones del TFA de este capítulo se basan en el siguiente lema.

Lema 1.24. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces la función $|p(z)| : \mathbb{C} \to \mathbb{R}$ alcanza un mínimo absoluto en algún punto $z_0 \in \mathbb{C}$.*

Demostración. Por el Lema 1.23, $|p(z)| \to \infty$ cuando $|z| \to \infty$, luego existe $M > 0$ tal que $|p(z)| \geq |a_0|$ para todo $z \in \mathbb{C}$ con $|z| > M$. Por un lado, como $|p(z)| : \overline{B}(0, M) \to \mathbb{R}$ es continua y $\overline{B}(0, M)$ es compacta en $\mathbb{C}$, por el Teorema 1.20, existe $z_0 \in \overline{B}(0, M)$ tal que

$$|p(z)| \geq |p(z_0)|$$

para cada $z \in \overline{B}(0, M)$. Por otro lado, para cada $z \in \mathbb{C}$ con $|z| > M$, se tiene que

$$|p(z)| \geq |a_0| = |p(0)| \geq |p(z_0)|.$$

En conclusión, $z_0 \in \mathbb{C}$ es el mínimo absoluto de $|p(z)|$. $\square$

1.5. Pruebas basadas en la nulidad del módulo mínimo de un polinomio

Según se describe en el libro *Numbers* [18, Part A, Chapter 4], las pruebas de esta sección serían variantes de la prueba de J. R. Argand de 1814. En dicho capítulo del libro nos brindan una demostración basada en la proporcionada por Argand. Otro ejemplo de este tipo de prueba se encuentra en el artículo de F. Terkelsen [42]. Este tipo de pruebas del TFA son consideradas las más cortas y simples.
La primera demostración del TFA que presentamos en este trabajo sigue lo descrito en [19, Chapter 3] y se basa en dos ideas fundamentales, el módulo de todo polinomio complejo alcanza su mínimo absoluto en $\mathbb{C}$, Lema 1.24 y todo polinomio complejo debe anularse en los puntos donde su módulo alcance un mínimo, como muestra el siguiente lema.

Lema 1.25. *Sean $p(Z) \in \mathbb{C}[Z]$ no constante y $z_0 \in \mathbb{C}$. Si $p(z_0) \neq 0$, entonces $|p(z_0)|$ no es el mínimo valor de $|p(z)|$.*

Demostración. Tomamos $p(Z) = a_n Z^n + a_{n-1}Z^{n-1} + \cdots + a_0$ un polinomio complejo de grado $n > 0$ y $z_0 \in \mathbb{C}$ tal que $p(z_0) \neq 0$. Supongamos por reducción al absurdo que $|p(z)|$ alcanza su mínimo en el punto z_0. Si consideramos el polinomio $q(Z) = p(Z + z_0)/p(z_0)$, observamos que $q(z)$ está bien definido y que presenta un mínimo en $z = 0$ debido a que $|p(z + z_0)| \geq |p(z_0)|$ por como hemos definido z_0. Por tanto, para cada $z \in \mathbb{C}$ se tiene que

$$|q(z)| = \frac{|p(z + z_0)|}{|p(z_0)|} \geq \frac{|p(z_0)|}{|p(z_0)|} = 1 = q(0) = |q(0)|.$$

Veamos que 1 no es el mínimo valor de $|q(z)|$. Podemos escribir $q(Z) = b_n Z^n + \cdots + b_k Z^k + 1$, con $b_n \neq 0$ y b_k el coeficiente distinto de cero de menor grado con $1 \leq k < n$. Como todo número complejo admite n raíces $n-$ésimas, se puede considerar $w \in \mathbb{C}$ una raíz $k-$ésima de $-b_k$, o sea, tal que $w^k = -b_k$, $w \neq 0$ porque b_k es distinto de cero. Tomamos ahora $z_r = r/w$ con $r \in (0, 1)$. Evaluando $q(z)$ en z_r vemos que

$$\begin{aligned} q(z_r) &= 1 + b_k \left(\frac{r}{w}\right)^k + \cdots + b_n \left(\frac{r}{w}\right)^n \\ &= 1 + b_k \frac{r^k}{-b_k} + r^{k+1}\left(b_{k+1}\frac{1}{w^{k+1}} + \cdots + b_n \frac{r^{n-k-1}}{w^n}\right) = 1 - r^k + r^{k+1} g(r), \end{aligned}$$

donde $g(r)$ es la función polinomial en r situada entre paréntesis en el tercer miembro de la igualdad. Haciendo uso de la desigualdad triangular tenemos que

$$|q(z_r)| = |1 - r^k + r^{k+1} g(r)| \leq |1 - r^k| + r^{k+1}|g(r)|.$$

Como $r^k < 1$ porque $r < 1$, concluimos que

$$|q(z_r)| \leq 1 - r^k + r^{k+1}|g(r)| = 1 - r^k(1 - r|g(r)|).$$

Como $r|g(r)| \to 0$ cuando $r \to 0$, podemos tomar r tan pequeño como haga falta para conseguir que $r|g(r)| < 1$. De esta manera, se ha encontrado un $z_r = r/w$, con $0 < r < 1$ tal que $|q(z_r)| < 1$, pero previamente hemos visto que $|q(z)|$ tenía un mínimo en $z = 0$ donde valía 1. Luego $z = 0$ no es el mínimo de $|q(z)|$ y, consecuentemente, $|p(z)|$ no alcanza su mínimo en z_0. □

Podemos dar una demostración alternativa del Lema 1.25 basada en el desarrollo en serie de Taylor de un polinomio. La idea de esta variante se encuentra en el artículo T.W. Körner [28]. Juntando la información de los Lemas 1.24 y 1.25 obtenemos la primera demostración del Teorema Fundamental del Álgebra.

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Del Lema 1.24 se deduce que $|p(z)|$ alcanza el mínimo en algún punto $z_0 \in \mathbb{C}$. Entonces por el Lema 1.25 se tiene que $|p(z_0)| = 0$, luego $p(z_0) = 0$. De esta forma, $p(Z)$ tiene una raíz compleja. □

Aunque la segunda prueba de esta sección emplea también el Lema 1.24, en lugar de razonar por reducción al absurdo y suponer que $|p|$ no se anula en el mínimo y llegar a una contradicción, se prueba directamente que $|p|$ se anula en el mínimo empleando las propiedades de los números complejos. Esta prueba se encuentra en el artículo de O. R. B. de Oliveira [34].

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z)$ un polinomio complejo de grado $n > 0$. Sabemos que $|p(z)|$ alcanza el mínimo por el Lema 1.24. Mediante una traslación, como en la demostración del Lema 1.25 podemos suponer que $z_0 = 0$. Consideramos $\mathbb{S}^1 = \{w \in \mathbb{C} : |w| = 1\}$, notemos que podemos expresar cualquier número complejo no nulo como $z = rw$ con $r > 0$ y $w \in \mathbb{S}^1$. Como $z_0 = 0$ es el mínimo, para todo $r > 0$ y todo $w \in \mathbb{S}^1$ se cumple que $|p(0)| \leq |p(rw)|$, luego

$$|p(rw)|^2 - |p(0)|^2 \geq 0$$

Como $p(Z)$ no es constante podemos escribir $p(z) = p(0) + z^k q(z)$ con $k \in \{1, \dots, n\}$ y $q(z)$ un polinomio tal que $q(0) \neq 0$. Sustituyendo esta expresión en la desigualdad y tomando $z = rw$ llegamos a que

$$|p(0) + (rw)^k q(rw)|^2 - |p(0)|^2 \geq 0.$$

Haciendo uso de las propiedades del módulo y la conjugación compleja observamos que

$$|p(0) + (rw)^k q(rw)|^2 - |p(0)|^2 = 2r^k \Re(\overline{p(0)} w^k q(rw)) + r^{2k} |w^k q(rk)|^2 \geq 0.$$

Dividiendo entre $r^k > 0$, para cada $r > 0$ y cada $w \in \mathbb{S}^1$ se tiene que

$$2\Re(\overline{p(0)} w^k q(rw)) + r^k |w^k q(rk)|^2 \geq 0.$$

Tomando límite cuando $r \to 0$, para cada $w \in \mathbb{S}^1$ tenemos que

$$2\Re(\overline{p(0)} q(0) w^k)) \geq 0.$$

Llamamos $\alpha = \overline{p(0)} q(0) = a + bi$. Veamos que la desigualdad implica que $\alpha = 0$. Sabemos por la Observación 1.18 que las raíces $k-$ésimas de un elemento de $\mathbb{S}^1$ están en $\mathbb{S}^1$. De tal forma que como la desigualdad anterior es cierta para todo punto de la circunferencia, podemos tomar las $k-$ésimas raíces de los números de la circunferencia que nos interesen:

- Tomando $w = 1$ se tiene que $2\Re(\alpha 1^k) \geq 0$, entonces $a \geq 0$.
- Tomando una $k-$ésima raíz de -1 tenemos que $2\Re(\alpha(-1)) \geq 0$, entonces $a \leq 0$.
- Tomando una $k-$ésima raíz de i tenemos que $2\Re((a + bi)i) \geq 0$, entonces $b \leq 0$.
- Tomando una $k-$ésima raíz de $-i$ tenemos que $2\Re((a+bi)(-i)) \geq 0$, entonces $b \geq 0$.

Por lo que $a = b = 0$ y, por tanto, $\alpha = 0$. Pero $0 = \alpha = \overline{p(0)} q(0)$ y habíamos dicho que $q(0) \neq 0$ por lo que $\overline{p(0)} = 0$ y concluimos que $p(0) = 0$. □

Capítulo 2

Pruebas basadas en Álgebra

En este segundo capítulo vamos a presentar tres pruebas del teorema fundamental del Álgebra, la primera de ellas basada en Álgebra lineal, la segunda emplea algunos resultados elementales de teoría de cuerpos y de los polinomios simétricos y, por último, se presenta una prueba basada en Teoría de Galois. Las tres pruebas del TFA presentadas en este capítulo se realizan por inducción y sólo necesitamos hacer uso de un resultado de cálculo diferencial que se obtiene como consecuencia del Teorema de Bolzano: todo polinomio real de grado impar tiene una raíz real. Comenzamos presentando los prerrequisitos necesarios para realizar cada una de las demostraciones.

2.1. Continuidad y conexión

Al igual que en la Sección 1.4 se ha empleado [38] para elaborar este resumen sobre continuidad y conexión. A partir de los axiomas del cuerpo de los números reales podemos probar, empleando la Proposición 1.9, la siguiente caracterización de los conjuntos conexos de $\mathbb{R}$.

Teorema 2.1. *Sea $E \subseteq \mathbb{R}$. Entonces E es conexo si y sólo si tiene la siguiente propiedad:*

$$\text{Si } x, y \in E \text{ y } x < z < y, \text{ entonces } z \in E.$$

Recordamos el teorema que describe la imagen de un conexo por una aplicación continua.

Teorema 2.2. *Sean (X, d_X) e (Y, d_Y) dos espacios métricos y $f : X \to Y$ una aplicación continua. Si $E \subseteq X$ es conexo, entonces $f(E)$ es conexo.*

De los Teoremas 2.1 y 2.2 se deduce el Teorema de Bolzano.

Teorema 2.3 (Teorema de Bolzano)**.** *Sea $f : [a, b] \to \mathbb{R}$ una función continua en $[a, b]$ y tal que $f(a)f(b) < 0$. Entonces, existe al menos un $c \in (a, b)$ tal que $f(c) = 0$.*

Dado $p(X) \in \mathbb{R}[X]$ un polinomio de grado impar, tenemos que o bien $p(x) \to \infty$ cuando $x \to \infty$ y $p(x) \to -\infty$ cuando $x \to -\infty$ o bien $p(x) \to -\infty$ cuando $x \to \infty$ y $p(x) \to \infty$ cuando $x \to -\infty$. Empleando el Teorema de Bolzano deducimos que

Teorema 2.4. *Todo polinomio real de grado impar tiene una raíz real.*

2.2. Matrices simétricas, matrices hermíticas y endomorfismos sobre espacios vectoriales de dimensión impar

Comenzamos demostrando un par de resultados del álgebra lineal que serán imprescindibles para la prueba de la Sección 2.6. Estos resultados se encuentran en el artículo de K. Conrad [14].

Definición 2.5. *Llamamos conjunto de* ***matrices simétricas*** *con entradas en* $\mathbb{C}$ *al conjunto* $\mathcal{S}_n(\mathbb{C}) = \{M \in Mat_{n\times n}(\mathbb{C}) : M^T = M\}$.

Teorema 2.6. *El conjunto* $\mathcal{S}_n(\mathbb{C})$ *es un* $\mathbb{C}-$*espacio vectorial con dimensión* $n(n+1)/2$.

Definición 2.7. *Llamamos conjunto de las* ***matrices hermíticas*** *al conjunto* $\mathcal{H}_n = \{M \in Mat_{n\times n}(\mathbb{C})\ : M^* = M\}$ *donde* $M^* = \overline{M}^T$ *denota la matriz conjugada y traspuesta de* M.

Teorema 2.8. *El conjunto* $\mathcal{H}_n$ *forma un* $\mathbb{R}-$*espacio vectorial de dimensión* n^2.

Lema 2.9. *Sea* $m > 1$ *un entero. Supongamos que para todo* $F-$*espacio vectorial* V *cuya dimensión no es divisible por* m *y todo endomorfismo* ϕ *en* V*, se cumple que* ϕ *tiene un vector propio en* V*. Entonces para todo* $F-$*espacio vectorial* V *cuya dimensión no es divisible por* m *y cada par de endomorfismos en* V *que conmutan, se cumple que tienen un vector propio común en* V.

Demostración. Razonamos por inducción sobre la dimensión d del espacio vectorial, haciendo que d recorra los enteros que no son divisibles por m.
En el caso base $d = 1$ tenemos que V es un espacio vectorial de dimensión 1, que no es divisible por $m > 1$. Un vector no nulo en un espacio vectorial unidimensional es un vector propio de cualquier endomorfismo en V. Se comprueba directamente que dos endomorfismos que conmutan tienen un vector propio en común, basta tomar cualquier vector no nulo.
Supongamos ahora que $d > 1$ no es divisible por m y que la propiedad se cumple para todo $d' < d$ con d' no divisible por m. Tomamos A_1 y A_2 endomorfismos que conmutan en un F-espacio vectorial V de dimensión d. Como d no es divisible por m, la hipótesis del lema nos dice que A_1 tiene un valor propio $\lambda \in F$. Definimos:

$$U = \mathrm{Im}(A_1 - \lambda Id), \quad W = \mathrm{Ker}(A_1 - \lambda Id).$$

Se comprueba que los subespacios U y W de V son invariantes por A_1. Notemos que $\dim_F W \geq 1$ puesto que λ es un valor propio de A_1. Veamos que U y W también son invariantes por A_2 aplicando que conmutan. Dado $u \in U$, podemos escribir $u = A_1(v) - \lambda v$ para algún $v \in V$. Entonces, se cumple que

$$A_2(u) = A_2(A_1(v)) - A_2(\lambda v) = A_1(A_2(v)) - \lambda(A_2(v)) = (A_1 - \lambda Id)(A_2(v))$$

que también pertenece a U. Dado $w \in W$ tenemos que $A_1(w) = \lambda w$, operando a la izquierda con A_2 y aplicando que conmutan obtenemos que

$$A_1(A_2(w)) = A_2(A_1(w)) = A_2(\lambda w) = \lambda(A_2(w)),$$

entonces $A_2(w) \in W$. De esta manera podemos considerar los endomorfismos

$$A_1|_U : U \to U, \quad A_1|_W : W \to W, \quad A_2|_U : U \to U, \quad A_2|_W : W \to W.$$

Por la fórmula de las dimensiones tenemos que $\dim_F U + \dim_F W = d$ que no es divisible por m. Por lo que U o W tienen una dimensión no divisible por m. Si el subespacio W es un subespacio propio de V entonces U también lo es, entonces aplicando la hipótesis de inducción se cumple que $A_1|_U$ y $A_2|_U$ o $A_1|_W$ y $A_2|_W$ tienen un vector propio común en ese subespacio y por lo tanto en V.
El otro caso es que los subespacios U y W sean uno todo V y otro $\{0\}$. Hemos visto previamente que $\dim_F W$ es positivo, luego sólo puede suceder que $W = V$. Pero por construcción de $W = \mathrm{Ker}(A_1 - \lambda Id)$, esto significa que todo vector de V es un vector propio de A_1. Por la hipótesis del lema A_2, tendrá un vector propio en V, así que A_1 y A_2 tendrán al menos ese vector propio en común. $\square$

Corolario 2.10. *Sea V un $\mathbb{R}-$espacio vectorial de dimensión impar, cada pareja de endomorfismos de V que conmutan, tienen un vector propio en común en V.*

Demostración. Cualquier endomorfismo en un espacio vectorial V real de dimensión impar tiene un vector propio en V puesto que su polinomio característico tiene grado impar y, por lo tanto, por el Teorema 2.4 tiene una raíz real, que es un valor propio real. Cualquier valor propio real conduce a un vector propio real. Si tomamos $F = \mathbb{R}$ y $m = 2$, del Lema 2.9 deducimos que toda pareja de endomorfismos que conmutan tienen un vector propio en común en V. $\square$

2.3. El dominio euclídeo de los polinomios en una variable con coeficientes en un cuerpo

Para realizar los prerrequisitos han servido las fuentes: *Algebra* [5, Chapter 11 and 12] y [19, Chapter 3]. Comenzamos recordando algunas propiedades elementales de los anillos.

Proposición 2.11. *Sean R un anillo conmutativo e I un ideal de R entonces R/I es cuerpo si y solo si I es un ideal maximal.*

Definición 2.12. *Sea D un dominio. Decimos que d es una* ***unidad*** *si tiene inverso para el producto. Sea $a \in D \setminus \{0\}$ que no es unidad, decimos que a es* ***irreducible*** *si se cumple que si $a = bc$ entonces b es una unidad o c es una unidad.*

Definición 2.13. *Sea D un dominio. Decimos que D es un* ***dominio de ideales principales (D.I.P.)*** *cuando todo ideal de D es principal, es decir, todo ideal está generado por un elemento.*

Proposición 2.14. *Sean D un D.I.P. y a un elemento de D que no sea unidad y distinto de cero. Entonces a es irreducible si y solo si el ideal generado por a que denotamos $\langle a \rangle$ es maximal.*

Definición 2.15. *Sea D un dominio. Decimos que D es un* ***dominio euclídeo*** *si existe una aplicación $\delta : D \setminus \{0\} \to \mathbb{N}$ tal que*

1. *Para todos $a, b \in D \setminus \{0\}$ se tiene que $\delta(a) \leq \delta(ab)$.*

2. *Para todos $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ tales que $a = bq + r$ con $\delta(r) < \delta(b)$ o $r = 0$.*

Proposición 2.16. *Todo dominio euclídeo es dominio de ideales principales.*

Proposición 2.17. *Sean D un dominio, $p(X), q(X) \in D[X]$ dos polinomios no nulos con $p(X) \cdot q(X) \neq 0$. Entonces,*

$$\operatorname{gr}(p(X) \cdot q(X)) = \operatorname{gr}(p(X)) + \operatorname{gr}(q(X)).$$

Teorema 2.18. *Sean D un dominio, $a(X), b(X) \in D[X]$ dos polinomios tal que el coeficiente de mayor grado de $b(X)$ es una unidad en D. Entonces, existen únicos $q(X), r(X) \in D[X]$ tales que*

$$a(X) = b(X) \cdot q(X) + r(X),$$

con $\operatorname{gr}(r(X)) < \operatorname{gr}(b(X))$ o $r(X) = 0$.

Como consecuencia el anillo de polinomios con coeficientes en un cuerpo es un dominio euclídeo.

Corolario 2.19. *Sea F un cuerpo. Entonces $F[X]$ es un dominio euclídeo para la aplicación $\delta(p(X)) = \operatorname{gr}(p(X))$.*

Las raíces de un polinomio están relacionadas con su descomposición en factores.

Teorema 2.20 (del Resto)**.** *Sean D un dominio, $a \in D$ y $p(X) \in D[X]$. Entonces se cumple que*

1. *$p(a)$ es el resto de dividir $p(X)$ entre $X - a$.*
2. *a es una raíz de $p(X)$ si y solo si existe $q(X) \in D[X]$ tal que $p(X) = (X - a)q(X)$.*

Definición 2.21. *Sean D y D' dominios con D subanillo de D' $a \in D[X]$ y $p(X) \in D[X]$, no nulo, tal que $p(a) = 0$. Llamamos **multiplicidad de a** como raíz de $p(X)$ al valor*

$$m = \max\{k \in \mathbb{N}_{\geq 1} : (X - a)^k \mid p(X) \quad \text{en} \quad D'[X]\}.$$

*Si $m = 1$, diremos que la raíz es **simple**.*

Proposición 2.22. *Sean D un dominio y $p(X) \in D[X]$ no nulo. Entonces $p(X)$ tiene a lo sumo $\operatorname{gr}(p(X))$ raíces en D contadas con su multiplicidad.*

Corolario 2.23. *Un polinomio irreducible de $F[X]$ de grado mayor que 1 no tiene raíces en F.*

Como $\mathbb{C}$ es un cuerpo podemos aplicar estos resultados. En concreto, tenemos que $\mathbb{C}[Z]$ es dominio euclídeo, por el Corolario 2.19 y un dominio de ideales principales por la Proposición 2.16. Por tanto, gracias a las Proposiciones 2.11 y 2.14, tenemos la siguiente observación:

Observación 2.24. *Sea $p(Z)$ un polinomio irreducible en $\mathbb{C}[Z]$ entonces $\mathbb{C}[Z]/\langle(p(Z))\rangle$ es un cuerpo.*

Observación 2.25. *En consecuencia, demostrar el TFA equivale a demostrar que un polinomio de $\mathbb{C}[Z]$ es irreducible si y solo si tiene grado uno.*

Empleando la fórmula cuadrática y que todo número complejo tiene una raíz cuadrada, podemos demostrar que los polinomios complejos de grado dos no son irreducibles.

Lema 2.26. *Todo polinomio complejo de grado dos tiene una raíz compleja.*

Concluimos la sección con algunas propiedades del polinomio conjugado.

