On Certain Algebraic Aspects of a Family of Orthogonal Polynomials

A Project Report Submitted
in Partial Fulfilment of the Requirements
for the Degree of

MASTER OF SCIENCE

in

MATHEMATICS

by

ARIJIT JANA
(Roll No. MA14MSCST11002)
SUPERVISOR : Dr. PRADIPTO BANERJEE

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

to the

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY HYDERABAD
HYDERABAD-502285, INDIA

April 2016

DECLARATION

I declare that I carried out this M.Sc. thesis with my Guide Dr. Pradipto Banerjee, cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations.

Arijit Jana

.....

IIT Hyderabad
April-2016

Arijit Jana
Roll No-MA14MSCST11002

CERTIFICATE

This is to certify that the work contained in this report entitled **"On Certain Algebraic Aspects of a Family of Orthogonal Polynomials"** submitted by **Arijit Jana** (**Roll No: MA14MSCST11002**) to Department of Mathematics, Indian Institute of Technology Hyderabad towards the requirement of the course **MA5980 and MA5990 Project** has been carried out by him under my supervision.

IIT Hyderabad
April-2016

(Dr. Pradipto Banerjee)
Project Supervisor

ACKNOWLEDGEMENTS

I thank Dr.Pradipto Banerjee for giving me an opportunity to do the project work with him and providing me all the support and guidance which helped me accomplish the project on time.
I would also like to thank my parents and my elder sisters Susmita, Moumita and Samita for inspiring me to follow my ambitions throughout my childhood. I would also like to thank my friends Smita Mondal, Soma Mondal, Jayanta Kamila for all their support and encouragement.
I am also grateful to the faculty and stuff of IIT Hyderabad for providing an excellent atmosphere for scholarly work.

ABSTRACT

We study the irreducibility properties of Generalized Laguerre Polynomials (GLP) $L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \binom{n+\alpha}{n-j} \frac{(-x)^j}{j!}$ for integral values of the parameter α. We also study a simple criteria for the Galois group of polynomial to be "large." We show that for positive integer α there is an effectively computable constant n_0 such that $L_n^{(\alpha)}(x)$ is irreducible over the rationals for all $n \geq n_0$. We also show that under these condition , the Galois group of $L_n^{(\alpha)}(x)$ is either the alternating or the symmetric group of n letters. We further prove that for a fixed integer $r \geq 0$, there is an effectively computable constant N_r such that every admissible modification of $L_n^{<r>}(x) := L_n^{(-1-n-r)}(x) = \sum_{j=0}^{n} \binom{n-j+r}{n-j} \frac{(-x)^j}{j!}$ are either irreducible or if it is reducible, then it has atmost one linear factor over the rationals. The results are obtained using the theory of Newton polygons.

Contents

Chapter 1

Introduction

The Generalized Laguerre Polynomial (GLP) is one parameter family defined by

$$L_n^{(\alpha)}(x) = (-1)^n \sum_{j=0}^{n} \binom{n+\alpha}{n-j} \frac{(-x)^j}{j!},$$

where n is a positive integer and α be an arbitrary complex number. The leading coefficient here is $1/n!$. Here the binomial coefficient $\binom{t}{k}$ is defined as $t(t-1)\cdots(t-k+1)$ for non negative integers k. The inclusion of the sign $(-1)^n$ is not standard. Sometimes it is more appropriate to work with the monic polynomials $\mathcal{L}_n^{(\alpha)}(x) = n!L_n^{(\alpha)}(x)$. We have second order linear (hyper-geometric) differential equation

$$x\frac{d^2y}{dx^2} + (\alpha + 1 - x)\frac{dy}{dx} + ny = 0 \quad \text{where} \quad y = L_n^{(\alpha)}(x),$$

as well as the difference equation

$$L_n^{(\alpha-1)}(x) - L_n^{(\alpha)}(x) = L_{n-1}^{(\alpha)}(x).$$

In this thesis, we are concerned with the irreducibility of $L_n^{(\alpha)}(x)$ over $\mathbb{Q}$ for integral values of α. Early investigations were introduced by Schur who established the irreducibility in the particular specializations $a_j = (-1)^j\binom{n}{j}$ and $a_j = (-1)^n$ corresponding to $\alpha = 0$ and $\alpha = -n-1$ respectively. Schur further established the irreducibility of $L_n^{(\alpha)}(x)$ for $\alpha = 1$ (see [28]) and $\alpha = 1/2$ (see [29]). Since, the work of Schur a number of authors considered the problem for various values of α, namely Filaseta (see [2]), Hajir (see [18]), Gow (see [16]) and others. Below we mention a couple of important works in this area.

Theorem 1. *(Filaseta -Lam Theorem) Let α be a rational number which is not a negative integer, then for all but finitely many positive integers n, the polynomials*

$$\sum_{j=0}^{n} a_j \frac{(n+\alpha)\cdot(n-1+\alpha)\cdots(j+1+\alpha)}{(n-j)!\cdot j!}(x)^j$$

is irreducible over the rationals provided $a_j \in \mathbb{Z}$ for $0 \leq j \leq n$, and $\mid a_0 \mid = \mid a_n \mid = 1$.

Theorem 2. *(Hajir's Theorem) Let $n \geq 3$ be an integer. Let K be a finite extension of $\mathbb{Q}$, then there is a finite set $S(K)$ of elements in K such that $L_n^{(\alpha)}(x)$ is irreducible in $K[x]$ for all $\alpha \notin S(K)$. In particular, in our context we find that for $n \geq 3$, there are at most finitely many integers α such that $L_n^{(\alpha)}(x)$ is reducible.*

In chapter 3, we give a proof of this theorem for $\alpha \in \mathbb{Z}^+$. In 1 the condition that α is not a negative integer. In chapter 4, we Study about the Galois theory of local fields, finite extensions of $\mathbb{Q}_p$. In chapter 5, first we define Newton index , then we discuss about a criteria for an irreducible polynomials to have a "large" Galois group. Below we mention a couple of important works in the area of large Galois groups of a irreducible polynomial.

Theorem 3. *Let $f \in \mathbb{Q}[x]$ be irreducible of degree n. Let $K/\mathbb{Q}$ be the splitting field of f. Then $\mathcal{N}(f)$ divides $|\mathrm{Gal}(K/\mathbb{Q})|$. Moreover, if there is a prime divisor $l \in (n-2, n/2)$ of $\mathcal{N}(f)$, then $\mathrm{Gal}(K/\mathbb{Q})$ contains A_n, the alternating group on n letters (i.e., as large as possible).*

Theorem 4. *Suppose α is a fixed non negative integer. Then for all but finitely many integers n , the Galois group of $L_n^{\alpha}(x)$ is A_n if Δ_n^{α} is square and S_n otherwise.*

The next corollary can be viewed as improvements of the above Hajir's theorem 19.

Corollary 1. *Fix a nonnegative integer $\alpha \notin \{1, 3, 5\}$. Then for all but finitely many positive integers n, the Galois group associated with $L_n^{(\alpha)}(x)$ over the rationals is S_n and if $\alpha \in \{1, 3, 5\}$ then the Galois group be A_n .*

In chapter 6, we show that for any $\alpha < 0$ with $\alpha \in [-n, -1]$, one has that

$$n! L_n^{(-\alpha)}(x) = (-x)^{(\alpha)}(n-\alpha)! L_{n-\alpha}^{(\alpha)}(x).$$

Thus for $\alpha \in [-n, -1]$, $L_n^{(-\alpha)}(x)$ is reducible. In (see [18]), Hajir addresses the irreducibility of $L_n^{(-\alpha)}(x)$ where α is negative integer and $\mid \alpha \mid > n$. We will

give a proof of this fact later. Among other results, the irreducibility of of $L_n^{(\alpha)}(x)$ has been considered by several authors for small values of $\mid \alpha \mid$ or n. In chapter 6, we introduce the parameter r defined by $\alpha = -1 - n - r$, and

$$L_n^{<r>}(x) = L_n^{(-1-n-r)}(x).$$

Note that, if we simplify the coefficients then

$$L_n^{<r>}(x) = \sum_{j=0}^{n} \binom{n-j+r}{n-j} \frac{(-x)^j}{j!}.$$

As mentioned earlier, Hajir considers the irreducibility of $L_n^{<r>}(x)$ for $r > 0$. For $1 \leq r \leq 8$, Hajir (see [18]) establishes the irreducibility of $L_n^{<r>}(x)$ for all n. Generally for $r \geq 0$, Hajir shows that $L_n^{<r>}(x)$ is irreducible for all but finitely many values of n.
After discussing all of this, we give a partial answer of a question posed by F.Hajir (see [18]) regarding the irreducibility of $L_n^{<r>}(x)$. The result is stated below.

Theorem 5. *For a fixed integer $r \geq 0$, then there exist an effectively computable constant N_r such that every admissible modification of $L_n^{<r>}(x)$ is either irreducible or if it is reducible, then it has at most one linear factor over $\mathbb{Q}$ for all $n \geq N_r$.*

Chapter 2

Newton polygons

In this chapter, we first introduce the concept of Newton polygons. Some discussion of Newton polygons can be found in Dorwart (see [10]), Weiss (see [31]) and Chao (see [7]). Let $f(x) = \sum_{j=0}^{n} a_j x^j$ with $a_0 a_n \neq 0$. Let p be a prime, for $j \in \{0, 1, \cdots, n\}$. We define $x_j = j$ and $y_j \in \mathbb{Z}^+ \bigcup \{0\} \bigcup \{\infty\}$ to the largest exponent of p dividing a_{n-j}.

