SOBRE EL GRUPO DE GALOIS DE LOS POLINOMIOS DE LEGENDRE

CRISTIN JULIETH MANTA CARO.

Proyecto Curricular de Matemáticas
Facultad de Ciencias y Educación
Universidad Distrital Francisco José de Caldas
Bogotá D.C.

2016

SOBRE EL GRUPO DE GALOIS DE LOS POLINOMIOS DE LEGENDRE

CRISTIN JULIETH MANTA CARO.

Monografía para optar al título de Matemática

Trabajo dirigido por:
Luis Oriol Mora Valbuena
Profesor de planta Universidad Distrital

Proyecto Curricular de Matemáticas
Facultad de Ciencias y Educación
Universidad Distrital Francisco José de Caldas
Bogotá D.C.
2016

Agradecimientos

Quiero agradecer a mi hermano, por su apoyo recibido en el transcurso de mi carrera; al profesor Luis Oriol Mora por su dedicación, acompañamiento y dirección en el desarrollo de este trabajo; a la Universidad Distrital Francisco José de Caldas por mi formación académica y a cada uno de los profesores que hicieron parte de ella.

Resumen

La presente monografía está basada en el artículo *On the Galois groups of Legendre polynomials* de John Cullinan y Garshid Hajir y pretende estudiar algunas propiedades algebraicas que los autores utilizan para ver cuál es el grupo de Galois de los polinomios de Legendre.

Palabras claves: Grupo de Galois, polinomios ortogonales, primos en intervalos, primos en progresiones aritméticas.

Abstract

This work is based on the article *On the Galois groups of Legendre polynomials* by John Cullinan and Garshid Hajir and pretends to study some algebraic properties that authors use to see what is the group of Galois of the Legendre polynomials.

Keywords: Galois group, orthogonal polynomials, primes in intervals, primes in arithmetic progressions

Índice general

Introducción

Los polinomios ortogonales desempeñan una función importante en varias áreas de la matemática y los polinomios de Legendre no son la excepción. En 1785 el matemático francés Adrien-Marie Legendre introdujo los polinomios que llevan su nombre, estos han jugado un papel importante en el análisis, la física e incluso la teoría de números; no obstante, las propiedades algebraicas de esta familia de polinomios no son bien conocidas. En 1890 Stieltjes conjeturó que dichos polinomios son irreducibles sobre $\mathbb{Q}$.

Asumiendo la conjetura de Stieltjes, la presente monografía tiene como finalidad el estudio parcial de los grupos de Galois de los polinomios de Legendre. Ésta busca exhibir conceptos y propiedades elementales sobre los polinomios ortogonales, junto con las propiedades de familias de polinómios como los polinómios de Legendre y los polinómios de Jacobi; y conceptos que relacionan el grupo de Galois y el discriminante de un polinomio. Además de ello, introduce conceptos de teoría de números analítica, como por ejemplo la función $\phi(x)$ de Chebyshev, que interviene para dar información adicional sobre el discriminante de un polinómio.

Específicamente, se representa los polinomios de Legendre en términos de otro tipo de polinomios que denotamos por $\mathscr{J}_n^{(\pm 1/2,0)}(x)$, y busca demostrar si el grupo de Galois de ellos está contenido en A_n, el grupo de todas las permutaciones pares. Dicho estudio está basada en el primer resultado del artículo *On the Galois groups of Legendre polynomials* de John Cullinan y Garshid Hajir [3], e intenta reconstruir parcialmente dicho artículo. Para ello se deben incluir conceptos previos de tres teorías: los polinomios ortogonales, el grupo de Galois de un polinomio y primos en progresiones aritméticas.

En forma detallada, el desarrollo de este trabajo se presenta de la siguiente manera: En el primer capítulo, *Preliminares*, se encuentran nociones básicas sobre divisibilidad y congruencias; junto con conceptos de extensiones de campos, automorfismos y algunas propiedades del grupo de permutaciones.

En el segundo capítulo, *Conceptos básicos*, se dan las herramientas necesarias para el desarrollo de nuestro objetivo general. Para ello se muestra la relación entre el grupo

de Galois y el discriminante de un polinomio, la definición y algunas propiedades de funciones especiales, necesarias para la definición de polinomios clásicos; se presenta la teoría de funcionales de momento y los correspondientes polinomios ortogonales; y por último se presenta la unión de dos resultados conocidos, el postulado de Bertrand y el teorema de Dirichlet.

Y para finalizar, en el tercer capítulo, *Sobre el grupo de Galois de los polinomios de Legendre*, se muestra el resultado en el que se centra este trabajo, utilizando las herramientas desarrolladas en el segundo capítulo. Se obtiene un teorema principal que proporciona información acerca del grupo de Galois de los polinomios $\mathscr{J}_n^{(\pm 1/2,0)}(x)$.

Capítulo 1

Preliminares

El objetivo principal de este trabajo gira entorno a tres ramas de la matemática, como ya se ha mencionado. En este capítulo se exhiben algunos conceptos de teoría de números y álgebra abstracta, como por ejemplo: la definición y propiedades de divisibilidad, congruencias, extensiones de campos, entre otros. Esto con el fin de dar las herramientas necesarias para el buen entendimiento de conceptos que se definirán en los siguientes capítulos y teoremas que relacionan estos conceptos.

1.1. Divisibilidad, MCD y Congruencias

Uno de los resultados que se dan en el tercer capítulo necesita de definiciones y teoremas elementales de teoría de números. La mayor parte de los enunciados de dichos teoremas y definiciones que se dan a lo largo de esta sección se han tomado de [9]. De esta manera, introducimos en primer lugar la definición de *divisibilidad*.

Definición 1.1. *Dados $a, b \in \mathbb{Z}$, decimos que a divide a b y denotamos $a|b$ si $b = ka$ para algún $k \in \mathbb{Z}$. De lo contrario, decimos que a no divide a b y escribimos $a \nmid b$*

Teorema 1.1. *Supongamos que a, b, c son números enteros. Entonces*

1. *Si $a \neq 0$ entonces $a|0$, $a|a$, $a|(-a)$.*
2. *$1|a$, $(-1)|a$.*
3. *Si $a|b$ entonces $a|bc$.*
4. *Si $a|b$ y $b|c$ entonces $a|c$.*
5. *Si $a|b$ y $a|c$ entonces para todo $x, y \in \mathbb{Z}$, $a|(bx + cy)$.*
6. *Si $a|b$ y $b \neq 0$ entonces $|a| \leq |b|$.*
7. *Si $a|b$ y $b|a$ entonces $a = b$ o $a = (-b)$*

Una definición sumamente relacionada con la divisibilidad de números enteros, es el máximo común divisor entre dos números enteros.

Definición 1.2. *Si d divide a dos enteros a y b, entonces d es llamado común divisor de a y b. El conjunto de todos los divisores d es un conjunto finito de números enteros. Al máximo de este conjunto se le denomina* ***Máximo Común Divisor****, y se denota por (a,b).*

Teorema 1.2. *Sean $a,b \in \mathbb{Z}$ no ambos cero. Entonces $d=(a,b)$ si y solo si d satisface las siguientes propiedades:*

1. $d>0$ *(d es no negativo)*
2. $d|a$ *y* $d|b$ *(d es común divisor de a y b)*
3. *Si* $f|a$ *y* $f|b$ *implica* $f|d$ *(todo común divisor divide a d)*

Teorema 1.3. *(Lema de Euclides). Si $a|bc$ y $(a,b)=1$ entonces $a|c$.*

Corolario 1.1. *Si p es primo y $p|ab$ entonces $p|a$ o $p|b$*

Teorema 1.4. *(Teorema fundamental de la aritmética) Todo entero $n>1$ o es primo, o se puede factorizar como producto de primos. Este producto es único salvo por el orden de los factores.*

Si tomamos un entero $n>1$ se pueden agrupar los primos iguales en su factorización debido al *Teorema fundamental de la aritmética* (TFA), a esta fórmula se le denomina **forma canónica** del entero n y está dada por:

$$n=\prod_{k=1}^{r} p_k^{a_k}, \tag{1.1}$$

donde $a_k>0$ y $p_i \neq p_j$ si $i \neq j$.

Ahora se enuncia la definición de congruencia y sus propiedades junto con algunos teoremas.

Definición 1.3. *Sean $a,b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Si $n|(a-b)$ decimos que a y b son* ***congruentes módulo n*** *y escribimos*

$$a \cong b \pmod{n}.$$

Teorema 1.5. *La congruencia módulo n es una relación de equivalencia sobre $\mathbb{Z}$.*

Teorema 1.6. *Si $a \cong b \pmod{n}$ y $c \cong d \pmod{n}$ entonces*

1. *Para todo par de enteros r y s, $ar+cs \cong br+ds \pmod{n}$.*
2. $ac \cong bd \pmod{n}$.
3. *Para todo entero r, $a+r \cong b+r \pmod{n}$ y $ar \cong br \pmod{n}$.*

A continuación introducimos la función ϕ de Euler, con el fin de enunciar el teorema de Euler y Fermat que será utilizado más adelante.

Definición 1.4. *Para cada entero positivo n, definimos $\phi(n)$ como el número de enteros positivos menores o iguales que n y primos relativos con n.*

De esta manera los primeros valores de $\phi(n)$ se pueden ver en la siguiente tabla:

n:	1	2	3	4	5	6	7	8	9	10
$\phi(n)$:	1	1	2	2	4	2	6	4	6	4

Teorema 1.7. *(Teorema de Euler) Si* $(a,n) = 1$ *entonces*

$$a^{\phi(n)} \cong 1 \pmod{n}.$$

Corolario 1.2. *(Teorema de Fermat) Si p es un número primo y* $(a,p) = 1$ *entonces*

$$a^{p-1} \cong 1 \pmod{p}.$$

La siguiente proposición es primordial para uno de los resultado de este trabajo y es una importante propiedad de los números primos.

Proposición 1.1. *La raíz de un número primo p es irracional*

Demostración: Sea p un primo. Supongamos que la raíz de p es racional, esto es,

$$\sqrt{p} = \frac{a}{b},$$

con $(a,b) = 1$. Así, elevando al cuadrado

$$p = \frac{a^2}{b^2}.$$

Por lo que $b^2 p = a^2$, de esta manera $p|a^2$, y así $p|a$. Luego existe k tal que $a = pk$, elevando al cuadrado tenemos $a^2 = k^2 p^2$, y obtenemos que $b^2 = pk^2$, de esta manera $p|b^2$, con lo que $p|b$. Lo cuál es una contradicción. □

El siguiente teorema se conoce como el *Teorema de Dirichlet*, es un resultado clásico de la teoría analítica de números. La demostración de dicho teorema es extensa y requiere de resultados complejos que no hacen parte de nuestro estudio. Sin embargo, para el objetivo de nuestro trabajo utilizamos una variación de él, cuya demostración está a nuestro alcance.

Teorema 1.8. *(Teorema de Dirichlet) Sean* $h,k > 0$ *dos enteros tales que* $(h,k) = 1$*, entonces existe al menos un número primo de la forma* $kn + h$*.*

Proposición 1.2. *Existen infinitos primos de la forma* $4k+3$

Demostración: Como $4k+3 = 4(k+1)-1$, basta demostrar que existen infinitos primos de la forma $4k-1$. Supongamos que existe un número finito de primos, $p_1, p_2, \ldots, p_n$, de la forma $4k-1$. Consideremos al entero $N = 4p_1 p_2 \ldots p_n - 1$, así

$$N \cong -1 \pmod{4}$$

Como $N > p_i$, para $1 \leq i \leq n$, y N es de la forma $4k-1$, por el TFA debe ser producto de números primos y debe tener como factor algún primo p_i de la forma $4k-1$. Así, $p_i|N$ y $p_i|4p_1 \cdots p_n$, por el item (5) del teorema 1.1, $p_i|4p_1 \cdots p_n - N$, por lo que $p_i|1$, lo cual es una contradicción. □

Proposición 1.3. *Existen infinitos primos de la forma* $4n+1$

Demostración: Sea N un entero cualquiera tal que $N>1$. Ahora, tomemos

$$m=(N!)^2+1.$$

Nótese que m es impar y $m>1$. Sea p el menor factor primo de m. Supongamos que $p\leq N$ entonces $p|(N!)^2$ y como $p|m$ entonces $p|1$, lo que es absurdo. Luego necesariamente $p>N$. También tenemos que

$$(N!)^2\cong -1 \pmod{p},$$

elevando a ambos lados por la potencia $(p-1)/2$ encontramos

$$(N!)^{p-1}\cong (-1)^{(p-1)/2} \pmod{p}. \tag{1.2}$$

Por el razonamiento anterior $p\not|(N!)^2$, por lo que $p\not|N!$ y así $(N!,p)=1$, luego por el teorema de Fermat

$$(N!)^{p-1}\cong 1 \pmod{p}. \tag{1.3}$$

De (1.2) y (1.3) obtenemos

$$(-1)^{(p-1)/2}\cong 1 \pmod{p}$$

Ahora la diferencia $(-1)^{(p-1)/2}-1$ es 0 o -2, y como $p\not|-2$ pues $p|m$ y m es impar, entonces $(-1)^{(p-1)/2}=1$, lo que implica que $(p-1)/2$ es par. Y así $p\cong 1 \pmod 4$. Luego existen infinitos primos de la forma $4k+1$. □

1.2. Permutaciones

En esta sección se dan algunas nociones de permutaciones y sus propiedades, basadas en [4].

Definición 1.5. *Una permutación de un conjunto A es una función de A en A biyectiva.*

Teorema 1.9. *Sea A un conjunto no vacío y sea S_A la familia de todas las permutaciones de A. Entonces S_A es un grupo bajo la composición.*

Si $A=\{1,2,\ldots,n\}$ entonces el grupo de todas las permutaciones de A es el grupo simétrico de n elementos y se denota por S_n. Este grupo tiene $n!$ elementos.

Definición 1.6. *Una permutación σ de un conjunto A es un ciclo de longitud k si existen $a_1,a_2,\ldots,a_n\in A$ tales que*

$$\sigma(a_1)=a_2,\quad \sigma(a_2)=a_3,\quad \sigma(a_1)=a_2,\quad \ldots,\quad \sigma(a_{n-1})=a_n\quad \sigma(a_n)=a_1.$$

y $\sigma(x)=x$ para toda $x\in A$ tal que $x\notin\{a_1,a_2,\ldots,a_n\}$.

Definición 1.7. *Un ciclo de longitud 2 es una transposición.*

Teorema 1.10. *Cualquier permutación de un conjunto finito de al menos dos elementos es un producto de transposiciones.*

Definición 1.8. *Una permutación de un conjunto finito es par (resp. impar) si se puede expresar como composición de un número par (resp. impar) de transposiciones.*

Teorema 1.11. *Si $n \geq 2$, la colección de todas las permutaciones pares de $\{1,2,\ldots,n\}$ forma un subgrupo de orden $n!/2$ del grupo simétrico S_n.*

Definición 1.9. *El subgrupo de S_n que consta de las permutaciones pares de n elementos es el grupo alternante A_n.*

1.3. Extensiones campos y Grupo de Galois

Con el fin de definir el grupo de Galois de un polinomio deben presentarse algunas definiciones y propiedades fundamentales del álgebra abstracta, éstas en su mayoría se basan en [4,5].