Definición 2.27. *Sea $p(Z) = a_nZ^n + \cdots + a_0$ un polinomio complejo, su* ***polinomio conjugado*** *se define como $\overline{p}(Z) = \overline{a_n}Z^n + \cdots + \overline{a_0}$. Dicho de otro modo, el conjugado de $p(Z)$ es el polinomio cuyos coeficientes son los conjugados de los coeficientes de $p(Z)$.*

Lema 2.28. *Sean $p(Z), q(Z) \in \mathbb{C}[Z]$, entonces si $p(Z)q(Z) = h(Z)$ entonces se cumple que $\overline{h}(Z) = \overline{p}(Z)\overline{q}(Z)$*

El siguiente teorema nos muestra que para probar el TFA nos basta con probar que todo polinomio real no constante tiene una raíz compleja.

Teorema 2.29. *Si todo polinomio real no constante tiene una raíz (compleja), entonces todo polinomio complejo no constante tiene una raíz (compleja).*

Demostración. Tomamos un polinomio complejo $p(Z) = a_0 + \cdots + a_nZ^n$ no constante y consideramos su producto con su conjugado, se tiene que $f(Z) = p(Z)\overline{p}(Z) \in \mathbb{R}[Z]$, porque haciendo uso del Lema 2.28 tenemos que

$$\overline{f}(Z) = \overline{p}(Z)\overline{\overline{p}}(Z) = \overline{p}(Z)p(Z) = f(Z).$$

Supongamos que existe z_0 raíz de $f(Z)$. Entonces $p(z_0)\overline{p}(z_0) = 0$, como $\mathbb{C}$ es un dominio, entonces $p(z_0) = 0$ o $\overline{p}(z_0) = 0$. En el segundo caso tenemos que

$$p(\overline{z_0}) = a_0 + \cdots + a_n\overline{z_0^n} = \overline{\overline{a_0}} + \cdots + \overline{\overline{a_n}z_0^n} = \overline{\overline{p}(z_0)} = \overline{0} = 0.$$

En ambos casos encontramos una raíz de p, z_0 en el primero y $\overline{z_0}$ en el segundo. □

2.4. Extensiones de cuerpos

A continuación desarrollamos la teoría de cuerpos que nos hará falta para la demostración de la Sección 2.7. En lo que resta de capítulo F denotará un cuerpo cualquiera. Como referencia de esta sección hemos seguido [19, Chapter 6].

Definición 2.30. *Sean F y F' cuerpos tales que F es un subcuerpo de F' . Decimos que F' es una* ***extensión*** *de F.*

Observación 2.31. *F' es un espacio vectorial sobre F.*

Definición 2.32. *Sea F' una extensión de F. Llamamos* ***grado de la extensión*** *a la dimensión de F' sobre F como espacio vectorial. El grado se denota $|F' : F|$. Si el grado es finito, o sea, F' es un espacio vectorial finito sobre F, entonces decimos que F' es una* ***extensión finita*** *de F.*

Observación 2.33. *Se cumple que $\mathbb{C}$ es una extensión finita de $\mathbb{R}$.*

Lema 2.34. *Sean $F \subseteq F' \subseteq F''$ cuerpos y F'' una extensión finita sobre F, entonces $|F' : F|$ y $|F'' : F'|$ también son finitos y $|F'' : F| = |F'' : F'||F' : F|$.*

En las condiciones del lema anterior decimos que F' es un **cuerpo intermedio.**

Definición 2.35. *Sean F' una extensión de F y $\alpha \in F'$. Se dice que α es un elemento* ***algebraico sobre F*** *si existe un polinomio $p(X) \in F[X]$ distinto de cero tal que $p(\alpha) = 0$. O sea, si α es una raíz de un polinomio con coeficientes en F.*
Si todo elemento de F' es algebraico sobre F, entonces F' es una ***extensión algebraica*** *de F.*

Teorema 2.36. *Sea F' una extensión finita de F, entonces F' es una extensión algebraica de F.*

Observación 2.37. *Se cumple que $\mathbb{C}$ es algebraico sobre $\mathbb{R}$.*

Teorema 2.38. *Sea $\alpha \in F'$ algebraico sobre F, entonces existe un único polinomio mónico e irreducible $p(X)$ tal que $p(\alpha) = 0$. Este polinomio se denota por $m_{\alpha,F}(X)$.*

Definición 2.39. *Sean F' una extensión de F, $\alpha \in F'$ algebraica sobre F y $p(X) = m_{\alpha,F}(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$. Denotamos por $F(\alpha)$ a* ***la extensión de F más pequeña que contiene*** *α y se comprueba que*

$$F(\alpha) = \{f_0 + f_1\alpha + \cdots + f_{n-1}\alpha^{n-1} : f_i \in F\}.$$

Teorema 2.40. *Sea F' una extensión de F y $\alpha \in F'$ algebraico sobre F, entonces $F(\alpha)$ forma una extensión algebraica finita de F con $|F(\alpha) : F| = \mathrm{gr}(m_{\alpha,F}(X))$ y además $F(\alpha)$ es el subcuerpo más pequeño de F' que contiene a α.*
A una extensión de la forma $F(\alpha)$ para algún α se la denomina una ***extensión simple*** *de F.*

Definición 2.41. *Sean $p(X) \in F[X]$ distinto de cero y F' una extensión de F. Entonces $p(X)$* ***escinde*** *en F' si $p(X)$ se factoriza en factores lineales en $F'[X]$. Lo que significa que todas las raíces de $p(X)$ están en F'.*
Decimos que F' es un ***cuerpo de escisión de p(X) sobre F*** *si F' es la extensión de F más pequeña en la que p(X) escinde.*

Teorema 2.42. *Sea $p(X) \in F[X]$ distinto de cero. Entonces existe un cuerpo de escisión para p(X) sobre F.*

Definición 2.43. *Se dice que F es* ***algebraicamente cerrado*** *si todo polinomio no constante de F[X] tiene una raíz en F. O equivalentemente, si todo polinomio no constante de $F[X]$ escinde completamente en $F[X]$.*

Definición 2.44. *Sea F' una extensión de F, decimos que F' es la* ***clausura algebraica*** *de F si F' es algebraico sobre F y F' es algebraicamente cerrado.*

Observación 2.45. *En este lenguaje, el Teorema Fundamental del Álgebra es equivalente a decir que $\mathbb{C}$ es un cuerpo algebraicamente cerrado.*

Definición 2.46. *Sean $Y_1, Y_2, \ldots, Y_n$ indeterminadas sobre F. Decimos que un polinomio $p(Y_1, Y_2, \ldots, Y_n) \in F[Y_1, Y_2, \ldots, Y_n]$ es un* ***polinomio simétrico en*** *$Y_1, Y_2, \ldots, Y_n$ si $p(Y_1, Y_2, \ldots, Y_n)$ no cambia bajo cualquier permutación σ de $\{Y_1, Y_2, \ldots, Y_n\}$. En otras palabras, para cada $\sigma \in S_n$ se tiene que $p(Y_1, Y_2, \ldots, Y_n) = p(\sigma(1), \sigma(2), \ldots, \sigma(n))$.*
Sean F' una extensión de F y $\alpha_1, \ldots, \alpha_n \in F'$, decimos que un polinomio $p(\alpha_1, \ldots, \alpha_n)$ con coeficientes en F es ***simétrico en*** *$\alpha_1, \ldots, \alpha_n$ si $p(\alpha_1, \ldots, \alpha_n)$ no cambia bajo cualquier permutación σ de $\{\alpha_1, \ldots, \alpha_n\}$.*

Definición 2.47. *Sean $X, Y_1, \ldots, Y_n$ indeterminadas sobre un cuerpo F o elementos de una extensión F' de F. Consideramos el polinomio*

$$p(X, Y_1, \ldots, Y_n) = (X - Y_1) \ldots (X - Y_n).$$

Para cada $i \in \{1, \ldots, n\}$ el polinomio

$$s_i(Y_1, \ldots, Y_n) = (-1)^i a_i(Y_1, \ldots, Y_n),$$

donde a_i es el coeficiente de X^{n-i} en el polinomio $p(X, Y_1, \ldots, Y_n)$, se denomina ***i-ésimo polinomio simétrico elemental****.*

Teorema 2.48 (Teorema Fundamental de los polinomios simétricos)**.** *Sea p un polinomio simétrico en las indeterminadas $Y_1, \ldots, Y_n$ sobre F, entonces existe un único $g \in F[Y_1, \ldots, Y_n]$ tal que $p(Y_1, \ldots, Y_n) = g(s_1, \ldots, s_n)$. Es decir, todo polinomio simétrico en $Y_1, \ldots, Y_n$ se puede expresar como un polinomio en los polinomios simétricos elementales $s_1, \ldots, s_n$.*

La demostración de este teorema se hace por inducción en el grado del mayor monomio con orden lexicográfico y se encuentra en [19, Chapter 6].

Lema 2.49. *Sea $p(X) \in F[X]$ supongamos que $p(X)$ tiene como raíces a $\alpha_1, \ldots, \alpha_n$ en el cuerpo de escisión F'. Entonces, los polinomios simétricos elementales en $\alpha_1, \ldots, \alpha_n$ pertenecen a F.*

Lema 2.50. *Sea $p(X) \in F[X]$ y sus raíces $\alpha_1, \ldots, \alpha_n$ en su cuerpo de escisión F'. Si $g(X) = g(X, \alpha_1, \ldots, \alpha_n) \in F'[X]$ y $g(X)$ es un polinomio simétrico en $\alpha_1, \ldots, \alpha_n$, entonces $g(X) \in F[X]$.*

Demostración. Si $g(X) = g(X, \alpha_1, \ldots, \alpha_n)$ es simétrico en $\alpha_1, \ldots, \alpha_n$, entonces por el Teorema 2.48 es un polinomio simétrico en los polinomios simétricos elementales en $\alpha_1, \ldots, \alpha_n$. Del Lema 2.49 estos están en F, luego los coeficientes de $g(X)$ están en F y por tanto $g(X) \in F[X]$. $\square$

2.5. Teoría de Galois

Seguimos ahora con la teoría de Galois necesaria para la prueba de la Sección 2.8. Como referencia de esta sección hemos seguido [19, Chapter 7]. Comenzamos recordando el primer Teorema de Sylow.

Definición 2.51. *Sea G un grupo y p un número primo, si todo elemento de G tiene orden de una potencia de p entonces decimos que G es un* ***p-grupo****. Si G es finito implica que $|G| = p^n$ para algún n natural.*

Lema 2.52. *Si G es un p-grupo finito de orden p^n, entonces G tiene un subgrupo de orden p^{n-1} y por tanto con índice p.*

Definición 2.53. *Sea G un grupo finito tal que $|G| = p^m\alpha$, con p un número primo y m.c.d.$(p, \alpha) = 1$. Entonces un subgrupo de G de orden p^m se llama* ***subgrupo p-Sylow*** *(que es un p-subgrupo maximal de G).*

Teorema 2.54 (Teorema de Sylow)**.** *Sea G un grupo finito de orden $p^m\alpha$, con p primo y* $\mathrm{m.c.d.}(p, \alpha) = 1$. *Entonces G tiene un subgrupo $p-Sylow$.*

En lo que sigue las extensiones con las que se va a trabajar son extensiones finitas.

Definición 2.55. *Sea K una extensión finita de F. Si K es el cuerpo de escisión sobre F de una familia de polinomios, entonces K se dice que es una* ***extensión normal*** *de F.*

Definición 2.56. *Decimos que α es* ***separable sobre F*** *si α es una raíz simple de $m_{\alpha,F}(X)$. Si todos los elementos de K son separables sobre F, diremos que K es una* ***extensión separable*** *de F.*

Teorema 2.57. *Si F' es una extensión de F con característica 0, entonces F' es una extensión separable de F.*

Observación 2.58. *Cualquier extensión de* $\mathbb{Q}, \mathbb{R}$ *o* $\mathbb{C}$ *es separable.*

Teorema 2.59. *Sea* K *una extensión finita separable de* F*. Entonces el número de automorfismos de* K *que fijan los elementos de* F *es finito e igual a* $|K : F|$*.*

Teorema 2.60. *Sea* K *una extensión finita separable de* F*. Entonces* K *es una extensión simple de* F*. Por tanto puede escribirse* $K = F(\alpha)$ *para algún* $\alpha \in K$*.*

Definición 2.61. *Sea* K *una extensión de* F*. Decimos que* K *es una* ***extensión de Galois*** *si* K *es una extensión finita, separable y normal de* F*. Dicho de otro modo, un cuerpo de escisión finito y separable sobre* F*.*

Observación 2.62. *Si* F *tiene característica 0, una extensión suya de Galois no es más que una extensión finita que es cuerpo de escisión sobre* F*.*

Definición 2.63. *Sea* K *una extensión de Galois de* F*. El grupo de automorfismos de* K *que fijan los elementos de* F *es el* ***grupo de Galois*** *de* K *sobre* F *y lo denotamos Gal(K/F). Si* H *es un subgrupo de Gal(K/F) entonces* K^H *denota los elementos de* K *fijados por* H*.*

Lema 2.64. *Sea* K *una extensión de Galois de* F *entonces* $|Gal(K/F)| = |K : F|$*.*

Teorema 2.65. *Sean* $F \subseteq E \subseteq K$ *con* K *extensión de Galois sobre* F*. Entonces*

1. K *es de Galois sobre* E *y* $Gal(K/E)$ *es un subgrupo de* $Gal(F/K)$*.*

2. *Si* H *es un subgrupo de* $Gal(F/K)$*, entonces* K^H *es un cuerpo intermedio y se cumple que* $Gal(K/K^H) = H$*.*

2.6. Prueba usando Álgebra Lineal

Habitualmente en los cursos de Álgebra Lineal se emplea el Teorema Fundamental del Álgebra para probar que todo endomorfismo sobre $\mathbb{C}^n$ tiene un vector propio. La idea de la prueba que describimos a continuación es demostrar que ambos resultados son equivalentes, es decir, emplear que todo endomorfismo sobre $\mathbb{C}^n$ tiene un vector propio para deducir que se cumple el Teorema Fundamental del Álgebra. Esta prueba se encuentra en [14], que es una ligera modificación de la prueba del artículo de H. Derksen [17].

Teorema 2.66. *Sea* $A \in Mat_{n\times n}(\mathbb{C})$*. Entonces* A *tiene un vector propio en* $\mathbb{C}^n$*.*

Demostración. Realizamos la demostración por inducción en la mayor potencia de 2 que divida a n. Escribimos $n = 2^k n'$ con $k \geq 0$ y n' es impar, hacemos inducción sobre k.
En el caso base $k = 0$, tenemos que $n = n'$ es impar. Para ver que A tiene un vector propio en $\mathbb{C}^n$, vamos a asociar a A un endomorfismo del espacio $\mathcal{H}_n$. Por el Teorema 2.8, tenemos que $\mathcal{H}_n$ tiene dimensión n^2 sobre $\mathbb{R}$ que, en este caso, es impar porque es el cuadrado de un número impar.
Por otro lado observamos que toda matriz $C \in Mat_{n\times n}(\mathbb{C})$ puede descomponerse como

$$C = \frac{C + C^*}{2} + i\frac{C - C^*}{2i}$$

donde $(C+C^*)/2$ y $(C-C^*)/2i$ son matrices hermíticas. Dada $B \in \mathcal{H}_n$ tomamos $C = AB$ y la expresión resultante es

$$AB = \frac{AB + (AB)^*}{2} + i\frac{AB - (AB)^*}{2i} = \frac{AB + BA^*}{2} + i\frac{AB - BA^*}{2i}.$$

Si consideramos los $\mathbb{R}$-endomorfismos $L_1, L_2 : \mathcal{H}_n \to \mathcal{H}_n$ definidos de la forma

$$L_1(B) = \frac{AB + BA^*}{2}, \qquad L_2(B) = \frac{AB - BA^*}{2i}.$$

Se comprueba de forma directa que L_1 y L_2 conmutan. Como $\mathcal{H}_n$ tenía dimensión impar, por el Corolario 2.10 podemos afirmar que existe una matriz $\hat{B} \neq 0$ tal que $L_1(\hat{B}) = \lambda_1 \hat{B}$ y $L_2(\hat{B}) = \lambda_2 \hat{B}$ con $\lambda_1, \lambda_2 \in \mathbb{R}$. Luego $A\hat{B} = L_1(\hat{B}) + iL_2(\hat{B}) = (\lambda_1 + i\lambda_2)\hat{B}$.
Por tanto, cualquier vector columna distinto de cero de $\hat{B}$ es un vector propio en $\mathbb{C}^n$ de A y concluimos que se cumple el caso base.
Supongamos que para un cierto $k \geq 1$ el resultado se cumple, es decir, que dada $A \in Mat_{n\times n}(\mathbb{C})$ con $d \geq 1$ tal que 2^k no divide a d, tenemos que existe un vector propio de A. Observamos que esta hipótesis de inducción es justo la hipótesis del Lema 2.9.
Asumimos que $n = 2^k n'$ con n impar y tomamos $A \in Mat_{n\times n}(\mathbb{C})$. Por el Teorema 2.6 el $\mathbb{C}-$espacio vectorial $\mathcal{S}_n(\mathbb{C})$ tiene dimensión $n(n+1)/2$. Observamos que la mayor potencia de 2 que divide a $n(n+1)/2$ es 2^{k-1} puesto que

$$\frac{n(n+1)}{2} = \frac{2^k n'(n+1)}{2} = \frac{2^k n'(2^k n' + 1)}{2} = 2^{k-1} n'(2^k n' + 1).$$

Como los factores n' y $2^k n' + 1$ son impares tenemos que $n(n+1)/2$ no es divisible por 2^k. Aplicando la hipótesis de inducción y el Lema 2.9 obtenemos que cada par de endomorfismos que conmutan de $\mathcal{S}_n(\mathbb{C})$ tienen un vector propio en en común en $\mathcal{S}_n(\mathbb{C})$.
Consideremos los endomorfismos $\mathcal{J}_1, \mathcal{J}_2 : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_n(\mathbb{C})$ dados por

$$\mathcal{J}_1(B) = AB + BA^T, \qquad \mathcal{J}_2(B) = ABA^T.$$

Tenemos que $\mathcal{J}_1$ y $\mathcal{J}_2$ son $\mathbb{C}$-endomorfismos que conmutan, y aplicando el Lema 2.9 $\mathcal{J}_1$ y $\mathcal{J}_2$ tienen un vector propio común en $\mathcal{S}_n(\mathbb{C})$. Por lo que existe una matriz $\tilde{B} \in \mathcal{S}_n(\mathbb{C})$ que cumple $A\tilde{B} + \tilde{B}A^T = \lambda\tilde{B}$ y $A\tilde{B}A^T = \mu\tilde{B}$ con $\lambda, \mu \in \mathbb{C}$. Multiplicando a la izquierda por A en la primera ecuación y simplificando con la segunda llegamos a que

$$AA\tilde{B} + A\tilde{B}A^T = A\lambda\tilde{B}.$$

operando y usando que $A\tilde{B}A^T = \mu\tilde{B}$ vemos que

$$A^2\tilde{B} + \mu\tilde{B} = \lambda A\tilde{B}.$$

Sacando factor común, deducimos que

$$(A^2 - \lambda A + \mu)\tilde{B} = 0.$$

Por el Lema 2.26 podemos afirmar que la ecuación anterior se escribe como

$$(A - \alpha I)(A - \beta I)\tilde{B} = 0$$

con $\alpha, \beta \in \mathbb{C}$. Si $(A - \beta I)\tilde{B} = 0$, entonces un vector columna de $\tilde{B}$ distinto de 0 es un vector propio de A con valor propio β. Si $(A - \beta I)\tilde{B} \neq 0$, entonces un vector columna distinto de cero de $(A - \beta I)\tilde{B}$ es un vector propio de A con valor propio α. □

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z) = Z^n + a_{n-1}Z^{n-1} \cdots + a_0$ un polinomio complejo de grado $n > 0$. Si consideramos $A \in Mat_{n\times n}(\mathbb{C})$ la matriz compañera de $p(Z)$

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

se comprueba por inducción que se satisface la ecuación $\det(ZId - A) = p(Z)$. Por el Teorema 2.66, A tiene un vector propio en $\mathbb{C}^n$ y por tanto, un valor propio $\lambda \in \mathbb{C}$, luego concluimos que λ es raíz de $p(Z)$. □

2.7. Prueba usando teoría de cuerpos y polinomios simétricos

Esta prueba está basada en la segunda prueba de Gauss en 1816, que a su vez está basada en la prueba de Laplace. Aunque como se nos cuenta en [18, Part A, Chapter 4], la prueba se suele atribuir a Gauss. La idea de la demostración es probar que todo polinomio real tiene una raíz razonando por inducción en la mayor potencia de 2 que divide al grado. Para el paso inductivo se hará uso de las propiedades de los polinomios simétricos. Esta prueba se encuentra en *Galois theory* [16, Part I, Chapter 3], en [18, Part A, Chapter 4], en [19, Chapter 6] y en *Galois' theory of algebraic equations* [43, Chapter 9].