Let $S = \{(x_0, y_0), (x_1, y_1), \cdots, (x_n, y_n)\}$ be the set of points in the extended plane. We consider the lower edges along the convex hull of these points. The left most edge has one end point being (x_0, y_0) and the right most edge has (x_n, y_n) as the end point. The end points of every edge belongs to the set S. If (x_i, y_i) and (x_j, y_j) are the two end points of such an edge, then every point (x_u, y_u) with $i < u < j$ lies on or above the line passing through (x_i, y_i) and (x_j, y_j). The polygonal path formed by these edges is called the Newton polygon associated with $f(x)$.

The construction of the Newton Polygon:-

Let us define $\nu_p(m) = \{r : p^r | m, p^{(r+1)} \nmid m$ i.e., $p^r \parallel m\}$.

Then we may easily deduce the following property.

(1) $\nu_p(a) = \nu_p(-a)$.

(2) If $p \nmid a$, then $\nu_p(a) = 0$; in particular, $\nu_p(\pm 1) = 0$.

(3) $\nu_p(0) = +\infty$; thus, ν is allowed to take values in the extended complex plane.

(4) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

(5) $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$, provided $b \neq 0$.

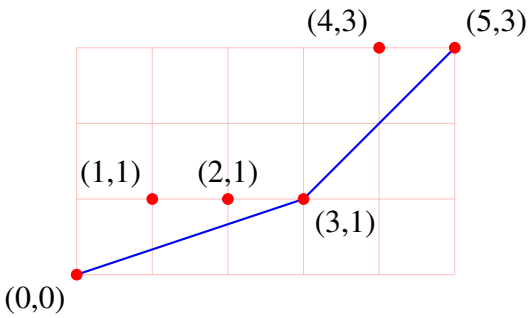

Figure 2.1: The Newton polygon for $f(x) = x^5 + 6x^4 + 6x^3 + 10x^2 + 24x + 40$ w.r.t. $p = 2$.

Then, we have

$$S = \{(0, \nu_p(a_{n-0})), (1, \nu_p(a_{n-1})), \cdots, (j, \nu_p(a_{n-j})), \cdots, (n, \nu_p(a_0))\}.$$

We observe that

(i) the slope of the edges of Newton polygon of $f(x)$ with respect to p increase from left to right;

(ii) all other points must be on or above edges of Newton polygon of $f(x)$ with respect to p.

Example 1. *Let us consider a polynomial* $f(x) = x^5+6x^4+6x^3+10x^2+24x+40$ *and consider the Newton polygon of* f *with respect to the prime* $p = 2$*, then*

$$\begin{aligned} S &= \{(0, \nu(a_5)), (1, \nu(a_4)), (2, \nu(a_3)), (3, \nu(a_2)), (4, \nu(a_1)), (5, \nu(a_0))\} \\ &= \{(0, \nu(1)), (1, \nu(6)), (2, \nu(6)), (3, \nu(10)), (4, \nu(24)), (5, \nu(40))\} \\ &= \{(0, 0), (1, 1), (2, 1), (3, 1), (4, 3), (5, 3)\}. \end{aligned}$$

Since, the slopes of the edges of Newton polygon increase left most edge to right most edge. Then, the Newton polygon for $f(x)$ *with respect to prime* $p = 2$ *consists* 2 *edges , one edge from* $(0, 0)$ *to* $(3, 1)$*, and another from* $(3, 1)$ *to* $(5, 3)$*.*

2.1 Dumas Theorem

Theorem 6. *Let* $g(x)$ *and* $h(x)$ *be in* $\mathbb{Z}[x]$ *with* $g(0)h(0) \neq 0$ *and let* p *be a prime. Let* k *be a non-negative integer such that* p^k *divides the leading coefficient*

of $g(x)h(x)$ but $p^{(k+1)}$ does not. Then the edges of Newton polygon for $g(x)h(x)$ with respect to p is formeds by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to the prime p, using exactly one translate for each edge of Newton polygons for $g(x)$ and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.

To explain the theorem, we consider an example below.

Example 2. *Take $p = 3$, and consider the two polynomials, $f_1(x) = x^3 + 3x^2 + 6x + 9$ and $f_2(x) = 4x^2 + 3x + 3$. The Newton polygon for $f_1(x)$ with respect to prime $p = 3$ consists of two edges one with slope $1/2$ and other with slope 1. The Newton polygon for $f_2(x)$ with respect to prime $p = 3$ consist of one edge with slope $1/2$. The Newton polygon for $f_1(x)f_2(x) = 4x^5 + 15x^4 + 36x^3 + 63x^2 + 45x + 27$ consists two edges one with slope $1/2$ and other with slope 1. The translates of the edges of the Newton polygons for $f_1(x)$ and $f_2(x)$ with slope $1/2$ have merged to form a single edge in the Newton polygon for $f_1(x)f_2(x)$. We emphasize that for our purposes when referring to "edges" of a Newton polygon, we shall not allow two different edges with same slope.*

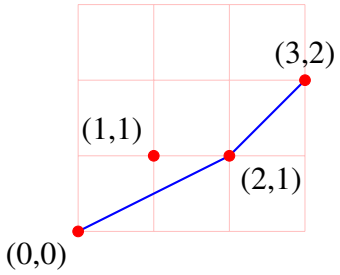

Figure 2.2: The Newton polygon for $f_1(x) = x^3 + 3x^2 + 6x + 9$ w.r.t. $p = 3$.

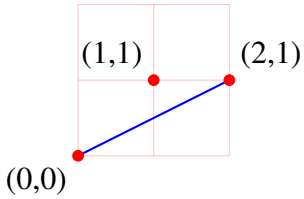

Figure 2.3: The Newton polygon for $f_2(x) = 4x^2 + 3x + 3$ w.r.t. $p = 3$.

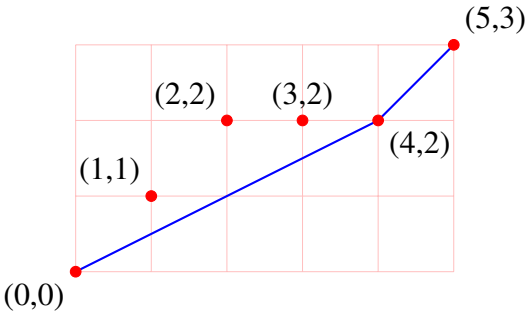

Figure 2.4: The Newton polygon for $f_1(x)f_2(x) = 4x^5 + 15x^4 + 36x^3 + 63x^2 + 45x + 27$ w.r.t. $p = 3$.

2.2 Eisenstein's criteria

Theorem 7. *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ and n be positive integer. Suppose there is a prime p such that*

(i) $p \mid a_i$ *where* $0 \leq i \leq n-1$ *but* $p \nmid a_n$, *and*

(ii) $p^2 \nmid a_0$,

then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Let $f(x) = \sum_{j=0}^{n} a_j x^j$.
Here

$$\begin{aligned} S &= \{(0, \nu_p(a_{n-0})), (1, \nu_p(a_{n-1})), \cdots, (n-1, \nu_p(a_1)), (n, \nu_p(a_0))\} \\ &= \{(0,0), (1, \geq 1), (2, \geq 1), \cdots, (n-1, \geq 1), (n, 1)\}. \end{aligned}$$

We get that $(x_0, y_0) = (0,0), (x_n, y_n) = (n, 1)$, and every other (x_j, y_j) lies on or above the line passing through (x_0, y_0) and (x_n, y_n). Observe that by Dumas theorem $f(x)$ is irreducible over $\mathbb{Q}$. Since if $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$ and with $\deg h(x) > 0$, then the Newton polygon for $f(x)$ with respect to p would be able to represented as translate of 2 or more edges. The latter is impossible because the only lattice points (the points with integral co-ordinates) on the Newton polygon for $f(x)$ are its endpoints (x_0, y_0) and (x_n, y_n). Thus, the theorem of Dumas can be viewed as a generalization of Eisenstein. □

2.3 A Theorem of I. Schur

In this section, we show how Newton polygons can be used to establish the following result due to Schur ([25]).

Theorem 8. *Let n be a positive integer and $a_0, a_1, \cdots, a_n$ be arbitrary integers with $\mid a_0 \mid = \mid a_n \mid = 1$, then*

$$\frac{a_n}{(n)!}x^n + \frac{a_{n-1}}{(n-1)!}x^{n-1} + \cdots + a_1 x + a_0$$

is irreducible over the rationals.

Our use of Newton polygons for obtaining Theorem 8 is summarized by the following lemma.

Lemma 1. *Let k and l be integers with $k > l \geq 0$. Suppose $g(x) = \sum_{j=0}^{n} b_j x^j$ and p be a prime such that $p \nmid b_n, p \mid b_j, \forall j \in \{0, 1, \cdots, n-l-1\}$ and right most edge of $NP_p(g)$ has slope $< 1/k$, then for any integers $a_0, a_1, \cdots, a_n$ with $\mid a_0 \mid = \mid a_n \mid = 1$, the polynomial $f(x) = \sum_{j=0}^{n} a_j b_j x^j$ can not have a factor with degree in the interval $[l+1, k]$.*

Proof. Case 1: Let us consider

$$a_j = 1, \forall j \in \{0, 1, \cdots, n\}.$$

Therefore, $f(x) = g(x)$. We will prove the lemma by contradiction. Assume $f(x)$ has a factor with degree in $[l+1, k]$. Let $f(x) = u(x)v(x)$ where $u(x), v(x) \in \mathbb{Z}[x]$ and $l + 1 \leq \deg u(x) \leq k$. Since, the slope of the edges of Newton polygon for $f(x)$ increase from left to right, the condition of the lemma implies that each edge of $NP_p(f)$ has slope in $[0, 1/k)$. If $NP_p(f)$ has an edge of slope 0, it must be left most edge. Now consider an edge slope > 0 of $NP_p(f)$ and $(a, b), (c, d)$ be any two consecutive lattice points on this edge.