Definición 1.10. *Sea F un campo. Un campo K se dice una extensión de F si $F \leq K$. Es decir, F es un subcampo de K.*

Definición 1.11. *Un elemento $\alpha \in K$ es **algebraico sobre F** si es raíz de algún polinomio no nulo, es decir si $f(\alpha) = 0$ para algún $f(x) \in F[x]$ no nulo. De lo contrario α es **trascendente sobre F**.*

Definición 1.12. *Sea F un campo. Un polinomio $p(x)$ no constante en $F[x]$ se dice **irreducible** si no puede expresarse como producto de dos polinomios de grado menor que el de $p(x)$. En otras palabras si $p(x) = q(x)s(x)$ con $q(x), s(x) \in F[x]$ entonces $q(x)$ o $s(x)$ es de grado cero, es decir, es una constante.*

Teorema 1.12. *Sea $\alpha \in K$ algebraico sobre F con K una extensión de F, entonces existe un polinomio irreducible $p(x) \in F[x]$ tal que $p(\alpha) = 0$.*

Al polinomio mónico del teorema anterior se le llama *polinomio irreducible para α sobre F* y se denota por $irr(\alpha, F)$. Como este polinomio es irreducible el ideal generado por él , denotado por $\langle irr(\alpha, F)\rangle$ es maximal y por tanto $F[x]/\langle irr(\alpha, F)\rangle$ es un campo, y lo denotamos por $F(\alpha)$.

Definición 1.13. *Si K es de dimensión finita como espacio vectorial sobre F, entonces se dice que K es un **extensión finita** sobre F. El grado de K sobre F es la dimensión de K como espacio vectorial sobre F y lo denotamos como $[K : F]$.*

Con la finalidad de encontrar un campo E, extensión finita de F y de grado minimal, en el cual un polinomio $p(x) \in F[x]$ de grado n, tenga todas sus raíces en K. Se necesitan las siguientes proposiciones:

Proposición 1.4. *Si $p(x) \in F[x]$ y si K es una extensión de F, entonces para cualquier elemento $b \in K$, $p(x) = (x-b)q(x) + p(b)$, donde $q(x) \in K[x]$ y $gr(q(x)) = gr(p(x)) - 1$, donde $gr(q(x))$ denota el grado de $q(x)$.*

Proposición 1.5. *Sea $f(x) \in F[x]$ de grado $n \geq 1$, Entonces existe una extensión E de F, con $[E:F] \leq n!$, en la que $f(x)$ tiene n raíces.*

Como resultado de las anteriores proposiciones obtenemos una extensión finita E en la que un polinomio $f(x) \in F[x]$, de grado n, tiene todas sus raíces en E, además $f(x)$ se puede descomponer completamente sobre E como producto de factores lineales. Para encontrar la extensión finita de grado minimal se da la siguiente definición:

Definición 1.14. *Si $f(x) \in F[x]$, una extensión finita E de F se dice que es un **campo de descomposición** de $f(x)$ sobre F si $f(x)$ puede ser descompuesto en un producto de factores lineales sobre E, pero no en ningún subcampo propio de E.*

Definición 1.15. *Sea σ una aplicación de K sobre si mismo, $\sigma : K \to K$. Dados $a, b \in K$ cualesquiera, se dice que σ es un **automorfismo del campo** K si:*

1. $\sigma(a+b) = \sigma(a) + \sigma(b)$
2. $\sigma(ab) = \sigma(a)\sigma(b)$

Dos automorfismos σ y τ se dice que son distintos si $\sigma(a) \neq \tau(a)$ para al menos un elemento $a \in K$.

Definición 1.16. *Sea K un campo y sea F un subcampo de K. Entonces **el grupo de automorfismos de** K **relativos a** F, que se denota como $G(K,F)$, es el conjunto de todos los automorfismos de K que dejan fijos todos los elementos de F, esto es, el automorfismo σ de K está en $G(K,F)$ si y sólo si $\sigma(a) = a$ para todo $a \in F$.*

Definición 1.17. *Sea $f(x)$ un polinomio en $F[x]$ y sea K un campo de descomposición sobre F. El **grupo de Galois de** $f(x)$ es el grupo $G(K,F)$ de todos los automorfismos de K que dejan fijos los elementos de F.*

El grupo de Galois de $f(x)$ puede considerarse como un grupo de permutaciones de sus raíces, ya que si α es una raíz de $f(x)$ y si $\sigma \in G(K,F)$ entonces $\sigma(\alpha)$ es también una raíz de F. Así, dicho grupo puede considerarse un subgrupo de S_n, donde S_n es el grupo de todas las permutaciones de $\alpha_1, \ldots, \alpha_n$.

Capítulo 2

Conceptos Básicos

2.1. Relación entre el grupo de Galois y el discriminante de un polinomio

En esta sección se definen el resultante y discriminante de un polinomio y se dan algunas propiedades de ellos, pues, el discriminante de un polinomio tiene una relación cercana con el grupo de Galois de un polinomio. Así, al finalizar esta sección se muestra la relación entre ellos.

2.1.1. Resultante y Discriminante

Sean $f(x)$ y $g(x)$ dos polinomios en $F[x]$, F un campo, y sea K, el campo de descomposición de $f(x)$ y $g(x)$ sobre F.

Definición 2.18. *Sea $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ y $g(x) = b(x-\beta_1)\cdots(x-\beta_m)$ la descomposición de f y g en $K[x]$. Entonces el **resultante** $R(f,g)$ de f y g está dado por las siguientes fórmulas equivalentes:*

$$\begin{aligned} R(f,g) &= a^m g(\alpha_1)\cdots g(\alpha_n) \\ &= (-1)^{nm} b^n f(\beta_1)\cdots f(\beta_m) \\ &= a^m b^n \prod_{\substack{1\le i\le n \\ 1\le j\le n}} (\alpha_i - \beta_j). \end{aligned}$$

Definición 2.19. *Si $f(x) \in F[x]$ es un polinomio de grado n tal que $f(x) = \sum_{i=0}^{n} a_i x^i$, se define el **discriminante** de $f(x)$, $disc(f)$, por medio de la siguiente expresión:*

$$disc(f) = (-1)^{\frac{1}{2}n(n-1)} \frac{1}{a_n} R(f, f'),$$

donde f' es la derivada de f.

Proposición 2.6. *Sea $f(x) \in F[x]$ un polinomio de grado n, y sean α_i las raíces de $f(x)$ en K. Entonces*

$$disc(f) = (a_n)^{n-1+deg(f')} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2. \tag{2.1}$$

donde $deg(f')$ es el grado del polinomio obtenido por la derivada de $f(x)$

Demostración: Sea $f(x) \in F[x]$ tal que $f(x) = \sum_{i=0}^{n} a_i x^i$. Podemos escribir

$$f(x) = a_n \prod_{i=1}^{n} (x - \alpha_i).$$

Derivando obtenemos

$$f'(x) = a_n \sum_i \prod_{j \neq i}^{n} (x - \alpha_j).$$

Así

$$f'(\alpha_i) = a_n \prod_{j \neq i}^{n} (\alpha_i - \alpha_j).$$

Entonces nosotros obtenemos que

$$R(f, f') = (a_n)^{n+deg(f')} (-1)^{n(n-1)/2} \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

esto prueba la proposición. □

Por medio de la proposición anterior y directamente de la definición de discriminante se obtiene el siguiente corolario.

Corolario 2.3. *Sea $f(x) \in F[x]$ un polinomio de grado n, y sean α_i las raíces de f en K. Entonces*

$$disc(f) = (-1)^{\frac{1}{2}n(n-1)} (a_n)^{n-2} \prod_{i=1}^{n} f'(\alpha_i). \tag{2.2}$$

Las propiedades del discriminante de un polinomio pueden obtenerse directamente de la definición, y se dan a continuación:

Lema 2.1. *Sea $f(x) \in F[x]$ un polinomio de grado n. Entonces*

1. *Para todo $k = cte$, se tiene que $disc(f(x+k)) = disc(f(x))$.*
2. *$disc(f(2x)) = 2^{n(n-1)} disc(f(x))$.*

Si $f(x) \in F[x]$ un polinomio mónico irreducible de grado n, con todas sus raíces $\alpha_1, \ldots, \alpha_n$ en un campo de descomposición K de $f(x)$ sobre F, y suponiendo que $f(x)$ se factoriza en $K[x]$ por

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i), \tag{2.3}$$

denotamos a la raíz cuadrada del discriminante de f, $\sqrt{disc(f(x))}$, por:

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j). \tag{2.4}$$

2.1.2. Grupo de Galois y Discriminante

A continuación se darán las proposiciones que relacionan el grupo de Galois de un polinomio y su discriminante.

Proposición 2.7. *Para cada $\sigma \in G(K,F) < S_n$, σ es una permutación par si y sólo si $\sigma(\Delta) = \Delta$, además σ es impar si y sólo si $\sigma(\Delta) = -\Delta$*

Demostración: Sea σ una tansposición, $\sigma = (\alpha_c \alpha_d)$ con $c < d$. Hacemos

$$\begin{aligned}\Delta(f) &= \prod_{i<j}(\alpha_i - \alpha_j) \\ &= (\alpha_c - \alpha_d)\cdot\rho_1\cdot\rho_2\cdot\rho_3\cdot\rho_4\cdot\rho_5\cdot\rho_6\cdot\rho_7,\end{aligned}$$

donde

$$\begin{aligned}\rho_1 &= \prod_{i<j}(\alpha_i - \alpha_j) \qquad \text{con } i,j \neq c,d \\ \rho_2 &= \prod_{i<c}(\alpha_i - \alpha_c) \\ \rho_3 &= \prod_{i<c}(\alpha_i - \alpha_d) \\ \rho_4 &= \prod_{c<i<d}(\alpha_i - \alpha_d) \\ \rho_5 &= \prod_{c<j<d}(\alpha_c - \alpha_j) \\ \rho_6 &= \prod_{d<j}(\alpha_c - \alpha_j) \\ \rho_7 &= \prod_{d<j}(\alpha_d - \alpha_j).\end{aligned}$$

De esta manera aplicando σ se tiene

$$\sigma(\Delta) = \sigma(\alpha_c - \alpha_d)\sigma(\rho_1)\sigma(\rho_2)\sigma(\rho_3)\sigma(\rho_4)\sigma(\rho_5)\sigma(\rho_6)\sigma(\rho_7). \tag{2.5}$$

Así,

$$\begin{aligned}&\sigma(\alpha_c - \alpha_d) = \sigma(\alpha_c) - \sigma(\alpha_d) = \alpha_d - \alpha_c = -(\alpha_c - \alpha_d) \\ &\sigma(\rho_1) = \sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = \prod_{i<j}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{i<j}(\alpha_i - \alpha_j) = \rho_1, \qquad i,j \neq c,d \\ &\sigma(\rho_2) = \sigma\left(\prod_{i<c}(\alpha_i - \alpha_c)\right) = \prod_{i<c}(\sigma(\alpha_i) - \sigma(\alpha_c)) = \prod_{i<c}(\alpha_i - \alpha_d) = \rho_3 \\ &\sigma(\rho_3) = \sigma\left(\prod_{i<c}(\alpha_i - \alpha_d)\right) = \prod_{i<c}(\sigma(\alpha_i) - \sigma(\alpha_d)) = \prod_{i<c}(\alpha_i - \alpha_c) = \rho_2\end{aligned}$$

$$\sigma(\rho_4) = \sigma\left(\prod_{c<i<d}(\alpha_i - \alpha_d)\right) = \prod_{c<i<d}(\sigma(\alpha_i) - \sigma(\alpha_d)) = (-1)^{d-c-1}\prod_{c<i<d}(\alpha_c - \alpha_i) = (-1)^{d-c-1}\rho_5$$

$$\sigma(\rho_5) = \sigma\left(\prod_{c<j<d}(\alpha_c - \alpha_j)\right) = \prod_{c<j<d}(\sigma(\alpha_c) - \sigma(\alpha_j)) = (-1)^{d-c-1}\prod_{c<j<d}(\alpha_j - \alpha_d) = (-1)^{d-c-1}\rho_4$$

$$\sigma(\rho_6) = \sigma\left(\prod_{d<j}(\alpha_c - \alpha_j)\right) = \prod_{d<j}(\sigma(\alpha_c) - \sigma(\alpha_j)) = \prod_{d<j}(\alpha_d - \alpha_j) = \rho_7$$

$$\sigma(\rho_7) = \sigma\left(\prod_{d<j}(\alpha_d - \alpha_j)\right) = \prod_{d<j}(\sigma(\alpha_d) - \sigma(\alpha_j)) = \prod_{d<j}(\alpha_c - \alpha_j) = \rho_6.$$

Por lo tanto $\sigma(\Delta) = (-1)^{2(d-c-1)+1}(\alpha_c - \alpha_d)\cdot\rho_1\cdot\rho_2\cdot\rho_3\cdot\rho_4\cdot\rho_5\cdot\rho_6\cdot\rho_7 = -\Delta$. Se sabe que una permutación es par (respectivamente impar) si es composición de un número par (respectivamente impar) de transposiciones. Por lo que queda probada la proposición. □

Teorema 2.13. *Sean F, f, K y Δ como se describen anteriormente.*

(a) *$f(x)$ tiene como factor el cuadrado de algún polinomio irreducible en $F[x]$ si y solo si $\Delta(f) = 0$.*

(b) *$(\Delta(f))^2 \in F$.*

(c) *$\Delta(f) \in F$ si y sólo si $G(K,F)$ es un subgrupo de A_n, el grupo de todas las permutaciones pares.*

Demostración:
(a) Sean $\alpha_1, \ldots, \alpha_n$ las raices de $f(x)$, si $\Delta(f) = 0$ se tiene que

$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j) = 0,$$

esto es, para algún factor de la productoria $\alpha_i - \alpha_j = 0$, con lo que $\alpha_i = \alpha_j$ para algún i. Como $f(x)$ se factoriza sobre $K[x]$

$$\begin{aligned} f(x) &= \prod_{i=1}^{n}(x - \alpha_i) \\ &= (x-\alpha_1)\cdots(x-\alpha_i)\cdots(x-\alpha_j)\cdots(x-\alpha_n) \\ &= (x-\alpha_1)\cdots(x-\alpha_i)^2\cdots(x-\alpha_{j-1})(x-\alpha_{j+1})\cdots(x-\alpha_n). \end{aligned}$$

Haciendo $f(x) = (x-\alpha_i)^2 g(x)$, se tiene que $f(x)$ tiene como factor el cuadrado de un polinomio irreducible sobre $F[x]$. Por otra parte si $f(x) = h(x)^2 k(x)$, con $h(x)$ irreducible en $F[x]$, h debe ser mónico de grado $m \leq n$. Por otra parte f se factoriza sobre $K[x]$ por (2.3), entonces

$$f(x) = h(x)^2 k(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

Como K es el campo de descomposición de f sobre F, las raíces $\beta_1,\ldots,\beta_m$ de $h(x)$ están en K y h se puede factorizar en $K[x]$, $h(x)=(x-\beta_1)\cdots(x-\beta_m)$. Al igual que las raices $\gamma_1\ldots,\gamma_s$ de $k(x)$. Por lo que

$$\begin{aligned} f(x) &= h(x)^2 k(x) \\ &= [(x-\beta_1)\cdots(x-\beta_m)]^2[(x-\gamma_1)\cdots(x-\gamma_s)] \\ &= (x-\beta_1)\cdots(x-\beta_m)(x-\beta_1)\cdots(x-\beta_m)(x-\gamma_1)\cdots(x-\gamma_s). \end{aligned}$$

De esta manera si $f(x)$ se factoriza por (2.3) algún $\alpha_i=\alpha_j$, y por tanto $\Delta(f)=0$.