TFA. *Sea $p(X) \in \mathbb{R}[X]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(X)$.*

Demostración. Tomamos $p(X)$ un polinomio real de grado $n > 0$. Supongamos que $n = 2^m q$ con q impar. Vamos a realizar la prueba por inducción en m. Si $m = 0$, entonces $p(X)$ tiene grado impar y el teorema es cierto por el Teorema 2.4, el caso base es cierto. Asumimos que el teorema es cierto para todos los polinomios de grado $d = 2^k q'$ donde $k < m$ y q' es impar. Suponemos que el grado de $p(X)$ es $n = 2^m q$.
Denotamos por F' al cuerpo de escisión de $p(X)$ sobre $\mathbb{R}$. En F' están las raíces $\alpha_1, \ldots, \alpha_n$ de $p(X)$. Veamos que al menos una de esas raíces es compleja.
Dado $h \in \mathbb{Z}$, consideramos el polinomio

$$H(X) = \prod_{i<j}(X - (\alpha_i + \alpha_j + h\alpha_i\alpha_j)) \in F'[X].$$

Calculamos el grado de $H(X)$. Observamos que cada factor que aparece en la construcción de $H(X)$ se corresponde con una elección de un par de raíces $\{\alpha_i, \alpha_j\}$. El número de formas de elegir dos elementos de $\{\alpha_1, \ldots, \alpha_n\}$ con $n = 2^m q$ es

$$\frac{n(n-1)}{2} = \frac{(2^m q)(2^m q - 1)}{2} = 2^{m-1}q',$$

con $q' = q(2^m q - 1)$ impar por ser producto de impares. Por lo tanto, el grado de $H(x)$ es $2^{m-1}q'$. Notemos además que $H(x)$ es un polinomio simétrico en las raíces $\alpha_1, \ldots, \alpha_n$. Lo que implica por el Lema 2.50 que $H(X) \in \mathbb{R}[X]$ con grado $2^{m-1}q'$. Así que por la hipótesis de inducción $H(X)$ tiene al menos una raíz compleja. Esto implica que existe una pareja $\{\alpha_i, \alpha_j\}$ tal que $\alpha_i + \alpha_j + h\alpha_i\alpha_j \in \mathbb{C}$. Como h es arbitrario, si tomo $h_1 \in \mathbb{Z}$ debe existir un par $\{\alpha_i, \alpha_j\}$ que cumpla que $\alpha_i + \alpha_j + h_1\alpha_i\alpha_j \in \mathbb{C}$. Como sólo hay finitas parejas de raíces y h_1 varía entre los enteros, existirá otro $h_2 \neq h_1$ tal que $z_1 = \alpha_i + \alpha_j + h_1\alpha_i\alpha_j \in \mathbb{C}$ y $z_2 = \alpha_i + \alpha_j + h_2\alpha_i\alpha_j \in \mathbb{C}$. Si hacemos la diferencia entre z_1 y z_2 obtenemos que $z_1 - z_2 = (h_1 - h_2)\alpha_i\alpha_j \in \mathbb{C}$. Dado que $h_1 - h_2 \in \mathbb{Z}$ entonces $\alpha_i\alpha_j \in \mathbb{C}$. Entonces también $h_1\alpha_i\alpha_j \in \mathbb{C}$ y consecuentemente $\alpha_i + \alpha_j \in \mathbb{C}$. Llegados a este punto podemos considerar

$$f(X) = (X - \alpha_i)(X - \alpha_j) = X^2 - (\alpha_i + \alpha_j)X + \alpha_i\alpha_j \in \mathbb{C}[X].$$

Pero $f(X)$ es un polinomio complejo de grado dos y por el Lema 2.26, esto implica que $\alpha_i, \alpha_j \in \mathbb{C}$ y entonces $p(X)$ tiene una raíz compleja. □

2.8. Prueba usando Teoría de Galois

La idea de esta demostración es probar que toda extensión de Galois de $\mathbb{C}$ debe ser trivial razonando por inducción en el grado de la extensión, reduciendo los casos a grado 1 sobre $\mathbb{R}$ y 2 sobre $\mathbb{C}$ mediante la teoría de Galois y la teoría de los grupos de Sylow. Lo que implica que $\mathbb{C}$ es algebraicamente cerrado y por tanto se satisface el TFA. Esta prueba se encuentra en [19, Chapter 7].

TFA. *El cuerpo $\mathbb{C}$ es algebraicamente cerrado.*

Demostración. Tomamos $p(Z)$ un polinomio complejo de grado $n > 0$ y consideramos K su cuerpo de escisión sobre $\mathbb{C}$, que sabemos que existe por el Teorema 2.42. En consecuencia, K es una extensión de Galois de $\mathbb{C}$, y por tanto lo es también de $\mathbb{R}$, por la Observación 2.33. Veamos que cualquier extensión de Galois no trivial de $\mathbb{C}$ tiene que ser igual a $\mathbb{C}$. Esto será equivalente al Teorema Fundamental del Álgebra.
Como K una extensión de Galois de $\mathbb{R}$, en particular es finita. Podemos suponer que $|K : \mathbb{R}| = 2^m q$ y $m.c.d.(2, q) = 1$. Si $m = 0$ entonces K es una extensión de grado impar de $\mathbb{R}$. Como también K es separable sobre $\mathbb{R}$, entonces por el Teorema 2.60 es una extensión simple. Por tanto, $K = \mathbb{R}(\alpha)$ donde el polinomio irreducible $m(\alpha, \mathbb{R})$ tiene grado impar. Sin embargo, como vimos en el Teorema 2.4, todo polinomio real de grado impar tiene una raíz real y entonces razonamos que $m(\alpha, \mathbb{R})$ es irreducible sólo si es de grado 1. Pero entonces $\alpha \in \mathbb{R}$ y $K = \mathbb{R}$. Por lo tanto, si K es una extensión no trivial de $\mathbb{R}$, tenemos que $m > 0$. Esto muestra que no hay extensiones finitas de $\mathbb{R}$ de grado impar.
Supongamos que K es una extensión de grado 2 de $\mathbb{C}$. Entonces $K = \mathbb{C}(\alpha)$ con grado $\mathrm{gr}(m(\alpha, \mathbb{C})) = 2$. Por el Lema 2.26, los polinomios cuadráticos complejos siempre tenían raíces en $\mathbb{C}$. Por ende, $\mathbb{C}$ no tiene extensiones de grado 2.
Si ahora suponemos que $|K : \mathbb{R}| = 2^m q$ con $m > 0$ y $m.c.d.(2, q) = 1$, podemos considerar $G = Gal(K/\mathbb{R})$ su grupo de Galois asociado. Observemos que $|G| = 2^m q$ por el Lema 2.64. Como $m > 0$ y $m.c.d.(2, q) = 1$, por el Teorema 2.54 tenemos que G tiene un subgrupo 2-Sylow de orden 2^m e índice q. Gracias al Teorema 2.65, este subgrupo se correspondería con un cuerpo intermedio E tal que $|K : E| = 2^m$ y $|E : \mathbb{R}| = q$. No obstante, entonces E sería una extensión finita de grado impar de $\mathbb{R}$. Por lo que $q = 1$ y entonces $E = \mathbb{R}$. Así que $|K : \mathbb{R}| = 2^m$ y $|G| = 2^m$ y consecuentemente $|K : \mathbb{C}| = 2^{m-1}$ por el Lema 2.34. Denotemos $G_1 = Gal(K/\mathbb{C})$, y notemos que es un 2-grupo. Si este no fuese trivial entonces por el Lema 2.52 existiría un subgrupo de orden 2^{m-2} e índice 2. De nuevo por el Teorema 2.65 se correspondería con un cuerpo intermedio H de grado 2 sobre $\mathbb{C}$. Pero ya habíamos dicho que $\mathbb{C}$ no tenía extensiones de grado 2. Por lo que concluimos diciendo que G_1 es trivial, es decir, que $|G_1| = 1$ y con ello $|K : \mathbb{C}| = 1$ y finalmente $K = \mathbb{C}$. □

Siguiendo los argumentos de esta prueba podemos extender este teorema a cuerpos real cerrados, que son cuerpos ordenados donde todo elemento positivo tiene una raíz cuadrada. De este modo probaríamos que si K es un cuerpo real cerrado, entonces $K[\sqrt{-1}]$ es algebraicamente cerrado. Este resultado es puramente algebraico, pero si quisiéramos aplicárselo a $\mathbb{R}$ deberíamos probar que $\mathbb{R}$ es real cerrado primero. Para ello, necesitamos hacer uso de alguna de las consecuencias analíticas del axioma del supremo.

Capítulo 3

Pruebas basadas en Topología y Cálculo Diferencial

En este tercer capítulo presentamos cuatro pruebas del Teorema Fundamental del Álgebra, las dos primeras son una versión de la primera prueba de Gauss, la primera más fiel a la prueba original y la segunda es una simplificación vía la teoría de los multiplicadores de Lagrange. En las últimas dos pruebas resultan fundamentales los Teoremas de la Función Implícita e Inversa y la estructura topológica de $\mathbb{C}$. En $\mathbb{C}$ sucede que al quitarle un conjunto finito de puntos, sigue siendo conexo, y esto es algo que en $\mathbb{R}$ no ocurre.
Señalamos que existen otras demostraciones del mismo carácter, que por las limitaciones de extensión, no se han incluido en la memoria. En concreto, en el artículo de B. H. Arnold [4] se da una demostración del TFA a partir del Teorema del punto fijo de Brouwer, pero dicha demostración contiene un error, la aplicación que se construye no es continua. Posteriormente en el artículo de M. K. Fort Jr [20] se da una demostración correcta. Otra demostración topológica más compleja se encuentra en el artículo de J. M. Almira, M. Jiménez y N. Del Toro [1], se prueba el TFA como consecuencia de la sobreyectividad de una aplicación de $\mathbb{C}^n$ en $\mathbb{C}^n$. Una prueba más se encuentra en el artículo de S. Basu [9], se demuestra el TFA por medio del concepto de polinomio intercalador.

3.1. Conexión, local compacidad y aplicaciones propias

Para el desarrollo de esta recopilación de resultados de topología se han usado las fuentes: *Introduction to topological manifolds* [30] y *Topology* [33].

Proposición 3.1. *Sea X un espacio topológico. Se cumple que X es conexo si y solo si los únicos subconjuntos de X que son abiertos y cerrados son $\varnothing$ y el propio X.*

Definición 3.2. *Sea X un espacio topológico. Decimos que X es* ***localmente compacto en*** *x si existe un subespacio compacto C de X que contiene un entorno abierto de x. Si X es localmente compacto en cada uno de sus puntos, diremos que X es* ***localmente compacto****.*

Observación 3.3. *El espacio $\mathbb{C}$ es localmente compacto.*

Definición 3.4. *Sean X e Y espacios topológicos y $f : X \to Y$ una aplicación. Diremos que f es* ***propia*** *si la preimagen de todo subconjunto compacto de Y es compacto en X.*

Lema 3.5. *Un polinomio complejo es una aplicación propia.*

Demostración. Tomamos $A \subseteq \mathbb{C}$ compacto, veamos que $p^{-1}(A)$ es compacto en $\mathbb{C}$. Sabemos que A es compacto, luego es cerrado, y como p es continua entonces $p^{-1}(A)$ es cerrado. Sabemos que A es acotado, luego existe $M > 0$ tal que para todo $w \in A$ se tiene que $|w| \leq M$. Por el Lema 1.23, $|p(z)| \to \infty$ cuando $|z| \to \infty$, por lo que existe $R > 0$ tal que si $z \notin B(0, R)$, entonces $|p(z)| > M$, luego $p^{-1}(A) \subseteq B(0, R)$. Por tanto, $p^{-1}(A)$ debe ser acotado y, por el Teorema 1.10, así $p^{-1}(A)$ es compacto y p es propia. $\square$

Definición 3.6. *Sea X un espacio topológico. Se dice que X está **generado por compactos** si cumple la siguiente propiedad: Para todo $A \subseteq X$ cuya intersección con cada compacto $K \subseteq X$ es cerrada en K, se cumple que A es cerrado en X.*

Lema 3.7. *Los espacios localmente compactos están generados por compactos.*

Teorema 3.8. *Sean X e Y espacios topológicos tales que Y está generado por compactos y es Hausdorff y $f : X \to Y$ una aplicación continua y propia. Entonces f es una aplicación cerrada.*

3.2. Sucesiones en espacios métricos

Recordamos algunas propiedades de las sucesiones en espacios métricos. Para elaborar esta sección se ha usado [38].

Proposición 3.9. *En un espacio métrico toda sucesión convergente es acotada.*

Teorema 3.10 (Bolzano-Weierstrass)**.** *Toda sucesión acotada en $\mathbb{R}^n$ tiene una subsucesión convergente.*

Proposición 3.11. *En un espacio métrico un subconjunto A es un conjunto cerrado si y solo si contiene a todos sus puntos límites si y solo si el límite de toda sucesión convergente de elementos de A pertenece al conjunto.*

Proposición 3.12. *Sean $(X, d_X), (Y, d_Y)$ espacios métricos y $f : X \to Y$ una aplicación. Entonces f es continua si y sólo si para toda sucesión $(x_n)_{n=0}^{\infty}$ de X tal que $x_n \to x$ con $x \in X$ se tiene $f(x_n) \to f(x)$.*

3.3. Cálculo diferencial en varias variables

Concluimos los prerrequisitos del capítulo enunciando algunos de los resultados de cálculo diferencial que emplearemos en las pruebas del TFA. Para aplicar estos resultados necesitaremos relacionar derivabilidad real y compleja para lo cual también introduciremos las ecuaciones de Cauchy-Riemann. Las fuentes usadas han sido los libros *Guía Práctica de Variable Compleja y Aplicaciones* [21], *Cálculo vectorial* [32] y [38].
Denotamos $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ e $y = (y_1, \ldots, y_m) \in \mathbb{R}^m$, de modo que podemos formar el vector $(x, y) = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}) \in \mathbb{R}^{n+m}$ donde $(y_1, \ldots, y_m) = (x_{n+1}, \ldots, x_{n+m})$.

Definición 3.13. *Sea $f : \mathbb{R}^n \to \mathbb{R}^m$ una función diferenciable en un punto $a \in \mathbb{R}^n$ con $f = (f_1, f_2, \ldots, f_m)$. La **diferencial** de f en a, denotada por $D_{(x_1,\ldots,x_n)}f(a)$ o simplemente*

$Df(a)$, es la aplicación lineal $D_{(x_1,\dots,x_n)}f(a):\mathbb{R}^n\to\mathbb{R}^m$ asociada a la matriz

$$D_{(x_1,\dots,x_n)}f(a)=\begin{pmatrix}\frac{\partial f_1}{\partial x_1}(a) & \frac{\partial f_1}{\partial x_2}(a) & \cdots & \frac{\partial f_1}{\partial x_n}(a)\\ \frac{\partial f_2}{\partial x_1}(a) & \frac{\partial f_2}{\partial x_2}(a) & \cdots & \frac{\partial f_2}{\partial x_n}(a)\\ \vdots & \vdots & \ddots & \vdots\\ \frac{\partial f_m}{\partial x_1}(a) & \frac{\partial f_m}{\partial x_2}(a) & \cdots & \frac{\partial f_m}{\partial x_n}(a)\end{pmatrix}.$$

*Cuando $n=m$, el determinante de esta matriz se llama **jacobiano** de f en a y se denota por $Jf(a)$. Cuando $m=1$ escribimos $(\nabla f)(a)=Df(a)$.*

Definición 3.14. *Sea $f:U\to\mathbb{R}^2$ una aplicación diferenciable de un conjunto abierto $U\subseteq\mathbb{R}^2$ en $\mathbb{R}^2$. Un punto $x\in U$ se dice que es un **punto regular** de f si $Df(x):\mathbb{R}^2\to\mathbb{R}^2$ es invertible. De lo contrario, se dice que x es un **punto crítico** de f. Un punto $y\in\mathbb{R}^2$ se dice que es un **valor crítico** de f si es la imagen de un punto crítico.*

Teorema 3.15 (Teorema de la Función Inversa)**.** *Sean U un abierto de $\mathbb{R}^n$, $f:U\to\mathbb{R}^n$ una función de clase $\mathcal{C}^1$ en U, y $a\in U$ tal que $Jf(a)\neq 0$. Entonces existe un conjunto abierto A con $a\in A\subseteq U$ en el que f es inyectiva, $B=f(A)$ es abierto, y la función inversa $g:B\to A$ es también de clase $\mathcal{C}^1$ en B.*

Teorema 3.16 (Teorema de la Función Implícita)**.** *Sean U abierto en $\mathbb{R}^{n+m}$ y $f:U\to\mathbb{R}^m$ una función de clase $\mathcal{C}^1$ en U, $(a,b)\in U$ tal que $f(a,b)=0$ y $\det(D_{(x_n,\dots,x_{n+m})}f(a,b))\neq 0$. Entonces existen un abierto V contenido en U, con $(a,b)\in V$, un abierto A en $\mathbb{R}^n$, y una función $g:A\to\mathbb{R}^m$ tales que: $a\in A$, $g(a)=b$, g es de clase $\mathcal{C}^1$ en A y se cumple que $\{(x,g(x)):x\in A\}=\{(x,y)\in V:f(x,y)=0\}$.*

Cuando apliquemos estos teoremas lo haremos para funciones complejas, por lo que identificando $\mathbb{C}$ con $\mathbb{R}^2$ debemos tener en cuenta lo siguiente:
Dada $f:\mathbb{C}\to\mathbb{C}$ y $z=x+iy\in\mathbb{C}$ podemos escribir $f:\mathbb{R}^2\to\mathbb{R}^2$ como $f(x,y)=(u(x,y),v(x,y))$ donde $u(x,y)=\Re(f(x,y))$ y $v(x,y)=\Im(f(x,y))$. Tomando $z_0\in\mathbb{C}$, al calcular las derivadas direccionales en z_0 tenemos que en el eje real

$$\begin{aligned}f'(z_0)&=\lim_{h\to 0}\left(\frac{u(x_0+h,y_0)-u(x_0,y_0)}{h}+i\frac{v(x_0+h,y_0)-v(x_0,y_0)}{h}\right)\\&=\frac{\partial u}{\partial x}(x_0,y_0)+i\frac{\partial v}{\partial x}(x_0,y_0).\end{aligned}$$

Análogamente en el eje imaginario obtenemos que

$$f'(z_0)=-i\frac{\partial u}{\partial y}(x_0,y_0)+\frac{\partial v}{\partial y}(x_0,y_0).$$

Por tanto, si existe $\lim_{h\to 0}(f(z_0+h)-f(z_0)/h$, obtenemos las ecuaciones de Cauchy-Riemann:

$$\frac{\partial u}{\partial x}=\frac{\partial v}{\partial y}\quad\text{y}\quad\frac{\partial u}{\partial y}=-\frac{\partial v}{\partial x}. \tag{3.1}$$

De tal forma que

$$J(f)(x_0,y_0)=\det\begin{pmatrix}\frac{\partial u}{\partial x} & \frac{\partial u}{\partial y}\\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial y}\end{pmatrix}=|f'(x_0,y_0)|^2$$

Recordamos la noción de curva de nivel y el teorema de los multiplicadores de Lagrange.

Definición 3.17. *Sea $f : \mathbb{R}^n \to \mathbb{R}$ una función, se llaman* ***curvas de nivel*** *a los conjuntos de puntos donde f toma un cierto valor constante, $N_{c,f} = \{x \in \mathbb{R}^n : f(x) = c\}$, es decir, el conjunto de soluciones de la ecuación $f(x) = c$. Fijando una función y $c \in \mathbb{R}$, dicho conjunto se llama* ***conjunto de nivel con valor c****.*

Teorema 3.18 (Teorema de los Multiplicadores de Lagrange)**.** *Sean $f, g : U \subseteq \mathbb{R}^n \to \mathbb{R}$ funciones $\mathcal{C}^1, x_0 \in U$ y $g(x_0) = c$, y sea $N_{c,g}$ el conjunto de nivel de g con valor c. Supongamos que $\nabla g(x_0) \neq 0$. Si $f|_{N_{c,g}}$, alcanza en x_0 un máximo o mínimo local en $N_{c,g}$, entonces existe un $\lambda \in \mathbb{R}$ tal que*

$$\nabla f(x_0) = \lambda \nabla g(x_0).$$

Dicho λ se llama ***multiplicador de Lagrange****.*

Definición 3.19. *Dada $f : \mathbb{R}^n \to \mathbb{R}$ y $c \in \mathbb{R}$ diremos que $N_{c,f}$ es singular si existe $a \in N_{c,f}$ tal que $(\nabla f)(a) = (0, \ldots, 0)$.*

3.4. Prueba basada en la primera demostración de Gauss

Vamos a ver que un polinomio real tiene al menos una raíz compleja. Si realizamos la prueba para este tipo de polinomios, el TFA quedará demostrado por el Teorema 2.29. Esta demostración está basada en la primera prueba original de Gauss. Esta prueba se encuentra en el artículo de S. Basu y D. J. Velleman [8]. En [19, Apendix A] se encuentra otra versión de esta prueba en la que considera los coeficientes también complejos.