By hypothesis,

$$\frac{1}{\mid (c-a) \mid} \leq \frac{\mid (d-b) \mid}{\mid (c-a) \mid} < \frac{1}{k}$$

$$\Rightarrow \mid c - a \mid > k \geq \deg u(x).$$

Thus, we get the translate of the edges of $NP_p(u)$ can not be found within those edges of the $NP_p(f)$, which have non zero slope i.e., $NP_p(u)$ is not a part of edges of $NP_p(f)$ which has a non zero slope.

Therefore, $NP_p(u)$ is contained within the edge of slope 0. Thus the length of slope 0 is $\geq deg(u)$, but the condition of lemma implies $\nu_p(b_{n-j}) \geq 1$ for $j \in \{l+1, l+2, \cdots, n\}$, so that, if the left most edge $NP_p(f)$ has slope 0 then it has a length $\leq l < \deg(u)$, which is a contradiction.

Case 2: Next we consider the case of arbitrary integers a_0, a_1,$\cdots$, a_n with $\mid a_0 \mid = \mid a_n \mid = 1$. The condition on a_0 and a_n implies that the left and right most end points of $NP_p(f)$ are the same as the left and right most end points $NP_p(g)$ respectively. Also p divides $a_j b_j$, for all $j \in \{0, 1, \cdots, n-l-1\}$, and $p \nmid a_n b_n$. All the edges of $NP_p(g)$ lie on or above the line containing the right most edge. The same statement holds for $f(x)$. Note that $\nu_p(a_j b_j) \geq \nu_p(b_j)$ for all $j \in \{0, 1, \cdots, n\}$. Hence, we also get that all the edges of $NP_p(f)$ lie on or above the line containing the right most edge of $NP_p(g)$.

Let $c_j = a_j b_j$ for all $j \in \{0, 1, \cdots, n\}$.

We have to show that

$$\max_{0 \leq j \leq n-1} \frac{\nu_p(c_0) - \nu_p(c_{n-j})}{n-j} < \frac{1}{k}.$$

Now

$$\begin{aligned}
&\max_{0\le j\le n-1}\frac{\nu_p(c_0)-\nu_p(c_{n-j})}{n-j}\\
&=\max_{1\le j\le n}\frac{\nu_p(c_0)-\nu_p(c_j)}{j}\\
&=\max_{1\le j\le n}\frac{\nu_p(b_0)-\nu_p(b_ja_j)}{j}\\
&=\max_{1\le j\le n}\{\frac{\nu_p(b_0)-\nu_p(b_j)}{j}-\frac{\nu_p(a_j)}{j}\}\\
&\le\max_{1\le j\le n}\frac{\nu_p(b_0)-\nu_p(b_j)}{j}\\
&<\frac{1}{k}
\end{aligned}$$

Therefore, $f(x)$ satisfies the same condition imposed on $g(x)$ in the statement of the lemma. So that, by appealing to the case 1 of the lemma follows. □

Proof of Theorem 8: Let $f(x)=\sum_{j=0}^{n}a_j\frac{x^j}{j!}$ where $|a_0|=|a_n|=1$.

Let

$$g_1(x)=\sum_{j=0}^{n}\frac{x^j}{j!},$$

and

$$g(x)=n!g_1(x)=\sum_{j=0}^{n}\frac{n!}{j!}x^j.$$

Let $h(x)=\sum_{j=0}^{n}a_j\frac{n!}{j!}x^j$. To prove the theorem, it is sufficient to show that $h(x)$ is irreducible over $\mathbb{Z}$.

If $h(x)$ is reducible, let k be the smallest degree of an irreducible factor of $h(x)$.

Necessarily, one has

$$k\le n/2\Rightarrow 2k\le n\Rightarrow k\le n-k.$$

Now, we have to find a prime p such that

(1) $p\mid\{\frac{n!}{0!},\frac{n!}{1!},\frac{n!}{2!},\cdots,\frac{n!}{(n-k)!}\}$

(2) slope of the right most edge is $<1/k$;

Thus, it is enough to find p such that $p \mid \frac{n!}{(n-k)!}$. By Sylvester theorem if $m \geq k$ then

$$P((m+1)(m+2)\cdots(m+k)) \geq k+1.$$

Taking $m = n-k$, we get

$$P((n-k+1)(n-k+2)\cdots(n-k+k)) \geq k+1.$$

So, $p \geq k+1$ exist and satisfies property (1).

We observe that for $g(x) = \sum_{j=0}^{n} b_j x^j$, the slope of the right most edge can be determined by

$$\max_{1\leq j\leq n} \frac{\nu_p(b_0) - \nu_p(b_j)}{j}.$$

In our case, we need to estimate

$$\max_{1\leq j\leq n} \frac{\nu_p(n!) - \nu_p(n!/j!)}{j}.$$

Now, we find that

$$\frac{\nu_p(n!) - \nu_p(n!/j!)}{j} = \frac{\nu_p(n!) - \nu_p(n!) + \nu_p(j!)}{j} = \frac{\nu_p(j!)}{j}.$$

Let us fix $j \in \{1, 2, \cdots, n\}$ as $p^{\nu_p(j!)}$ to be the largest power of p which divides $j!$. Let t be the non- negative integer for which $p^t \leq n < p^{t+1}($ for $j \in \{1, 2, \cdots, n\}$. Now, we observe that

$$\begin{aligned}
\frac{\nu(j!)}{j} &= \frac{\{[j/p] + [j/p^2] + \cdots + [j/p^t]\}}{j} \\
&\leq \frac{(j/p + j/p^2 + \cdots + j/p^t)}{j} \\
&= \frac{(p^t - 1)}{p^t(p-1)} \\
&< \frac{1}{p-1} \\
&< 1/k.
\end{aligned}$$

Hence, the right most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Proof is done. □

Question 1. *Let n and k be positive integers and let $f(x)$ be defined by*

$$\int_0^x (t^{k-1} + t^k + t^{k+1} + \cdots + t^{k-1+n})dt = x^k f(x).$$

Therefore,

$$f(x) = \frac{1}{k} + \frac{x}{k+1} + \cdots + \frac{x^n}{k+n}.$$

Prove that if there is a prime $p > n$ for which $p \mid k(k+n)$ but $p^2 \nmid k(k+n)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Given

$$f(x) = \frac{1}{k} + \frac{x}{k+1} + \cdots + \frac{x^n}{k+n}. \tag{2.1}$$

Let

$$g(x) = (k+1)(k+2)\cdots(k+n)+k(k+2)\cdots(k+n)x+\cdots+k(k+1)\cdots(k+n-1)x^n. \tag{2.2}$$

Clearly,

$$f(x) = \frac{1}{k(k+1)\cdots(k+n-1)(k+n)}g(x). \tag{2.3}$$

Let there is a prime $p > n$ such that

$$p \mid (k+n) \quad p^2 \nmid k(k+n).$$

Now, $p \mid k(k+n)$. Since, p is a prime, $p \mid k$ or $p \mid k+n$ or both $p \mid k$ and $p \mid (k+n)$. Since, $p > n$, $p \mid k$ and $p \mid (k+n)$ does not hold together. Now, $p^2 \nmid k(k+n)$ implies $p^2 \nmid k$ and $p^2 \nmid (k+n)$.

Case -i ($p \mid k$ but $p \nmid (k+n)$ and $p^2 \nmid k, p^2 \nmid (k+n)$)
Since,

$$g(x) = (k+1)(k+2)\cdots(k+n)+k(k+2)\cdots(k+n)x+\cdots+k(k+1)\cdots(k+n-1)x^n.$$

Here,

$$\begin{aligned} S &= \{(0, \nu_p(a_{n-0})), (1, \nu_p(a_{n-1})), \cdots, (j, \nu_p(a_{n-j})), \cdots, (n, \nu_p(a_0))\} \\ &= \{(0,1), (1,1), \cdots, (n-1,1)(n,0)\}. \end{aligned}$$

Since, the slope of the edges of Newton polygon increases left most edge to right most edge and all other points must be on or above edges of Newton polygon of $g(x)$ with respect to p, then the Newton polygon for $g(x)$ with respect to prime p

consist one edge from $(0,1)$ to $(n,0)$. In this case, $g(x)$ is irreducible over $\mathbb{Q}$.

Case-ii: ($p \mid (k+n)$ but $p \nmid k$ and $p^2 \nmid k, p^2 \nmid (k+n)$)
Here,

$$S = \{(0,0),(1,1),(2,1),\cdots(n-1,1)(n,1)\}.$$

For the same reason stated above the Newton polygon for $g(x)$ with respect to prime p consist one edge from $(0,0)$ to $(n,1)$. In this case also, $g(x)$ is irreducible over $\mathbb{Q}$. Therefore, in both cases, $g(x)$ is irreducible over $\mathbb{Q}$. So, from the equation (2.3), we say that $f(x)$ is irreducible over $\mathbb{Q}$. We are done. □

Chapter 3

Irreducibility of $L_n^{(\alpha)}(x)$ where $\alpha \in \mathbb{N} \cup \{0\}$

The generalized Laguerre polynomial is defined by

$$\begin{aligned} L_n^{(\alpha)}(x) &= \sum_{j=0}^{n} \frac{(n+\alpha)\cdot(n-1+\alpha)\cdots(j+1+\alpha)}{(n-j)!\cdot j!}(-x)^j \\ &= \sum_{j=0}^{n} \frac{(n+\alpha)!}{(j+\alpha)!(n-j)!}\frac{(-x)^j}{j!}, \end{aligned}$$

where n is a positive integer and α is an arbitrary complex number. The leading coefficient here is $1/n!$.