(b) Sea $\sigma\in G(K,F)$, así $\sigma(\Delta^2)=(\sigma(\Delta))^2$ y por proposición 2.7 $\sigma(\Delta^2)=(\pm\Delta)^2=\Delta^2$, así $\Delta^2\in F$.

(c) Si $\Delta\in F$, para cada $\sigma\in G(K,F)$, se tiene $\sigma(\Delta)=\Delta$, y por la proposición 2.7 el $sgn(\sigma)=1$, siendo sgn la función signo, luego $\sigma\in A_n$.

Sea $G(K,F)$ subgrupo de A_n. Sabemos que si $\sigma\in G(K,F)$ entonces $\sigma(\Delta)=\pm\Delta$. Por otro lado, $\sigma\in A_n$ si y solo si $sgn(\sigma)=1$, es decir σ es par, y por proposición 2.7 $\sigma(\Delta)=\Delta$, así como Δ queda fijo por los elementos de $G(K,F)$, entonces $\Delta\in F$. □

2.2. Funciones Especiales

En esta sección se definen algunas funciones especiales: la función Gamma, la función hipergeométrica y el factorial de Pochhammer, la definición y propiedades de estas funciones pueden encontrarse en [6]. Estas funciones nos ayudan a definir un tipo de polinomios ortogonales clásicos, los polinomios de Jacobi. Estos polinomios hacen parte fundamental de este trabajo, pues trabajaremos con sus propiedades, debido a que los polinomios de Legendre pueden expresarse por medio de los polinomios de Jacobi.

2.2.1. Función Gamma y Propiedades

La función gamma fue introducida por primera vez en el año 1729, por el matemático Leonhard Euler; pero en 1811, el matemático Adrien Legendre la mofidicó y la llamó Gamma Γ. Dicha función juega un papel importante en la definición del factorial de Pohlhammer.

Así, se puede definir la función gamma por medio de la integral de Euler, además se mostrarán algunas propiedades de dicha función.

Definición 2.20. *Para $x\in\mathbb{R}$ la función gamma, $\Gamma:\mathbb{R}\to\mathbb{R}$, se define por:*

$$\Gamma(x)=\int_0^\infty e^{-t}t^{x-1}\,dt \qquad\qquad x>0. \tag{2.6}$$

A continuación se puede ver la gráfica de la función Gamma.

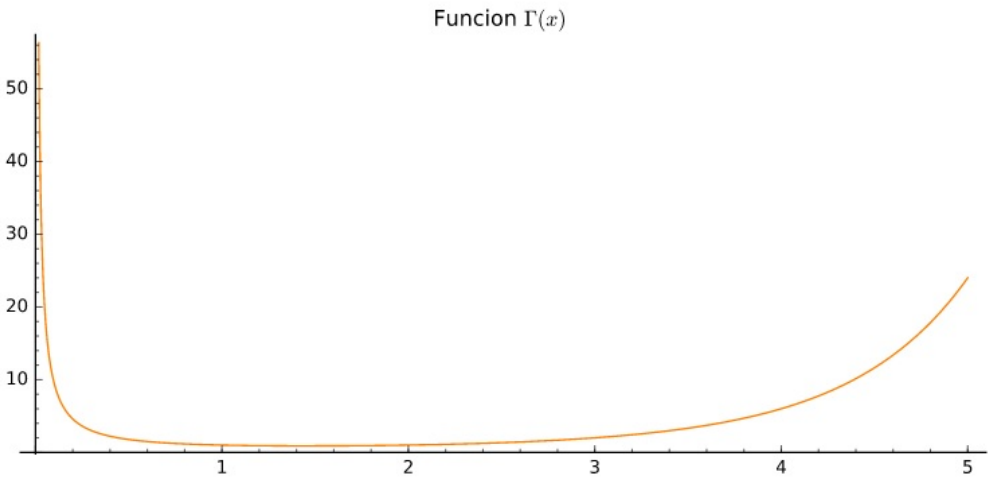

Figura 2.1: Función Gamma

Proposición 2.8. *Para todo $x \in \mathbb{R}$ tal que $x > 0$, se tiene que*

$$\Gamma(x+1) = x\Gamma(x),$$

además $\Gamma(1) = 1$ y si $n \in \mathbb{Z}^+$, $\Gamma(n) = (n-1)!$.

Demostración:
Para $x \in \mathbb{R}$ con $x > 0$, por definición de Γ e integrando por partes obtenemos

$$\begin{aligned} \Gamma(x+1) &= \int_0^\infty e^{-t} t^x \, dt \\ &= -t^x e^{-t}\big|_0^\infty + \int_0^\infty x e^{-t} t^{x-1} \, dt \\ &= x \int_0^\infty e^{-t} t^{x-1} \, dt \\ &= x\Gamma(x). \end{aligned} \tag{2.7}$$

Ahora evaluando en $\Gamma(x)$ cuando $x = 1$, tenemos

$$\Gamma(1) = \int_0^\infty e^{-t} \, dt = -e^{-t}\big|_0^\infty = 1. \tag{2.8}$$

Para finalizar nótese que si $n \in \mathbb{Z}^+$ la propiedad $\Gamma(n) = (n-1)!$ se sigue utilizando las ecuaciones (2.7) y (2.8). □

2.2.2. Factorial de Pochhhammer

Definición 2.21. *La función $(\alpha)_n$ es llamada la función factorial y se define por*

$$\begin{aligned} (\alpha)_n &= \prod_{k=1}^{n} (\alpha + k - 1) \\ &= \alpha(\alpha+1)(\alpha+2)\cdots(\alpha+n-1), && n \geq 1, \\ (\alpha)_0 &= 1, && \alpha \neq 0. \end{aligned}$$

Esta función es una generalización del factorial elemental, pues $n! = (1)_n$.

Proposición 2.9. *Si α es distinto de cero y no es un entero negativo, entonces*

$$(\alpha)_n = \frac{\Gamma(\alpha+n)}{\Gamma(\alpha)}. \tag{2.9}$$

Demostración:
Por la proposición 2.8 y para $n \in \mathbb{Z}^+$, tenemos

$$\begin{aligned}\Gamma(\alpha+n) &= (\alpha+n-1)\Gamma(\alpha+n-1)\\ &= (\alpha+n-1)(\alpha+n-2)\Gamma(\alpha+n-2)\\ &= \cdots\\ &= (\alpha+n-1)(\alpha+n-2)\cdots\alpha\Gamma(\alpha).\end{aligned}$$

Por lo que se deduce la ecuación (2.9). □

Proposición 2.10. *Si α es distinto de cero y no es un entero negativo, se cumplen las siguientes propiedades:*

1. $n(\alpha)_n = \alpha((\alpha+1)_n - (\alpha)_n)$.
2. $(\alpha)_{n+1} = (\alpha+n)(\alpha)_n = \alpha(\alpha+1)_n$.
3. $\dfrac{n}{(\alpha)_n} = \dfrac{\alpha-1}{(\alpha-1)_n} - \dfrac{\alpha-1}{(\alpha)_n}$.

2.2.3. Función Hipergeométrica

Definición 2.22. *La función hipergeométrica está dada por la serie de potencias*

$$F(a,b;c;z) = 1 + \sum_{n=1}^{\infty} \frac{(a)_n(b)_n}{(c)_n n!} z^n = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n n!} z^n, \tag{2.10}$$

para $c \in \mathbb{Z}^+$ y $c \neq 0$. Donde $(x)_n$ es el factorial de Pochhammer.

Nótese que si a, b, c son diferentes de cero y no negativos, la serie converge en los $z \in \mathbb{C}$, $|z| < 1$ y diverge para $|z| > 1$, pues si aplicamos el criterio de D'Alembert, obtenemos

$$\lim_{n\to\infty} \left| \frac{(a)_{n+1}(b)_{n+1} z^{n+1}}{(c)_{n+1}(n+1!)} \cdot \frac{(c)_n n!}{(a)_n (b)_n z^n} \right| = \lim_{n\to\infty} \left| \frac{(a+n)(b+n)z}{(c+n)(n+1)} \right| = |z|.$$

Proposición 2.11. *Para $|z| < 1$ la función hipergeométrica satisface la ecuación diferencial lineal de segundo orden*

$$z(1-z)w'' + [c-(a+b+1)z]w' - abw = 0, \tag{2.11}$$

*a esta ecuación diferencial se le denomina **ecuación diferencial hipergeométrica**.*

Demostración: Se define el operador $D = z\frac{d}{dz}$ y denotemos por

$$w = F(a,b;c;z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n.$$

De esta manera, aplicando D y por la propiedad (3) de la proposición 2.10 se obtiene

$$\begin{aligned} Dw &= \sum_{n=0}^{\infty} \frac{n(a)_n (b)_n}{(c)_n n!} z^n \\ &= \sum_{n=0}^{\infty} \left(\frac{c-1}{(c-1)_n} - \frac{c-1}{(c)_n} \right) \frac{(a)_n (b)_n}{n!} z^n \\ &= (c-1) \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c-1)_n n!} z^n - (c-1) \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n \\ &= (c-1)F(a,b;c-1;z) - (c-1)w. \end{aligned}$$

Por lo que

$$(D+c-1)w = (c-1)F(a,b;c-1;z).$$

Aplicando nuevamente D a la ecuación anterior y junto con la propiedad (2) de la proposición 2.10, se tiene

$$\begin{aligned} D(D+c-1)w &= (c-1) \sum_{n=1}^{\infty} \frac{(a)_n (b)_n}{(c-1)_n n!} n z^n \\ &= \sum_{n=1}^{\infty} \frac{(a)_n (b)_n}{(c)_{n-1} (n-1)!} z^n. \end{aligned}$$

Haciendo un cambio de índice

$$\begin{aligned} D(D+c-1)w &= \sum_{n=0}^{\infty} \frac{(a)_{n+1} (b)_{n+1}}{(c)_n n!} z^{n+1} \\ &= z \sum_{n=0}^{\infty} \frac{a(a+1)_n b(b+1)_n}{(c)_n n!} z^n \\ &= zabF(a+1,b+1;c;z) \\ &= z(D+a)(D+b)w. \end{aligned}$$

Así

$$[D(D+c-1) - z(D+a)(D+b)]w = 0. \tag{2.12}$$

Nótese que $Dw = zw'$ y $D(D-1)w = z^2 w''$. Así, por un lado

$$D(D+c-1)w = D(D-1) + cDw = z^2 w'' + czw',$$

y por otro lado

$$\begin{aligned} z(D+a)(D+b)w &= z(D+a)(D-1+(b+1))w \\ &= z(D(D-1+(b+1)) + a(D+b))w \\ &= z(z^2 w'' + (b+1)zw' + azw' + abw). \end{aligned}$$

Reemplazando en la ecuación (2.12) y factorizando obtenemos

$$z(1-z)w'' + [c-(a+b+1)z]w' - abw = 0.$$

Con lo que la función hipergeométrica cumple (2.11). □

2.3. Funcionales de momento y propiedades

En esta sección se dan algunas definiciones y propiedades fundamentales sobre un funcional de momentos y los correspondientes polinomios ortogonales, en su mayoría tomadas de [2, 10]. Entre estas se encuentran la ortogonalidad, la fórmula fundamental de recurrencia, la existencia de una sucesión de polinomios ortogonales, funcional positivo, entre otras.

2.3.1. Ortogonalidad y fórmula fundamental de recurrencia

Definición 2.23. *Una transformación $\mathscr{L} : \mathbb{C}[x] \to \mathbb{C}$ lineal se denomina funcional de momentos, en otras palabras, una transformación $\mathbb{C}-$lineal del espacio de los polinomios con coeficientes complejos en el campo de los números complejos.*

Definición 2.24. *[2, pag.7] Se dice que una sucesión $\{P_n(x)\}_{n=0}^{\infty}$ de polinomios mónicos es una **SPO**(sucesión de polinomios ortogonales o un sistema de polinomios ortogonales) con respecto a un funcional de momentos $\mathscr{L}$ si para todo entero no negativo n y m, se tiene :*

(i) $P_n(x)$ *es de grado* n.

(ii) $\mathscr{L}(P_n(x)P_m(x)) = \lambda_n \delta_{nm}$, *con* $\lambda_n \neq 0$

Donde δ_{nm} *es el delta de Kronecker.*

Por simplicidad se denota la sucesión de polinomios $\{P_n(x)\}_{n=0}^{\infty}$ como $\{P_n(x)\}$. El siguiente teorema muestra una importante característica de los polinomios ortogonales, muestra que, dado un funcional de momentos y su correspondiente SPO, los polinomios ortogonales pueden escribirse en términos de los polinomios inmediatamente anteriores.

Teorema 2.14. *Si $\{P_n(x)\}$ es una SPO para $\mathscr{L}$, existen $B_n, C_n \in \mathbb{C}$, $n \geq 0$, con $C_n \neq 0$, $n \geq 1$, de tal manera que se satisface la siguiente recurrencia:*

$$P_{n+1}(x) = (x - B_n)P_n(x) - C_n P_{n-1}(x), \tag{2.13}$$

donde $P_{-1}(x) = 0$ y $P_0(x) = 1$., y así la SPO queda determinada de manera única por (2.13).

Demostración: Por hipótesis $\{P_n(x)\}$ es un SPO, luego $P_n(x)$ es de grado n, por lo que $\{P_n(x)\}$ es una base de $\mathbb{C}[x]$. Como $xP_n(x)$ es un polinomio de grado $n+1$ podemos escribirlo como combinación lineal

$$xP_n(x) = \sum_{i=0}^{n+1} a_{n,i} P_i(x) \quad \text{para } n \geq 0, \tag{2.14}$$

donde los $a_{n,i} \in \mathbb{C}$ y $a_{n,n+1} = 1$.

Para $n = 0$ y $n = 1$ la recurrencia (2.13) se tiene, luego supongamos $n \geq 2$. Al multiplicar $P_k(x)$ con $0 \leq k \leq n-2$ a ambos lados de (2.14) se tiene

$$xP_n(x)P_k(x) = \sum_{i=0}^{n+1} a_{ni} P_i(x)P_k(x). \tag{2.15}$$

Además $xP_k(x)$ lo podemos escribir como combinación lineal, esto es

$$xP_k(x) \sum_{j=0}^{k+1} a_{kj} P_j(x).$$

Aplicando $\mathscr{L}$ se tiene

$$\mathscr{L}(xP_k(x)P_n(x)) = \sum_{j=0}^{k+1} a_{kj} \mathscr{L}(P_j(x)P_n(x)).$$

Como $k \leq n-2$ se tiene para $j \leq k+1$ que $j \leq n-1 < n$. Así $\mathscr{L}(xP_k(x)P_n(x)) = 0$ por definición, y además $\mathscr{L}(xP_k(x)P_n(x)) = a_{kn}\lambda_k$. Como $\lambda : k \neq 0$, implica que $a_{kn} = 0$ para $0 \leq k \leq n-2$. Luego reemplazando en (2.14) y haciendo $a_{nn} = B_n$ y $a_{n,n-1} = C_n$ se obtiene la relación (2.13).