TFA. *Sea $p(Z) \in \mathbb{R}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z) = Z^n + a_{n-1}Z^{n-1} + \cdots + a_0$ un polinomio real mónico de grado $n > 0$ y $a_0 \neq 0$. Considerando la forma exponencial de los números complejos, para r y θ reales, definimos

$$R_r(\theta) := \Re(p(re^{i\theta})) = \Re\left[r^n(\cos(\theta) + i\operatorname{sen}(\theta))^n + \sum_{j=0}^{n-1} a_j r^j (\cos(\theta) + i\operatorname{sen}(\theta))^j\right],$$

$$I_r(\theta) := \Im(p(re^{i\theta})) = \Im\left[r^n(\cos(\theta) + i\operatorname{sen}(\theta))^n + \sum_{j=0}^{n-1} a_j r^j (\cos(\theta) + i\operatorname{sen}(\theta))^j\right].$$

Para un $r > 0$ fijo, podemos expresar cada una de estas funciones como un polinomio de grado n en $\cos(\theta)$ y $\operatorname{sen}(\theta)$ expandiendo las potencias de $\cos(\theta) + i\operatorname{sen}(\theta)$. Además, la potencia de $\operatorname{sen}(\theta)$ en cada término de $R_r(\theta)$ será par, así que reemplazando $\operatorname{sen}^2(\theta)$ por $1 - \cos^2(\theta)$, podemos escribir $R_r(\theta)$ de la forma

$$R_r(\theta) = P_r(\cos(\theta)),$$

donde P_r es un polinomio con coeficientes reales de grado n. De manera similar, la potencia de $\operatorname{sen}(\theta)$ en cada término de $I_r(\theta)$ será impar, por lo que tenemos

$$I_r(\theta) = \operatorname{sen}(\theta)\, Q_r(\cos(\theta)),$$

donde Q_r es un polinomio con coeficientes reales de grado $n - 1$.
Con la fórmula $R_r(\theta) = P_r(\cos(\theta))$, vemos que la ecuación $R_r(\theta) = 0$ tiene a lo sumo $2n$ soluciones (módulo 2π), y la única forma de que tenga $2n$ soluciones es que P_r tenga n

distintas raíces, todas en el intervalo $(-1,1)$, de modo que cada una sea igual a $\cos(\theta)$ para dos valores de θ (módulo 2π). En ese caso, P_r se factoriza en factores lineales y su signo cambia en cada raíz, por lo que se deduce que el signo de R_r cambia en cada cero. En otras palabras, si los ceros de R_r, listados en orden creciente, son $\alpha_1, \alpha_2, \dots, \alpha_{2n}$, entonces el signo de $R_r(\theta)$ para $\alpha_{j-1} < \theta < \alpha_j$ es el opuesto de $\alpha_j < \theta < \alpha_{j+1}$.
Lo mismo sucede para I_r. A partir de la fórmula $I_r(\theta) = \operatorname{sen}(\theta)\, Q_r(\cos(\theta))$, vemos que todo múltiplo entero de π es una solución de la ecuación $I_r(\theta) = 0$. Las otras soluciones son los valores de θ para los cuales Q_r se anula. Hay como mucho $2n-2$ de estas (módulo 2π), o sea que hay a lo sumo $2n$ ceros de I_r (módulo 2π), y si hay $2n$ ceros, entonces el signo de I_r cambia en cada solución.
Veamos que R_r e I_r toman el número máximo posible de ceros cuando r es suficientemente grande. Intuitivamente, esto se deduce del hecho de que si $|z|$ es grande, entonces el término z^n domina sobre los demás términos de $p(z)$, y las partes real e imaginaria de z^n cambian de signo $2n$ veces en cualquier círculo $|z| = r$. Para hacer esta idea precisa, se toma

$$r^* := \text{máx}\left(1, \sqrt{2}\sum_{j=0}^{n-1}|a_j|\right),$$

y consideramos cualquier $r > r^*$. Para cada entero k tal que $0 \le k \le 4n$, definimos

$$\theta_k := \frac{(2k-1)\pi}{4n}, \quad z_k := re^{i\theta_k}.$$

Entonces, para cada k, $0 \le k \le 4n$ y cada $r > r^*$ se tiene que

$$\left|\sum_{j=0}^{n-1} a_j z_k^j\right| \le \sum_{j=0}^{n-1}|a_j| r^j < \left(\sum_{j=0}^{n-1}|a_j|\right)\cdot r^{n-1} \le \frac{r^*}{\sqrt{2}}\cdot r^{n-1} < \frac{\sqrt{2}}{2}\cdot r^n.$$

Debido a que $\arg(z_1^n) = n\theta_1 = \pi/4$, tenemos que

$$\Re(z_1^n) = \frac{\sqrt{2}}{2}r^n > \left|\sum_{j=0}^{n-1} a_j z_1^j\right|.$$

Por lo tanto, $R_r(\theta_1) = \Re(p(z_1)) > 0$. Por otro lado, $\arg(z_2^n) = 3\pi/4$, por lo que

$$\Re(z_2^n) = -\frac{\sqrt{2}}{2}\cdot r^n < -\left|\sum_{j=0}^{n-1} a_j z_2^j\right|,$$

luego $R_r(\theta_2) < 0$. Esto implica por el Teorema de Bolzano (Teorema 2.3) que R_r tiene que tener un cero en el intervalo (θ_1, θ_2). Puede usarse el mismo razonamiento para mostrar que $I_r(\theta_0) < 0 < I_r(\theta_1)$, por lo que I_r tiene un cero en el intervalo (θ_0, θ_1). Si seguimos examinando los signos de $R_r(\theta_k)$ e $I_r(\theta_k)$, se tiene que R_r tiene un cero en cada uno de los intervalos $(\theta_1, \theta_2), (\theta_3, \theta_4), \dots, (\theta_{4n-2}, \theta_{4n})$, e I_r tiene un cero en cada uno de los intervalos $(\theta_0, \theta_1), (\theta_2, \theta_3), \dots, (\theta_{4n-1}, \theta_{4n-1})$. El cero de I_r en el intervalo $(\theta_0, \theta_1) = (-\pi/(4n), \pi/(4n))$ es 0, y en el intervalo $(\theta_{2n}, \theta_{2n+1}) = (\pi/(4n), \pi + \pi/(4n))$ el cero es π. Entonces las funciones R_r e I_r tienen ambas $2n$ ceros (módulo 2π), y estos ceros están intercalados, lo que significa que entre dos ceros de cualquiera de las funciones está un cero de la otra.

Digamos que un número $r > 0$ es un radio intercalador si cada una de las funciones R_r e I_r tiene $2n$ ceros (módulo 2π) y estos están intercalados. Hemos demostrado en el párrafo previo que todos los radios $r > r^*$ son intercaladores. Para cualquier r intercalador, sean $\alpha_1(r), \ldots, \alpha_{2n}(r)$ los ceros de R_r en el intervalo $[0, 2\pi)$, y $\beta_1(r), \ldots, \beta_{2n}(r)$ los ceros de I_r en el mismo intervalo, ambos en orden creciente. El que las raíces estén intercaladas significa que:

$$0 = \beta_1(r) < \alpha_1(r) < \beta_2(r) < \alpha_2(r) < \cdots < \beta_{2n}(r) < \alpha_{2n}(r) < 2\pi = \beta_1(r) + 2\pi.$$

Por nuestras anteriores observaciones, los signos de R_r e I_r cambian en cada cero.
Veamos que el conjunto de radios intercaladores es abierto, y que las funciones α_j y β_j, para $1 \leq j \leq 2n$, son continuas en este conjunto. Para ver que esto es cierto, supongamos que $c > 0$ es un radio intercalador y $\varepsilon > 0$. Tomamos un número positivo $t \leq \varepsilon$ suficientemente pequeño tal que los intervalos $(\alpha_j(c) - t, \alpha_j(c) + t)$ y $(\beta_j(c) - t, \beta_j(c) + t)$ sean todos disjuntos (módulo 2π), en otras palabras

$$t = \beta_1(c)+t < \alpha_1(c)-t, \quad \alpha_1(c)+t < \beta_2(c)-t, \quad \ldots, \quad \alpha_{2n}(c)+t < \beta_1(c)-t+2\pi = 2\pi-t.$$

Como el signo de R_c cambia en cada cero, para t suficientemente pequeño $R_c(\alpha_j(c) - t)$ y $R_c(\alpha_j(c) + t)$ deben tener signos opuestos, y de forma análoga $I_c(\beta_j(c) - t)$ y $I_c(\beta_j(c) + t)$ también. Elegimos δ de modo que $0 < \delta < c$ y δ sea lo suficientemente pequeño para que si $|r-c| < \delta$, entonces para todo j, como $R_x(\theta)$ es continua en x para θ fijo, $R_r(\alpha_j(c)-t)$ tiene el mismo signo que $R_c(\alpha_j(c)-t)$, e igual para $R_r(\alpha_j(c)+t)$, $I_r(\beta_j(c)-t)$ e $I_r(\beta_j(c)+t)$. Por lo que R_r tiene un cero en cada uno de los intervalos $(\alpha_j(c)-t, \alpha_j(c)+t)$. Lo mismo ocurre con I_r, que tiene un cero en cada intervalo $(\beta_j(c) - t, \beta_j(c) + t)$. Dado que estos intervalos son disjuntos, se deduce que r es intercalador. Observamos que el cero de I_r en el intervalo $(\beta_1(c) - t, \beta_1(c) + t)$ es $0 = \beta_1(r) = \beta_1(c)$. Por lo tanto, para cada $r \in (c - \delta, c + \delta)$ se tiene que $\alpha_j(r)$ pertenece al intervalo $(\alpha_j(c) - t, \alpha_j(c) + t)$, por lo que $|\alpha_j(r) - \alpha_j(c)| < \varepsilon$, y de igual forma $|\beta_j(r) - \beta_j(c)| < \varepsilon$. En consecuencia, esto establece que el conjunto de radios intercaladores es abierto, y que las funciones α_j y β_j son continuas en este conjunto.
Dado que $p(0) \neq 0$ y los coeficientes de p son reales, $\Re(p(0))$ es distinto de cero. Por lo tanto, por continuidad, para todo valor $r > 0$ suficientemente pequeño, R_r no tiene ceros, luego r no es un radio intercalador. Así, el conjunto de radios positivos que no son intercaladores es no vacío y está acotado superiormente, por lo que tiene un supremo que llamamos r_0, ver Sección 1.2. Puesto que el conjunto de radios intercaladores es abierto, r_0 no puede ser un radio intercalador.
Tomamos $(r_k)_{k=1}^{\infty}$ una sucesión decreciente de radios intercaladores que converge a r_0. Como para todo $k \in \mathbb{N}$ se cumple que $\alpha_1(r_k) \in [0, 2\pi)$, entonces $(\alpha_1(r_k))_{k=0}^{\infty}$ es una sucesión acotada. Aplicando el teorema de Bolzano-Weierstrass (Teorema 3.10) si fuera necesario y considerando una subsucesión adecuada, podemos suponer que $\lim_{k\to\infty} \alpha_1(r_k)$ existe. Análogamente, pasando a una subsucesión si fuese necesario, también podemos asumir que $\lim_{k\to\infty} \beta_1(r_k)$ existe, y repitiendo este razonamiento un número finito de veces podemos suponer que todas las sucesiones $(\alpha_j(r_k))_{k=1}^{\infty}$ y $(\beta_j(r_k))_{k=1}^{\infty}$ convergen.
Definimos $A_j = \lim_{k\to\infty} \alpha_j(r_k)$ y $B_j = \lim_{k\to\infty} \beta_j(r_k)$. Por la continuidad de $R_r(\theta)$ e $I_r(\theta)$, como funciones de r y de θ, y como $R_{r_k}(\alpha_j(r_k)) = 0$ e $I_{r_k}(\beta_j(r_k)) = 0$ tenemos que $R_{r_0}(A_j) = 0$ e $I_{r_0}(B_j) = 0$, y por el orden de las funciones α_j y β_j,

$$0 = B_1 \leq A_1 \leq B_2 \leq A_2 \leq \cdots \leq B_{2n} \leq A_{2n} \leq 2\pi = B_1 + 2\pi.$$

Si todas las desigualdades son estrictas, entonces r_0 es intercalador, lo que es una contradicción. Por tanto, al menos una de las desigualdades no es estricta. Así que existen j y k, tales que $A_j = B_k$ (módulo 2π). Pero entonces $R_{r_0}(A_j) = 0$ e $I_{r_0}(A_j) = I_{r_0}(B_k) = 0$, por lo que $r_0 e^{iA_j}$ es una raíz de p. $\square$

Hasta que concluimos que el conjunto de radios intercaladores es abierto y que las funciones α_j y β_j son continuas, esta prueba no difiera mucho de la prueba de Gauss. Nuestras curvas polares $(r, \alpha_j(r))(r, \beta_j(r))$ son parte de las ramas de las curvas algebraicas $\Re(p(z)) = 0$ y $\Im(p(z)) = 0$. El procedimiento de Gauss consistía en elegir un radio intercalador r y seguir una de estas ramas desde un punto de la circunferencia de radio r al interior del círculo. En su demostración afirmaba, sin detallarlo, que la rama salía del círculo pasando por otro punto diferente de la circunferencia de radio r. En esta versión se estudian todas las ramas a la vez en el círculo $|z| = r$ y se muestra que dos ramas deben intersecar.

3.5. Prueba usando los Multiplicadores de Lagrange

La demostración que se presenta en esta sección puede entenderse como una versión alternativa de la primera demostración de Gauss, aunque más sencilla gracias al uso de las ecuaciones de Cauchy-Riemann y de la teoría de los multiplicadores de Lagrange. La idea es probar que las curvas de nivel cero definidas por la parte real e imaginaria del polinomio se cortan en un punto. Esta prueba se encuentra en el artículo de T. de Jong [26].

Dado un polinomio $p(z) = z^n + \cdots + a_0$ con $n > 0$ y $z = x + iy$ y denotamos

$$p(x + iy) = P(x, y) + iQ(x, y),$$

donde $P(x, y)$ y $Q(x, y)$ son polinomios reales. Notemos que como $p(x, y)$ es una función diferenciable en $\mathbb{R}^2$, P y Q también, luego son continuas y existen sus derivadas parciales. Vamos a estudiar las curvas de nivel para $c \in \mathbb{R}$ de cada función, denotadas por

$$N_{c,P} := \{(x, y) : P(x, y) = c\} \quad \text{y} \quad N_{c,Q} := \{(x, y) : Q(x, y) = c\}.$$

Queremos aplicar el Teorema 3.18 a la curva $N_{c,P}$ y a las funciones P y Q^2.

Lema 3.20. *Para una cantidad infinita de valores $c \in \mathbb{R}$, $N_{c,P}$ es no vacía y no singular en todos los puntos de $N_{c,P}$.*

Demostración. Por un lado, nótese que $P(x, 0) = x^n + \cdots + \Re(a_0)$, por lo que $P(x, 0)$ es una función no constante que toma infinitos valores porque $P(x, 0) \to \infty$ cuando $x \to \infty$, luego las curvas de nivel $N_{c,P}$ son distintas del vacío para infinitos valores de c. Por otro lado, queremos ver que para una infinidad de estos valores $N_{c,P}$ es no singular, es decir, que para todos los puntos (a, b) en $N_{c,P}$ se cumpla que

$$\nabla P(a, b) = \left(\frac{\partial P}{\partial x}(a, b), \frac{\partial P}{\partial y}(a, b) \right) \neq (0, 0).$$

Veamos que a lo sumo sólo puede haber un número finito de curvas de nivel $N_{c,P}$ que son singulares. Como $p'(z)$ tiene solo un número finito de raíces y como, por las ecuaciones de Cauchy-Riemann (3.1), se tiene que

$$p'(z) = \frac{\partial P}{\partial x}(x, y) - i \frac{\partial P}{\partial y}(x, y),$$

deducimos que sólo hay un número finito de curvas de nivel de $N_{c,P}$ que tienen un punto singular. $\square$

Además si la curva $N_{c,P}$ no es singular en (a, b) como, por las ecuaciones de Cauchy-Riemann (3.1), tenemos que

$$\frac{\partial P}{\partial x}(x, y) - i\frac{\partial P}{\partial y}(x, y) = \frac{\partial Q}{\partial y}(x, y) + i\frac{\partial Q}{\partial x}(x, y),$$

la curva de nivel $N_{d,Q}$ con $d = Q(a, b)$ también es no singular en (a, b).
La idea principal de la demostración del TFA se encuentra en el siguiente lema:

Lema 3.21. *Supongamos que la curva de nivel $N_{c,P}$ no es vacía y no singular. Entonces, existe un $(a, b) \in N_{c,P}$ tal que $Q(a, b) = 0$.*

Demostración. Consideramos la función $Q^2|_{N_{c,P}} : N_{c,P} \to \mathbb{R}_{\geq 0}$. Veamos que tiene un mínimo global. Por el Lema 1.23, si fijamos $(r, s) \in N_{c,P}$, podemos encontrar un $R > 0$ suficientemente grande tal que

$$P^2(x, y) + Q^2(x, y) = c^2 + Q^2(x, y) > c^2 + Q^2(r, s),$$

para todo $(x, y) \in N_{c,P}$ con $x^2 + y^2 > R^2$. En el conjunto compacto $\overline{B}(0, R) \cap N_{c,P}$, aplicando el Teorema de Weierstrass (Teorema 1.20) la función $Q^2|_{N_{c,P}}$ alcanza un mínimo puesto que es continua por ser restricción de producto de continuas. Digamos que lo alcanza en el punto (a, b). Se tiene que $Q^2(a, b) \leq Q^2(r, s)$ porque $(r, s) \in \overline{B}(0, R)$. Por tanto, $Q^2|_{N_{c,P}}$ tiene un mínimo global en $(a, b) \in N_{c,P}$.
Cumpliéndose todas las hipótesis, se puede aplicar el Teorema 3.18 a la función Q^2 junto con la curva $N_{c,P}$ no singular y no vacía. Luego existe un $\lambda \in \mathbb{R}$ tal que $\nabla Q^2(a, b) = \lambda \nabla P(a, b)$. Lo que significa que

$$2Q(a, b)\left(\frac{\partial Q}{\partial x}(a, b), \frac{\partial Q}{\partial y}(a, b)\right) = \lambda\left(\frac{\partial P}{\partial x}(a, b), \frac{\partial P}{\partial y}(a, b)\right).$$

Usando otra vez las ecuaciones de Cauchy-Riemann (3.1) obtenemos que

$$2Q(a, b)\left(-\frac{\partial P}{\partial y}(a, b), \frac{\partial P}{\partial x}(a, b)\right) = \lambda\left(\frac{\partial P}{\partial x}(a, b), \frac{\partial P}{\partial y}(a, b)\right).$$

Razonamos por reducción al absurdo y supongamos que $Q(a, b) \neq 0$. Multiplicando escalarmente a ambos lados de la ecuación por el vector $\left(-\frac{\partial P}{\partial y}(a, b), \frac{\partial P}{\partial x}(a, b)\right)$ vemos que

$$2Q\left(\left(\frac{\partial P}{\partial y}\right)^2 + \left(\frac{\partial P}{\partial x}\right)^2\right) = \lambda\left(-\frac{\partial P}{\partial y}\frac{\partial P}{\partial x} + \frac{\partial P}{\partial y}\frac{\partial P}{\partial x}\right) = 0,$$

donde todas las funciones de la igualdad anterior están evaluadas en (a, b). Como $Q(a, b) \neq 0$, la norma del vector $\nabla P(a, b)$ sería cero, pero no puede ser porque habíamos asumido que $N_{c,P}$ era no singular y entonces $\nabla P(a, b) \neq (0, 0)$. Llegando a una contradicción. □
Todo lo probado sobre $N_{c,P}$ y Q también se cumple análogamente al intercambiar los roles de $N_{c,P}$ y $N_{d,Q}$, así como los de Q y P. Con la notación que hemos seguido esta sección, el objetivo va a ser encontrar un punto de intersección entre las curvas $N_{0,P}$ y $N_{0,Q}$. Dicho punto será una raíz de $p(Z)$.

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Por el Lema 3.20 hay infinitos valores de $c \in \mathbb{R}$ tales que $N_{c,P}$ es no vacía y no singular. Aplicando el Lema 3.21, existe algún $(a, b) \in N_{c,P}$, tal que $Q(a, b) = 0$, por lo que la curva de nivel $N_{0,Q}$ es distinta del vacío.
Si $N_{0,Q}$ no es singular, podemos aplicar el Lema 3.21 nuevamente intercambiando los roles de las funciones y las curvas para mostrar que existe un punto $(r, s) \in N_{0,Q} \cap N_{0,P}$ con $P(r, s) = 0$. Por lo tanto, se tiene que $p(r + is) = 0$.
En cambio si $N_{0,Q}$ es singular, notemos que no puede ser singular en (a, b). Porque de serlo entonces también lo sería en $N_{c,P}$ por las ecuaciones de Cauchy-Riemann (3.1). Observamos que Q es no constante en todo entorno de de (a, b) porque $\nabla Q(a, b) \neq 0$. Entonces podemos construir una sucesión $((a_n, b_n))_{n=1}^{\infty}$ con $(a_n, b_n) \in B((a, b), 1/n)$ y tal que $c_n := Q(a_n, b_n) \neq 0$ para cada $n \geq \mathbb{N}_{\geq 1}$. Por construcción $(a_n, b_n) \to (a, b)$ cuando $n \to \infty$ y por continuidad de Q, tenemos que $c_n = Q(a_n, b_n) \to Q(a, b) = 0$. Se cumple que $N_{c_n,Q} \neq \varnothing$ para todo $n \in \mathbb{N}_{\geq 1}$ porque $(a_n, b_n) \in N_{c_n,Q}$. Como Q tiene una cantidad finita puntos críticos y $c_n \neq 0$, a lo sumo habrá finitas curvas $N_{c_n,Q}$ que sean singulares. Si se da el caso en el que alguna de ellas sea singular, podemos pasar si fuese necesario a una subsucesión de $(c_n)_{n=1}^{\infty}$ tal que las correspondientes curvas de nivel son no singulares y no vacías. Abusando de la notación asumiremos que $(c_n)_{n=1}^{\infty}$ tiene esa propiedad.
Aplicando el Lema 3.21, para cada $n \in \mathbb{N}_{\geq 1}$ encontramos $(f_n, g_n) \in N_{c_n,Q}$ con $P(f_n, g_n) = 0$. Por el Lema 1.23, vemos que $((f_n, g_n))_{n=1}^{\infty}$ está acotada y por el Teorema de Bolzano-Weierstrass (Teorema 3.10), existe $((f_{n_k}, g_{n_k}))_{k=1}^{\infty}$ que converge a un límite que denotamos por (f, g). Entonces

$$P(f, g) = \lim_{k\to\infty} P(f_{n_k}, g_{n_k}) = 0,$$
$$Q(f, g) = \lim_{k\to\infty} Q(f_{n_k}, g_{n_k}) = \lim_{k\to\infty} c_{n_k} = 0.$$

Por lo tanto, en este caso también hemos encontrado un punto de intersección entre $N_{0,P}$ y $N_{0,Q}$. □

3.6. Prueba usando la conexión y el Teorema de la Función Implícita

La idea fundamental de la tercera demostración que presentamos en este capítulo es que si al plano complejo le quitamos un conjunto finito de puntos el conjunto resultante sigue siendo conexo. En concreto, gracias a la conexión y al teorema de la función implícita, probaremos que si $c \in \mathbb{C}$ no es valor crítico de un polinomio dado $p(z)$, entonces $p(Z) - c$ tiene al menos una raíz, lo que nos permitirá concluir la prueba. Esta prueba se encuentra en el artículo de R. Pérez-Marco [36].

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z) = a_n Z^n + a_{n-1}Z^{n-1} + \cdots + a_0$ un polinomio complejo de grado $n > 0$. Con la notación de los prerrequisitos, consideremos los siguientes tres conjuntos: el conjunto

$$C = \{z \in \mathbb{C} : p'(z) = 0\}$$

el conjunto de puntos críticos de $p(z)$, es decir, las raíces de $p'(Z)$; el conjunto

$$D = p(C) = \{p(z) \in \mathbb{C} : z \in C\}$$

de valores críticos de $p(z)$; y el conjunto

$R = \{c \in \mathbb{C} :$ el polinomio $p(Z) - c$ tiene al menos una raíz simple y ninguna doble en $\mathbb{C}\}$.

