Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 25 (2014) 534–552

indagationes mathematicae

www.elsevier.com/locate/indag

On the Galois groups of Legendre polynomials

John Cullinan[a], Farshid Hajir[b,*]

[a] Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12504, United States

[b] Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01002, United States

Received 14 June 2013; received in revised form 10 January 2014; accepted 27 January 2014

Communicated by T.H. Koornwinder

Abstract

Ever since Legendre introduced the polynomials that bear his name in 1785, they have played an important role in analysis, physics and number theory, yet their algebraic properties are not well-understood. Stieltjes conjectured in 1890 how they factor over the rational numbers. In this paper, assuming Stieltjes' conjecture, we formulate a conjecture about the Galois groups of Legendre polynomials, to the effect that they are "as large as possible," and give theoretical and computational evidence for it.

Keywords: Legendre polynomials; Galois group; Sophie-Germain primes; Hardy–Littlewood conjectures

1. Introduction

The sequence $(P_m(x))_{m\geq 0}$ of *Legendre polynomials* is an orthogonal family on $[-1, 1]$, first introduced by Adrien-Marie Legendre in 1785 [15] as coefficients in a series expansion for the gravitational potential of a point mass. For $m \geq 0$ we can define $P_m(x)$ via the Rodrigues formula

$$P_m(x) := \frac{(-1)^m}{2^m m!}\left(\frac{d}{dx}\right)^m (1-x^2)^m.$$

* Corresponding author.

E-mail addresses: cullinan@bard.edu (J. Cullinan), hajir@math.umass.edu (F. Hajir).

http://dx.doi.org/10.1016/j.indag.2014.01.004

As a solution $y = P_m(x)$ of the Legendre differential equation

$$\frac{d}{dx}\left[(1-x^2)\frac{dy}{dx}\right] + m(m+1)y = 0,$$

$P_m(x)$ is an eigenfunction of the self-adjoint operator $\frac{d}{dx}(1-x^2)\frac{d}{dx}$ with eigenvalue $-m(m+1)$. It is easy to see that $P_m(-x) = (-1)^m P_m(x)$, prompting us to define the even polynomial of degree $2\lfloor m/2\rfloor$:

$$L_m(x) = \begin{cases} P_m(x) & \text{if } m \text{ is even;} \\ P_m(x)/x & \text{if } m \text{ is odd.} \end{cases}$$

While their importance in classical physics and analysis dates back to Legendre's paper, the role of Legendre polynomials in number theory became manifest a bit later, for instance as the Hasse invariant

$$W_p(E_\lambda) := (1-\lambda)^m P_m\left(\frac{1+\lambda}{1-\lambda}\right)$$

for the Legendre-form elliptic curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ over $\mathbf{F}_p$, where $p = 2m+1$ is prime (see [3] and its references). As an indication of the arithmetic depth of this fact, we mention one of its consequences, thanks to the theory of elliptic curves with complex multiplication: say $m = (p-1)/2$ is odd; then the class number of $\mathbf{Q}(\sqrt{-p})$ is one-third the number of linear factors of $P_m(x)$ over $\mathbf{F}_p$ (see Brillhart–Morton [3, Theorem 1(a)] and Morton [18]).

The algebraic properties of many similar families of hypergeometric polynomials (Laguerre, Chebyshev, Hermite, Bessel) have been extensively explored using methods pioneered by Schur [21], but results of this nature for Legendre polynomials continue to be fragmentary at best. As regards how Legendre polynomials factor over the rationals, Stieltjes put forward the following conjecture in an 1890 letter to Hermite [22]: $P_{2n}(x)$ and $P_{2n+1}(x)/x$ are irreducible over $\mathbf{Q}$, i.e $L_m(x)$ is irreducible over $\mathbf{Q}$ for all m. Some cases of Stieltjes' conjecture have been verified by Holt, Ille, Melnikov, Wahab, McCoart [11,12,14,17,24,25,16]; the articles [24,16] provide useful summaries. The flavor of these results is that if m or $m/2$ is within a few units of a prime number, then $L_m(x)$ is irreducible over $\mathbf{Q}$ (see for example Corollary 3.4(b), a result of Holt completed by Wahab, which we re-derive). There has been no significant improvement of these results for several decades. From a number-theoretic viewpoint, for primes $p = 2m+1 \equiv 3 \bmod 4$, the irreducibility of $P_m(x)$ has the intriguing consequence, thanks to the result of Brillhart and Morton quoted above, that the class number of $\mathbf{Q}(\sqrt{-p})$ is "governed" by the number field cut out by a non-zero root of $P_m(x)$, specifically by how the prime p splits in it. We should point out that recent work of Bourgain and Rudnick [2] places Stieltjes' conjecture in a much more general context of expectations for the behavior of eigenfunctions of Laplacians; perhaps a resurgence of interest in the question will ensue.

We assume Stieltjes' conjecture, and turn our attention to the next natural question, namely "What is the Galois group of the degree $2\lfloor m/2\rfloor$ polynomial $L_m(x)$?" We explore this question here, and conjecture that these Galois groups are as large as possible, namely $S_2 \wr S_n$ where $n = \lfloor m/2\rfloor$. Our starting point is to note that $L_m(x)$ is an even polynomial, so if we write $m = 2n + \delta$ with $\delta \in \{0, 1\}$, then

$$L_m(x) = P_{2n+\delta}(x)/x^\delta = (-1)^n p_n^{(\delta)}(-x^2),$$