Por otra parte, si $n \geq 1$, al multiplicar por $P_n(x)$ en (2.13) se obtiene

$$P_n^2(x) = (x - B_{n-1})P_{n-1}(x)P_n(x) - C_{n-1}P_{n-2}(x)P_n(x).$$

Aplicando $\mathscr{L}$ se tiene que

$$\mathscr{L}(P_n^2(x)) = \mathscr{L}(xP_{n-1}(x)P_n(x)).$$

Por otro lado

$$P_{n-1}(x)P_{n+1}(x) = (x - B_n)P_{n-1}(x)P_n(x) - C_n P_{n-1}^2(x).$$

De igual manera aplicando $\mathscr{L}$

$$\mathscr{L}(P_n^2(x)) = C_n \mathscr{L}(P_{n-1}^2(x)$$

Como $\mathscr{L}(P_n^2(x)) \neq 0$ para $n \geq 1$, de esta manera $C_n \neq 0$. Lo que concluye la prueba. □

El inverso del teorema 1.1, el cual justifica que cualquier sucesión de polinomios satisface la relación de recurrencia (2.13) es un SPO, esta inversa se le atribuye a J. Favard en 1935, y se presenta a continuación:

Teorema 2.15. *(Teorema de Fovard). Sean* $\{B_n\}_{n=0}^{\infty}$ *y* $\{C_n\}_{n=0}^{\infty}$ *sucesiones arbitrarias de números complejos, con* $C_n \neq 0$*, y sea* $\{P_n(x)\}$ *una sucesión de polinomios mónicos definidos por la relación de recurrencia:*

$$\begin{aligned} &xP_n(x) = P_{n+1}(x) + B_nP_n(x) + C_nP_{n-1}(x) \quad \text{para } n \geq 0, \\ &P_{-1}(x) = 0, P_0(x) = 1, \end{aligned} \tag{2.16}$$

existe un único funcional de momentos $\mathscr{L}$ *tal que*

$$\mathscr{L}(1) = 1 \qquad \mathscr{L}(P_mP_n(x)) = 0 \qquad \text{para } m \neq n,\ m, n = 0, 1, \ldots$$

$\mathscr{L}$ *está bien definido y* $\{P_n(x)\}_{n=0}^{\infty}$ *es su correspondiente SPO mónico. Además*

$$\lambda_n = \mathscr{L}(P_n^2(x)) = C_1 \cdots C_n.$$

Demostración: Definamos el funcional de momentos $\mathscr{L}$ con las condiciones

$$\mathscr{L}(1) = \mu_0 = 1, \qquad \mathscr{L}(P_n(x)) = 0 \qquad n \geq 1. \tag{2.17}$$

Como $\{P_n(x)\}$ cumple (2.16) podemos extender el funcional de momentos por linealidad a todo $\mathbb{C}[x]$. Esto es, definimos μ_1 por la condición

$$\mathscr{L}(P_1(x)) = \mathscr{L}((x - B_0)P_0(x) - C_0P_{-1}(x)) = \mathscr{L}(x) - B_0\mathscr{L}(1) = \mu_1 - B_0\mu_0 = 0,$$

luego definimos μ_2 por

$$\begin{aligned} \mathscr{L}(P_2(x)) &= \mathscr{L}((x - B_1)P_1(x) - C_1P_0) = \mathscr{L}(x^2) - (B_0 + B_1)\mathscr{L}(x) + (B_1B_0 - C_1)\mathscr{L}(1) \\ &= \mu_2 - (B_0 + B_1)\mu_1 + (B_0B_1 - C_1)\mu_0 = 0, \end{aligned}$$

y así, siguiendo el proceso para obtener μ_n. De esta manera $\mathscr{L}$ será una transformación lineal de $\mathbb{C}[x]$ en $\mathbb{C}$.

Se prueba por inducción que para $m \geq 0$ fijo, $\mathscr{L}(x^mP_n(x)) = 0$ para todo $n > m$. Si $m = 0$ tenemos que $\mathscr{L}(x^mP_n(x)) = \mathscr{L}(P_n(x)) = 0$, por (2.17). Supongamos que se cumple para $m \leq k$ con $0 \leq k + 1 < n$, esto es, $\mathscr{L}(x^kP_n(x)) = 0$. Como

$$x^{k+1}P_n(x) = xx^kP_n(x) = x^k[P_{n+1}(x) + B_nP_n(x) + C_nP_{n-1}(x)].$$

Aplicando $\mathscr{L}$ y por linealidad, se obtiene

$$\mathscr{L}(x^{k+1}P_n(x)) = \mathscr{L}(x^kP_{n+1}(x)) + B_n\mathscr{L}(x^kP_n(x)) + C_n\mathscr{L}(x^kP_{n-1}(x)).$$

Así, por hipótesis de inducción cuando $m = k + 1$

$$\mathscr{L}(x^{k+1}P_n(x)) = 0. \tag{2.18}$$

Luego si $m \neq n$, $\mathscr{L}(P_m(x)P_n(x)) = 0$. Si $n = m$ se tiene que para $n \geq 1$

$$\begin{aligned}
\mathscr{L}(x^n P_n) &= \mathscr{L}(x^{n-1} x P_n(x)) \\
&= \mathscr{L}(x^{n-1} P_{n+1}(x)) + B_n \mathscr{L}(x^{n-1} P_n) + C_n \mathscr{L}(x^{n-1} P_{n-1}(x)) \\
&= C_n \mathscr{L}(x^{n-2} x P_{n-1}(x)) \\
&= C_n [\mathscr{L}(x^{n-2} P_n(x)) + B_{n-1} \mathscr{L}(x^{n-2} P_{n-1}(x)) + C_{n-1} \mathscr{L}(x^{n-2} P_{n-2}(x))] \\
&= C_n C_{n-1} \mathscr{L}(x^{n-2} P_n - 2(x)) \\
&\quad \vdots \\
&= C_n \cdots C_1.
\end{aligned}$$

Por consiguiente $\mathscr{L}$ está bien definido y $\{P_n(x)\}$ es el correspondiente SPO si y sólo si $C_n \neq 0$ para $n \neq 1$. □

Del anterior teorema también se puede deducir que si $R(x)$ es un polinomio de grado menor que n, entonces $\mathscr{L}(R(x)P_n(x)) = 0$.

2.3.2. Existencia de SPO

Definición 2.25. *Un funcional de momentos $\mathscr{L}$ se dice **regular**, si admite una SPOM, sucesión de polinomios ortogonales mónicos.*

Cabe resaltar que no todo funcional de momentos admite una sucesión de polinomios ortogonales. A continuación se verá la condición suficiente y necesaria para que $\mathscr{L}$ sea regular. Si $\mathscr{L}$ es un funcional de momentos, se denotará como $\{\mu_n\}_{n=0^\infty}$ a la sucesión de momentos , o por simplicidad $\{\mu_n\}$,donde $\mu_n = Lf(x^n)$. Y definamos

$$\Gamma_n = \det(\mu_{i+j})_{i,j=0}^n = \begin{vmatrix} \mu_0 & \mu_1 & \cdots & \mu_n \\ \mu_1 & \mu_2 & \cdots & \mu_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_n & \mu_{n+1} & \cdots & \mu_{2n} \end{vmatrix}. \tag{2.19}$$

Teorema 2.16. *Sea $\mathscr{L}$ un funcional de momentos y $\{\mu_n\}$ la correspondiente sucesión de momentos. Una condición necesaria y suficiente para la existencia de una SPO para $\mathscr{L}$ es*

$$\Gamma_n \neq 0, \qquad n = 0, 1, 2, \ldots \tag{2.20}$$

Demostración: Supongamos que $\mathscr{L}$ es regular y sea $\{P_n(x)\}$ un SPMO con respecto a $\mathscr{L}$. Si Γ_n está definida por (2.19). Veamos que $\Gamma_n \neq 0$ para $n \neq 0$. Para $n = 0$ se tiene que $\Gamma_0 = \mu_0 = \mathscr{L}(x^0) = 1$. Supongamos que se cumple para $m \leq k$, esto es, $\Gamma_k \neq 0$. Sea

$$P(x) = \frac{1}{\Gamma_k} \begin{vmatrix} \mu_0 & \cdots & \mu_k & \mu_{k+1} \\ \mu_1 & \cdots & \mu_{k+1} & \mu_{k+2} \\ \vdots & \ddots & \vdots & \vdots \\ \mu_k & \cdots & \mu_{2k} & \mu_{2k+1} \\ 1 & \cdots & x^k & x^{k+1} \end{vmatrix} \tag{2.21}$$

definido así, $P(x)$ es mónico de grado $k+1$, y así existen $a_i \in \mathbb{C}$ de tal forma que podemos escribir

$$P(x) = P_{k+1}(x) \sum_{i=0}^{k} a_i P_i(x).$$

Si $m < k+1$, sabemos que $\mathscr{L}(P(x)P_m(x)) = 0$, y además para cada $m = 0, 1, \ldots, k$ se tiene que

$$\begin{aligned}\mathscr{L}(P_m(x)P(x)) &= \mathscr{L}(P_m(x)P_{k+1}(x)) + \sum_{i=0}^{k} a_i \mathscr{L}(P_m(x)P_i(x)) \\ &= a_m \mathscr{L}(P_m^2(x)) = 0.\end{aligned}$$

Como $\mathscr{L}(P_m^2(x)) \neq 0$, entonces $a_m = 0$, para cada $m = 0, 1, \ldots, k$, así $P(x) = P_{k+1}(x)$. Por otro lado

$$\mathscr{L}(x^m P_n(x)) = \frac{1}{\Gamma_{n-1}} \begin{vmatrix} \mu_0 & \mu_1 & \cdots & \mu_n \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{n-1} & \mu_n & \cdots & \mu_{2n-1} \\ \mathscr{L}(x^m) & \mathscr{L}(x^{m+1}) & \cdots & \mathscr{L}(x^{m+n} \end{vmatrix}. \tag{2.22}$$

De esta manera

$$\mathscr{L}(P_{k+1}^2(x)) = \mathscr{L}(x^{k+1}P_{k+1}(x)) = \frac{\Gamma_{k+1}}{\Gamma_k}. \tag{2.23}$$

Así $\Gamma_{k+1} \neq 0$.

Recíprocamente, si $\Gamma_n \neq 0$, veamos que para $m \neq n$ se tiene que $\mathscr{L}(P_m(x)P_n(x)) = 0$ y además $\mathscr{L}(P_n^2(x)) \neq 0$. Si $m < n$ entonces en el determinante de la ecuación (2.22) una de las filas se repite, pues $\mathscr{L}(x^k) = \mu_k$, y por propiedades del determinante obtenemos que $\mathscr{L}(x^m P_n(x)) = 0$. Por otra parte, de la ecuación (2.23) y como por hipótesis $\Gamma_n \neq 0$, entonces $\mathscr{L}(P_n^2(x)) \neq 0$, de esta manera $\mathscr{L}$ es regular, lo que concluye la prueba. □

2.3.3. Funcional positivo

Definición 2.26. *Sea $\mathscr{L}$ un funcional regular, se dice que $\mathscr{L}$ es un* ***funcional positivo*** *si el correspondiente SPOM está dado por la recurrencia (1.1) y $C_n > 0$ para $n \geq 1$.*

Lema 2.2. *Sea $\pi(x) \neq 0$ un polinomio con coeficientes reales que no toma valores negativos en el eje real, esto es $\pi(x) \geq 0$ para todo $t \in \mathbb{R}$. Si $\mathscr{L}$ es positivo, entonces $\mathscr{L}(\pi(x)) > 0$.*

Demostración: Si $\pi(x) > 0$ para todo $t \in \mathbb{R}$ entonces existen polinomios reales $P(x)$ y $Q(x)$ tales que $\pi(x) = P^2(x) + Q^2(x)$, luego basta ver que $\mathscr{L}(P^2(x)) > 0$. Como $\{P_n(x)\}$ el SPO de $\mathscr{L}$ es una base para $\mathbb{R}[x]$, podemos escribir

$$P(x) = \sum_{i=0}^{m} a_i P_i(x) \qquad\qquad a_i \in \mathbb{R} \tag{2.24}$$

donde $m \geq 0$ es el grado de P(x) y $a_m \neq 0$. Veamos que

$$\begin{aligned} P^2(x) &= \left(\sum_{i=0}^{m} a_i P_i(x) \right)^2 \\ &= \sum_{i=0}^{m} a_i^2 P_i^2(x) + 2 \sum_{0 \leq i < j \leq m} a_i a_j P_i(x) P_j(x). \end{aligned}$$

Aplicando $\mathscr{L}$ y como $a_m^2 > 0$ se tiene

$$\mathscr{L}(P^2(x)) = \sum_{i=0}^{m} a_i^2 \mathscr{L}(P_i^2(x)) > 0. \tag{2.25}$$

$$\tag{2.26}$$

Lo que concluye la prueba. □

Teorema 2.17. *(Fórmula de cuadratura de Gauss) Sea $\mathscr{L}$ un funcional positivo. Existen números $A_k > 0$ con $k = 1, \ldots, n$ tales que para todo polinomio $Q(x)$ de grado a lo más $2n-1$,*

$$\mathscr{L}(Q(x)) = \sum_{k=1}^{n} A_k Q(x_k). \tag{2.27}$$

Demostración: Sea $\{P_n(x)\}$ el correspondiente SPOM de $\mathscr{L}$. Sea $Q(x)$ un polinomio arbitrario de grado menor que 2n, y construimos la interpolación polinómica de Lagrange, entonces

$$\frac{Q(x)}{P_n(x)} = \sum_{i=1}^{n} \frac{Q(x_i)}{P_n'(x_i)(x - x_i)} + R(x),$$

donde $x_1, \ldots, x_n$ son las raíces de $P_n(x)$ y $R(x)$ es un polinomio de grado menor que n. Si hacemos

$$L_n(x) = \sum_{i=1}^{n} Q(x_i) \ell_i(x),$$

donde

$$\ell_i(x) = \frac{P_n(x)}{P_n'(x_i)(x - x_i)},$$

podemos escribir

$$Q(x) = L_n(x) + R(x) P_n(x).$$

Aplicando $\mathscr{L}$ y como $R(x)$ es de grado menor que n, entonces

$$\begin{aligned} \mathscr{L}(Q(x)) &= \mathscr{L}(L_n(x)) + \mathscr{L}(R(x) P_n(x)) \\ &= \mathscr{L}(L_n(x)) \\ &= \sum_{i=0}^{n} Q(x_i) \mathscr{L}(\ell_i(x)). \end{aligned}$$

Llamemos $A_i = \mathscr{L}(\ell_i(x))$. Si elegimos el siguiente polinomio de grado menor que 2n

$$Q(x) = \ell_m^2(x) = \left(\frac{P_n(x)}{P_n'(x_m)(x-x_m)}\right)^2,$$

y aplicando $\mathscr{L}$ a dicho polinomio se obtiene

$$\begin{aligned}\mathscr{L}(\ell_m^2(x)) &= \sum_{i=0}^{n} \ell_m^2(x_i)\mathscr{L}(\ell_i(x)) \\ &= \sum_{i=0}^{n} \ell_m^2(x_i) A_i \\ &= A_m > 0.\end{aligned}$$

Luego los A_k son todos positivos, lo que concluye la demostración. □

Notas.