Como el número de raíces de $p'(Z)$ es finito, C es finito y D también lo es.

Observemos que si $c \in D$, entonces $c = p(z_0)$ para algún punto crítico $Z_0 \in C$ y, por tanto, $p'(z_0) = 0$. En consecuencia, el polinomio $f(Z) = p(Z) - c$ tiene z_0 como raíz doble, porque $f(z_0) = p(z_0) - c = c - c = 0$ y $f'(z_0) = p'(z_0) = 0$. Recíprocamente, si $c \in \mathbb{C}$ es tal que $f(Z) = p(Z) - c$ tiene una raíz doble, entonces $c \in D$. Por consiguiente, se cumple que

$$\mathbb{C} \setminus D = \{c \in \mathbb{C} : p(Z) - c \quad \text{no tiene raíces dobles.}\} \tag{3.2}$$

y deducimos que $R \subseteq \mathbb{C} \setminus D$. Como D es finito, tenemos que D es cerrado en $\mathbb{C}$, luego $\mathbb{C} \setminus D$ es abierto. Además es conexo por ser conexo por caminos.

Veamos que $R = \mathbb{C} \setminus D$, para ello veremos que R es un conjunto no vacío, abierto y cerrado en $\mathbb{C} \setminus D$ y como $\mathbb{C} \setminus D$ es conexo, podremos aplicar la Proposición 3.1. Comenzamos probando que R es abierto en $\mathbb{C} \setminus D$. Tomamos $c_0 \in R$ y $z_0 \in \mathbb{C}$ una raíz de $p(Z) - c_0$. Consideramos la función $F : \mathbb{C}^2 \to \mathbb{C}$ dada por $F(c, z) = p(z) - c$, que es de clase $\mathcal{C}^1$. Vemos que $F(c_0, z_0) = 0$ y que $\partial F/\partial z(c_0, z_0) = p'(z_0) \neq 0$ porque como $c_0 \in R$ entonces z_0 es raíz simple y no doble. Luego podemos aplicar el Teorema de la Función Implícita (Teorema 3.16) a F. Entonces existe un entorno $U \subseteq \mathbb{C}$ de c_0 y una función $g : U \to \mathbb{C}$ de clase $\mathcal{C}^1$ tal que $g(c_0) = z_0$ y que $\{(c, g(c)) : c \in U\} = \{(c, z) \in \mathbb{C}^2 : F(c, z) = 0\}$. Entonces para todo $c \in U$ tenemos que $g(c) = z_c$ es una raíz del polinomio $p(Z) - c$. Veamos que z_c no es doble. Teníamos que $p'(g(c_0)) = p'(z_0) \neq 0$, y notemos que $p'(g(c))$ es continua por ser composición de continuas. Luego tomando U más pequeño si fuese necesario, podemos garantizar que $p'(g(c)) \neq 0$ para todo $c \in U$. Por lo que z_c no es raíz doble. Como $\mathbb{C} \setminus D$ es abierto, podemos tomar $U \subseteq \mathbb{C} \setminus D$ y como $p(Z) - c$ tiene a z_c como raíz simple entonces $U \subseteq R$ y concluimos que R es abierto en $\mathbb{C} \setminus D$.

Veamos que R es cerrado empleando la caracterización de la Proposición 3.11. Consideremos una sucesión $(c_n)_{n=0}^{\infty}$ de puntos de R que converge hacia un punto $c \in \mathbb{C} \setminus D$. Como $(c_n)_{n=0}^{\infty}$ es convergente, por la Proposición 3.9, también es acotada. Para cada $n \in \mathbb{N}$, como $c_n \in R$, tomamos $z_n \in \mathbb{C}$ una raíz simple de $p(Z) - c_n$. Razonando de igual manera que en la demostración del Lema 3.5 deducimos que $(z_n)_{n=0}^{\infty}$ es acotada. Por lo tanto, aplicando el Teorema de de Bolzano-Weierstrass (Teorema 3.10), deducimos que podemos extraer una subsucesión $(z_{n_k})_{k=0}^{\infty}$ de $(z_n)_{n=0}^{\infty}$ convergente. Denotamos por $\tilde{z}$ al límite de la subsucesión $(z_{n_k})_{k=0}^{\infty}$. Tenemos que $p(z_{n_k}) - c_{n_k} = 0$ para cada $k \in \mathbb{N}$. Como $p(z)$ es una función continua y $(z_{n_k})_{k=0}^{\infty}$ es una sucesión convergente, entonces por la Proposición 3.12, se tiene que $p(z_{n_k}) - c_{n_k} \to p(\tilde{z}) - \tilde{c}$ cuando $k \to \infty$. En consecuencia, se tiene que $p(\tilde{z}) - \tilde{c} = 0$ y deducimos que $p(Z) - c$ tiene una raíz simple y como $c \in \mathbb{C} \setminus D$, por la ecuación (3.2), $p(Z) - c$ no tiene raíces dobles en $\mathbb{C}$, luego $c \in R$.

Veamos que $R \neq \varnothing$. Buscamos un $c \in \mathbb{C}$ tal que $p(Z) - c$ tenga al menos una raíz simple y ninguna doble. Para cada $a \in \mathbb{C}$ se tiene que $c = p(a)$, luego $p(Z) - c$ tiene al menos $z = a$ como raíz. Si tomamos $a \in \mathbb{C} \setminus p^{-1}(D)$, entonces $a \notin p^{-1}(D)$, por lo que $p(a) \notin D$. Por tanto, tomando $c = p(a) \in \mathbb{C} \setminus D$, tenemos por (3.2), que $p(Z) - c$ no tiene raíces dobles y como $z = a$ es raíz de $p(Z) - c$ concluimos que $p(a) \in R$.

En consecuencia, hemos visto que R es abierto, cerrado en $\mathbb{C} \setminus D$ y distinto del vacío. Por tanto, como $\mathbb{C} \setminus D$ es conexo, llegamos que $R = \mathbb{C} \setminus D$.

Para concluir distinguimos dos casos $0 \in D$ y $0 \notin D$. Si $0 \in D$, entonces $0 = p(z_0)$ para un punto crítico z_0 de $p(z)$ y, por tanto, también z_0 es una raíz de $p(Z)$. Si $0 \notin D$, entonces $0 \in \mathbb{C} \setminus D = R$ y la ecuación $p(Z) - 0 = 0$ tiene al menos una raíz simple. $\square$

3.7. Prueba usando la conexión y el Teorema de la Función Inversa

En la cuarta demostración de este capítulo vamos a probar que un polinomio complejo no constante define una aplicación $p : \mathbb{C} \to \mathbb{C}$ sobreyectiva. De nuevo, es crucial el hecho de que al quitarle un número finito de puntos a $\mathbb{C}$ sigue siendo conexo. Esta prueba se encuentra en el artículo de A. Sen [40].

TFA. *La función polinomial $p : \mathbb{C} \to \mathbb{C}$ definida por un polinomio complejo no constante $p(Z) \in \mathbb{C}[Z]$ es sobreyectiva.*

Demostración. Tomamos $p(Z)$ un polinomio complejo de grado $n > 0$ y consideramos su función polinomial $p : \mathbb{C} \to \mathbb{C}$.
Con la notación de la demostración anterior, consideramos los conjuntos $A = \mathbb{C} \setminus p^{-1}(D)$ y $B = \mathbb{C} \setminus D$. Como en la demostración anterior, se comprueba que D y $p^{-1}(D)$ son finitos, luego son conjuntos cerrados en $\mathbb{C}$. Entonces A y B son abiertos. Como $\mathbb{C}$ sin un conjunto finito de puntos es conexo por caminos entonces tenemos que A y B son conexos, que además son abiertos.
Teniendo en cuenta la Observación 3.3 y el Lema 3.7 tenemos que $\mathbb{C}$ está generado por compactos. Por el Teorema 3.8, como $\mathbb{C}$ es Hausdorff y está generado por compactos entonces tenemos que p es cerrada como aplicación. De tal forma que $\mathrm{Im}(p) = p(\mathbb{C})$ es un conjunto cerrado puesto que $\mathbb{C}$ es cerrado en $\mathbb{C}$ y p es cerrada.
Veamos que $p(A) = B \cap \mathrm{Im}(p)$. Tomamos $y \in p(A)$ entonces existe $x \in A$ tal que $p(x) = y$. Como $x \in A$ entonces $x \in \mathbb{C}$ y $x \notin p^{-1}(D)$. Entonces $p(x) = y \in \mathbb{C}$ y $p(x) \notin p(p^{-1}(D)) \subseteq D$, luego $y \in B$. También $y = p(x) \in p(\mathbb{C}) = \mathrm{Im}(p)$. Recíprocamente, tomamos $y \in B \cap \mathrm{Im}(p)$ entonces $y \in \mathbb{C}, y \notin D$ y existe$x \in \mathbb{C}$ tal que $p(x) = y$. Como $y \notin D$ entonces $x \in A$ y $p(x) = y \in p(A)$.
En consecuencia, $p(A)$ es cerrado en B. Como $A = \mathbb{C} \setminus p^{-1}(D)$ tenemos que los puntos de A no son puntos críticos de p, luego $p'(z) \neq 0$ para cada $z \in A$. Por el Teorema de la Función Inversa (Teorema 3.15), para cada $x \in A$ con $y = p(x)$, existen entornos abiertos U de x y V de y tales que $p|_U : U \to V$ es biyectiva. Luego todo punto $y \in p(A)$ tiene un entorno abierto contenido en $p(A)$, entonces, como B es abierto, $p(A)$ es abierto en B. Como B es conexo y $A \neq 0$, por la Proposición 3.1 concluimos que $p(A) = B$.
Acabamos de probar que $\mathbb{C} \setminus D = B = p(A) = p(\mathbb{C} \setminus p^{-1}(D))$, o sea que $\mathbb{C} \setminus D \subseteq \mathrm{Im}(p)$ y por definición de D también $D \subseteq \mathrm{Im}(p)$. De modo que $\mathbb{C} \setminus D \cup D = \mathbb{C} \subseteq \mathrm{Im}(p) \subseteq \mathbb{C}$ y entonces $\mathrm{Im}(p) = \mathbb{C}$. □

Capítulo 4

Pruebas basadas en Topología Algebraica

En este cuarto capítulo vamos a presentar tres pruebas del Teorema Fundamental del Álgebra, la primera está basada en el número de rotación de un lazo, la segunda y tercera se basan en la teoría del grado de Brouwer en dimensión uno. Para llegar a ellas será necesario introducir la teoría de homotopía.
Durante la elaboración de este capítulo se valoró incluir la prueba del TFA que se encuentra en [19, Chapter 9] y en *Topology* [25, Chapter 6] basada en la teoría del grado de aplicaciones continuas entre $n-$esferas, también llamado grado de Brouwer. Sin embargo, dada la extensión y la complejidad de los prerrequisitos necesarios para introducir esta noción finalmente no se ha incluido en este trabajo. Nos limitaremos a comentar en esta introducción las ideas en las que se fundamenta. Haciendo uso de la teoría de homología, se calcularía en primer lugar $H_n(\mathbb{S}^n)$, que es el $n-$ésimo grupo de homología de $\mathbb{S}^n$, resultando que $H_n(\mathbb{S}^n)$ es $\mathbb{Z}$. Nótese que probar esta afirmación es uno de los objetivos del Trabajo de Fin de Grado de L. González [22]. En segundo lugar se vería como asociar a una aplicación continua $f : \mathbb{S}^n \to \mathbb{S}^n$ el homomorfismo $f_* : H_n(\mathbb{S}^n) \to H_n(\mathbb{S}^n)$ para poder extender el concepto de grado (Definición 4.23) a esferas de mayor dimensión. Con estas nociones, la estrategia de la demostración consiste en construir una aplicación continua de $\mathbb{S}^2$ a $\mathbb{S}^2$ a partir de un polinomio $p(Z) \in \mathbb{C}[Z]$ no constante, mediante la proyección estereográfica, y de esta forma aplicar la teoría del grado de Brouwer para deducir que $p : \mathbb{C} \to \mathbb{C}$ es sobreyectiva. Por los mismos motivos la demostración del artículo de S. K. Stein [41] basada en teoría de homología relativa tampoco se ha incluido en este capítulo.

4.1. Homotopía

A lo largo de este capítulo E, X e Y denotarán espacios topológicos e I el intervalo real $[0, 1]$.
Para la elaboración de los prerrequisitos se ha seguido las fuentes: *Apuntes de la asignatura Topología Algebraica* [15], [19, Chapter 9], [30] y [33].

Definición 4.1. *Un* ***camino*** *en X es una aplicación continua $\gamma : I \to X$. El punto $\gamma(0)$ se denomina punto inicial u origen del camino y $\gamma(1)$ se denomina punto final o extremo del camino.*

Definición 4.2. *Un camino $\gamma : I \to X$ es* ***cerrado*** *en X si $\gamma(0) = \gamma(1)$, es decir, si los puntos inicial y final coinciden. Un camino cerrado también se llama* ***lazo****.*

Definición 4.3. *Un camino $\gamma : I \to X$ es **simple** en X si $\gamma(s) \neq \gamma(t)$ para $s \neq t$, o sea, si no tiene autointersecciones. (Con la excepción de $\gamma(a) = \gamma(b)$ para caminos cerrados).*

Definición 4.4. *Sean γ y $\delta : I \to X$ dos caminos en X. Decimos que γ es **homótopo** a δ relativo a $\{0,1\}$ si existe una aplicación continua $F : I \times I \to X$ tal que*

1. $F(s,0) = \gamma(s)$ *si* $s \in I$.
2. $F(s,1) = \delta(s)$ *si* $s \in I$.
3. $F(0,t) = \gamma(0) = \delta(0)$ *si* $t \in I$.
4. $F(1,t) = \gamma(1) = \delta(1)$ *si* $t \in I$.

*A la aplicación F se la denomina **homotopía de caminos**.*

Lema 4.5. *La relación de ser homótopo relativo a $\{0,1\}$ define una relación de equivalencia en el conjunto de caminos en X con origen en x_0 y extremo en x_1.*

Definición 4.6. *Consideramos un punto $x_0 \in X$ y la relación anterior de equivalencia. Denotamos por $\pi_1(X, x_0)$ al conjunto de **clases de equivalencia** $[\gamma]$ **de lazos** γ con base en x_0.*

Teorema 4.7. *Dados $[\gamma], [\delta] \in \pi_1(X, x_0)$ la operación definida por $[\gamma] \cdot [\delta] = [\gamma * \delta]$, siendo $*$ la concatenación de caminos, dota al conjunto $\pi_1(X, x_0)$ de estructura de grupo. Se denomina a $\pi_1(X, x_0)$ el **grupo fundamental** de X en el punto x_0.*

Definición 4.8. *Un espacio topológico X es **simplemente conexo** si es conexo por caminos y todo lazo es homótopo al lazo constante.*

Definición 4.9. *Sea $f : X \to Y$ una aplicación continua. Tomando $x_0 \in X$ y sea $y_0 = f(x_0)$, definimos el **homomorfismo inducido por la aplicación continua** f, a la aplicación $f_* : \pi_1(X, x_0) \to \pi_1(Y, y_0)$ dada por $f_*([\sigma]) = [f \circ \sigma]$.*

Definición 4.10. *Sean $f, g : X \to Y$ aplicaciones continuas, decimos que f es **homótopa** a g si existe una aplicación continua $H : X \times I \to Y$ tal que $H(x,0) = f(x)$ y $H(x,1) = g(x)$ para cada $x \in X$. Si g es una aplicación constante se dice que f es **homotópicamente nula.***

Lema 4.11. *Sean $p(Z) \in \mathbb{C}[Z]$ no constante de grado $n > 0$ y $f : \mathbb{C} \to \mathbb{C}$ la aplicación dada por $f(z) = z^n$, se cumple que $p : \mathbb{C} \to \mathbb{C}$ es homótopa a f.*

4.2. Aplicación de recubrimiento, número de rotación y grado

Vamos a introducir las nociones de número de rotación y grado de una aplicación.

Definición 4.12. *Una aplicación continua $\rho : E \to X$ es una **aplicación de recubrimiento** o **aplicación recubridora** si es sobreyectiva y para todo $x \in X$ existe un entorno abierto U de x tal que $\rho^{-1}(U) = \cup_{i \in I} V_i$ con $V_i \cap V_j = \varnothing$ si $i \neq j$, para todo $i \in I$ V_i abierto de E y $\rho|_{V_i} : V_i \to U$ es un homeomorfismo.*

Definición 4.13. *Sean $\rho : E \to X$ una aplicación de recubrimiento y $f : Y \to X$ una aplicación continua. Un **levantamiento** de f es una aplicación continua $\tilde{f} : Y \to E$ tal que $\rho \circ \tilde{f} = f$.*

Teorema 4.14. *Sea $\rho : E \to X$ una aplicación de recubrimiento. Dado un camino $\sigma : I \to X$ con $\sigma(0) = x_0$, entonces para cada $e_0 \in \rho^{-1}(x_0)$, existe un único camino $\tilde{\sigma} : I \to E$ tal que $\tilde{\sigma}(0) = e_0$ y $\rho \circ \tilde{\sigma} = \sigma$. En otras palabras, existe un levantamiento del camino y es único.*

Corolario 4.15. *Sean $\rho : E \to X$ una aplicación de recubrimiento, $x_0 \in X$ y $e_0 \in \rho^{-1}(x_0)$. Si $\sigma, \tau : I \to X$ son caminos homótopos en X con $\sigma(0) = \tau(0) = x_0$, entonces sus levantamientos $\tilde{\sigma}, \tilde{\tau} : I \to E$ con $\tilde{\sigma}(0) = \tilde{\tau}(0) = e_0$ también son homótopos en E y además $\tilde{\sigma}(1) = \tilde{\tau}(1)$.*

Definición 4.16. *Sea $\rho : \mathbb{R} \to \mathbb{S}^1$ la aplicación de recubrimiento dada por $\rho(s) = e^{2\pi i s}$. Definimos la aplicación $N : \pi_1(\mathbb{S}^1, 1) \to \mathbb{Z}$ dada por $N([\sigma]) = \tilde{\sigma}(1)$ donde $\tilde{\sigma}$ es el levantamiento de σ que empieza en 0, es decir, $x_0 = 1$ y $e_0 = 0$. El número $N([\sigma])$ se denomina* ***número de rotación*** *del lazo σ.*

Si σ es un lazo simple en $\mathbb{C} \setminus \{0\}$, entonces $\sigma/|\sigma|$ es un lazo en $\mathbb{S}^1$, lo que nos permite definir la noción de orientación.

Definición 4.17. *Sea σ un lazo simple en $\mathbb{C} \setminus \{0\}$. Diremos que σ es un* ***lazo orientado positivamente*** *si el número de rotación de $\sigma/|\sigma|$ es igual a 1.*

Intuitivamente, dado un lazo $\sigma : I \to \mathbb{C} \setminus \{0\}$ el número de rotación de $\sigma/|\sigma|$ representa el "número de vueltas en sentido antihorario" que σ da alrededor del origen.

Teorema 4.18. *La aplicación N de la Definición 4.16 es un isomorfismo de grupos entre $\pi_1(\mathbb{S}^1, 1)$ y $\mathbb{Z}$.*

Definición 4.19. *Llamamos* ***campo de vectores (plano)*** *a una aplicación continua $V : \mathbb{R}^2 \to \mathbb{R}^2$. Un punto $q \in V$ es* ***singular*** *si $V(q) = 0$. En caso contrario diremos que es* ***regular****. Denotamos por $\mathrm{Sing}(V)$ al conjunto de puntos singulares de V.*

Definición 4.20. *Sea V un campo de vectores. Para todo lazo $\sigma : I \to \mathbb{R}^2 \setminus \mathrm{Sing}(V)$ definimos el* ***índice de V con respecto a*** *σ, denotado por $\mathrm{Ind}(V, \sigma)$ como el número de rotación del lazo $f_\sigma : I \to \mathbb{S}^1$ dado por $f_\sigma(s) = V(\sigma(s))/|V(\sigma(s))|$.*

Teorema 4.21. *El $\mathrm{Ind}(V, \sigma) = N([f_\sigma])$ sólo depende de la clase de homotopía de σ.*

Proposición 4.22. *Sea $h : \mathbb{S}^1 \to X$ una aplicación continua. Entonces las afirmaciones siguientes son equivalentes:*

1. *h es homotópicamente nula.*

2. *h se extiende a una aplicación continua $K : \overline{B}(0, 1) \to X$.*

Definición 4.23. *Sea $h : \mathbb{S}^1 \to \mathbb{S}^1$ una aplicación continua, el homomorfismo asociado $h_* : \pi_1(\mathbb{S}^1, b_0) \to \pi_1(\mathbb{S}^1, h(b_0))$ puede interpretarse, vía el Teorema 4.18, como un homomorfismo $h_* : \mathbb{Z} \to \mathbb{Z}$ y el valor $d = h_*(1)$ se denomina* ***grado*** *de h.*

Teorema 4.24. *Sea σ un lazo en $\mathbb{C} \setminus \{0\}$ y $g(s) = \sigma(s)/|\sigma(s)|$. La aplicación g induce vía la aplicación cociente $c : I \to \mathbb{S}^1$ dada por $c(s) = e^{2\pi i s}$, una aplicación continua $h : \mathbb{S}^1 \to \mathbb{S}^1$. Se tiene que $N([g])$ coincide con el grado de h.*

Lema 4.25. *Sea $f : \mathbb{S}^1 \to \mathbb{S}^1$ la función $f(z) = z^n$ con $n > 0$. Se cumple que el grado de f es n.*

Proposición 4.26. *Sean $h, k : \mathbb{S}^1 \to \mathbb{S}^1$ funciones continuas se cumple que:*

1. *Las funciones h y k son homótopas si y solo si tienen el mismo grado.*

2. *Si k es una aplicación constante, entonces el grado de k es 0.*

Teorema 4.27 (Teorema de Rouché)**.** *Sean $\alpha, \beta : I \to \mathbb{C}$ lazos tales que $|\alpha(t)| < |\beta(t)|$ para todo $t \in I$, entonces $\beta/|\beta|$ y $(\beta+\alpha)/|(\beta+\alpha)|$ tienen el mismo número de rotación, es decir, vía la aplicación de paso al cociente $c : I \to \mathbb{S}^1$ dada por $c(s) = e^{2\pi i s}$, las respectivas aplicaciones continuas de $\mathbb{S}^1$ en $\mathbb{S}^1$ tienen el mismo grado.*

4.3. Prueba usando el número de rotación

Esta prueba está basada en las ideas de las pruebas dadas en [19, Chapter 8] y en el artículo de M. D. Hirschhorn [24]. Dado un polinomio de grado $n > 0$ con $p(0) \neq 0$ podemos considerar el campo de vectores asociado $p : \mathbb{C} \to \mathbb{C}$. En la demostración veremos que el índice de p respecto a una circunferencia de radio r es una constante independientemente de r. Por otro lado, veremos que para r pequeño debe ser 0 y para r suficientemente grande debe ser n llegando a una contradicción. La prueba de este último hecho, no se presenta de un modo riguroso en las citadas referencias puesto que en ellas se define el número de rotación como el número de vueltas que da una curva alrededor de un punto sin más detalles. En la demostración que presentamos en esta sección hemos tratado de precisar los argumentos, para lo cual hemos necesitado introducir la noción de índice y sus propiedades cuidadosamente.