As an example if $\alpha = 1$,

$$\begin{aligned} L_n^{(1)}(x) &= \sum_{j=0}^{n} \frac{(n+1)\cdot(n)\cdots(j+2)}{(n-j)!\cdot j!}(-x)^j \\ &= \sum_{j=0}^{n} \frac{(n+1!)}{(n-j)!\cdot(j!)\cdot(j+1)!}(-x)^j \\ &= \sum_{j=0}^{n} \binom{n+1}{j+1}\frac{(-x)^j}{j!}. \end{aligned}$$

3.1 Irreducibility of $L_n^{(\alpha)}(x)$ where $\alpha = 0$

The classical Laguerre polynomials corresponds to $\alpha = 0$ is

$$\begin{aligned} L_n^{(0)}(x) &= \sum_{j=0}^{n} \frac{(n)\cdot(n-1)\cdots(j+1)}{(n-j)!\cdot j!}(-x)^j \\ &= \sum_{j=0}^{n} \frac{n!}{(n-j)!\cdot j!\cdot j!}(-x)^j \\ &= \sum_{j=0}^{n} \binom{n}{j}\frac{(-x)^j}{j!}. \end{aligned}$$

Now, comparing this polynomial with the polynomial $\sum_{j=0}^{n} a_j \frac{(-x)^j}{j!}$, we get $|a_0| = |a_n| = 1$. So, Schur's theorem implies that the classical Laguerre Polynomial is irreducible over the rationals.

3.2 Irreducibility of $L_n^{(\alpha)}(x)$ where $\alpha \in \mathbb{N}$

We want to prove that $\mathcal{L}_n^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$, where

$$\begin{aligned} \mathcal{L}_n^{(\alpha)}(x) &= (-1)^n n! L_n^{(\alpha)}(x) \\ &= \sum_{j=0}^{n} (-1)^{n+j} \binom{n}{j} (n+\alpha)\cdot(n+\alpha-1)\cdots(j+1+\alpha)\, x^j. \end{aligned}$$

Clearly, $\mathcal{L}_n^{(\alpha)}(x)$ is monic polynomial and has integral coefficients. To prove the result, we use some software technology (SAGE). Our main result is stated below.

Theorem 9. *There is an effectively computable constant n_0 such that $\mathcal{L}_n^{(\alpha)}(x)$ is irreducible over the rationals for all $n \geq n_0$.*

This method would imply the irreducibility of a slightly more general polynomials.
Let $\widetilde{\mathcal{L}}_n^{(\alpha)}(x) \in \mathbb{Z}[x]$ defined as

$$\widetilde{\mathcal{L}}_n^{(\alpha)}(x) = \sum_{j=0}^{n} a_j \binom{n}{j} (n+\alpha)\cdot(n+\alpha-1)\cdot(n+\alpha-2)\cdots(j+1+\alpha)\, x^j,$$

where a_j are arbitrary integers with satisfies the condition that $|a_n| = |a_0| = 1$. We shall denote a polynomial of the form $\widetilde{\mathcal{L}}_n^{(\alpha)}(x)$ by $f(x)$. Such a polynomial

$\widetilde{\mathcal{L}}_n^{(\alpha)}$ is sometimes called an *admissible modification* of the original polynomial $\mathcal{L}_n^{(\alpha)}$.

Let $g(x)$ denote the polynomial

$$g(x) = \sum_{j=0}^{n} \binom{n}{j} (n+\alpha) \cdot (n+\alpha-1) \cdot (n+\alpha-2) \cdots (j+\alpha+1)\, x^j.$$

Thus, both $\widetilde{\mathcal{L}}_n^{(\alpha)}$ and $\mathcal{L}_n^{(\alpha)}$, are admissible modifications of $g(x)$. Our main tool in establishing the irreducibility of $\mathcal{L}_n^{(\alpha)}(x)$ is the following lemma of Filaseta (see [2]).

Lemma 2. *Let k be a positive integer. Suppose, $g(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$, and there is prime p satisfying*

(i) $p \nmid b_n$, but p divides b_j for $j \in \{0, 1, \cdots, n-k\}$, and

(ii) the rightmost edge of the Newton polygon $NP_p(g)$ of $g(x)$ with respect to p has slope $< 1/k$.

Then any admissible modification of g does not have a factor of degree k over $\mathbb{Q}$.

Now, we restate Lemma 2 in terms of the function ν, namely, we have its following version.

Lemma 3. *Let k be a positive integer. Suppose, $g(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$, and there is prime p satisfying*

(i) $\nu_p(b_n) = 0$, but $\nu_p(b_j) \geq 1$ for $j \in \{0, 1, \cdots n-k\}$, and

(ii) for any $j \in \{1, 2, \cdots, n\}$, one has

$$\frac{\nu_p(b_0) - \nu_p(b_j)}{j} < 1/k.$$

Then any admissible modification of $g(x)$ does not have a factor of degree k over $\mathbb{Q}$.

Example 3. *As an example of lemma 3, we can deduce the irreducibility of*

$$\frac{x^{19}}{20!} + \frac{x^{18}}{19!} + \cdots + \frac{x^2}{3!} + \frac{x}{2!} + 1$$

over the rationals by multiplying by $20!$, and considering the prime $p = 5, 19$.

Proof. Let

$$f_1(x) = \frac{x^{19}}{20!} + \frac{x^{18}}{19!} + \cdots + \frac{x^2}{3!} + \frac{x}{2!} + 1,$$

and

$$g_1(x) = 20! f_1(x).$$

Then

$$g_1(x) = x^{19} + \frac{20!}{19!}x^{18} + \cdots + \frac{20!}{3!}x^2 + \frac{20!}{2!}x + 20!.$$

In this case, we take prime $p = 19$. Comparing the above equation with $g_1(x) = \sum_{j=0}^{19} b_j x^j$, then we observe that

(i) $\nu_p(b_{19}) = 0, \quad \nu_p(b_j) = 1 \forall j \in \{0, 1, \cdots, 17\}$,

(ii) for any $j \in \{1, 2, \cdots, 19\}$, one has

$$\frac{\nu_p(b_0) - \nu_p(b_j)}{j} < 1/2.$$

This implies that $g_1(x)$ only may have a linear factor over $\mathbb{Q}$.
Now the Newton polygon of $g_1(x)$ with respect to $p = 5$, consist two edges. The edges are $(0, 0)$ to $(15, 3)$, and $(15, 3)$ to $(19, 4)$. The left most edge of $NP_5(g_1(x))$ has two lattice points at $(5, 1)$ and $(10, 2)$. Then by Dummas theorem it may have factor of degree five or degree ten, but not have a linear factor. Therefore, $g_1(x)$ does not contain a linear factor.
In both case of different prime, we observe that $g_1(x)$ does not have facto of any degree, Therefore, $g_1(x)$ is irreducible over $\mathbb{Q}$. Therefore, $f_1(x)$ is irreducible over $\mathbb{Q}$.

□

It is easy to understand that $g(x)$ is a monic with integer coefficients of degree n. Let us assume that g is reducible, then it has a factor with degree in $[1, n/2]$. Since g is reducible over $\mathbb{Q}$, it is also reducible over $\mathbb{Z}$. Therefore, we deduce that if g is reducible, then it has a factor with integer coefficients and degree $\leq n/2$. In Lemma 3, we take

$$\begin{aligned} b_j &= \binom{n}{j}(n+\alpha)\cdot(n+\alpha-1)\cdot(n+\alpha-2)\cdots(j+\alpha+1) \\ &= \binom{n}{j}\frac{(n+\alpha)!}{(j+\alpha)!} = \binom{n}{j}c_j \text{ (say)}. \end{aligned}$$

If $i < j$

$$\frac{c_i}{c_j} = \frac{(n+\alpha)!}{(i+\alpha)!} \cdot \frac{(j+\alpha)!}{(n+\alpha)!} = \frac{(j+\alpha)!}{(i+\alpha)!} = (j+\alpha) \cdot (j+\alpha-1) \cdots (i+\alpha+1).$$

This implies if $i < j$ then c_j/c_i.

Now,

$$\begin{aligned}
&\frac{\nu_p(b_0) - \nu_p(b_j)}{j} \\
&= \frac{\nu_p((n+\alpha)!/(\alpha)!) - \nu_p((n+\alpha)!/(j+\alpha)!) - \nu_p\Big(\binom{n}{j}\Big)}{j} \\
&= \frac{(\nu_p((n+\alpha)!) - \nu_p((\alpha)! - \nu_p\Big(\binom{n}{j}\Big) - \nu_p((n+\alpha)! + \nu_p((j+\alpha)!}{j} \\
&\leq \frac{\nu_p((j+\alpha)!)}{j}.
\end{aligned}$$

By using the formula, $\nu_p(a!) = \sum_{i=1}^{\infty} \left[\frac{a}{p^i}\right]$ where $[\cdot]$ denotes the greatest integer function, we get

$$\frac{\nu_p((j+\alpha)!)}{j} = \frac{1}{j} \sum_{i=1}^{\infty} \left[\frac{j+\alpha}{p^i}\right] < \frac{1}{j} \sum_{i=1}^{\infty} \frac{j+\alpha}{p^i} = \frac{1}{j} \frac{j+\alpha}{p-1} \leq \frac{1+\alpha}{p-1}.$$

Therefore, if we are to show that g does not have a factor of degree k, it is sufficient to show that there exist a prime p such that p satisfies the both condition

(i) p/b_j for all $j \in \{0, 1, \cdots, n-k\}$,

(ii) $(1+\alpha)/(p-1) \leq 1/k$ i.e $p \geq (1+\alpha)k + 1$.