- Si $\mathscr{L}$ un funcional regular puede representarse de la forma

  $$\mathscr{L}(P(x)) = \int_{-\infty}^{\infty} P(t)\, d\sigma(t),$$

  donde σ es una medida positiva con soporte en el eje real. Además, dado $\{P_n(x)\}$ es su SPOM, que cumple la relación (2.13) y si el soporte de σ es infinito, entonces $\mathscr{L}$ es automáticamente positivo.

- Además, si $P(x) \neq 0$ es un polinomio con coeficientes reales, entonces

  $$\int_{-\infty}^{\infty} P^2(t)\, d\sigma(t) > 0.$$

- Por lo que se puede concluir que bajo las anteriores condiciones podemos definir un producto interno en $\mathbb{R}[x]$, como

  $$\langle p(x), q(x)\rangle = \int_{-\infty}^{\infty} p(t)q(t)\, d\sigma(t).$$

2.4. Los polinomios de Legendre

La sucesión $\{P_n(x)\}_{m=0}^{\infty}$ de **polinomios de Legendre** es una familia de polinomios ortogonales con respecto al producto interno definido en $L^2[-1,1]$, los introdujo por primera vez el matemático francés Adrien-Marie Legendre en 1785.

2.4.1. Ecuación Diferencial de Legendre

Dichos polinomios son soluciones de la *ecuación diferencial de Legendre*. Se puede definir para $n \in \mathbb{N}$ la ecuación

$$\frac{d}{dx}\left[(1-x^2)\frac{dy}{dx}\right] + n(n+1)y = 0. \tag{2.28}$$

Se puede ver una expresión explícita de los polinomios de Legendre hallando la solución de la ecuación (2.28). Así, asumimos una solución y en series de potencias, esto es:

$$y(x) = \sum_{k=0}^{\infty} a_k x^k. \tag{2.29}$$

Calculamos la primera y segunda derivada de (2.29)

$$y'(x) = \sum_{k=1}^{\infty} k a_k x^{k-1} \qquad\qquad y''(x) = \sum_{k=2}^{\infty} k(k-1) a_k x^{k-2}. \tag{2.30}$$

Nótese que las dos sumatorias en (2.30) pueden iniciar con $k = 0$ sin afectarse, luego reemplazando (2.29) junto con (2.30) en (2.28) se obtiene

$$(1-x^2)\sum_{k=0}^{\infty} k(k-1)a_k x^{k-2} - 2x\sum_{k=0}^{\infty} k a_k x^{k-1} + n(n+1)\sum_{k=0}^{\infty} a_k x^k = 0.$$

Así, expandiendo la ecuación anterior se tiene

$$\sum_{k=0}^{\infty} k(k-1)a_k x^{k-2} - \sum_{k=0}^{\infty} k(k-1)a_k x^k - 2\sum_{k=0}^{\infty} k a_k x^k + n(n+1)\sum_{k=0}^{\infty} a_k x^k = 0. \tag{2.31}$$

Nótese que

$$\sum_{k=0}^{\infty} k(k-1)a_k x^{k-2} = \sum_{k=0}^{\infty} (k+2)(k+1)a_{k+2} x^k. \tag{2.32}$$

Reemplazando en (2.31)

$$\sum_{k=0}^{\infty} (k+2)(k+1)a_{k+2} x^k - \sum_{k=0}^{\infty} k(k-1)a_k x^k - 2\sum_{k=0}^{\infty} k a_k x^k + n(n+1)\sum_{k=0}^{\infty} a_k x^k = 0. \tag{2.33}$$

Con lo que

$$\sum_{k=0}^{\infty} \left[(k+2)(k+1)a_{k+2} - k(k-1)a_k - 2k a_k + n(n+1)a_k\right] x^k = 0. \tag{2.34}$$

Luego

$$(k+2)(k+1)a_{k+2} - [(k(k-1) + 2k - n(n+1)]a_k = 0. \tag{2.35}$$

Así

$$a_{k+2} = \frac{k(k+1) - n(n+1)}{(k+2)(k+1)} a_k = -\frac{(n-k)(n+k+1)}{(k+2)(k+1)} a_k. \tag{2.36}$$

Los primeros coeficientes

$$
\begin{aligned}
a_2 &= -\frac{n(n+1)}{1\cdot 2}a_0 \\
a_3 &= -\frac{2-n(n+1)}{6}a_1 = -\frac{(n+2)(n-1)}{1\cdot 2\cdot 3}a_1 \\
a_4 &= \frac{6-n(n+1)}{12}a_2 = \frac{(n+3)(n-2)(n+1)n}{1\cdot 2\cdot 3\cdot 4}a_0 \\
a_5 &= \frac{12-n(n+1)}{20}a_3 = \frac{(n+4)(n-3)(n+2)(n-1)}{1\cdot 2\cdot 3\cdot 4\cdot 5}a_1
\end{aligned}
$$

Así, probando por inducción se tiene que:

- si $k = 2m$

$$a_{2m} = (-1)^m \frac{n\cdots(n-2m+2)(n+1)\cdots(n+2m-1)}{2m!}a_0 \tag{2.37}$$

- si $k = 2m+1$

$$a_{2m+1} = (-1)^m \frac{(n-1)\cdots(n-2m+1)(n+2)\cdots(n+2m)}{(2m+1)!}a_1 \tag{2.38}$$

Así la solución y de la ecuación (2.28) es

$$y(x) = a_0 y_1(x) + a_1 y_2(x) \tag{2.39}$$

donde a_0 y a_1 son constantes arbitrarias y

$$y_1(x) = 1 + \sum_{m=1}^{\infty} (-1)^m \frac{n\cdots(n-2m+2)(n+1)\cdots(n+2m-1)}{2m!}x^{2m} \tag{2.40}$$

$$y_2(x) = x + \sum_{m=1}^{\infty} (-1)^m \frac{(n-1)\cdots(n-2m+1)(n+2)\cdots(n+2m)}{(2m+1)!}x^{2m+1} \tag{2.41}$$

2.4.2. Polinomios de Legendre

A partir de las soluciones $y_1(x)$ y $y_2(x)$ de la ecuación (2.28) se pueden obtener los polinomios de Legendre. Veamos que para cada $n \in \mathbb{N}$ se obtiene un polinomio de grado n, en efecto, si en (2.36) se tiene $k = n$ entonces

$$a_{n+2} = \frac{n(n+1)-n(n+1)}{(n+2)(n+1)}a_n = 0,$$

y así $a_{n+4} = 0, a_{n+6} = 0, \ldots$. De esta manera

- Si n es par entonces $y_1(x)$ se reduce a un polinomio de grado n

$$
\begin{aligned}
y_1(x) &= 1, && n = 0 \\
y_1(x) &= 1 - 3x^2, && n = 2 \\
y_1(x) &= 1 - 10x^2 + \tfrac{35}{3}x^4, && n = 4
\end{aligned}
$$

- Similarmente, si n es impar se tiene la misma afirmación para $y_2(x)$

$$\begin{aligned} y_2(x) &= x, && n=1 \\ y_2(x) &= x - \tfrac{5}{3}x^3, && n=3 \\ y_2(x) &= x - \frac{14}{3}x^3 + \tfrac{21}{5}x^5, && n=5 \end{aligned}$$

Definición 2.27. *Los **polinomios de Legendre** de grado n, denotados por $P_n(x)$, son los polinomios $y_1(x)$ y $y_2(x)$ de grado n, multiplicados por una constante y de tal manera que satisfacen la condición $P_n(1) = 1$.*

Para ver una ecuación explícita de los polinomios de Legendre, tomamos una conveniente elección para el coeficiente a_n de la potencia x^n como sigue

$$a_n = \frac{(2n)!}{2^n (n!)^2}.$$

Si se coloca la relación de recurrencia (2.36) en términos de a_n, se obtiene

$$a_k = -\frac{(k+2)(k+1)}{(n-k)(n+k+1)} a_{k+2} \qquad k \le n-2,$$

Si tomamos $k = n-2$ y reemplazando en la ecuación anterior, junto con el coeficiente a_n se obtiene

$$\begin{aligned} a_{n-2} &= -\frac{n(n-1)}{2(2n-1)} a_n \\ &= -\frac{n(n-1)}{2(2n-1)} \cdot \frac{(2n)!}{2^n (n!)^2} \\ &= -\frac{n(n-1)2n(2n-1)(2n-2)!}{2(2n-1)2^n n(n-1)!n(n-1)(n-2)!} \\ &= \frac{(2n-2)!}{2^n (n-1)!(n-2)!}. \end{aligned}$$

Similarmente, si tomamos $k = n-4$

$$\begin{aligned} a_{n-4} &= -\frac{(n-2)(n-3)}{4(2n-3)} a_{n-2} \\ &= \frac{(2n-4)!}{2^n 2!(n-2)!(n-4)!}. \end{aligned}$$

En general, cuando $n - 2m \ge 0$ obtenemos

$$a_{n-2n} = (-1)^m \frac{(2n-2m)!}{2^n m!(n-m)!(n-2m)!}.$$

De esta manera los **polinomios de Legendre** $P_n(x)$ de grado n se pueden obtener por

$$P_n(x) = \sum_{m=0}^{N} (-1)^m \frac{(2n-2m)!}{2^n m!(n-m)!(n-2m)!} x^{n-2m}, \tag{2.42}$$

donde $N = n/2$ si n es par y $N = (n-1)/2$ si n es impar. Asi los primeros polinomios de Legendre vienen dados por

$$P_0(x) = 1 \qquad P_1(x) = x$$
$$P_2(x) = \frac{1}{2}(3x^2 - 1) \qquad P_3(x) = \frac{1}{2}(5x^3 - 3x)$$
$$P_4(x) = \frac{1}{8}(35x^4 - 30x^2 + 3) \qquad P_5(x) = \frac{1}{8}(63x^5 - 70x^3 + 15x)$$

La siguiente gráfica muestra los primeros polinomios de Legendre:

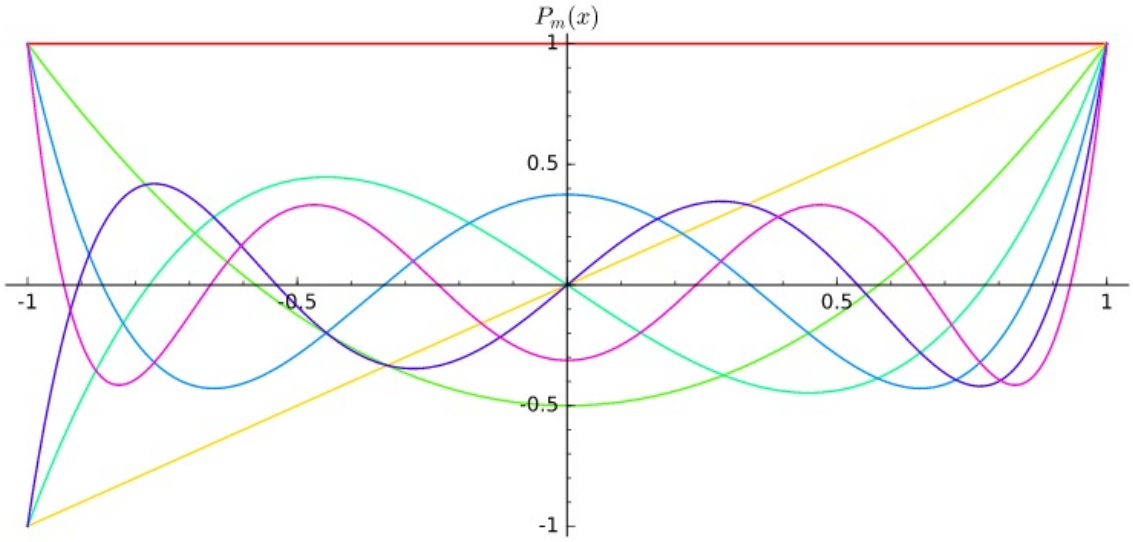

Figura 2.2: Polinomios de Legendre

2.4.3. Fórmula de Rodrigues

Una manera de expresar los polinomios de Legendre de grado n, $P_n(x)$, es mediante la fórmula de Rodrigues.

Proposición 2.12. *Para $n \geq 0$ los polinomios de Legendre de grado n, $P_n(x)$, están dados por*

$$P_n(x) := \frac{1}{2^n n!}\frac{d^n}{dx^n}[(x^2-1)^n]. \tag{2.43}$$

Demostración: Sea $\phi(x) = (x^2-1)^n$, veamos que $\phi^{(k)}$ satisface la ecuación

$$(1-x^2)\phi^{(k+2)} + 2x(n-k-1)\phi^{(k+1)} + (2n-k)(k+1)\phi^{(k)} = 0. \tag{2.44}$$

La ecuación (2.44) se probará por inducción. Así, derivando ϕ se tiene $\phi'(x) = 2nx(x^2-1)^{n-1}$, y por tanto

$$(1-x^2)\phi' + 2nx\phi = 0 \tag{2.45}$$

Al derivar la ecuación anterior se obtiene

$$(1-x^2)\phi'' + 2(n-1)x\phi' + 2ny = 0.$$

Así la ecuación (2.44) se cumple para $k=0$. Supongamos que se cumple para $k-1$, esto es

$$(1-x^2)\phi^{(k+1)} + 2x(n-k)\phi^{(k)} + (2n-k+1)k\phi^{(k-1)} = 0.$$

Derivando la ecuación anterior se obtiene

$$(1-x^2)\phi^{(k+2)} - 2x\phi(k+1) + 2(n-k)\phi^{(k)} + 2x(n-k)\phi(k+1) + (2n-k+1)k\phi^{(k)} = 0,$$

la cual es precisamente (2.44).

Ahora si tomamos $k=n$ en (2.44) y definimos $\varphi(x) = \phi^{(n)}(x)$ vemos que φ es un polinomio de grado n que satisface la *ecuación de Legendre* (2.28), luego por *definición 2.27* basta encontrar K de tal forma que $P_n(x) = K\varphi(x)$ y $P_n(1) = 1$. Usando la regla de Leibniz, nótemos que

$$\begin{aligned}
\varphi(x) = \phi^{(n)}(x) &= ((x^2-1)^n)^{(n)} \\
&= ((x+1)^n(x-1)^n)^{(n)} \\
&= \sum_{k=0}^{n} \binom{n}{k} ((x+1)^n)^{(k)} ((x-1)^n)^{(n-k)} \\
&= (x+1)^n n! + (x-1)q(x).
\end{aligned}$$

Así $\varphi(1) = 2^n n!$. Por lo tanto

$$P_n(x) = \frac{1}{2^n n!}\varphi = \frac{1}{2^n n!}\frac{d^n}{dx^n}[(x^2-1)^n].$$

2.5. Polinomios de Jacobi

Los polinomios de Legendre pueden ser representados por medio de los polinomios de Jacobi, a continuación se definirán y se enunciarán sus propiedades. Szegö [10, cap. 4] desarrolla una sección completa para estos polinomios y muestra todas sus propiedades. En esta sección tomaremos algunas de estas propiedades, las utilizadas para el objetivo de nuestro trabajo, especialmente el **discriminante** de los polinomios de Jacobi. La definición formal de discrimnante se dará en la siguiente sección, con el fin de trabajar sus propiedades.