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z) = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_0$ un polinomio complejo de grado $n > 0$ con $a_0 \neq 0$. Supongamos que $p(z) \neq 0$ para todo $z \in \mathbb{C}$. Tenemos que p como aplicación es un campo de vectores, y con la anterior suposición deducimos que $\mathrm{Sing}(p) = \varnothing$. Tomamos $r \geq 0$, definimos el lazo $\sigma_r : I \to \mathbb{C}$ dado por $\sigma_r(s) = re^{2\pi i s}$, que no es más que una circunferencia de radio r y centro el origen recorrida en sentido antihorario y la aplicación nula para $r = 0$. Para cada $r \geq 0$ consideramos $f_{\sigma_r} = p(\sigma_r)/|p(\sigma_r)|$, queremos probar que el número de rotación $N([f_{\sigma_r}])$ tiene un valor constante independientemente de r. En otras palabras, queremos ver que existe $k \in \mathbb{Z}$ tal que para todo $r \geq 0$ se tiene que

$$N([f_{\sigma_r}]) = \mathrm{Ind}(p, \sigma_r) = k.$$

Notemos que todas las circunferencias de radio positivo con centro el origen son homótopas. Dados $r, R \geq 0$, podemos construir la aplicación $F : I \times I \to \mathbb{C}$ dada por

$$F(s,t) = (1-t)\sigma_r(s) + t\sigma_R(s),$$

que es continua y nos da una homotopía entre σ_r y σ_R para cualesquiera $r, R \geq 0$. Empleando F construimos la aplicación $H : I \times I \to \mathbb{S}^1$ dada por $p(F)/|p(F)|$. Notemos que es una aplicación continua por ser composición de continuas y que el denominador no se anula puesto que habíamos supuesto que $p(Z)$ no tenía raíces, luego está bien definida. La aplicación H nos da una homotopía entre f_{σ_r} y f_{σ_R}, luego $[f_{\sigma_r}] = [f_{\sigma_R}]$. En consecuencia, como por el Teorema 4.21 el índice $\mathrm{Ind}(p, \sigma)$ sólo depende de la clase de homotopía de σ, podemos decir que para todos $r, R \geq 0$ se cumple que

$$N([f_{\sigma_r}]) = \mathrm{Ind}(p, \sigma_r) = \mathrm{Ind}(p, \sigma_R) = N([f_{\sigma_R}]).$$

Por lo tanto, podemos concluir que $N([f_{\sigma_r}])$ es constante para todo $r \geq 0$.
A continuación vamos a calcular $N([f_{\sigma_r}])$ para $r = 0$ y para valores grandes de r. Si tomamos $r = 0$ obtenemos que $f_{\sigma_0} = a_0/|a_0|$ es un lazo constante en $\mathbb{S}^1$. Luego su clase es el elemento neutro del grupo $\pi_1(\mathbb{S}^1, 1)$. Sabemos por el Teorema 4.18 que N es homomorfismo de grupos, y como tal, el neutro tendrá que ir a parar al neutro, es decir, $N([f_{\sigma_0}]) = 0$ que es el neutro de $\mathbb{Z}$. Por lo que, el número de rotación $N([f_{\sigma_r}])$ de estos lazos debería ser cero para cualquier radio.
Tomemos ahora un radio r tan grande como sea necesario. Sabemos que $p(z)$ es homótopa a z^n en $\mathbb{C}$ por el Lema 4.11. Si sustituimos $z = re^{2\pi is}$ tenemos que $p(re^{2\pi is})$ es homótopa a $(re^{2\pi is})^n$ en $\mathbb{C}$ al ser resultado de componer funciones homótopas con una misma función continua. O sea que $p(\sigma_r)$ es homótopa a $r^n e^{2\pi nis}$ en $\mathbb{C}$. Si dividimos entre el módulo llegamos a que $p(\sigma_r)/|p(\sigma_r)|$ y $r^n e^{2\pi nis}/|r^n e^{2\pi nis}|$ son lazos homótopos en $\mathbb{S}^1$. Así que f_{σ_r} es homótopo al lazo que denotamos $\alpha : I \to \mathbb{S}^1$ dada por $\alpha(s) = e^{2\pi nis}$. Consideramos la aplicación de recubrimiento $\rho : \mathbb{R} \to \mathbb{S}^1$ dada por $\rho(s) = e^{2\pi is}$. Gracias al Corolario 4.15 podemos decir que los levantamientos de f_{σ_r} y α por ρ son homótopos y tienen misma llegada. Para calcular el número de rotación de f_{σ_r} podemos calcular explícitamente un levantamiento de α que será más fácil. Debe cumplirse que $\rho \circ \tilde{\alpha} = \alpha$ por definición de levantamiento. De tal forma que $e^{2\pi i\tilde{\alpha}(s)} = e^{2\pi nis}$, por lo que $\tilde{\alpha}(s) = ns$. Así que $N([f_{\sigma_r}]) = \tilde{f_{\sigma_r}}(1) = \tilde{\alpha}(1) = n$.
Concluimos con un absurdo puesto que la constancia del número de rotación obliga a que $n = 0$ pero no puede ser porque por hipótesis el grado de p era mayor o igual que 1. □
El número de rotación también puede definirse de manera menos general con variable compleja, encontramos otra versión de esta prueba en [19, Appendix D]. Otra demostración similar con una notación diferente se encuentra en *Algebraic Topology* [23, Chapter 1].

4.4. Prueba usando el grado de aplicaciones entre circunferencias

La idea de la segunda demostración que presentamos en este capítulo es similar a la idea de la demostración de la sección anterior. Dado un polinomio de grado $n > 0$ sin raíces construiremos una aplicación de $\mathbb{S}^1$ en $\mathbb{S}^1$. Calcularemos el grado de esta aplicación de dos maneras diferentes probando que es simultáneamente 0 y n y llegando a una contradicción. Esta prueba se encuentra en el libro de J. R. Munkres [33, Capítulo 9]. Además, esta prueba se presentó en la asignatura de Topología Algebraica durante el curso 24/25 impartida por N. Corral.

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z) = Z^n + a_{n-1}Z^{n-1} + \cdots + a_0$ un polinomio complejo de grado $n > 0$. Supongamos que $p(Z)$ no tiene ninguna raíz, es decir, $p(z) \neq 0$ para todo $z \in \mathbb{C}$.
<u>Caso de los coeficientes pequeños</u>
Supongamos que $|a_{n-1}| + \cdots + |a_1| + |a_0| < 1$. Tomamos $K : \overline{B}(0,1) \to \mathbb{S}^1$ la aplicación definida por

$$K(z) = \frac{p(z)}{|p(z)|} = \frac{z^n + a_{n-1}z^{n-1} + \cdots + a_0}{|z^n + a_{n-1}z^{n-1} + \cdots + a_0|}$$

donde el denominador no se anula por hipótesis. Definimos $h := K|_{\mathbb{S}^1}$, como h se extiende a una aplicación continua de $\overline{B}(0,1)$ en $\mathbb{S}^1$, entonces h es homotópicamente nula por la

Proposición 4.22. Por tanto, por la Proposición 4.26, el grado de h es igual al grado de una aplicación constante, que es igual a cero.
Calculemos el grado de h de otro modo. Consideremos la aplicación continua $F : \mathbb{S}^1 \times I \to \mathbb{S}^1$ dada por

$$F(z,t) = \frac{z^n + t(a_{n-1}z^{n-1} + \cdots + a_0)}{|z^n + t(a_{n-1}z^{n-1} + \cdots + a_0)|}.$$

Notemos que F está bien definida y es continua si $z^n + t(a_{n-1}z^{n-1} + \cdots + a_0) \neq 0$. Observamos que si $z^n + t(a_{n-1}z^{n-1} + \cdots + a_0) = 0$, entonces $z^n = -t(a_{n-1}z^{n-1} + \cdots + a_0)$. Por lo que tenemos que para $z \in \mathbb{S}^1$ se cumpliría que

$$1 = |z^n| = t|a_{n-1}z^{n-1} + \cdots + a_0| \leq |a_{n-1}z^{n-1} + \cdots + a_0| \leq |a_{n-1}| + \cdots + |a_1| + |a_0| < 1,$$

lo que es imposible por nuestra hipótesis. Por tanto, F está bien definida y es continua en $\mathbb{S}^1 \times I$. tenemos que $F(z,0) = z^n/|z^n| = z^n$ dado que $|z^n| = 1$ y $F(z,1) = h(z)$. De lo que deducimos que z^n y $h(z)$ son funciones homótopas en $\mathbb{S}^1$ y, por tanto, por la Proposición 4.26 tienen el mismo grado. Pero esto es una contradicción porque haciendo uso del Lema 4.25 razonamos que el grado de z^n es $n \neq 0$ que es el grado de h.
Caso general
Dado $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$, tomando $c > 0$ y haciendo el cambio de variable $z = cx$, tenemos que $p(cx) = (cx)^n + a_{n-1}(cx)^{n-1} + \cdots + a_0$. Podemos considerar

$$q(x) = \frac{p(cx)}{c^n} = x^n + \frac{a_{n-1}}{c}x^{n-1} + \cdots + \frac{a_1}{c^{n-1}}x + \frac{a_0}{c^n}.$$

El punto $x = x_0$ es una raíz de $q(X)$ si y solo si $z_0 = c \cdot x_0$ es una raíz de $p(Z)$. Si tomamos c suficientemente grande de forma que

$$|\frac{a_{n-1}}{c}| + |\frac{a_{n-2}}{c^2}| + \cdots + |\frac{a_1}{c^{n-1}}| + |\frac{a_0}{c^n}| < 1$$

entonces estamos en las condiciones del Caso de los coeficientes pequeños. □

4.5. Prueba usando el Teorema de Rouché

Si usamos el Teorema de Rouché (Teorema 4.27), podemos simplificar las pruebas de las dos secciones anteriores eligiendo de manera adecuada los lazos α y β. Esta prueba se encuentra en [19, Appendix D].

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z) = a_nZ^n + a_{n-1}Z^{n-1} + \cdots + a_0$ un polinomio complejo de grado $n > 0$ con $a_0 \neq 0$. Supongamos que $p(Z)$ no tiene raíces. Definimos la aplicación continua $p_r : \mathbb{S}^1 \to \mathbb{S}^1$ dada por $p_r(z) = p(rz)/|p(rz)|$ donde $r \geq 0$. La aplicación está bien definida por no tener $p(Z)$ raíces. Podemos dar la aplicación $H : \mathbb{S}^1 \times I \to \mathbb{S}^1$ dada por $H(z,t) = p(rtz)/|p(rtz)|$, que al igual que la anterior, está bien definida y es continua por ser composición de funciones continuas. Esta aplicación H nos da una homotopía entre $p_r(z)$ y la aplicación constante $p_0(z) = a_0/|a_0|$. De esta manera, por la Proposición 4.26 obtenemos que $p_r(z)$ tiene el mismo grado que $p_0(z)$, es decir, 0.
Si fijamos un radio $R > \text{máx}(1, \sum_{k=0}^{n-1} |a_i|/|a_n|)$, se tiene que

$$|a_{n-1}z^{n-1} + \cdots + a_0| \leq \sum_{k=0}^{n-1} |a_k||z|^k \leq (\sum_{k=0}^{n-1} |a_k|)|z|^{n-1} < |a_n||z|^n,$$

para todo z con $|z| = R$. Definimos los lazos $\beta, \alpha : I \to \mathbb{C}$ dados por $\beta(t) = a_n(Re^{2\pi it})^n$ y $\alpha(t) = a_0 + \cdots + a_{n-1}(Re^{2\pi it})^{n-1}$. Por la desigualdad anterior $|\alpha(t)| < |\beta(t)|$ para todo $t \in I$. Aplicando el Teorema de Rouché (Teorema 4.27) razonamos que $\beta/|\beta|$ y $(\alpha+\beta)/(|\alpha+\beta|)$ tienen el mismo número de rotación, y vía la aplicación cociente $c : I \to \mathbb{S}^1$ dada por $c(s) = e^{2\pi is}$ podremos construir aplicaciones continuas que denotamos β_c y $(\alpha+\beta)_c$ de $\mathbb{S}^1$ a $\mathbb{S}^1$ que tienen el mismo grado.
Se comprueba que $\beta_c(z) = z^n$ y por el Lema 4.25 afirmamos que tiene grado n. Se comprueba también que $(\alpha+\beta)_c(z) = p_R(z)$. Es decir, el grado de p_R es n, pero previamente hemos visto que su grado es 0. Lo que nos lleva a una contradicción. $\square$

Capítulo 5

Pruebas basadas en Variable Compleja

En este quinto capítulo presentamos siete demostraciones del Teorema Fundamental del Álgebra, todas ellas serán consecuencia de principales resultados de la teoría de variable compleja, que se podrán aplicar gracias a la holomorfía de las funciones polinomiales. En concreto presentaremos pruebas basadas en el Teorema de Liouville y una variante de ella aplicando el Teorema del Valor Medio Integral, el Teorema Integral de Cauchy, el Principio del Mínimo, el Principio del Argumento, el Teorema de Rouché y el Pequeño Teorema de Picard.
Durante este capítulo U denotará un subconjunto abierto de $\mathbb{C}$ y Ω una región de $\mathbb{C}$, o sea, un subconjunto abierto y conexo de $\mathbb{C}$.

5.1. Holomorfía

A continuación se enuncian los resultados correspondientes a variable compleja que serán necesarios para las demostraciones de este capítulo. Para la elaboración de los mismos se han consultado las siguientes fuentes: *Complex Variables* [6], *Complex analysis* [7] (en los que están basados los apuntes de C. Beltrán de la asignatura de Variable Compleja del Grado), [21], y el Teorema 5.28 del libro *Real and Complex Analysis* [39, Theorem 16.22]. Comenzaremos recordando la noción de holomorfía y los conceptos básicos relacionados.

Definición 5.1. *Sean $f : U \to \mathbb{C}$ una función y z_0 un punto de U. Se dice que f es **derivable en** z_0 si existe y es finito el límite*

$$\lim_{w \to 0} \frac{f(z_0 + w) - f(z_0)}{w}.$$

Dicho límite se denomina derivada de f en z_0 y se denota por $f'(z_0)$.

Lema 5.2. *Sea $f : U \to \mathbb{C}$ una función derivable en z_0 y $f'(z_0) = L$ con $L \neq 0$, entonces $1/f(z)$ es derivable en z_0 y $(1/f(z))' = -f'(z_0)/(f(z_0))^2$.*

Definición 5.3. *Sea $f : U \to \mathbb{C}$ una función. Se dice que f es **holomorfa en** U si es derivable en todo punto de U.*

Proposición 5.4. *Sea $f : U \to \mathbb{C}$ una función compleja. Si f es derivable en el punto $z_0 \in U$, entonces f es continua en z_0. Como consecuencia, si f es holomorfa en U, entonces f es continua en U.*

Teorema 5.5 (Condiciones de Cauchy-Riemann)**.** *Sea $f : U \to \mathbb{C}$ una función dada por $f(z) = f(a + bi) = u(a, b) + iv(a, b)$. Es condición necesaria y suficiente para que f sea derivable en $(a, b) \in U$ que las funciones u y v sean diferenciables en el punto (a, b) y que se verifiquen las ecuaciones de Cauchy-Riemann* (3.1)*.*

Definición 5.6. *Una función $\varphi : \Omega \to \mathbb{R}$ es **armónica** si su laplaciano se anula en todo punto de Ω, es decir, si $\Delta\varphi = \left(\partial^2\varphi/\partial x^2\right) + \left(\partial^2\varphi/\partial y^2\right) = 0$.*

Teorema 5.7. *Sea $f = u(x, y) + iv(x, y) : \Omega \to \mathbb{C}$ una función holomorfa en Ω, entonces sus partes reales e imaginarias u y v son funciones armónicas.*

Definición 5.8. *Una función $f : \mathbb{C} \to \mathbb{C}$ se dice que es **entera** si es holomorfa en $\mathbb{C}$.*

Observación 5.9. *Todo polinomio complejo es una función entera.*

Proposición 5.10. *La función exponencial es entera.*

Observación 5.11. *Cualquier determinación del logaritmo complejo es una función holomorfa en su dominio.*

5.2. Teorema Integral de Cauchy y sus consecuencias

A continuación enunciamos el teorema integral de Cauchy junto con algunas de sus consecuencias directas.

Teorema 5.12 (Teorema Integral de Cauchy)**.** *Sean $f : \Lambda \to \mathbb{C}$ una función holomorfa con Λ un subconjunto de $\mathbb{C}$ simplemente conexo y γ un lazo contenido en Λ. Entonces se tiene que*

$$\int_\gamma f dz = 0.$$

Definición 5.13. *Sean $f : \Omega \to \mathbb{C}$ una función holomorfa en un entorno del punto $z_0 \in \mathbb{C}$ y $k \in \mathbb{N}$. Se dice que f tiene **un cero de orden o multiplicidad** k **en** el punto z_0 si*

$$f(z_0) = f'(z_0) = \cdots = f^{(k-1)}(z_0) = 0 \qquad y \qquad f^{(k)}(z_0) \neq 0.$$

*Se llama $Z(f) = \{a \in \Omega : f(a) = 0\}$ al **conjunto formado por los ceros** de f. La multiplicidad del cero de f en a se denotará por $m(f, a)$.*

Enunciamos teoremas que emplearemos en las cuatro primeras pruebas del TFA de este capítulo.

Teorema 5.14 (Teorema de Liouville)**.** *Sea $f : \mathbb{C} \to \mathbb{C}$ entera. Si f está acotada, entonces f es constante.*

Teorema 5.15 (Teorema del Valor Medio Integral)**.** *Sean $f : U \to \mathbb{C}$ holomorfa y $B_r(z_0)$ un disco de radio $r > 0$ y con centro en z_0 contenido en U. Tomando la parametrización $\gamma(t) = z_0 + re^{it}$, $0 \leq t \leq 2\pi$, en $\partial B_r(z_0)$ se tiene que*

$$f(z_0) = \frac{1}{2\pi} \int_0^{2\pi} f(z_0 + re^{it})dt \qquad y \qquad |f(z_0)| \leq \max_{w \in \partial B(z_0, r)} |f(w)|.$$

Teorema 5.16 (Principio del Módulo Mínimo)**.** *Sea $f : \Omega \to \mathbb{C}$ holomorfa. Si la función f presenta un mínimo local en algún punto $z_0 \in \Omega$, es decir, si existe un entorno V de z_0 con $V \subseteq \Omega$ de modo que $|f(z_0)| \leq |f(z)|$ para todo $z \in V$, entonces o f es constante en Ω o f tiene un cero en Ω.*

5.3. Funciones meromorfas

Recordamos la noción de punto singular y el concepto de función meromorfa.

Definición 5.17. *Sea $f : U \to \mathbb{C}$ una función holomorfa excepto en el punto $z_0 \in U$. Se dice que f tiene una **singularidad aislada en** el punto z_0.*
*Si $|f(z)| \to \infty$ cuando $z \to z_0$, decimos que la singularidad es **polar** o que z_0 es un **polo** de la función f.*

Teorema 5.18. *Sea $f : U \to \mathbb{C}$ una función holomorfa con una singularidad en $z_0 \in U$, entonces f tiene un polo en z_0 si y solo si existe $m \in \mathbb{N}$ tal que $(z - z_0)^m f(z)$ tiende a un número finito distinto de cero cuando $z \to z_0$. Este número m es el orden o multiplicidad del polo.*

Definición 5.19. *Sea $f : U \to \mathbb{C}$ una función holomorfa. Se llama*

$$P(f) = \{b \in U : b \text{ es un polo de } f\}$$

*al **conjunto formado por los polos** de f. La multiplicidad del polo de f en $b \in U$ se denotará por $n(f, b)$.*

Definición 5.20. *Sea X localmente compacto y Hausdorff. Decimos que la **compactificación por un punto de X** es el espacio topológico $\hat{X}$ que se define de la siguiente manera. Tomamos ∞ un elemento que no está en X, definimos $\hat{X} := X \cup \{\infty\}$ con la topología $\tau = \{\text{subconjuntos abiertos de } X\} \cup \{U \subseteq \hat{X} : \hat{X} \setminus U \text{es un subconjunto compacto de } X\}$.*

Teorema 5.21. *El espacio $\hat{X}$ descrito en la definición anterior es compacto.*

Definición 5.22. *Como $\mathbb{C}$ es localmente compacto y Hausdorff, podemos considerar su compactificación por un punto que denotamos por $\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ y denominamos **esfera de Riemann** o **plano complejo ampliado**.*

Definición 5.23. *Sea $N = (0, 0, 1)$ el polo norte de la esfera $\mathbb{S}^2 = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$. Identificamos $\mathbb{C}$ con el plano $z = 0$ y llamamos **proyección estereográfica** a la aplicación $\Pi : \mathbb{S}^2 \to \hat{\mathbb{C}}$ dada por*

1. *Si $p = (x, y, z) \in \mathbb{S}^2$ con $p \neq N$, entonces $\Pi(p)$ es el resultado de proyectar p sobre $\mathbb{C}$ desde N, es decir, la intersección con el plano $z = 0$ de la recta que pasa por N y p.*
2. *Se define $\Pi(N) = \infty$.*

Teorema 5.24. *La proyección estereográfica Π es un homeomorfismo entre $\mathbb{S}^2$ y $\hat{\mathbb{C}}$.*

Empleando la compactificación de $\mathbb{C}$, ver Definición 5.22 podemos establecer la noción de función meromorfa.