We will give different arguments for various sizes of k with respect to n. For $k \geq 2$, we will achieve our result by showing that there is a prime $p \geq (1+\alpha)k+1$ that divides $c_0, c_1, \cdots, c_{n-k}$. since, c_j/c_i if $i < j$, it is enough to show that $p|c_{n-k}$. As a corollary, we have the following result.

Corollary 2. *For a positive integer n, define $h(x) \in \mathbb{Q}[x]$ as*

$$h(x) = \frac{a_n x^n}{(n+\alpha)!} + \cdots + \frac{a_j x^j}{(j+\alpha)!} + \cdots + \frac{a_1 x}{(\alpha+1)!} + \frac{a_0}{(\alpha)!}, \quad |a_0| = |a_n| = 1.$$

Then either $h(x)$ is irreducible, or, if h is reducible, then h has at most a linear factor.

Proof. Here

$$h(x) = \frac{a_n x^n}{(n+\alpha)!} + \cdots + \frac{a_j x^j}{(j+\alpha)!} + \cdots + \frac{a_1 x}{(\alpha+1)!} + \frac{a_0}{(\alpha)!}, \quad |a_0| = |a_n| = 1.$$

$$= \sum_{j=0}^{n} \frac{a_j}{(j+\alpha)!} x^j$$

$$= \frac{1}{(n+\alpha)!} \sum_{j=0}^{n} \frac{(n+\alpha)!}{(j+\alpha)!} a_j x^j$$

$$= \frac{1}{(n+\alpha)!} \sum_{j=0}^{n} a_j c_j x^j, \quad \text{where} \quad c_j = \frac{(n+\alpha)!}{(j+\alpha)!}.$$

Let us consider the polynomial

$$g(x) = \sum_{j=0}^{n} c_j x^j, \quad \text{where} \quad c_j = \frac{(n+\alpha)!}{(j+\alpha)!}.$$

Since, there is a prime p that divides $c_0, c_1, \cdots, c_{n-k}$ i.e.,

$$\nu_p(c_j) \geq 1 \quad \text{for all} \quad j \in \{0, 1, \cdots, n-k\},$$

but $\nu_p(c_n) = 0$. Then by lemma 3, any admissible modification of $g(x)$ i.e.,

$$\widetilde{g}(x) = \sum_{j-0}^{n} a_j c_j x^j$$

does not have a factor of degree k over $\mathbb{Q}$.
Since, $h(x) = \frac{1}{(n+\alpha)!}\widetilde{g}(x)$, it follows that $h(x)$ is irreducible over $\mathbb{Q}$.

□

We will prove the case later when $k = 1$. We begin by considering the cases for $k \geq 2$. But our strategy is:

$$\text{Find a prime } p \geq (1+\alpha)k + 1 \text{ such that } p | c_{n-k}.$$

Case (i): $2n/\log n < k \leq n/2$.

For k in the indicated range, we will show that there is a prime p in the interval $(n-k+\alpha, n+\alpha]$. First of all, any prime p in $(n-k+\alpha, n+\alpha]$ divides

$$c_{n-k} = (n+\alpha)(n+\alpha-1)(n+\alpha-2)\cdots(n-k+\alpha+1)$$

and hence, p divides c_j for all $j \in \{0, 1, \cdots, n-k\}$. Now observe that this prime p satisfies

$$p > n - k + \alpha = n - n/2 + \alpha = n/2 + \alpha.$$

Thus, $2p > n + 2\alpha$. Consequently, $\nu(c_j) = 1$ for all $j \in \{0, 1, \cdots, n-k\}$ (i.e., p divides c_j exactly once for all $j \in \{0, 1, \cdots, n-k\}$). Next, let us try to figure out if p divides any other c_j. Note that, since $2p > n + 2\alpha$, p divides $c_j = (n+\alpha)(n+\alpha-1)(n+\alpha-2)\cdots(j+\alpha+1)$ if and only if p appears as one of the factors in the product formula for c_j. That is, $p|c_j$ if and only if $p \in [j+1+\alpha, n+\alpha]$, i.e., if and only if $j \leq p-1-\alpha$. Therefore, we have

$$\nu(c_j) = \begin{cases} 1 & \text{if} \quad 0 \leq j \leq p-1-\alpha \\ 0 & \text{if} \quad j \geq p-\alpha. \end{cases}$$

It is easy to understand that the Newton polygon $NP_p(h)$ has only two edges, one joining $(0,0)$ and $(n-p+\alpha, 0)$; and the other edge joining $(n-p+\alpha, 0)$ and $(n, 1)$. Thus, the slope of the rightmost edge of $NP_p(h)$ is $1/(p-\alpha)$. Now, we observe that

$$p - \alpha > n - k \geq k \quad (\text{since}, \ n \geq 2k).$$

Therefore, we may now conclude that the slope of the rightmost edge of $NP_p(h)$ is $< 1/k$. By appealing to Lemma 2, we deduce that $h(x)$ does not have a factor of degree k in this cases.

Thus, it remains to show that there is a prime p in the interval $(n-k+\alpha, n+\alpha]$ for $2n/\log n < k \leq n/2$ By explicit gap estimates on primes [3], we have

$$\pi(x) > \frac{x}{\log x - 0.5} \quad \text{for} \quad x \geq 67, \tag{3.1}$$

and

$$\pi(x) < \frac{x}{\log x - 1.5} \quad \text{for} \quad x \geq e^{1.5}. \tag{3.2}$$

It is sufficient to show that $\pi(n+\alpha) - \pi(n+\alpha-2(n+\alpha)/\log n) > 0$. Let us take $u = (\log n)/2$. Then, we have

$$\begin{aligned} &\pi(n+\alpha) - \pi((n+\alpha)(1-1/u)) \\ &> \frac{n+\alpha}{\log(n+\alpha) - 0.5} - \frac{(n+\alpha)(1-1/u)}{\log(n+\alpha) + \log(1-1/u) - 1.5}, \end{aligned}$$

provided, $n + \alpha \geq 67$ and $(n+\alpha)(1-1/u) \geq e^{1.5}$. Since α is a positive integer ≥ 1 then $67(1 - 2/\log 66) > e^{1.5}$, we just have to take $n \geq 66$. The expressions on the right hand side above upon simplification yields

$$\frac{(n+\alpha)\{\log(n+\alpha)+\log(1-1/u)-1.5-\log(n+\alpha)+\frac{\log(n+\alpha)}{u}+0.5-\frac{1}{2u}\}}{(\log(n+\alpha)-0.5)(\log(n+\alpha)+\log(1-1/u)-1.5)}.$$

For $n \geq 66$, clearly the factors in the denominator above are > 0, and $n+\alpha > 0$. Thus, the expression above is positive if and only if

$$\log(n+\alpha) > u + 1/2 - u\log(1-1/u).$$

Now, we have

$$\begin{aligned} -u\log(1-1/u) &= 1 + \frac{1}{2u} + \frac{1}{3u^2} + \cdots \\ &< \frac{1}{2} + \frac{1}{2}\left(1 + \frac{1}{u} + \frac{1}{u^2} + \cdots\right) \\ &= \frac{1}{2}\left(1 + \frac{u}{u-1}\right) \\ &< 3/2. \end{aligned}$$

Therefore, it is sufficient to show that $\log(n+\alpha) > u+2$, i.e., $\log((n+\alpha)^2/n) > 4$ which is equivalent to have $(n+\alpha)^2/n > e^4$. Since $67^2/66 > e^4$, our assertion follows for $n \geq 66$. A quick search with SAGE (a mathematical open source software), it follows that the interval $(n - 2n/\log n, n]$ contains a prime for each $n \in [8, 65]$. So, we are done in case (i) for every $n \geq 8$.

Case (ii): $n^{2/3} < k \leq 2n/\log n$. Our main tool in this section and in the next case as well, is a lemma due to Erdós, which gives effective lower bounds on the largest prime factor of product of consecutive integers. But first, let us define the quantity $\Delta(u,k)$ as

$$\Delta(u,k) = u(u+1)\cdots(u+k-1), \quad u \in \mathbb{Z}.$$

For a positive integer a, let $P(a)$ denote the largest prime factor of a. Sylvester showed that if $u \geq k$, then $P(\Delta(u,k)) > k$. For $k = u$, this precisely the statement of Bertrand's postulate. The following lemma is based on an idea of Erdós which generalizes Sylvester's result.