2.5.1. Definición y propiedades

Definición 2.28. *Los **polinomios de Jacobi** de grado n $P_n^{(\alpha,\beta)}(x)$ se pueden definir vía la función hipergeométrica por*

$$P_n^{(\alpha,\beta)}(x) = \frac{(1+\alpha)_n}{n!} F\left(-n, n+\alpha+\beta+1; \alpha+1; \frac{1-x}{2}\right). \tag{2.46}$$

Proposición 2.13. *Los polinomios de Jacobi pueden expresarse de la siguiente manera*

$$P_n^{(\alpha,\beta)}(x) = \frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}(n+\alpha+b+1)_k(\alpha+k+1)\cdots(\alpha+n)\left(\frac{x-1}{2}\right)^k, \tag{2.47}$$

donde $(x)_k$ *es el factorial de Pochhammer.*

Demostración: Directamente de la definición (2.28) y de función hipergeométrica se tiene que,

$$\begin{aligned}P_n^{(\alpha,\beta)}(x) &= \frac{(1+\alpha)_n}{n!}\sum_{k=0}^{\infty}\frac{(-n)_k(n+\alpha+\beta+1)_k}{(\alpha+1)_k k!}\left(\frac{1-x}{2}\right)^2 \\ &= \frac{(1+\alpha)_n}{n!}\left[\sum_{k=0}^{n}\frac{(-n)_k(n+\alpha+\beta+1)_k}{(\alpha+1)_k k!}\left(\frac{1-x}{2}\right)^2 + \sum_{k=n+1}^{\infty}\frac{(-n)_k(n+\alpha+\beta+1)_k}{(\alpha+1)_k k!}\left(\frac{1-x}{2}\right)^2\right]\end{aligned}$$

Nótese que $(-n)_k = 0$ para $k \geq n+1$, y como $n \in \mathbb{Z}^+$, entonces $(-n)_k = (-1^k)\frac{n!}{(n-k)!}$

$$\begin{aligned}P_n^{(\alpha,\beta)}(x) &= \frac{(1+\alpha)_n}{n!}\sum_{k=0}^{n}(-1^k)\frac{n!}{(n-k)!k!}\frac{(n+\alpha+\beta+1)_k}{(\alpha+1)_k}\left(\frac{1-x}{2}\right)^2 \\ &= \frac{1}{n!}\sum_{k=0}^{n}(-1^k)\frac{n!}{(n-k)!k!}(n+\alpha+\beta+1)_k(\alpha+k+1)\cdots(\alpha+n)\left(\frac{1-x}{2}\right)^2 \\ &= \frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}(n+\alpha+b+1)_k(\alpha+k+1)\cdots(\alpha+n)\left(\frac{x-1}{2}\right)^k.\end{aligned}$$

Al igual que los polinomios de Legendre, se puede expresar los polinomios de Jacobi de grado n, $P_n^{(\alpha,\beta)}(x)$, por medio de la fórmula de Rodrigues.

Proposición 2.14. *Para* $n \geq 0$ *los polinomios de Jacobi de grado n,* $P_n^{(\alpha,\beta)}(x)$*, están dados por*

$$P_n^{(\alpha,\beta)}(x) := \frac{(-1)^n}{2^n n!}(1-x)^{-\alpha}(1+x)^{-\beta}\left(\frac{d}{dx}\right)^n\left[(1-x)^{n+\alpha}(1+x)^{n+\beta}\right]. \tag{2.48}$$

De esta manera, si tomamos $\alpha = \beta = 0$ se puede ver fácilmente que los polinomios de Jacobi son exactamente los polinomios de Legendre, esto es, $P_n(x) = P_n^{(0,0)}(x)$.

Proposición 2.15. *Las siguientes fórmulas se cumplen*

$$P_{2k}^{(\alpha,\alpha)}(x) = (-1)^k\frac{\Gamma(2k+\alpha+1)\Gamma(k+1)}{\Gamma(k+\alpha+1)\Gamma(2k+1)}P_k^{(-\frac{1}{2},\alpha)}(1-2x^2), \tag{2.49}$$

$$P_{2k+1}^{(\alpha,\alpha)}(x) = (-1)^k\frac{\Gamma(2k+\alpha+2)\Gamma(k+1)}{\Gamma(k+\alpha+1)\Gamma(2k+2)}xP_k^{(\frac{1}{2},\alpha)}(1-2x^2). \tag{2.50}$$

Teorema 2.18. *El discriminante de* $P_n^{(\alpha,\beta)}$ *está dado por*

$$D_n^{(\alpha,\beta)} = 2^{-n(n-1)}\prod_{k=1}^{n}k^{k-2n+2}(k+\alpha)^{k-1}(k+\beta)^{k-1}(n+k+\alpha+\beta)^{n-k}.$$

2.6. Primos de clase de congruencia prescritos en intervalos cortos

En esta sección se enunciará y demostrará el postulado de Bertrand, que asegura la existencia de un primo en un intervalo. Esto con el fin de asociarlo con el teorema de Dirichlet, que indica que existen infinitos primos en una progresión aritmética. Estos dos resultados se desean unir con el fin de encontrar clases de congruencias de primos en un intervalo. Más específicamente, esta sección busca dar las herramientas para demostrar que para $x \geq 9$ el intervalo $[x, 2x-5]$ contiene al menos un primo congruente con 1 módulo 4 y al menos un primo congruente con 3 módulo 4. Las primeras definiciones de esta sección se pueden encontrar en [1].

2.6.1. Función $\Lambda(n)$ de Mangoldt y funciones $\psi(x)$ y $\vartheta(x)$ de Chebyshev

Introducimos la función de Mangoldt Λ, la cuál juega un papel importante en la distribución de primos.

Definición 2.29. *Para un entero $n \geq 1$ definimos*

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m \text{ para algún } p \text{ primo y algún } m \geq 1 \\ 0 & \text{en otros casos} \end{cases} \tag{2.51}$$

De esta manera los primeros valores de $\Lambda(n)$ se pueden ver en la siguiente tabla:

n:	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

Proposición 2.16. *Si $n \geq 1$ se tiene que*

$$\log n = \sum_{d|n} \Lambda(d). \tag{2.52}$$

Demostración: Si $n = 1$, la ecuación (2.52) se cumple. Asumamos que $n > 1$ y utilizando el teorema fundamental de la aritmética, escribimos

$$n = \prod_{k=1}^{r} p_k^{a_k},$$

donde $p_1, \ldots, p_r$ son primos distintos y $a_1, \ldots, a_r > 0$. Así, y por propiedades de logaritmos

$$\log n = \sum_{k=1}^{r} a_k \log p_k.$$

Sabemos que $d|n$ si y sólo si

$$d = \prod_{k=1}^{r} p_k^{m_k},$$

donde $0 \leq m_i \leq a_i$ para $i = 1, \ldots, r$. Por la definición de Λ, para cada d, $\Lambda(d) \neq 0$ si $d = p_i^m$. Así

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = log n.$$

Con lo que se cumple (2.52). □

La suma parcial de la función de Mangoldt define una nueva función introducida por Chebyshev en 1848.

Definición 2.30. *Para $x > 0$ la función ψ de Chebyshev está dada por la fórmula*

$$\psi(x) = \sum_{n \leq x} \Lambda(n). \tag{2.53}$$

Sabemos que $\Lambda(n) = 0$ de no ser que n sea potencia de un primo, por lo cual podemos escribir la función ψ como sigue

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \sum_{p} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} \log p.$$

Nótese que suma sobre m es finita, pues si $x^{1/m} < 2$ entonces la suma sobre p es vacía. Esto es, si $(1/m)\log x < \log 2$, o si

$$m > \frac{\log x}{\log 2} = \log_2 x.$$

De esta manera ψ puede escribirse como

$$\psi(x) = \sum_{m \leq \log_2 x} \sum_{p \leq x^{1/m}} \log p.$$

Estas fórmulas pueden ser escritas de una manera ligeramente diferente , haciendo uso de la función ϑ de Chebyshev, es decir, se puede escribir una en términos de la otra. Por lo que a continuación definimos la función ϑ formalmente:

Definición 2.31. *Si $x > 0$ la función ϑ de Chebyshev está dada por la ecuación*

$$\vartheta(x) = \sum_{p \leq x} \log p, \tag{2.54}$$

donde p recorre todos los primos menores iguales que x.

Por lo que las fórmulas de $\psi(x)$ pueden reescribirse como sigue:

$$\psi(x) = \sum_{m=1}^{\infty} \vartheta(x^{1/m}) \qquad\qquad \psi(x) = \sum_{m \leq \log_2 x} \vartheta(x^{1/m}) \tag{2.55}$$

Proposición 2.17. *Para $x > 1$, la siguiente fórmula se cumple:*

$$\log[x]! = \sum_{m \leq x} \psi\left(\frac{x}{m}\right),$$

donde $[x]$ es la parte entera de x.

La demostración de la proposición anterior se obtiene directamente de la proposición 2.16 y de la definición 2.30.

2.6.2. Postulado de Bertrand

En 1845, el matemático francés Joseph Louis François Bertrand introdujo por primera vez el postulado que lleva su nombre. La primera demostración de este postulado fue dada cinco años más tarde, en 1850, por su colega ruso Pafnuti Lvóvich Chebyshov, quién utilizó métodos no elemntales, y por ello es algunas veces conocido como el teorema de Chebyshev. En 1919, Srinivasa Ramanujan otorgó una demostración más simple basada en la función Gamma [7]. Y en 1932, Paul Erdős dio una prueba aún más simple basada en las propiedades básicas de los coeficientes binomiales.

Teorema 2.19. *(Postulado de Bertrand) Para todo $n \geq 1$, existe un número primo p con $n < p \leq 2n$*

Demostración: De la proposición 2.17 y de la ecuación (2.55) se obtienen las siguientes ecuaciones

$$\psi(x) - 2\psi(x^{1/2}) = \vartheta(x) - \vartheta(x^{1/2}) + \vartheta(x^{1/3}) - \vartheta(x^{1/4}) + \dots$$
$$\log[x]! - 2\log[\tfrac{1}{2}x]! = \psi(x) - \psi(\tfrac{1}{2}x) + \psi(\tfrac{1}{3}x) - \psi(\tfrac{1}{4}x) + \dots$$

Como la parte derecha de las ecuaciones son series alternadas de las funciones ψ y ϑ de Chebishev, las cuales son crecientes, se obtiene

$$\psi(x) - 2\psi(x^{1/2}) \leq \vartheta(x) \leq \psi(x); \tag{2.56}$$

y

$$\psi(x) - \psi(\tfrac{1}{2}x) \leq \log[x]! - 2\log[\tfrac{1}{2}x]! \leq \psi(x) - \psi(\tfrac{1}{2}x) + \psi(\tfrac{1}{3}x).$$

Utilizando la relación de Ramanujan

$$\log\Gamma(x) - 2\log\Gamma(\tfrac{1}{2}x + \tfrac{1}{2}) \leq \log[x]! - 2\log[\tfrac{1}{2}x]! \leq \log\Gamma(x+1) - 2\log\Gamma(\tfrac{1}{2}x + \tfrac{1}{2}). \tag{2.57}$$

Ahora usando la aproximación de Stirling, $x! > \sqrt{2\pi x}(\frac{x}{e})^x$, en la ecuación (2.57) se deduce que

$$\log[x]! - 2\log[\tfrac{1}{2}x]! < \tfrac{3}{4}x \qquad \text{si } x > 0;$$
$$\log[x]! - 2\log[\tfrac{1}{2}x]! > \tfrac{2}{3}x \qquad \text{si } x > 300.$$

Con lo que

$$\psi(x) - \psi(\tfrac{1}{2}x) < \tfrac{3}{4}x \qquad \text{si } x > 0; \tag{2.58}$$

y

$$\psi(x) - \psi(\tfrac{1}{2}x) + \psi(\psi(x) - \psi(\tfrac{1}{3}x)) > \tfrac{2}{3}x \qquad \text{si } x > 300. \tag{2.59}$$

Ahora reemplazando x por $\frac{1}{2}x, \frac{1}{4}x, \frac{1}{8}x, \dots$ en (2.58), se obtiene

$$\psi(\tfrac{1}{2}x) - \psi(\tfrac{1}{4}x) < \tfrac{3}{8}x$$
$$\psi(\tfrac{1}{4}x) - \psi(\tfrac{1}{8}x) < \tfrac{3}{16}x$$
$$\psi(\tfrac{1}{8}x) - \psi(\tfrac{1}{16}x) < \tfrac{3}{32}x$$
$$\vdots$$

y sumando los resultados anteriores junto con (2.58), obtenemos

$$\psi(x) < \tfrac{3}{2}x \qquad \text{si } x > 0. \tag{2.60}$$

Así, de las ecuaciones (2.56)

$$\psi(x) - \psi(\tfrac{1}{2}x) + \psi(\tfrac{1}{3}x) \leq \vartheta(x) + 2\psi(x^{1/2}) - \vartheta(\tfrac{1}{2}x) + \psi(\tfrac{1}{3}x)$$

y de la ecuación (2.60)

$$\vartheta(x) + 2\psi(x^{1/2}) - \vartheta(\tfrac{1}{2}x) + \psi(\tfrac{1}{3}x) < \vartheta(x) - \vartheta(\tfrac{1}{2}x) + \tfrac{1}{2}x + 3x^{1/2}. \tag{2.61}$$

De esta manera de las ecuaciones (2.59) y (2.61)

$$\vartheta(x) - \vartheta(\tfrac{1}{2}x) > \tfrac{1}{6}x - 3x^{1/2} \qquad \text{si } x > 300.$$

Además $\frac{1}{6}x - 3x^{1/2} \geq 0$, si $x \geq 324$. Así

$$\vartheta(2x) - \vartheta(x) > 0 \qquad \text{si } x \geq 162.$$

Por lo que existe al menos un primo entre x y $2x$ si $x \geq 162$. □

2.6.3. Primos de clases de congruencias en intervalos

Como ya se ha visto, el postulado de Bertrand (Teorema 2.19) asegura la existencia de un número primo en un intervalo de tamaño adecuado, por otra parte el teorema 1.8 de Dirichlet asegura que una progresión aritmética contiene una cantidad infinita de números primos. A continuación se dará una manera de unir estos dos resultados. En primer lugar, definiremos una nueva función θ, la cual, es una variación de la función ϑ de Chebyshev.

Definición 2.32. *Sean $a, k > 0$ dos enteros tales que $(a,k) = 1$, y p un primo, definimos:*

$$\theta(x;k,a) = \sum_{\substack{p \cong a(k) \\ p \leq x}} \log p. \tag{2.62}$$

Esta suma es sobre los primos que no exceden a x en la clase de congruencia de a mód k.

Teorema 2.20. *Sean $x, y \in \mathbb{R}^+$, el intervalo $(x,y]$ contiene un primo en la clase de congruencia de a* mód *k si y sólo si $\theta(y;k,a) - \theta(x;k,a) > 0$.*

Nótese que $\theta(y;k,a) - \theta(x;k,a) > 0$ si y sólo si

$$\sum_{\substack{p \cong a(k) \\ x < p \leq y}} \log p > 0.$$

Como la función logaritmo es una función monónota creciente, la serie también lo es. Por lo que existiría al menos un primo p, tal que $p \cong a \pmod{k}$, en el intervalo $(x,y]$.