Definición 5.25. *Sean U un abierto en $\hat{\mathbb{C}}$ y $f : U \to \hat{\mathbb{C}}$ una aplicación, se dice que f es una **función meromorfa en** U si:*

1. *f es continua en U.*
2. *$A = \{a \in U : f(a) = \infty\}$ es un conjunto de puntos aislados en U (es decir, $A' \cap U = \varnothing$).*
3. *La función $f : U \setminus (A \cup \{\infty\}) \to \mathbb{C}$ es holomorfa.*

Concluimos los prerrequisitos con tres teoremas, cada uno de los cuales emplearemos emplearemos en una demostración diferente del TFA.

Teorema 5.26 (Principio del Argumento). *Sea $f : U \to \mathbb{C}$ una función meromorfa y no constante en U y γ un lazo simple, orientado positivamente contenido en U y que no pasa por ninguno de los ceros ni de los polos de f, entonces se tiene que*

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz = \sum_{a\in Z(f)\cap D} m(f,a) - \sum_{b\in P(f)\cap D} n(f,b),$$

donde D es la componente acotada de $\mathbb{C}\backslash\gamma$, es decir, la integral de $f'(z)/2\pi i f(z)$ sobre γ es igual al número de ceros de f menos el número de polos de f en D contados con sus respectivas multiplicidades.

El Teorema 4.27 admite una versión en la teoría de variable compleja que, en lugar del grado, relaciona el número de ceros de las funciones holomorfas.

Teorema 5.27 (Teorema de Rouché). *Sean $f, g : \Omega \to \mathbb{C}$ funciones holomorfas y γ un camino cerrado simple contenido en Ω. Si $|f(z)| > |g(z)|$ a lo largo de γ, entonces se cumple que*

$$\sum_{a\in Z(f+g)\cap D} m(f+g,a) = \sum_{a\in Z(f)\cap D} m(f,a),$$

donde D es la componente acotada de $\mathbb{C}\backslash\gamma$, es decir, f y $f+g$ tienen el mismo número de ceros contando con su multiplicidad en D.

Concluimos con el pequeño teorema de Picard que nos dice que si una función entera no admite dos valores debe ser constante.

Teorema 5.28 (Pequeño Teorema de Picard). *Sea $f : \mathbb{C} \to \mathbb{C}$ una función entera y $a, b \in \mathbb{C}$ con $a \neq b$ tales que $a, b \notin \mathrm{Im}(f)$. Entonces f es constante.*

5.4. Prueba usando el Teorema Integral de Cauchy

En esta demostración supondremos que hay un polinomio no constante sin raíces en $\mathbb{C}$ y con dicho polinomio construiremos una función continua en $\mathbb{R}$, estrictamente positiva en todo punto de $\mathbb{R}$, pero, usando el Teorema Integral de Cauchy, se prueba que tiene integral nula en $\mathbb{R}$, llegando a una contradicción. Esta prueba se encuentra en [19, Appendix C]. En el artículo de R. P. Boas Jr. [11] se puede encontrar una demostración similar, pero se considera un camino de integración diferente.

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Tomamos $p(Z)$ un polinomio complejo de grado $n > 0$ y suponemos que no tiene raíces en $\mathbb{C}$. Razonando de igual forma que en el Teorema 2.29, tenemos que $g(Z) = p(Z)\overline{p}(Z)$ es un polinomio de grado par con coeficientes reales y sin raíces complejas. Además $g(x) = |p(x)|^2$ para $x \in \mathbb{R}$. Como $1/g(z)$ es entera en $\mathbb{C}$, por el Teorema Integral de Cauchy (Teorema 5.12) y dado $r > 0$

$$\int_{-r}^{r} \frac{dx}{|p(x)|^2} + \int_{\gamma_r} \frac{dz}{g(z)} = 0$$

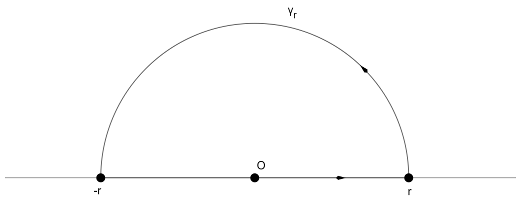

Figura 5.1: Camino cerrado definido por $[-r, r]$ y γ_r.

donde $\gamma_r(t) = re^{it}$ con $t \in [0, \pi]$, es el semicírculo de radio r y centro 0 recorrido en sentido antihorario (ver Figura 5.1). Por el Lema 1.23, se cumple que

$$|g(z)|^{-1} \leq \frac{4}{|a_n|^2|z|^{2n}}$$

para $|z| \geq r$, con r suficientemente grande. Entonces si se considera que

$$\left|\int_{\gamma_r} \frac{dz}{g(z)}\right| \leq \max_{z\in\gamma_r}\left|\frac{1}{g(z)}\right| \pi r \leq \pi\frac{4}{|a_n|^2 r^{2n-1}},$$

se tiene que

$$\lim_{r\to\infty}\int_{\gamma_r}\frac{dz}{g(z)} = 0$$

porque $n > 0$. Pero entonces deducimos que

$$\lim_{r\to\infty}\int_{-r}^{r}\frac{dx}{|p(x)|^2} = 0.$$

Cosa que es imposible debido a que para cada $x \in \mathbb{R}$ se tiene que $|p(x)|^2 > 0$. □

5.5. Prueba usando el Teorema de Liouville

La idea de la demostración es razonar por reducción al absurdo suponiendo que un polinomio no constante no tiene raíces en $\mathbb{C}$, eso nos permite construir una función entera no constante y acotada contradiciendo el Teorema de Liouville. Esta prueba se encuentra en [6, Chapter 2], en [7, Chapter 5] y en [19, Chapter 5]. Además también se presentó en la asignatura de Variable Compleja impartida por J.M. Herrera durante el curso 22/23.

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Por la Observación 5.9, $p(z)$ con $z \in \mathbb{C}$ define una función entera. Por reducción al absurdo, suponemos que $p(Z)$ no tiene raíces en $\mathbb{C}$. Por lo tanto, $f(z) = 1/p(z)$ define una función entera. Por el Lema 1.23, $|p(z)| \to \infty$ cuando $|z| \to \infty$, luego $|f(z)| \to 0$ cuando $|z| \to \infty$. Empleando este hecho, la Proposición 5.4 y el Teorema 1.20, concluimos que $f(z)$ está acotada. Por el Teorema de Liouville (Teorema 5.14), esto implica que $f(z)$, y por tanto $p(z)$, son constantes, generando una contradicción. □

En la demostración anterior en lugar de aplicar el Teorema ed Liouville a la función f para llegar a una contradicción podemos aplicar el Teorema del Valor Medio Integral (Teorema 5.15). Por este teorema se tiene que

$$|f(0)| \leq \max_{\partial B(0,r)} |f(z)|.$$

Por el Lema 1.23, se tiene que $|f(z)| \to 0$ cuando $|z| \to \infty$, lo que quiere decir que $f(0) = 0$, contradiciendo que $f(0) = 1/p(0) \neq 0$.
Este razonamiento se encuentra en una prueba de [19, Appendix C].

5.6. Prueba usando el Principio del Mínimo

La demostración de esta sección es similar a la presentada en la Sección 1.5, se emplea un razonamiento similar al Lema 1.24, pero se concluye de un modo más directo empleando el Principio del Módulo Mínimo. Esta prueba se encuentra en [19, Appendix C] y en [7, Answers, Chapter 6].

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Dado $r > 0$ y $\overline{B}(0, r)$, denotamos así la bola cerrada de centro 0 y radio r. Cada $\overline{B}(0, r)$ es compacto y como $p(z)$ es continua, $|p(z)|$ alcanza el mínimo en algún punto $z_r \in \overline{B}(0, r)$, por el Teorema 1.20. Como $|p(z)| \to \infty$ cuando $|z| \to \infty$ y como en la demostración del Lema 1.24, podemos probar que el mínimo no está en la frontera para R suficientemente grande, es decir, $z_R \in B(0, R)$.
Por tanto, hemos deducido que $|p(z_R)| < |p(z)|$ para todo $z \in \overline{B}(0, R)$. Dado que z_R está en el interior, existe $\varepsilon > 0$ tal que $\overline{B}(z_R, \varepsilon)$, la bola cerrada con radio ε y centro z_R que está contenida en $B(0, R)$. Sin embargo, $p(z)$ es entera, luego en particular, es holomorfa en $\overline{B}(z_R, \varepsilon)$, así que, $|p(z_R)| \leq |p(z)|$ para todo $z \in \overline{B}(z_R, \varepsilon)$. O sea que $p(z)$ presenta un mínimo local. Por el Principio del Mínimo (Teorema 5.16), se concluye que o $p(z_R) = 0$ o $p(z)$ es constante en $\mathbb{C}$. Como $p(z)$ no es constante, se cumple que $p(Z)$ tiene una raíz compleja. □

5.7. Prueba usando el Principio del Argumento

En esta sección probaremos que un polinomio de grado n tiene exactamente n raíces complejas. Para ello aplicaremos el Principio del Argumento al polinomio dado y luego n veces, al polinomio Z y calcularemos la diferencia entre ambas integrales para concluir la demostración. Esta demostración se encuentra en el artículo de P.C. Rosenbloom [37].

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante con grado n. Entonces $p(Z)$ tiene exactamente n raíces complejas.*

Demostración. Sabemos que $p(z)$ es una función entera, luego no tiene polos. Dado $r > 0$ suficientemente grande, podemos razonar por el Principio del Argumento (Teorema 5.26) que

$$\frac{1}{2\pi i} \int_{\partial B(0,r)} \frac{p'(z)}{p(z)} dz = \sum_{a \in Z(p) \cap B(0,R)} m(p, a)$$

donde $\partial B(0, r)$ es el círculo de centro 0 y radio r con orientación contraria a las agujas del reloj. Denotamos por N, al miembro de la derecha de la igualdad anterior. Si consideramos la integral de n/z sobre $\partial B(0,r)$ dividida entre $2\pi i$ observamos que es igual a n por el Principio del Argumento y porque Z tiene un único cero en $B(0,r)$, es decir,

$$\frac{1}{2\pi i}\int_{\partial B(0,r)} \frac{n}{z}dz = n.$$

Si consideramos la diferencia entre estas funciones, tenemos que

$$N - n = \frac{1}{2\pi i}\int_{\partial B(0,r)} (\frac{p'(z)}{p(z)} - \frac{n}{z})dz = \frac{1}{2\pi i}\int_{\partial B(0,r)} \frac{zp'(z) - np(z)}{zp(z)}dz.$$

El numerador de la fracción tiene como mucho grado $n-1$, mientras que el denominador tiene grado $n+1$. Por lo tanto, para r suficientemente grande

$$\left|\int_{\partial B(0,r)} \frac{zp'(z) - np(z)}{zp(z)}dz\right| \leq 2\pi r \max_{\partial B(0,r)} \left|\frac{zp'(z) - np(z)}{zp(z)}\right| \leq 2\pi r\frac{M}{r^2} = \frac{2\pi M}{r}$$

para algún $M > 0$. Por lo que, si hacemos tender r a infinito obtenemos que $N - n = 0$ y por lo tanto $N = n$. □

5.8. Prueba usando el Teorema de Rouché

En esta sección, probaremos que dado un polinomio de grado n, este tiene exactamente n raíces complejas. Para ello aplicaremos el Teorema de Rouché al polinomio formado por el $n-$ésimo coeficiente y al polinomio formado por todos los coeficientes salvo el $n-$ésimo del polinomio dado. De esa manera podremos averiguar la cantidad de ceros del polinomio inicial. Esta demostración se encuentra en [7, Answers, Chapter 10] y también se presentó en la asignatura de Variable Compleja impartida por J.M. Herrera durante el curso 22/23.

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante con grado n. Entonces $p(Z)$ tiene exactamente n raíces complejas.*

Demostración. Tomamos $p(Z) = a_nZ^n + a_{n-1}Z^{n-1} + \cdots + a_0$ un polinomio de grado $n > 0$ y denotamos por $q(Z) = a_nZ^n$ y $r(Z) = a_{n-1}Z^{n-1} + \cdots + a_0$, luego $p(z) = q(z) + r(z)$. Como en la demostración de la Sección 4.5, comprobamos que para $R > 0$ suficientemente grande, dentro de la curva $\partial B(0,R)$ se tiene que

$$|a_{n-1}z^{n-1} + \cdots + a_0| < |a_n||z|^n.$$

Entonces tenemos que $|r(z)| < |q(z)|$, lo que significa por el Teorema de Rouché (Teorema 5.27), aplicando que $f(z) = q(z)$ y $g(z) = r(z)$ concluimos que $q(z)$ y $q(z) + r(z) = p(z)$ tienen el mismo número de ceros en $B(0,R)$. Por ello, se tiene que

$$\sum_{a\in Z(p)\cap B(0,R)} m(p,a) = m(q,0) = n,$$

esto quiere decir que $p(Z)$ tiene también exactamente n raíces dentro del disco contadas con su multiplicidad. □

Esta prueba es parecida a la de la Sección 4.5. En ambas hay que hacer el mismo cálculo para aplicar su correspondiente Teorema de Rouché, pero en esta se cuentan directamente los ceros de una función holomorfa y en la otra se calcula el grado de una función continua de dos maneras distintas para llegar a una contradicción.

5.9. Prueba usando el Pequeño Teorema de Picard

La última prueba de este capítulo consiste en razonar por reducción al absurdo y suponer que un polinomio no constante no tiene raíces en $\mathbb{C}$. De esa manera, el 0 no pertenece a la imagen de la aplicación polinomial. A partir de esta premisa, probaremos que existe otro punto que no puede pertenecer a la imagen. Así, podremos aplicar el Pequeño Teorema de Picard y llegar a una contradicción. Esta prueba se encuentra en el artículo de R. P. Boas Jr. [10].

TFA. *Sea $p(Z) \in \mathbb{C}[Z]$ no constante. Entonces existe $z_0 \in \mathbb{C}$ raíz de $p(Z)$.*

Demostración. Supongamos que $p(Z)$ no tiene raíces. Sabemos que $p(z)$ es entera y en particular continua por la Observación 5.9 y la Proposición 5.4. Por el Lema 1.23 se puede afirmar que existe un radio $R > 0$ suficientemente grande para el que $|p(z)| > 1$ para todo $|z| > R$. Veamos que $p(z)$ no toma uno de los valores $1/k$ con $k \in \mathbb{N}_{\geq 1}$. Supongamos que toma todos los valores $1/k$ para todo $k \in \mathbb{N}_{\geq 1}$. Entonces estamos diciendo que existen $z_k \in \mathbb{C}$ tales que $p(z_k) = 1/k$ para todo $k \in \mathbb{N}_{\geq 1}$ y todos ellos tendrán que estar dentro del disco de radio R. Como $(z_k)_{k=0}^{\infty}$ es una sucesión acotada, por el Teorema de Bolzano-Weierstrass (Teorema 3.10) admite una subsucesión convergente, es decir, existe $w \in \overline{B}(0, R)$ tal que $z_{k_l} \to w$ cuando $l \to w$. Como p es continua, se tiene que

$$p(w) = \lim_{l \to \infty} p(z_{k_l}) = \lim_{l \to \infty} \frac{1}{k_l} = 0.$$

Pero es absurdo porque habíamos dicho que $0 \notin \mathrm{Im}(p)$. Luego acabamos de ver que no pueden estar en la imagen ni el 0 ni el $1/m$ para algún $m \in \mathbb{N}_{\geq 1}$. Y por el Teorema de Picard (Teorema 5.28) deducimos que $p(z)$ ha de ser constante, lo que es una contradicción. $\square$

Capítulo 6

Prueba basada en Geometría Diferencial

En este último capítulo se presentará una misma demostración del Teorema Fundamental del Álgebra con variantes en las construcciones y en los razonamientos. A partir de un polinomio no constante sin raíces veremos dos formas diferentes de construir una métrica de Riemann de la esfera $\mathbb{S}^2$. Con estas métricas probaremos dos lemas auxiliares que emplearemos para razonar por reducción al absurdo de dos maneras distintas.
Este capítulo está basado en los artículos de J. M. Almira y A. Romero Sarabia [2] y [3].

6.1. Geometría de Riemann

Comenzamos introduciendo algunas nociones básicas de geometría de Riemann, para lo cual se han utilizado las siguientes fuentes: *Differential geometry of curves & surfaces* [12], *Foundations of differential geometry. Vol I* [27, Chapter IV and VI] y el teorema de Gauss Bonnet (Teorema 6.10) de *Introduction to Riemannian manifolds* [31, Theorem 9.7].

Definición 6.1. *Una* ***superficie abstracta*** *(variedad diferenciable de dimensión 2) es un conjunto* S *dotado de una familia de aplicaciones inyectivas* $\mathbf{x}_\alpha : U_\alpha \to S$ *definidas en conjuntos abiertos* $U_\alpha \subseteq \mathbb{R}^2$ *con valores en* S *tales que:*

1. $\bigcup_\alpha \mathbf{x}_\alpha(U_\alpha) = S$.
2. *Para cada pareja* α, β *con* $\mathbf{x}_\alpha(U_\alpha) \cap \mathbf{x}_\beta(U_\beta) = W \neq \varnothing$, *tenemos que* $\mathbf{x}_\alpha^{-1}(W)$ *y* $\mathbf{x}_\beta^{-1}(W)$ *son conjuntos abiertos en* $\mathbb{R}^2$ *y* $\mathbf{x}_\beta^{-1} \circ \mathbf{x}_\alpha$, $\mathbf{x}_\alpha^{-1} \circ \mathbf{x}_\beta$ *son aplicaciones diferenciables.*

Cada aplicación $\mathbf{x}_\alpha$ *se llama* ***carta*** *y la inversa de una compuesta con otra, se denomina* ***cambio de cartas****.*

Definición 6.2. *Sea* S *una superficie abstracta. Entonces una aplicación diferenciable* $\gamma : (-\epsilon, \epsilon) \to S$ *se denomina una* ***curva sobre S.*** *Supongamos que* $\gamma(0) = p$ *y sea* D *el conjunto de las funciones sobre* S *que son diferenciables en* p. *El* ***vector tangente a la curva*** γ *en* $t = 0$ *es la función* $\gamma'(0) : D \to \mathbb{R}$ *definida por*

$$\gamma'(0)(f) = \frac{d(f \circ \gamma)}{dt}|_{t=0}, \quad f \in D.$$

Un ***vector tangente en un punto*** $p \in S$ *es el vector tangente en* $t = 0$ *a alguna curva* $\gamma : (-\epsilon, \epsilon) \to S$ *con* $\gamma(0) = p$.

Se tiene que el conjunto de los vectores tangentes en p, con las operaciones usuales, es un espacio vectorial de dimensión dos que se denomina el **espacio tangente** de S en p y denotamos por $T_p(S)$. La elección de una parametrización $\mathbf{x} : U \to S$ en torno a p determina una base asociada $\{\partial\mathbf{x}/\partial u(q), \partial\mathbf{x}/\partial v(q)\}$ de $T_q(S)$ para todo $q \in \mathbf{x}(U)$.

Definición 6.3. *Una **superficie de Riemann** o **variedad riemanniana** de dimensión dos, es una superficie abstracta S tal que para cada $p \in S$ existe producto interior $\langle\ ,\ \rangle_p$ en cada $T_p(S)$, que varía diferenciablemente con respecto a p en el sentido siguiente: Para alguna (por tanto, para toda) parametrización $\mathbf{x} : U \to S$ en torno a p, las funciones*

$$E(u,v) = \left\langle \frac{\partial}{\partial u}, \frac{\partial}{\partial u} \right\rangle, \quad F(u,v) = \left\langle \frac{\partial}{\partial u}, \frac{\partial}{\partial v} \right\rangle, \quad G(u,v) = \left\langle \frac{\partial}{\partial v}, \frac{\partial}{\partial v} \right\rangle$$

*son funciones diferenciables en U. El producto interior $\langle\ ,\ \rangle$ se denomina habitualmente una **métrica riemanniana** o **métrica de Riemann** sobre S.*

Sea S una superficie de Riemann con la parametrización $\mathbf{x} : U \to S$, podemos definir con ecuaciones implícitas los **símbolos de Christoffel** efectuando el producto interior de las derivadas parciales de $\mathbf{x}$ del siguiente modo:

$$\begin{cases}
\Gamma_{11}^1 E + \Gamma_{11}^2 F = \left\langle \frac{\partial^2\mathbf{x}}{\partial u^2}, \frac{\partial\mathbf{x}}{\partial u} \right\rangle = \frac{1}{2}\frac{\partial E}{\partial u}, \\
\Gamma_{11}^1 F + \Gamma_{11}^2 G = \left\langle \frac{\partial^2\mathbf{x}}{\partial u^2}, \frac{\partial\mathbf{x}}{\partial v} \right\rangle = \frac{\partial F}{\partial u} - \frac{1}{2}\frac{\partial E}{\partial v}, \\
\Gamma_{12}^1 E + \Gamma_{12}^2 F = \left\langle \frac{\partial^2\mathbf{x}}{\partial u\partial v}, \frac{\partial\mathbf{x}}{\partial u} \right\rangle = \frac{1}{2}\frac{\partial E}{\partial v}, \\
\Gamma_{12}^1 F + \Gamma_{12}^2 G = \left\langle \frac{\partial^2\mathbf{x}}{\partial u\partial v}, \frac{\partial\mathbf{x}}{\partial v} \right\rangle = \frac{1}{2}\frac{\partial G}{\partial u}, \\
\Gamma_{22}^1 E + \Gamma_{22}^2 F = \left\langle \frac{\partial^2\mathbf{x}}{\partial v^2}, \frac{\partial\mathbf{x}}{\partial u} \right\rangle = \frac{\partial F}{\partial v} - \frac{1}{2}\frac{\partial G}{\partial u}, \\
\Gamma_{22}^1 F + \Gamma_{22}^2 G = \left\langle \frac{\partial^2\mathbf{x}}{\partial v^2}, \frac{\partial\mathbf{x}}{\partial v} \right\rangle = \frac{1}{2}\frac{\partial G}{\partial v}.
\end{cases}$$

A partir de los símbolos de Christoffel obtenemos una expresión para definir la **curvatura de Gauss** K de S :

$$\frac{\partial\Gamma_{12}^2}{\partial u} - \frac{\partial\Gamma_{11}^2}{\partial v} + \Gamma_{12}^1\Gamma_{11}^2 + \Gamma_{12}^2\Gamma_{12}^2 - \Gamma_{11}^2\Gamma_{22}^2 - \Gamma_{11}^1\Gamma_{12}^2 = -EK.$$

Veamos una forma más sencilla de calcular K bajo ciertas condiciones.