Lemma 4. *Let $C \geq 1$ and $0 < \theta < 1$ be given. Suppose the integer k satisfies $n^\theta < k \leq 2n/\log n$. Further suppose that $u \geq n/2$ is an integer. Then there is a constant $k_0 = k_0(C,\theta)$ such that*

$$P(\Delta(u,k)) > Ck \quad \textit{for all} \quad k \geq k_0.$$

Proof. We will prove the lemma by contradiction. Let us assume that $P(\Delta(u,k)) \leq Ck$ for all $k \in (n^\theta, 2n/\log n]$. Let us define the set $\mathcal{T}$ as

$$\mathcal{T} = \{u, u+1, \cdots, u+k-1\}.$$

For each prime $p \leq Ck$, let $e = e(p)$ be the highest exponent of p that divides some element of $\mathcal{T}$ (p^e may divide more than one element of $\mathcal{T}$). Choose one such element and let us call this element u_p. Now, consider the set

$$\mathcal{S} = \mathcal{T}/\{u_p : p \leq Ck\}.$$

Since, for each prime $p \leq Ck$, we are omitting at most one element from $\mathcal{T}$. We deduce that

$$|\mathcal{S}| \geq |\mathcal{T}| - \pi(Ck) = k - \pi(Ck).$$

We know that

$$\pi(x) < 1.25x/\log x \quad \text{for all} \quad x \geq 114.$$

So, we take $n \geq (114/C)^{1/\theta}$, so that, $Ck \geq 114$. For such values of of Ck, we have

$$\pi(Ck) < 1.25Ck/\log Ck \leq 1.25Ck/\log k.$$

Therefore, we have

$$|\mathcal{S}| > k(1 - 1.25C/\log k).$$

Let us define $\Delta_{\mathcal{S}} = \Delta_{\mathcal{S}}(u,k)$ as

$$\Delta_{\mathcal{S}} = \prod_{s \in \mathcal{S}} s.$$

Note that $\Delta_{\mathcal{S}} | \Delta(u,k)$. It is given that each element of $\mathcal{T}$, and hence, every element of $\mathcal{S}$, is $\geq n/2$. Therefore,

$$\Delta_{\mathcal{S}} \geq \left(\frac{n}{2}\right)^{k(1-1.25C/\log k)}.$$

Next, we estimate an upper bound for $\Delta_{\mathcal{S}}$ that, in the end, will contradict the above lower bound, and thereby proving the lemma. Note that, since all prime factors of $\Delta_{\mathcal{S}}$ are $\leq Ck$, and $\nu_p(\Delta_{\mathcal{S}}) = 0$ if $p \nmid \Delta_{\mathcal{S}}$, we have

$$\Delta_{\mathcal{S}} = \prod_{p | \Delta_{\mathcal{S}}} p^{\nu_p(\Delta_{\mathcal{S}})} = \prod_{p \leq Ck} p^{\nu_p(\Delta_{\mathcal{S}})}.$$

Note that the highest exponent of $p \leq Ck$ that divides a $s \in \mathcal{S}$ is $\leq e = e(p)$. For a fixed $1 \leq j \leq e$, the number of multiples of p^j in $\mathcal{T}$ is $\leq [k/p^j]+1$. Note that

at least one of these multiples is u_p defined earlier (To see this, observe that $p^e | u_p$, and that $j \leq e$, so that, u_p is a multiple of p^j). Since, $u_p \notin \mathcal{S}$ and $\Delta_{\mathcal{S}} | \Delta(u,k)$, we deduce that the number of multiples of p^j in $\mathcal{S}$ is equal to the number of multiples of p^j in $\mathcal{T}$ minus 1, i.e.,

$$\leq \left[\frac{k}{p^j}\right].$$

Let $\chi(j) = \chi_p(j)$ denote the number of multiples of p^j in $\mathcal{S}$. We know that $\chi(j) \leq [k/p^j]$. Note that

$$\nu_p(\Delta_{\mathcal{S}}) = \sum_{s \in \mathcal{S}} \nu_p(s) = \sum_{j=1}^{e} \sum_{\substack{s \in \mathcal{S} \\ \nu_p(s)=j}} j = \sum_{j=1}^{e} \sum_{\substack{s \in \mathcal{S} \\ \nu_p(s) \geq j}} 1 = \sum_{j=1}^{e} \chi(j) \leq \sum_{j=1}^{e} \left[\frac{k}{p^j}\right].$$

The last quantity in the above expression is $\leq \nu_p(k!)$. Hence, we have

$$\Delta_{\mathcal{S}} = \prod_{p \leq Ck} p^{\nu_p(\Delta_{\mathcal{S}})} \leq \prod_{p \leq Ck} \nu_p(k!) = k! < k^k.$$

Since, we have assumed that $k \leq 2n/\log n$, we have that

$$\Delta_{\mathcal{S}} < \left(\frac{2n}{\log n}\right)^k.$$

Now, comparing this with the lower bound obtained for $\Delta_{\mathcal{S}}$, we find that

$$\frac{2n}{\log n} > \left(\frac{n}{2}\right)^{(1-1.25C/\log k)}.$$

Rewriting, we have

$$\frac{4^{1-1.25C/2\log k}}{\log n} > \frac{1}{n^{1.25C/\log k}}.$$

Next we use the trivial bound $\log n > \log k$, and the bound $k > n^\theta$ for the right hand side. We further take $k > \exp(1.25C/2)$, so that the quantity $1 - 1.25C/2\log k < 1$. Thus the last inequality above implies

$$\frac{4}{\log k} > \frac{1}{k^{1.25C/\theta \log k}} = \frac{1}{e^{1.25C/\theta}}.$$

Therefore, we deduce from above that

$$k < k_1 = \exp(4\exp(1.25C/\theta)).$$

Thus, if we set

$$k_0 = 1 + \max\{114/C, \exp(1.25C/2), \exp(4\exp(1.25C/\theta))\},$$

then we have a contradiction for $k \geq k_0$, and the proof of the lemma is done. $\square$

For our purposes, we take $u = n - k + 1 + \alpha$, $C = 1 + \alpha$ and $\theta = 2/3$ in Lemma 4, so that, we have

$$k_0 = 1 + e^{4e^{3.75\frac{(1+\alpha)}{2}}}.$$

Note that $k \leq 2n/\log n$ and $n > k$, it follows that

$$\log n > \log k \Rightarrow \frac{1}{\log n} < \frac{1}{\log k} \Rightarrow \frac{2n}{\log n} < \frac{2n}{\log k} \Rightarrow k < \frac{2n}{\log k},$$

$k < 2n/\log k$. Accordingly, we take $n \geq (k \log k)/2 \geq (k_0 \log k_0)/2$. For these values of n, we deduce that $h(x)$ does not have a factor of degree k where k is in the range $(n^{2/3}, 2n/\log n]$.

Case(iii): ($k_2 < k \leq n^{2/3}$) Here k_2 is fixed, and will be specified later. The treatment in this case is similar to that in case(ii). We even use the same sets $\mathcal{T}$ and $\mathcal{S}$. As before, we take $C = (1 + \alpha)$ and $\theta = 2/3$. Only in the last step in the proof of Lemma 4, we make a small adjustment. Here, we replace the upper bound $2n/\log n$ of k by $n^{2/3}$. We further note that for $k \geq e^{\frac{(12.5)(1+\alpha)}{2}}$, one has

$$1 - 1.25(1 + \alpha)/\log k > 0.8.$$

So, we take $k_2 = e^{\frac{(12.5)(1+\alpha)}{2}}$, and after making these changes, we have that

$$n^{2/3} > \left(\frac{n}{2}\right)^{0.8}.$$

The last inequality clearly does not hold for $n \geq 2^6$. Since, we have taken $k \geq k_2$, we must take $n \geq k^{3/2} \geq k_2^{3/2}$. Thus, for $n \geq k_2^{3/2}$, the polynomial $h(x)$ does not have factor of degree in $(k_2, n^{2/3}]$. This settles case (iii).

Case(iv): $1 < k \leq k_2$. The arguments in this section are based on effective versions of Thúe's theorem due to Baker [1].

Theorem 10. *Let $f(x, y) \in \mathbb{Z}[x]$ be absolutely irreducible (i.e., it is irreducible over the fields of complex numbers $\mathbb{C}$). Let $\deg f = m$, and let H denote the height (maximum of the absolute values of coefficients of f). If (x, y) is an integral solution of $f(x, y) = 0$, then we have*

$$\max\{|x|, |y|\} < \exp\exp\exp\left((2H)^{10^{m^{10}}}\right).$$

Finally, we will need the following estimate from [3].

Theorem 11. *For any $z \geq 1$, we have*

$$\sum_{\substack{p \leq z \\ p-a\ prime}} \log p < 1.02z.$$

We begin by proving a lemma concerning the largest prime factor of $m(m+\alpha)$.

Lemma 5. *If $P(\cdot)$ denotes the largest prime factor of a number, and α be any positive integer then*

$$\lim_{m \to \infty} P(m(m+\alpha)) = \infty.$$

Proof. We will proof the lemma by contradiction. Let us assume that for any $K > 0$, and any $M > 0$, there is a $m > M$ such that $P(m(m+\alpha)) \leq K$. Fixing $K > 0$, and let us define

$$\mathcal{P} = \{p \leq K : p, \text{a prime}\} \quad \text{and} \quad P(K) = \prod_{p \leq K} p.$$

Now, we define a new set

$$\mathcal{A} = \{p : P(m(m+\alpha)) \leq K.\}$$

We assume that $|\mathcal{A}| = \infty$. Now by using the fundamental theorem of arithmetic, we can express every integer l as

$$l = l_1 l_2^3,$$

where l_1 is cub-free. Thus, there exist integers $X = X_m$, $Y = Y_m$, and cube-free integers $A = A_m$ and $B = B_m$ such that

$$m + \alpha = AX^3 \quad \text{and} \quad m = BY^3; \quad m \quad \text{be an positive integer.}$$

Therefore, we get the equation

$$AX^3 - BY^3 - \alpha = 0. \tag{3.3}$$

Since, our assumption that $|\mathcal{A}| = \infty$, it clearly implies that at least one of the following sets is infinite:

$$\mathcal{A}_1 = \{X_m : m \in \mathcal{A}\}, \quad \mathcal{A}_2 = \{Y_m : m \in \mathcal{A}\}.$$

For fixed cube-free positive integers A and B, (6.16) is absolutely irreducible. Now, we prove it by proving the following lemma.