En el artículo *primes in arithmetic progressions* [8], Ramaré y Rumely realizan una estimación explícita en el cual se establecen dos cotas para la función $\theta(x;k,a)$ en los rangos $x \geq 10^{10}$ y $x < 10^{10}$. A continuación se enuncia el teorema que proporciona dichas cotas.

Teorema 2.21. *[8, p. 398] Dados a,k primos relativos. Para cualquier tripla (k,ε,x_0) dada, se tiene que:*

$$\max_{1\leq y\leq x}\left|\theta(y;k,a)-\frac{y}{\phi(k)}\right|\leq \varepsilon\frac{x}{\phi(k)}, \qquad x\geq x_0. \tag{2.63}$$

Los autores proporcionan una estimación para ciertos valores de la tripla (k,ε,x_0) (ver [8, Tabla 1]). Por ejemplo, si $k=4$ entonces $\varepsilon = 0{,}002238$ para $x_0 = 10^{10}$.

Teorema 2.22. *[8, p. 398] Para $x \leq 10^{10}$, y $(a,k)=1$ se tiene que*

$$\max_{1\leq y\leq x}\left|\theta(y;k,a)-\frac{y}{\phi(k)}\right|\leq 2{,}072\sqrt{x}. \tag{2.64}$$

Capítulo 3

Sobre el grupo de Galois de los polinomios de Legendre

Se sabe que los polinomios de Legendre $P_n(x)$ de grado n pueden representarse por la ecuación (2.42) o por la fórmula de rodrigues (2.43). Ahora bien, en 1890 Stieltjes envía una carta a Hermite conjeturando que los polinomios $P_{2n}(x)$ y $P_{2n+1}(x)$ son irreducibles sobre $\mathbb{Q}$. Esto lleva a definir los polinomios $L_m(x)$ de grado par, o más específicamente de grado $2\lfloor m/2 \rfloor$, como

$$L_n(x) = \begin{cases} P_n(x) & \text{si n es par.} \\ P_n(x)/x & \text{si n es impar.} \end{cases} \tag{3.1}$$

De esta manera los polinomios $L_n(x)$ son irreducibles sobre $\mathbb{Q}$ para todo n. Se ha verificado algunos casos de la conjetura por muchos autores, pero mostrar estos resultados no son objetivo de este trabajo. Los primeros polinomios irreducibles de Legendre $L_n(x)$ se dan acontinuación:

$$L_0(x) = 1 \qquad L_1(x) = 1$$
$$L_2(x) = \frac{1}{2}(3x^2 - 1) \qquad L_3(x) = \frac{1}{2}(5x^2 - 3)$$
$$L_4(x) = \frac{1}{8}(35x^4 - 30x^2 + 3) \qquad L_5(x) = \frac{1}{8}(63x^4 - 70x^2 + 15)$$

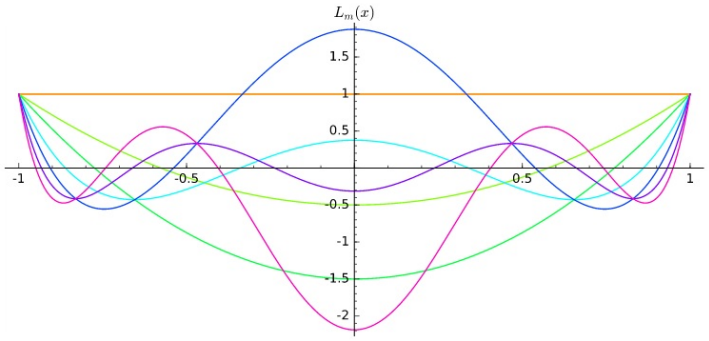

Figura 3.1: Polinomios $L_m(x)$

3.1. Definición de los polinomios $\mathscr{J}_n(x)$

En la sección 2.4 se definen los polinomios de Jacobi por (2.46) y se dedujeron ciertas propiedades. Ahora bien, definimos el polinomio $J_n^{(\alpha,\beta)}(x)$ a través de un desplazamiento de los polinomios de Jacobi, como sigue:

$$J_n^{(\alpha,\beta)}(x) := P_n^{(\alpha,\beta)}(2x+1). \tag{3.2}$$

Proposición 3.18. *Los polinomios de $J_n^{(\alpha,\beta)}(x)$ tienen la forma*

$$J_n^{(\alpha,\beta)}(x) = \sum_{k=0}^{n} \binom{n+\alpha}{n-k}\binom{n+\alpha+\beta+k}{k} x^k. \tag{3.3}$$

Demostración: Utilizando la fórmula de la proposición 2.13, evaluando $P_n^{(\alpha,\beta)}(2x+1)$ y por la ecuación 2.9 tenemos que

$$\begin{aligned}
P_n^{(\alpha,\beta)}(2x+1) &= \frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}(n+\alpha+b+1)_k(\alpha+k+1)\cdots(\alpha+n)x^k \\
&= \frac{1}{n!}\sum_{k=0}^{n}\frac{n!}{(n-k)!k!}(n+\alpha+b+1)_k(\alpha+k+1)\cdots(\alpha+n)x^k \\
&= \sum_{k=0}^{n}\frac{\Gamma(n+\alpha+\beta+k+1)}{(n-k)!\Gamma(k+1)\Gamma(n+\alpha+\beta+1)}(\alpha+k+1)\cdots(\alpha+n)x^k \\
&= \sum_{k=0}^{n}\binom{n+\alpha+\beta+k}{k}\frac{\Gamma(n+\alpha+1)}{\Gamma(n-k+1)\Gamma(\alpha+k+1)}x^k \\
&= \sum_{k=0}^{n}\binom{n+\alpha}{n-k}\binom{n+\alpha+\beta+k}{k}x^k.
\end{aligned}$$

Por lo que los polinomios $J_n^{(\alpha,\beta)}(x)$ están dados por la ecuación (3.3). □

En base a los polinomios anteriores se quiere representar los polinomios $L_m(x)$ en términos de los polinomios $J_n^{(\alpha,\beta)}(x)$. Y para ello definimos los polinomios $\mathscr{J}_n^{(\alpha,\beta)}(x)$ como sigue:

$$\mathscr{J}_n^{(\alpha,\beta)}(x) := 2^n n! J_n^{(\alpha,\beta)}(x). \tag{3.4}$$

El siguiente lema muestra la relación entre los polinomios de Legendre $L_m(x)$ y los nuevos polinomios que hemos definido anteriormente.

Lema 3.3. *Supongamos $m = 2n+\delta$ donde $n \geq 0$, $\delta \in \{0,1\}$ y $\epsilon = 2\delta - 1$. Entonces*

$$(-1)^n L_m(x) = J_n^{(\epsilon/2,0)}(-x^2), \qquad (-2)^n n! L_m(x) = \mathscr{J}_n^{(\epsilon/2,0)}(-x^2). \tag{3.5}$$

Demostración: Sea $n \geq 0$ y tomando $\delta = 0$, se tiene que $\epsilon = -1$ y $m = 2n$. Ahora, sabemos que para $m = 2n$, el polinomio $L_{2n}(x) = P_{2n}(x) = P_{2n}^{(0,0)}(x)$ y por la proposición 2.15

tenemos que

$$\begin{aligned} P_{2n}^{(0,0)}(x) &= (-1)^n \frac{\Gamma(2n+1)\Gamma(n+1)}{\Gamma(n+1)\Gamma(2n+1)} P_n^{(-1/2,0)}(1-2x^2) \\ &= (-1)^n P_n^{(-1/2,0)}(1-2x^2) \\ &= (-1)^n P_n^{(-1/2,0)}(2(-x^2)+1) \\ &= (-1)^n J_n^{(-1/2,0)}(-x^2). \end{aligned}$$

Por otra parte, y con ayuda de la ecuación anterior obtenemos

$$\mathscr{J}_n^{(-1/2,0)}(-x^2) = 2^n n! J_n^{(-1/2,0)}(-x^2) = 2^n n!(-1)^n L_{2n}(x).$$

Análogamente, si tomamos $\delta = 1$, se tiene que $\epsilon = 1$ y $m = 2n+1$. Ahora, sabemos que para $m = 2n+1$, el polinomio $L_{2n+1}(x) = P_{2n+1}(x)/x = P_{2n}^{(0,0)}(x)/x$ y por la proposición 2.15 tenemos que

$$\begin{aligned} P_{2n+1}^{(0,0)}(x) &= (-1)^n \frac{\Gamma(2n+2)\Gamma(n+1)}{\Gamma(n+1)\Gamma(2n+2)} x P_n^{(1/2,0)}(1-2x^2) \\ &= (-1)^n x P_n^{(1/2,0)}(1-2x^2) \\ &= (-1)^n x J_n^{(1/2,0)}(-x^2). \end{aligned}$$

Utilizando la ecuación anterior podemos ver que

$$\mathscr{J}_n^{(1/2,0)}(-x^2) = 2^n n! J_n^{(1/2,0)}(-x^2) = 2^n n!(-1)^n L_{2n+1}(x).$$

De esta manera se satisface el lema. □

3.2. Discriminante de $\mathscr{J}_n(x)$

El objetivo de esta sección es obtener una fórmula explícita para el discriminate de los polinomios $\mathscr{J}_n^{(\epsilon/2,0)}(x)$, esto nos motiva a desarrollar el siguiente lema.

Lema 3.4. *Para $n > 1$ y $\epsilon \in \{\pm 1\}$, el discriminante de $\mathscr{J}_n^{(\epsilon/2,0)}(x)$ está dado por la fórmula*

$$disc(\mathscr{J}_n^{(\epsilon/2,0)}) = 2^{n^2-n} \prod_{k=1}^{n} k^{2k-1}(2k+\epsilon)^{k-1}(2k+2n+\epsilon)^{n-k}. \tag{3.6}$$

Demostración: Por el teorema 2.18 el discriminante de $P_n^{(\pm 1/2,0)}$ está dado por

$$\begin{aligned} D_n^{(\pm 1/2,0)} &= 2^{-n(n-1)} \prod_{k=1}^{n} k^{2k-2n+1}(k \pm 1/2)^{k-1}(n+k \pm 1/2)^{n-k} \\ &= 2^{-2n(n-1)} \prod_{k=1}^{n} k^{1-2(n-k)}(2k \pm 1)^{k-1}(2n+2k \pm 1)^{n-k}. \end{aligned}$$

Ahora veamos que el discriminante de $2^n n! P_n^{(\pm 1/2,0)}$ es igual a $disc 2^n n! P_n^{(\pm 1/2,0)} = (2^n n!)^{2n-2} D_n^{(\pm 1/2,0)}$, y escribiendo $n!^{2n-2} = \prod_{k=1}^{n} k^{2n-1}$, tenemos que

$$\begin{aligned} disc(2^n n! P_n^{(\pm 1/2,0)}) &= n!^{2n-2} \prod_{k=1}^{n} k^{1-2(n-k)} (2k \pm 1)^{k-1} (2n + 2k \pm 1)^{n-k} \\ &= \prod_{k=1}^{n} k^{2k-1} (2k \pm 1)^{k-1} (2n + 2k \pm 1)^{n-k}. \end{aligned}$$

Por el lema 2.1, el discriminante es invariante bajo traslaciones y se cumple la fórmula $disc(f(2x)) = 2^{n(n-1)} disc(f(x))$ donde $n > 1$ es el grado del polinomio $f(x)$. Así como $J_n^{(\pm 1/2,0)}(x) = P_n^{(\pm 1/2,0)}(2x+1)$ entonces

$$disc\left(J_n^{(\pm 1/2,0)}(x)\right) = 2^{n(n-1)} disc\left(P_n^{(\pm 1/2,0)}(x)\right).$$

Finalmente como $\mathscr{J}_n^{(\pm 1/2,0)}(x) = 2^n n! J_n^{(\pm 1/2,0)}(x)$, su discriminante es igual a

$$disc(\mathscr{J}_n^{(\pm 1/2,0)}(x)) = 2^{n(n-1)} \prod_{k=1}^{n} k^{2k-1} (2k \pm 1)^{k-1} (2n + 2k \pm 1)^{n-k}. \tag{3.7}$$

que es precisamente lo que se quería probar. □

3.3. La raíz $disc\,\mathscr{J}_n$ no es racional

En esta sección se prueba que $\sqrt{disc\,\mathscr{J}_n^{(\pm 1/2,0)}} \notin \mathbb{Q}$, y como consecuencia del Teorema 2.13 el grupo de Galois de $\mathscr{J}_n^{(\pm 1/2,0)}(x)$ no está contenido en A_n. Se sabe por la proposición 1.3 que existen infinitos primos de la forma $4k+1$ y por la proposición 1.2 que existen infinitos primos de la forma $4k+3$, pero no sabemos cuántos primos de dichas formas hay en un intervalo. Para ello se presenta el siguiente lema:

Lema 3.5. *Para todo $x \geq 9$ entero, el intervalo $[x, 2x-5]$ contiene al menos un primo congruente con 1 modulo 4 y al menos un primo congruente con 3 modulo 4.*

Demostración: Como $(4,1) = 1$ y $(4,3) = 1$, por el teorema 2.20 basta demostrar que

$$\theta(2x-5;4,a) - \theta(x;4,a) > 0.$$

Si $x \geq 10^{10}$, por el teorema 2.21 y usando la estimación $\varepsilon = 0{,}002238$ dada en [8, p. 419], se tiene que

$$\max_{1 \leq y \leq 2x-5} \left| \theta(y;4,a) - \frac{y}{\phi(4)} \right| \leq \varepsilon \frac{2x-5}{\phi(4)} \qquad y \qquad \max_{1 \leq y \leq x} \left| \theta(y;4,a) - \frac{y}{\phi(4)} \right| \leq \varepsilon \frac{x}{\phi(4)}$$

Así

$$\theta(2x-5;4,a) \geq (1-\varepsilon) \frac{2x-5}{\phi(4)} \qquad y \qquad \theta(x;4,a) \geq (1-\varepsilon) \frac{x}{\phi(4)}$$

Por lo que

$$\begin{aligned}\theta(2x-5;4,a)-\theta(x;4,a) &\geq (1-\varepsilon)\frac{2x-5}{\phi(4)}-(1-\varepsilon)\frac{x}{\phi(4)}\\ &= (1-\varepsilon)\frac{(x-5)}{2}\\ &= 0{,}498881(x-5)>0.\end{aligned}$$

Luego para $x \geq 10^{10}$ existe un primo congruente con 1 módulo 4 y uno congruente con 3 módulo 4, en el intervalo $[x, 2x-5]$.

Por otra parte, por el teorema 2.22, si $x \leq 10^{10}$, entonces

$$\max_{1\leq y\leq 2x-5}\left|\theta(y;4,a)-\frac{y}{\phi(4)}\right| \leq 2{,}072\sqrt{2x-5} \quad y \quad \max_{1\leq y\leq x}\left|\theta(y;4,a)-\frac{y}{\phi(4)}\right| \leq 2{,}072\sqrt{x}$$

Así

$$\theta(2x-5;4,a) \geq \frac{2x-5}{\phi(4)}-2{,}072\sqrt{2x-5} \qquad y \qquad -\theta(x;4,a) \geq -\frac{x}{\phi(4)}-2{,}072\sqrt{x}$$

Por lo que

$$\theta(2x-5;4,a)-\theta(x;4,a) \geq \frac{x-5}{2}-2{,}072(\sqrt{2x-5}+\sqrt{x}). \tag{3.8}$$

Sin embargo la ecuación 3.8 es extríctamente mayor que cero para

$$x > \frac{1036\sqrt{614773}+883097}{15625} \approx 108{,}5054911.$$

Luego para $109 \leq x < 10^{10}$ existe un primo congruente con 1 módulo 4 y uno congruente con 3 módulo 4, en el intervalo $[x, 2x-5]$.