Definición 6.4. *Sean S una superficie de Riemann y $\mathbf{x} : U \subseteq \mathbb{R}^2 \to S$ una parametrización, decimos que es una parametrización **isoterma** si $E = G > 0$ y $F = 0$.*

Proposición 6.5. *Sea S una superficie de Riemann. Si $\mathbf{x} : U \subseteq \mathbb{R}^2 \to S$ es una parametrización que es isoterma, entonces*

$$K = -\frac{1}{2\lambda}\Delta(\ln\lambda),$$

donde $E = G = \lambda$ y $\Delta\varphi$ representa el laplaciano de la función φ.

Sigamos con la definición de derivada covariante de un campo vectorial.

Definición 6.6. *Un* ***campo vectorial (tangente)*** *en un conjunto abierto $U \subset S$ de una superficie de Riemann S es una correspondencia $w : U \to \cup_{p\in U} T_p(U)$. El campo vectorial w es diferenciable en p si, para alguna parametrización $x(u,v)$ en p, las componentes a y b de $w = a\partial x/\partial u + b\partial x/\partial v$ con respecto a la base $\{\partial x/\partial u, \partial x/\partial v\}$ son funciones diferenciables en p. Si w es diferenciable en cada $p \in U$ entonces w es diferenciable en U.*

Se puede definir la **derivada covariante** de un campo vectorial a lo largo de curvas en función de los símbolos de Christoffel como

$$\begin{aligned}\frac{Dw}{dt} &= (a' + \Gamma^1_{11}a' + \Gamma^1_{12}av' + \Gamma^1_{12}bu' + \Gamma^1_{12}bv')\frac{\partial \mathbf{x}}{\partial u} \\ &\quad + (b' + \Gamma^2_{11}a' + \Gamma^2_{12}av' + \Gamma^2_{12}bu' + \Gamma^2_{22}bv')\frac{\partial \mathbf{x}}{\partial v}.\end{aligned}$$

Una **geodésica** es una curva tal que el campo de sus vectores tangentes tiene derivada covariante igual a cero.
Intuitivamente, una curva geodésica es aquella que "no se curva" vista desde la propia superficie.

Definición 6.7. *Decimos que una* ***triangulación*** *de una superficie S es una familia finita $\mathcal{T} = \{T_i : i \in \{1,2,\ldots,n\}\}$, tal que:*

1. $\bigcup_{i=1}^{n} T_i = S$.
2. *Cada T_i es homeomorfo a un triángulo del plano $\mathbb{R}^2$.*
3. *Si $T_i \cap T_j \neq \varnothing$, para $i \neq j$ entonces o bien $T_i \cap T_j$ es un lado común a T_i y a T_j, o bien un vértice común a T_i y a T_j.*

Dada una triangulación $\mathcal{T}$ de una superficie S, denotaremos por C al número de triángulos (caras), por L al número de lados (aristas), y por V al número de vértices de la triangulación. El número

$$C - L + V = \chi$$

se denomina la ***característica de Euler-Poincaré*** *de la triangulación.*

Proposición 6.8. *La característica de Euler-Poincaré no depende de la triangulación. Es un invariante topológico.*

Proposición 6.9. *La característica de Euler-Poincaré de la esfera es 2.*

El teorema de Gauss-Bonnet 6.10 será clave para la primera demostración de la Sección 6.3.

Teorema 6.10 (Teorema de Gauss-Bonnet)**.** *Sea S es una superficie de Riemann compacta que admite triangulación. Entonces*

$$\int_S K\, dA = 2\pi\chi(S)$$

donde dA es el elemento de área y $\chi(S)$ es la característica de Euler-Poincaré de la superficie.

Observación 6.11. *Si consideramos el teorema anterior sobre la esfera obtenemos que $\int_{\mathbb{S}^2} K\, dA = 4\pi$, puesto que $\chi(\mathbb{S}^2) = 2$.*

Definición 6.12. *Una superficie de Riemann S es* **completa** *si para cada punto $p \in S$, cualquier geodésica parametrizada $\gamma : [0, \epsilon) \to S$ de S, que comience en $p = \gamma(0)$, puede prolongarse a una geodésica parametrizada $\overline{\gamma} : \mathbb{R} \to S$.*

Las geodésicas del plano euclídeo son las rectas contenidas en él. Luego pueden prolongarse a todo $\mathbb{R}$ y así el plano es completo. La esfera $\mathbb{S}^2$ es una superficie completa por la siguiente proposición.

Teorema 6.13. *Una superficie de Riemann compacta es completa.*

El siguiente teorema será imprescindible para la segunda demostración de la Sección 6.3.

Teorema 6.14. *Cualesquiera dos superficies de Riemann conexas, simplemente conexas y completas de curvatura constante K son isométricas entre sí.*

6.2. Construcciones de la métrica de Riemann

El objetivo de esta sección es construir una métrica de Riemann para la esfera $\mathbb{S}^2$ a partir de un polinomio sin raíces en $\mathbb{C}$. Para ello, primero, construiremos la esfera como una superficie de Riemann. La idea es hacerlo mediante dos proyecciones estereográficas, una desde el polo norte y otra desde el polo sur.
Podemos identificar $\mathbb{R}^2$ con $\mathbb{C}$ y a la esfera $\mathbb{S}^2$ (esfera de Riemann (Definición 5.22)) con $\hat{\mathbb{C}}$ mediante la proyección estereográfica 5.23. Tomamos $U = \{p \in \hat{\mathbb{C}} \ : p \neq \infty\}$, $V = \{q \in \hat{\mathbb{C}} : q \neq 0\}$ y sus correspondientes cartas $\mathbf{x_U} : \mathbb{C} \to U$ y $\mathbf{x_V} : \mathbb{C} \to V$ dadas por $\mathbf{x_U}(p) = p$ y $\mathbf{x_V}(q) = 1/q$ respectivamente. Se comprueba que $\{(\mathbb{C}, \mathbf{x}_U), (\mathbb{C}, \mathbf{x}_V)\}$ cumplen todas las condiciones para que la esfera de Riemann sea una superficie abstracta con cambio de cartas $\mathbf{x_V}^{-1} \circ \mathbf{x_U} : U \cap V \to U \cap V$ dada por $\mathbf{x_V}^{-1} \circ \mathbf{x_U}(z) = 1/z$.
Podemos definir una métrica de Riemann sobre $\hat{\mathbb{C}}$ considerando $\lambda(z)|dz|^2$ sobre U con $dz = dx + idy$ y $\mu(w)|dw|^2$ sobre V con $dw = d\tilde{x} + id\tilde{y}$. Siendo λ, μ funciones C^∞, ambas positivas y además imponiendo la condición de que $\mu(1/z)/|z|^4 = \lambda(z)$ sobre $U \cap V$. Debido a que si tomamos $w = 1/z$ con el cambio de cartas obtenemos que

$$\mu(w)|dw|^2 = \mu\left(\frac{1}{z}\right)\left|d\left(\frac{1}{z}\right)\right|^2 = \mu\left(\frac{1}{z}\right)\left|\frac{-1}{z^2}dz\right|^2 = \frac{1}{|z|^4}\mu\left(\frac{1}{z}\right)|dz|^2.$$

Tenemos dos formas de construir la métrica, la primera de ellas es algebraica y se presenta en el siguiente lema.

Lema 6.15. *Si existe un polinomio irreducible $p(Z)$ de grado $n > 1$. Entonces existe una métrica de Riemann g en la esfera $\mathbb{S}^2$ tal que su curvatura de Gauss, K_g, se anula idénticamente.*

Demostración. Supongamos que $p(Z)$ es un polinomio irreducible de grado $n > 1$. Esto implica que el cociente $A := \mathbb{C}[Z]/\langle p(Z)\rangle$ es un cuerpo por la Observación 2.24. Además, la aplicación $\tau : \mathbb{C}^n \to A$ dada por

$$\tau(a_0, \ldots, a_{n-1}) = a_0 + a_1 Z + \cdots + a_{n-1} Z^{n-1} + \langle p(Z)\rangle$$

define un isomorfismo de espacios vectoriales complejos. En particular, se cumple que si denotamos por $B_c = \{e_1, \ldots, e_n\}$ a la base canónica de $\mathbb{C}^n$, entonces

$$\beta = \{\tau(e_1), \ldots, \tau(e_n)\}$$

es una base de A. Además, tenemos que $\tau(-w, 1, 0, \ldots, 0), \tau(-1, w, 0, \ldots, 0) \neq 0$ para todo $w \in \mathbb{C}$. Puesto que son vectores distintos de cero y τ es biyectiva. Por lo tanto, se tiene que

$$H(w) = \tau(-w, 1, 0, \ldots, 0)\tau(-1, w, 0, \ldots, 0) \neq 0$$

porque todo cuerpo es dominio. Consideramos $M(w)$ la matriz asociada, con respecto a la base β mencionada, al endomorfismo $L_w : A \to A$ dado por

$$L_w(\tau(a_0, \ldots, a_{n-1})) = H(w)\ \tau(a_0, \ldots, a_{n-1}).$$

Tenemos que L_w es un isomorfismo, puesto que $H(w) \neq 0$ y A es un cuerpo. Por lo tanto, $\det(M(w)) \neq 0$ para todo $w \in \mathbb{C}$. Además, definimos $f(w) := \det(M(w))$ y observamos que $f(w)$ es una función polinomial.
La linealidad de τ garantiza que, para todo $w \in \mathbb{C} \setminus \{0\}$,

$$\begin{aligned} H(1/w) &= \tau(-1/w, 1, 0, \ldots, 0)\ \tau(-1, 1/w, 0, \ldots, 0) \\ &= \left[\frac{1}{w}\tau(-1, w, 0, \ldots, 0)\right]\ \left[\frac{1}{w}\tau(-w, 1, 0, \ldots, 0)\right] = \frac{1}{w^2}H(w). \end{aligned}$$

Por lo tanto, se tiene que

$$f(1/w) = \det(M(1/w)) = \det\left(\frac{1}{w^2}M(w)\right) = \frac{1}{w^{2n}}\det(M(w)) = \frac{1}{w^{2n}}f(w).$$

Podemos tomar $\lambda(z) = 1/|f(z)|^{2/n}$ y $\mu(w) = 1/|f(w)|^{2/n}$. De esta manera se tiene que $E = G = \lambda(z)$, $F = 0$ sobre U y $E = G = \mu(z)$, $F = 0$ sobre V. Se comprueba que por cómo hemos tomado f se cumplen todas las condiciones previas necesarias para que sea una métrica de Riemann sobre $\hat{\mathbb{C}}$. Resultando que la métrica g es

$$g = \frac{1}{|f(z)|^{\frac{2}{n}}}|dz|^2 \quad \text{para} \quad z \in U = \mathbb{C} \quad \text{y}$$

$$g = \frac{1}{|f(1/z)|^{\frac{2}{n}}}|d(1/z)|^2 \quad \text{para} \quad z \in V = \hat{\mathbb{C}} \setminus \{0\}.$$

Si calculamos la curvatura de Gauss sobre U aplicando la Proposición 6.5 vemos que

$$K_g(z) = -\frac{1}{2}|f(z)|^{\frac{2}{n}}\Delta\ \ln\left(\frac{1}{|f(z)|^{\frac{2}{n}}}\right) = \frac{|f(z)|^{\frac{2}{n}}}{n}\Delta\Re(\log f(z)).$$

Debido a la Observación 1.16 y utilizando el Teorema 5.7 gracias a la Observación 5.11, tenemos que $K_g = 0$. Por la continuidad de K_g, implica que $K_g = 0$ en toda la esfera. □
Para la segunda construcción de la métrica g no necesitamos asumir que $p(Z)$ es irreducible. En este caso f se construye directamente a partir del polinomio y su polinomio recíproco.

Lema 6.16. *Si existe un polinomio $p(Z)$ de grado $n > 0$, tal que $p(z) \neq 0$ para todo $z \in \mathbb{C}$. Entonces existe una métrica de Riemann g en la esfera $\mathbb{S}^2$ tal que su curvatura de Gauss, K_g, se anula idénticamente.*

Demostración. Si $p(Z) = a_n Z^n + \cdots + a_0$ definimos $p_*(Z) = a_n + \cdots + a_0 Z^n$, esto es, el coeficiente $i-$ésimo de p_* es el coeficiente $(n-i)-$ésimo de $p(Z)$. Se comprueba que se cumple que $p_*(z) = z^n p(1/z)$ para todo $z \in \mathbb{C} \setminus \{0\}$. Consideremos el producto de ambos polinomios $f(z) = p(z)p_*(z)$, realizando el cálculo vemos que se satisface la ecuación $|f(1/z)| = |f(z)|/|z|^{2n}$ para todo $z \in \mathbb{C} \setminus \{0\}$.
Al igual que en la demostración del Lema 6.15 podemos tomar $\lambda(z) = 1/|f(z)|^{2/n}$ y $\mu(w) = 1/|f(w)|^{2/n}$. Razonando análogamente como en el final de dicha demostración, obtenemos una métrica de Riemann sobre la esfera con curvatura de Gauss constantemente nula. □

6.3. Contradicciones con los lemas auxiliares

De los lemas auxiliares deducimos que existe una métrica de forma que la esfera es plana. Vamos a ver que es imposible de dos formas diferentes. En primer lugar, llegaremos a contradicción empleando el Teorema de Gauss-Bonnet (Teorema 6.10). Por la Observación 2.25, podemos demostrar el TFA de la siguiente manera.

TFA. *Los polinomios irreducibles de* $\mathbb{C}[z]$ *son de grado 1.*

Demostración. Por el Lema 6.15 o por el Lema 6.16 tenemos que la curvatura de Gauss es 0 en toda la esfera $(\mathbb{S}^2, g)$, así que no puede tener puntos elípticos de curvatura positiva. Sin embargo, por la Observación 6.11 tenemos que la integral de la curvatura de Gauss sobre la esfera es positiva. Lo que implica la existencia de al menos un punto elíptico, lo que supone una contradicción. $\square$

En segundo lugar llegaremos a una contradicción aplicando el Teorema de clasificación de superficies de Riemann.

TFA. *Sea* $p(Z) \in \mathbb{C}[Z]$ *no constante. Entonces existe* $z_0 \in \mathbb{C}$ *raíz de* $p(Z)$.

Demostración. Como la esfera y el plano euclídeo son conexos, simplemente conexos, completos y tienen curvatura de Gauss constante igual a 0, deducimos que la esfera $(\mathbb{S}^2, g)$ es isométrica al plano euclídeo por el Teorema 6.14. Luego en particular son homeomorfos, pero esto es una contradicción debido a que la esfera es compacta y el plano no. $\square$

En el artículo [3] nos dan otro posible argumento aplicando el principio del máximo y la relación conforme entre la métrica de Riemann usual en la esfera con curvatura de Gauss igual a 1 y la métrica que se ha construido con curvatura de Gauss nula.

Bibliografía

[1] J. M. Almira, M. Jiménez and N. Del Toro, Another topological proof of the fundamental theorem of algebra, Elem. Math. **57** (2002), no. 1, 32–37.

[2] J. M. Almira and A. Romero Sarabia, Yet another application of the Gauss-Bonnet theorem for the sphere, Bull. Belg. Math. Soc. Simon Stevin **14** (2007), no. 2, 341–342.

[3] J. M. Almira and A. Romero Sarabia, Some Riemannian geometric proofs of the fundamental theorem of algebra, Differ. Geom. Dyn. Syst. **14** (2012), 1–4.

[4] B. H. Arnold, A topological proof of the fundamental theorem of algebra, Amer. Math. Monthly **56** (1949), 465–466.

[5] M. Artin, *Algebra*, Prentice Hall, Englewood Cliffs, NJ, 1991.

[6] R.B. Ash; W.P. Novinger *Complex Variables.* 2. ed, Dover, 2007.

[7] J. Bak and D.J. Newman, *Complex analysis*, third edition, Undergraduate Texts in Mathematics, Springer, New York 2010.

[8] S. Basu and D. J. Velleman, On Gauss's first proof of the fundamental theorem of algebra, Amer. Math. Monthly **124** (2017), no. 8, 688–694.

[9] S. Basu, Strictly real fundamental theorem of algebra using polynomial interlacing, Bull. Aust. Math. Soc. **104** (2021), no. 2, 249–255.

[10] R. P. Boas Jr., Questions, Discussions, and Notes: A Proof of the Fundamental Theorem of Algebra, Amer. Math. Monthly **42** (1935), no. 8, 501–502.

[11] R. P. Boas Jr.,Yet Another Proof of the Fundamental Theorem of Algebra, The American Mathematical Monthly, vol. 71, no. 2, 1964, p. 180.

[12] M. P. do Carmo, *Differential geometry of curves & surfaces*, revised & updated second edition, Dover, Mineola, NY, 2016.

[13] B. Cipra, A Bicentennial for the Fundamental Theorem of Algebra, Math Horizons, vol. 7, no. 2, 1999, pp. 5–7.

[14] K. Conrad, The fundamental theorem of algebra via linear algebra, expository paper. Disponible en: `https://kconrad.math.uconn.edu/blurbs/fundthmalg/fundthmalglinear.pdf`.

[15] N. Corral, *Apuntes de la asignatura Topología Algebraica*, Universidad de Cantabria, 2024.

[16] D. A. Cox, *Galois theory*, Pure and Applied Mathematics (New York), Wiley-Intersci., Hoboken, NJ, 2004.

[17] H. Derksen, The fundamental theorem of algebra and linear algebra, Amer. Math. Monthly **110** (2003), no. 7, 620–623.

[18] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel and R. Remmert, *Numbers*, translated from the second 1988 German edition by H. L. S. Orde Translation edited and with a preface by J. H. Ewing, Graduate Texts in Mathematics Readings in Mathematics, 123, Springer, New York, 1991.

[19] B. Fine and G. Rosenberger, *The fundamental theorem of algebra*, Undergraduate Texts in Mathematics, Springer, New York, 1997.

[20] M. K. Fort Jr., Some properties of continuous functions, Amer. Math. Monthly **59** (1952), 372–375.

[21] F. Galindo Soto, J. Gómez, J. Sanz and L. Tristán, *Guía Práctica de Variable Compleja y Aplicaciones*. Universidad de León; Universidad de Valladolid, 2013.

[22] L. González, *Homología singular y CW-complejos*, Trabajo de Fin de Grado, Universidad de Cantabria, 2018.

[23] A. E. Hatcher, *Algebraic topology*, Cambridge Univ. Press, Cambridge, 2002.

[24] M. D. Hirschhorn, The fundamental theorem of algebra, College Math. J. **29** (1998), no. 4, 276–277.

[25] J. G. Hocking and G. S. Young Jr., *Topology*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London, 1961.

[26] T. de Jong, Lagrange multipliers and the fundamental theorem of algebra, Amer. Math. Monthly **116** (2009), no. 9, 828–830.

[27] S. Kobayashi and K. Nomizu, *Foundations of differential geometry. Vol I*, Interscience Publishers (a division of John Wiley & Sons, Inc.), New York-London, 1963.

[28] T.W. Körner, On the fundamental theorem of algebra, Amer. Math. Monthly **113** (2006), no. 4, 347–348.

[29] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, 211, Springer, New York, 2002.

[30] J. M. Lee, *Introduction to topological manifolds*, Graduate Texts in Mathematics, 202, Springer, New York, 2000.

[31] J. M. Lee, *Introduction to Riemannian manifolds*, second edition, Graduate Texts in Mathematics, 176, Springer, Cham, 2018.

[32] J. E. Marsden, A. J. Tromba, *Cálculo Vectorial*, Quinta Edición. Pearson Educación, 2004.

[33] J.R. Munkres, *Topology*, second edition, Prentice Hall, Upper Saddle River, NJ, 2000.

[34] O. R. B. de Oliveira, The fundamental theorem of algebra: an elementary and direct proof, Math. Intelligencer **33** (2011), no. 2, 1–2.

[35] A. Ostrowski, Über Den Ersten Und Vierten Gauss'schen Beweis Des Fundamentalsatzes Der Algebra. 1920.

[36] R. Pérez-Marco, Prueba Elemental Del Teorema Fundamental Del Álgebra, revista de La Facultad de Ciencias, vol. 10, no. 2, 2021, pp. 6–8.

[37] P. C. Rosenbloom, An elementary constructive proof of the fundamental theorem of algebra, Amer. Math. Monthly **52** (1945), 562–570.

[38] W. Rudin, *Principles of mathematical analysis*, third edition, International Series in Pure and Applied Mathematics, McGraw-Hill, New York-Auckland-Düsseldorf, 1976.

[39] W. Rudin, *Real and complex analysis*, third edition, McGraw-Hill, New York, 1987.

[40] A. Sen, Notes: Fundamental Theorem of Algebra – Yet Another Proof, Amer. Math. Monthly **107** (2000), no. 9, 842–843.

[41] S. K. Stein, The fundamental theorem of algebra, Amer. Math. Monthly **61** (1954), 109.

[42] F. Terkelsen, The fundamental theorem of algebra, Amer. Math. Monthly **83** (1976), no. 8, 647.

[43] J.-P. Tignol, *Galois' theory of algebraic equations*, World Sci. Publ., River Edge, NJ, 2001.