Lemma 6. *For fixed cube-free positive integers A and B, and α be any positive integer then $Ax^3 - By^3 - \alpha$ is absolutely irreducible.*

Proof. Let A, B are fixed cube free, and α be any positive integer. Let

$$u(x, y) = Ax^3 - By^3 - \alpha. \tag{3.4}$$

We want to show that $u(x, y)$ is absolutely irreducible. We will prove it by contradiction. Let us assume that $u(x, y)$ is reducible over $\mathbb{C}$.
Let

$$u(x, y) = v(x, y)w(x, y). \tag{3.5}$$

Then

$$\deg u = \deg v + \deg w.$$

Let

$$v(x, y) = a_1x + a_2y + a_3,$$

and

$$w(x, y) = b_1x^2 + b_2y^2 + b_3xy + b_4x + b_5y + b_6.$$

$$\begin{aligned} v(x, y)w(x, y) = a_1b_1x^3 + a_2b_1x^2y + a_1b_3x^2y + a_1b_5xy + a_2b_4xy + a_3b_3xy \\ +a_1b_2xy^2 + a_2b_3xy^2 + a_2b_2y^3 + a_1b_6x + a_3b_4x \\ +a_2b_6y + a_3b_5y + a_3b_1x^2 + a_1b_4x^2 + a_3b_2y^2 \\ +a_2b_5y^2 + a_3b_6. \end{aligned}$$

Now, comparing the coefficients in the above equation with those in the equation (6.17), we get

$$a_1b_1 = A, \tag{3.6}$$

$$a_2b_2 = -B, \tag{3.7}$$

$$a_3b_6 = -\alpha, \tag{3.8}$$

$$a_2b_1 + a_1b_3 = 0, \tag{3.9}$$

$$a_1b_2 + a_2b_3 = 0, \tag{3.10}$$

$$a_1b_6 + a_3b_4 = 0, \tag{3.11}$$

$$a_1b_4 + a_3b_1 = 0, \tag{3.12}$$

$$a_2b_6 + a_3b_5 = 0, \tag{3.13}$$

$$a_3b_2 + a_2b_5 = 0, \tag{3.14}$$

$$a_1b_5 + a_2b_4 + a_3b_3 = 0. \tag{3.15}$$

Now, solving the equations ((6.22) and (6.23)), ((6.24) and (6.25)), and ((6.26) and (6.27)), we get

$$b_3^2 = b_1 b_2, \tag{3.16}$$

$$b_4^2 = b_1 b_6, \tag{3.17}$$

$$b_5^2 = b_6 b_2. \tag{3.18}$$

From equations ((6.29), (6.30) and (6.31)), we can say that b_1, b_2, b_6 must have the same sign. Now from equation (6.19) , it is clear that a_1 and b_1 have same sign. Also from equation (6.20), it is clear that a_2 and b_2 has opposite sign. Again from equation 6.21, it is clear that a_3 and b_6 have opposite sign. Since b_2, b_6 have same sign, then a_2, a_3 have same sign. Again from the equation (6.24), we get $b_4 = -a_1 b_6/a_3$, this implies b_4, a_1 have same sign. Again from the equation (6.27), we get $b_5 = -a_3 b_2/a_2$, this implies b_5, b_2 has opposite sign. Again from the equation (6.22) we get $b_3 = -a_2 b_1/a_1$, this implies b_3, b_1 have same sign. From the above observation we conclude that $b_1, b_2, b_3, b_4, b_6, a_1$ has same sign, and a_2, a_3, b_5 has same sign. Therefore, we get the result that a_1, b_5 have opposite sign. a_2, b_4 and a_3, b_3 also have opposite sign. Therefore, the sign of $a_1 b_5, a_2 b_4, a_3 b_3$ are all negative. Then this cannot satisfy the equation (6.28), if it is satisfied, then all are zeros. So, we arrive at a contradiction. Therefore, our original assumption was wrong. This implies $u(x, y)$ is absolutely irreducible. □

Hence, by Theorem 10, we deduce that any integral solution (X, Y) of (6.16) must satisfy

$$\max\{X, Y\} < \exp\exp\exp\left((2H)^{10^{3^{10}}}\right), \quad \text{where} \quad H = \max\{A, B\}.$$

Since $P(m(m+\alpha)) \leq K$, we deduce that m and $m+\alpha$ are made up of primes $\leq K$. Since A is a cube-free divisor of m, we have $A|P(K)^2$. Similarly, $B|P(K)^2$. Thus, one has

$$\max\{X, Y\} < \exp\exp\exp\left((2e^{2.04K})^{10^{3^{10}}}\right) = n_K, \text{ a fixed number.}$$

But this implies both $\mathcal{A}_1$ and $\mathcal{A}_2$ to be finite, and therefore, we arrive a contradiction. So our original assumption is wrong. Thus $|\mathcal{A}| < \infty$, and the lemma follows. □

Let us now get back to the polynomial $h(x)$. Since, we are trying to show that $h(x)$ does not have a factor with degree in $(1, k_2]$. We take $K = (1+\alpha)k_2 + 1$ in Lemma 18. We further take $n = \deg h$ to be

$$n > P(K)^2 n_K^3.$$

Then from Lemma 18, we deduce that $P(n(n+\alpha)) > K = (1+\alpha)k_2 + 1$. Next, we note that for any $2 \leq k \leq k_2$, one has that

$$n(n+\alpha)|c_j \quad \text{for all} \quad j \in \{0, 1, \cdots, n-k\}.$$

Let $p = P(n(n+\alpha))$. Thus, we have for any $2 \leq k \leq k_2$ that

$$p|n(n+\alpha)|c_j \quad \forall j \in \{0, 1, \cdots, n-k\}, \text{and} \quad p \geq (1+\alpha)k_2 + 1 \geq (1+\alpha)k + 1.$$

Our conclusion in case (iv) now follows from Lemma 3.

Case(v): $k = 1$. As indicated earlier, we will consider the polynomial $g(x)$ instead of $h(x)$ in this case. The coefficients of g are given by.

$$b_j = \binom{n}{j}(n+\alpha)\cdot(n+\alpha-1)\cdot(n+\alpha-2)\cdots(j+1+\alpha) = \binom{n}{j}c_j.$$

Clearly, $nc_j|b_j$ for any $1 \leq j \leq n-1$. Also, $(n+\alpha)|c_j$ for any $j \leq n-1$. For $j = 0, n|b_j$. Therefore, $n(n+\alpha)|b_j$ for all $j \leq n-1$. Once again, we take $n > P(K)^2 n_K^3$, but with $K = \alpha+2$. Then we deduce that $P(n(n+\alpha)) \geq (\alpha+2)$. If p denotes $P(n(n+\alpha))$, then we deduce that there is a prime $p \geq (\alpha+2)$ $(= (1+\alpha)\cdot 1 + 1)$ such that

$$p|n(n+\alpha)|b_j \quad \text{for all} \quad j \in \{0, 1, \cdots, n-1\}.$$

Thus, by appealing to Lemma 3, we conclude that g cannot have a linear factor. This completes case (v).
Let n_0 be the maximum of all the lower bounds on n in cases (i) through (v), i.e., n_0 is largest among the following:

- 8 from case (i)
- $(k_0 \log k_0)/2$, where $k_0 = 1 + e^{4e^{3.75(1+\alpha)/2}}$ from case (ii)
- $\exp((18.75)(1+\alpha)3/4)$ from case (iii)
- $P(K)^2 n_K^3$ from case (iv) where

  $$P(K) = \prod_{p \leq K} p, n_K = \quad \exp\exp\exp\left((2e^{2.04K})^{10^{3^{10}}}\right),$$

  and

  $$K = (1+\alpha)\exp((18.75)(1+\alpha)/2) + 1.$$

- $P_3^2 n_3^3$ from case (v)

Clearly, the fourth item gives the maximum value, and this gives us an explicit estimate for n_0 (albeit too large).

Chapter 4

Galois theory of Local Fields

4.1 Preliminaries on Valuation and Completion

In this section we recall certain facts from the valuation theory. Let F be a field. A subring V of F is said to be a *valuation ring* of F if for every $a \neq 0$ in F, at least one of a or a^{-1} belongs to V. We list down all the relevant attributes of a valuation ring in the next proposition.

Proposition 1. *Let V and F be as above. Then we have the following.*

(i) The field of fractions of V is K.

(ii) V is a local ring (i.e., has a unique maximal ideal).

(iii) V is integrally closed in F (only elements of F integral over V are those of V).

(iv) If I and J are ideals in V, then either $I \subseteq J$ or $J \subseteq I$. Thus the set of ideals of V is totally ordered under inclusion.

(v) If V is Noetherian, then V is a PID. Furthermore, for some prime $p \in V$, every ideal is of the form (p^n). For any such prime p, one has that $\cap_{n=1}^{\infty}(p^n) = (0)$.

Proof. If $a \neq 0$ is an element of F, then one of a or a^{-1} is in V. Since, a can be expressed as $a/1$ or $1/(a^{-1})$, part (i) now follows.

For part (ii), we show that the set $\mathcal{M}$ of all non-units forms an ideal of V. Since, $\mathcal{M}$ does not contain a unit, it is a proper ideal of V. Since, every proper ideal of V is contained in $\mathcal{M}$, we deduce that $\mathcal{M}$ must be the unique maximal ideal of V. To prove our claim, observe that if a and b are nonzero non-units, then one of a/b or b/a is in V. If $a/b \in V$, then $a + b = b(1 + a/b)$, i.e., $a + b = bv$

for some $v \in V$. Now, if $a+b$ is a unit, then it forces b to be a unit, contrary to our assumption on b. Consequently, $a+b \in \mathcal{M}$. Similarly, if $b/a \in V$, then $a+b \in \mathcal{M}$. Lastly, if $a \in V$ and $v \in V$, then va is again a non-unit in V, and consequently, $va \in \mathcal{M}$. Therefore, $\mathcal{M}$ is an ideal as claimed.