Ahora para $9 \leq x \leq 108$ se puede verificar caso a caso (ver tabla 3.1).

Tabla 3.1: Primos en el intervalo $[x, 2x-5]$ para $9 \leq x \leq 108$.

x	$2x-5$	$p \cong 1 \pmod 4$	$p \cong 3 \pmod 4$
9	13	13	11
10	15	13	11
11	17	13	11
12	19	13, 17	19
13	21	13, 17	19
14	23	17	19, 23
15	25	17	19, 23
16	27	17	19, 23
17	29	17, 29	19, 23
18	31	29	19, 23, 31
19	33	29	19, 23, 31
20	35	29	23, 31
21	37	29, 37	23, 31
22	39	29, 37	23, 31
23	41	29, 37, 41	23, 31
24	43	29, 37, 41	31, 43
25	45	29, 37, 41	31, 43
26	47	29, 37	31, 43, 47
27	49	29, 37	31, 43, 47
28	51	29, 37	31, 43, 47
29	53	29, 37, 53	31, 43, 47
30	55	37, 53	31, 43, 47
31	57	37, 53	31, 43, 47
32	59	37, 53	43, 47, 59
33	61	37, 53, 61	43, 47, 59
34	63	37, 53, 61	43, 47, 59
35	65	37, 53, 61	43, 47, 59
36	67	37, 53, 61	43, 47, 59, 67
37	69	37, 53, 61	43, 47, 59, 67
38	71	53, 61	43, 47, 59, 67, 71
39	73	53, 61, 73	43, 47, 59, 67, 71
40	75	53, 61, 73	43, 47, 59, 67, 71
41	77	53, 61, 73	43, 47, 59, 67, 71
42	79	53, 61, 73	43, 47, 59, 67, 71, 79
43	81	53, 61, 73	43, 47, 59, 67, 71, 79
44	83	53, 61, 73	47, 59, 67, 71, 79, 83
45	85	53, 61, 73	47, 59, 67, 71, 79, 83
46	87	53, 61, 73	47, 59, 67, 71, 79, 83
47	89	53, 61, 73, 89	47, 59, 67, 71, 79, 83
48	91	53, 61, 73, 89	59, 67, 71, 79, 83

Tabla 3.1 (Continuación)

x	$2x-5$	$p \cong 1 \pmod 4$	$p \cong 3 \pmod 4$
49	93	53, 61, 73, 89	59, 67, 71, 79, 83
50	95	53, 61, 73, 89	59, 67, 71, 79, 83
51	97	53, 61, 73, 89, 97	59, 67, 71, 79, 83
52	99	53, 61, 73, 89, 97	59, 67, 71, 79, 83
53	101	53, 61, 73, 89, 97, 101	59, 67, 71, 79, 83
54	103	61, 73, 89, 97, 101	59, 67, 71, 79, 83, 103
55	105	61, 73, 89, 97, 101	59, 67, 71, 79, 83, 103
56	107	61, 73, 89, 97, 101	59, 67, 71, 79, 83, 103, 107
57	109	61, 73, 89, 97, 101, 109	59, 67, 71, 79, 83, 103, 107
58	111	61, 73, 89, 97, 101, 109	59, 67, 71, 79, 83, 103, 107
59	113	61, 73, 89, 97, 101, 109, 113	59, 67, 71, 79, 83, 103, 107
60	115	61, 73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107
61	117	61, 73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107
62	119	73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107
63	121	73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107
64	123	73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107
65	125	73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107
66	127	73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107, 127
67	129	73, 89, 97, 101, 109, 113	67, 71, 79, 83, 103, 107, 127
68	131	73, 89, 97, 101, 109, 113	71, 79, 83, 103, 107, 127, 131
69	133	73, 89, 97, 101, 109, 113	71, 79, 83, 103, 107, 127, 131
70	135	73, 89, 97, 101, 109, 113	71, 79, 83, 103, 107, 127, 131
71	137	73, 89, 97, 101, 109, 113, 137	71, 79, 83, 103, 107, 127, 131
72	139	73, 89, 97, 101, 109, 113, 137	79, 83, 103, 107, 127, 131, 139
73	141	73, 89, 97, 101, 109, 113, 137	79, 83, 103, 107, 127, 131, 139
74	143	89, 97, 101, 109, 113, 137	79, 83, 103, 107, 127, 131, 139
75	145	89, 97, 101, 109, 113, 137	79, 83, 103, 107, 127, 131, 139
76	147	89, 97, 101, 109, 113, 137	79, 83, 103, 107, 127, 131, 139
77	149	89, 97, 101, 109, 113, 137, 149	79, 83, 103, 107, 127, 131, 139
78	151	89, 97, 101, 109, 113, 137, 149	79, 83, 103, 107, 127, 131, 139, 151
79	153	89, 97, 101, 109, 113, 137, 149	79, 83, 103, 107, 127, 131, 139, 151
80	155	89, 97, 101, 109, 113, 137, 149	83, 103, 107, 127, 131, 139, 151
81	157	89, 97, 101, 109, 113, 137, 149, 157	83, 103, 107, 127, 131, 139, 151
82	159	89, 97, 101, 109, 113, 137, 149, 157	83, 103, 107, 127, 131, 139, 151
83	161	89, 97, 101, 109, 113, 137, 149, 157	83, 103, 107, 127, 131, 139, 151
84	163	89, 97, 101, 109, 113, 137, 149, 157	103, 107, 127, 131, 139, 151, 163
85	165	89, 97, 101, 109, 113, 137, 149, 157	103, 107, 127, 131, 139, 151, 163
86	167	89, 97, 101, 109, 113, 137, 149, 157	103, 107, 127, 131, 139, 151, 163, 167
87	169	89, 97, 101, 109, 113, 137, 149, 157	103, 107, 127, 131, 139, 151, 163, 167

Tabla 3.1 (Continuación)

x	$2x-5$	$p \cong 1 \pmod 4$	$p \cong 3 \pmod 4$
88	171	89, 97, 101, 109, 113, 137, 149, 157	103, 107, 127, 131, 139, 151, 163, 167
89	173	89, 97, 101, 109, 113, 137, 149, 157, 173	103, 107, 127, 131, 139, 151, 163, 167
90	175	97, 101, 109, 113, 137, 149, 157, 173	103, 107, 127, 131, 139, 151, 163, 167
91	177	97, 101, 109, 113, 137, 149, 157, 173	103, 107, 127, 131, 139, 151, 163, 167
92	179	97, 101, 109, 113, 137, 149, 157, 173	103, 107, 127, 131, 139, 151, 163, 167, 179
93	181	97, 101, 109, 113, 137, 149, 157, 173, 181	103, 107, 127, 131, 139, 151, 163, 167, 179
94	183	97, 101, 109, 113, 137, 149, 157, 173, 181	103, 107, 127, 131, 139, 151, 163, 167, 179
95	185	97, 101, 109, 113, 137, 149, 157, 173, 181	103, 107, 127, 131, 139, 151, 163, 167, 179
96	187	97, 101, 109, 113, 137, 149, 157, 173, 181	103, 107, 127, 131, 139, 151, 163, 167, 179
97	189	97, 101, 109, 113, 137, 149, 157, 173, 181	103, 107, 127, 131, 139, 151, 163, 167, 179
98	191	101, 109, 113, 137, 149, 157, 173, 181	103, 107, 127, 131, 139, 151, 163, 167, 179, 191
99	193	101, 109, 113, 137, 149, 157, 173, 181, 193	103, 107, 127, 131, 139, 151, 163, 167, 179, 191
100	195	101, 109, 113, 137, 149, 157, 173, 181, 193	103, 107, 127, 131, 139, 151, 163, 167, 179, 191
101	197	101, 109, 113, 137, 149, 157, 173, 181, 193,197	103, 107, 127, 131, 139, 151, 163, 167, 179, 191
102	199	109, 113, 137, 149, 157, 173, 181, 193,197	103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199
103	201	109, 113, 137, 149, 157, 173, 181, 193,197	107, 127, 131, 139, 151, 163, 167, 179, 191, 199
104	203	109, 113, 137, 149, 157, 173, 181, 193,197	107, 127, 131, 139, 151, 163, 167, 179, 191, 199
105	205	109, 113, 137, 149, 157, 173, 181, 193,197	107, 127, 131, 139, 151, 163, 167, 179, 191, 199
106	207	109, 113, 137, 149, 157, 173, 181, 193,197	107, 127, 131, 139, 151, 163, 167, 179, 191, 199
107	209	109, 113, 137, 149, 157, 173, 181, 193,197	107, 127, 131, 139, 151, 163, 167, 179, 191, 199
108	211	109, 113, 137, 149, 157, 173, 181, 193,197	127, 131, 139, 151, 163, 167, 179, 191, 199, 211

Lema 3.6. *Para todo $x \geq 2$ y $\epsilon \in \{\pm 1\}$, la raíz del discriminante de $\mathscr{J}_n^{(\epsilon/2,0)}(x)$ no pertenece a $\mathbb{Q}$.*

Demostración: Por el lema 3.4 tenemos que

$$disc\,\mathscr{J}_n^{(\epsilon/2,0)} = 2^{n^2-n} \prod_{k=1}^{n} k^{2k-1}(2k+\epsilon)^{k-1}(2k+2n+\epsilon)^{n-k}.$$

Para $\epsilon = 1$ el último factor de la productoria del discriminante es $(2k+2n+1)^{n-k}$. Ahora, por el lema 3.5, para $n \geq 3$, el intervalo $[2n+3, 4n+1]$ contiene un primo, p_0, tal que $p_0 \cong 3 \pmod 4$. Nótese que este intervalo se elige pues en la productoria del discriminante cuando $k = 1$ su último factor es $2n+3$ y cuando $k = n$ es $4n+1$. Si escribimos p_0 de la forma

$$p_0 = 2k_0 + 2n + 1 \qquad\qquad 1 \leq k_0 \leq n,$$

como $p_0 = 2k_0 + 2n + 1 \cong 3 \pmod 4$ tenemos que $k_0 + n \cong 1 \pmod 2$, por lo que $n + k_0$ es impar, al igual que $n - k_0$. Luego $p_0 = 2k_0 + 2n + 1$ estaría elevado a una potencia impar y al hacer

$$\sqrt{disc\,\mathscr{J}_n^{(1/2,0)}},$$

tendríamos la raíz de p_0, y por la proposición 1.1, ésta es irracional. Luego la raíz del discriminante de $\mathscr{J}_n^{(1/2,0)}(x)$ no está en $\mathbb{Q}$.

De la misma manera, si $\epsilon = -1$ el último factor de la productoria del discriminante es $(2k+2n-1)^{n-k}$. Para $n \geq 4$ el intervalo $[2n+1, 4n-3]$ contiene un primo, p_1, tal que

$p_1 \cong 1 \pmod 4$. Escribimos p_1 de la forma

$$p_1 = 2k_1 + 2n - 1 \qquad\qquad 1 \leq k_1 \leq n,$$

Así $p_1 = 2k_0 + 2n - 1 \cong 1 \pmod 4$, de esta manera, $n + k_1$ y $n - k_1$ son impares. Análogamente al razonamiento anterior la raíz del discriminante de $\mathscr{J}_n^{(-1/2,0)}(x)$ no pertenece a $\mathbb{Q}$. Con lo que se concluye la prueba. □

Teniendo demostrado el lema anterior, y como se ha mencionado, como consecuencia del Teorema 2.13 podemos enunciar el siguiente teorema, y así obtenemos el resultado final de este trabajo.

Teorema 3.23. *Para todo $x \geq 2$ y $\epsilon \in \{\pm 1\}$, la raíz del discriminante de $\mathscr{J}_n^{(\epsilon/2,0)}(x)$ no está en $\mathbb{Q}$. Así, asumiendo que $\mathscr{J}_n^{(\epsilon/2,0)}(x)$ es irreducible, su grupo de Galois no está contenido en A_n*

Conclusiones

Las propiedades algebraicas de los polinomios de Legendre son poco conocidas y al ser una sucesión de polinomios ortogonales su estudio requiere de conceptos avanzados de diferentes áreas de la matemática. En primer lugar, se debe dar por hecho la conjetura de Stieltjes y asumir que los polinomios $L_n(x)$ son irreducibles y expresarlos en términos de otro tipo de polinomios, los polinomios $\mathscr{J}_n^{(\pm 1/2,0)}(x)$, para poder obtener información acerca de su grupo de Galois. La relación entre el grupo de Galois y el discriminante de un polinomio es muy estrecha, y aunque éste no proporciona el grupo de Galois exacto de un polinomio si ayuda a da una idea de a qué tipo de grupo es isomorfo.

Las propiedades análiticas de los polinomios de Jacobi, $P_n^{(\alpha,\beta)}(x)$, proporcionan una expresión para el discriminante de los polinomios $\mathscr{J}_n^{(\pm 1/2,0)}(x)$ pero esto no es suficiente para saber si la raíz de dicho discriminantes pertenece o no a $\mathbb{Q}$, es por esto que es necesario utilizar conceptos de teoría de números analítica y unir dos resultados conocidos, el postulado de Bertrand y el teorema de Dirichlet.

Al estudiar todos los conceptos necesarios se puede asegurar que el grupo de Galois de $\mathscr{J}_n^{(\pm 1/2,0)}(x)$ no está contenido en A_n, el grupo de las permutaciones pares, es decir, el grupo de Galois de $\mathscr{J}_n^{(\pm 1/2,0)}(x)$ contiene al menos una permutación impar y es isomorfo a algún subgrupo de S_n que contenga alguna permutación impar.

Bibliografía

[1] Tom M Apostol, *Introduction to analytic number theory*, Springer Science & Business Media, 2013.

[2] Theodore S. Chihara, *An introduction to orthogonal polynomials*, Courier Corporation, 2011.

[3] John Cullinan and Farshid Hajir, *On the galois groups of legendre polynomials*, Indagationes Mathematicae **25** (2014), no. 3, 534–552.

[4] John B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley, 2003.

[5] Israel N. Herstein, *Álgebra moderna: grupos, anillos, campos, teoría de Galois*, Ed. Trillas, México (1973).

[6] Earl David Rainville, *Special functions*, Macmillan, New York, 1960.

[7] Srinivasa Ramanujan, *A proof of bertrand's postulate*, Journal of the Indian Mathematical Society **11** (1919), no. 181-182, 27.

[8] Olivier Ramaré and Robert Rumely, *Primes in arithmetic progressions*, Mathematics of Computation of the American Mathematical Society **65** (1996), no. 213, 397–425.

[9] Gustavo N Rubiano, *Teoría de números para principiantes*, Universidad Nacional de Colombia (2004).

[10] Gabor Szego, *Orthogonal polynomials*, Vol. 23, American Mathematical Soc., 1939.