We next prove part (iii). If $a \in F$ is integral over V, then there exists elements $c_0, c_1, \cdots, c_{n-1}$ in V such that

$$a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0.$$

If $a \in V$, then there is nothing to prove. So, we assume $a \notin V$. Therefore, $1/a \in V$. Multiplying the last equation by $1/a^{n-1}$ and rearranging, we have

$$a = -(c_{n-1} + c_{n-2}/a + \cdots + c_0/a^{n-1}) \in V,$$

thereby proving part (iii).

For part (iv), assume that I and J are ideals of V and that $I \not\subseteq J$. We will show that $J \subseteq I$. If not, then let j be in $J \backslash I$ and i in $I \backslash J$. Now, one of j/i or i/j is in V. Clearly, $j/i \notin V$, else $j = (j/i)i \in J$, a contradiction. But if $i/j \in V$, then $i = (i/j)j \in J$ is also an impossibility. It now follows that $J \subseteq I$.

Finally, for part (v), We let I be an ideal of Noetherian ring V, and let $\{a_1, a_2, \cdots a_n\}$ be a finite set of generators for I. By the last part, after relabeling suitably, we may assume that

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n).$$

But then one has

$$I \subseteq < a_1, a_2, \cdots, a_n > \subseteq (a_n) \subseteq I.$$

Thus, $I = (a_n)$ and V is a PID. The maximal ideal $\mathcal{M}$ is thus a principal ideal. If $\mathcal{M} = (p)$, then it follows that p is a prime (maximal ideals are prime). In fact, it is easy to see that all other primes are associates of p. To see this, note that if (q) is another prime ideal, then $(q) \subseteq (p)$ implies $p|q$. Since, a prime is irreducible, the assertion follows at once. Recall that in a PID, irreducible elements are prime, and as such, it follows that p is the unique (up to associates) irreducible element of V. Next, consider a nonzero ideal $I = (a)$ in V. Since, a PID is also a UFD, a can be expressed uniquely as a product of a unit and a finitely many irreducible elements in V. As p is the unique irreducible element in V, we therefore have that $a = up^m$ where u is a unit in V. Now, we can easily see that $I = (a) = (p^m)$. The last assertion of part (v) follows similarly. For, if a is in $\cap_{n=1}^{\infty}(p^n)$, then $p^n|a$ for all n. Since V is a UFD, it follows that $a = 0$. □

We will now introduce the notion of an *absolute value* on a field F.

Definition 1. *An absolute value on a field F is a map $|\cdot| : F \to \mathbb{R}$ having the following properties:*

(i) $|x| \geq 0$ *for all* $x \in F$ *and* $|x| = 0 \iff x = 0$.

(ii) $|xy| = |x||y|$ *for all* x *and* y *in* F.

(iii) $|x + y| \leq |x| + |y|$ *for all* x *and* y *in* F.

The absolute value is said to be nonarchimedean *if it satisfies following stronger version of (iii).*

(v) $|x + y| \leq \max\{|x|, |y|\}$ *for all* x *and* y *in* F.

The usual absolute values on $\mathbb{R}$ or $\mathbb{C}$ is an *archimedean* absolute value. Our interest however will be in the nonarchimedean ones which are mostly induced by *valuations*.

Definition 2. *A discrete valuation* $\nu(\cdot)$ *is a function* $\nu : F \to \mathbb{Q} \cup \{\infty\}$ *satisfying the following properties:*

(i) $\nu(x) = \infty$ *if and only if* $x = 0$ *(by convention).*

(ii) $\nu(xy) = \nu(x) + \nu(y)$ *for all* x *and* y *in* F.

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ *for all* x *and* y *in* F.

It is easily seen that a valuation ν *induces a nonarchimedean absolute value* $|x| = |x|_\nu = c^{-\nu(x)}$ *where* $c > 1$ *is a real number.*

Note that $\nu : F^* \to \mathbb{Q}$ is a group homomorphism from the multiplicative group of nonzero elements F^* in F to an additive subgroup of $\mathbb{Q}$. Consequently, its image must be a cyclic subgroup of $\mathbb{Q}$, i.e., it is of the form $r\mathbb{Z}$ where $r \in \mathbb{Q}$. We remark that any *discrete subgroup* of $(\mathbb{R}, +)$ would work. We will be concerned with nonarchimedean absolute values of number fields induced by p-adic valuations.

Proposition 2. *Let* ν *be a discrete valuation on a field* F. *Then*

$$\mathcal{O} = \mathcal{O}_F = \{x \in F : \nu(x) \geq 0\} = \{x \in F : |x| \leq 1\}$$

is the valuation ring (called the discrete valuation ring or DVR) with the unique maximal ideal $\mathfrak{m}$ *given by*

$$\mathfrak{m} = \{x \in F : \nu(x) > 0\} = \{x \in F : |x| < 1\}.$$

Consequently, by Proposition 1, $\mathcal{O}$ *is integrally closed in* F.

Proof. The fact that $\mathcal{O}$ is a ring follows from the nonarchimedean and multiplicative properties of the absolute value. For any $x \neq 0$ in F, we have $|x||x^{-1}| = 1$. It now follows from the definition of $\mathcal{O}$ that it is a valuation ring. From Proposition 1, we find that $\mathcal{O}$ has a unique maximal ideal consisting of all the non-units in $\mathcal{O}$. It can be easily seen that for $x \in \mathcal{O}$, one has $|x| = 1$ if and only if x is a unit in $\mathcal{O}$ if and only if $\nu(x) = 0$. The last part of the proposition now follows. □

Recall that $\nu(F^*) = r\mathbb{Z}$ where $r \in \mathbb{Q}$. Thus, r is the smallest positive element in the image of ν. This means there is an element $\pi \in F^*$ with $\nu(\pi)$. Thus $\pi \in \mathfrak{m}$. Such an element is called a *uniformizer* of $\mathcal{O}$.

Proposition 3. *We have $\mathfrak{m} = (\pi) = \pi\mathcal{O}$. Any element x of F^* can be expressed uniquely as $x = u\pi^n$ where u is a unit in $\mathcal{O}$ and $n \in \mathbb{Z}$. Thus, in particular, we have $F = \mathcal{O}[1/\pi]$.*

Proof. It is clear that $(\pi) \subseteq \mathfrak{m}$. Now let $a \neq 0$ be in $\mathfrak{m}$. Note that from the choice of π, it follows that $\nu(a) \geq \nu(\pi)$. Thus, $\nu(a\pi^{-1}) = \nu(a) - \nu(\pi) \geq 0$. Consequently, $a\pi^{-1} \in \mathcal{O}$, and hence, $a \in (\pi)$.

For the second part, we note that for any $a \in F^*$, there is an integer n such that

$$\nu(a) = nr = n\nu(\pi) = \nu(\pi^n).$$

It follows that $\nu(a\pi^{-n}) = 0$, i.e., $a\pi^{-n} \in \mathcal{O}^*$ (the group of units in $\mathcal{O}$). Thus $a = u\pi^n$ where u is a unit in $\mathcal{O}$. Since n is unique (depends on a only), it forces u to be unique as well. This proves the uniqueness part. The last bit follows at once now. □

As our final exercise on DVR, we show that $\mathcal{O}$ is a PID (in fact, it is an Euclidean Domain).

Proposition 4. *Let I be an ideal in $\mathcal{O}$. Then $I = \mathfrak{m}^n = (\pi^n)$ for some nonnegative integer n. Thus, $\mathcal{O}$ is a PID. Moreover, we have $\cap_{n=1}^{\infty}\mathfrak{m}^n = (0)$.*

Proof. Let $nr = \min\{\nu(x) : x \in I\}$ where n is a positive integer. Thus $nr > 0$ (else, I contains a unit). Let $a \in I$ be the element with $\nu(a) = nr$. Thus by Proposition 3, we have $a = u\pi^n$, and consequently, $\mathfrak{m}^n = (\pi^n) = (a) \subseteq I$. Conversely, suppose, $b \in I$, and let $\nu(b) = kr = k\nu(\pi) = \nu(\pi^k)$. By our construction, it follows that $k \geq n$. Also, by Proposition 3, there is a unit u' such that $b = u'\pi^k$. Therefore, $b \in (\pi^k)$. Since, $k \geq n$, we have $(\pi^k) \subseteq (\pi^n)$. Thus, $b \in (\pi^n) = \mathfrak{m}^n$. From our choice of n, we also find that it is unique. The last is proved by working similarly to the proof of Proposition 1. □

We now take up the completion (topological) of F with respect to the metric induced by a discrete valuation ν.

Definition 3. *Let $\mathscr{C} = \mathscr{C}_\nu(F)$ denote the set of Cauchy sequences in F with respect to the absolute value induced by ν. It is easy to see that $\mathscr{C}$ has a natural commutative ring structure with addition and multiplication inherited from F. Let $\mathscr{N}$ denote the set of all null sequences in F. Thus, $\mathscr{N}$ is clearly an ideal in $\mathscr{C}$. In fact, $\mathscr{N}$ can be shown to be a* maximal *ideal. The quotient ring $\mathscr{C}/\mathscr{N}$, which is thus a field, is called the* completion *of F with respect to the absolute value $|\cdot|_\nu$ induced by ν and is denoted by F_ν. Essentially, F_ν consists of all the equivalence classes of Cauchy sequences in F. That it is a field, follows from the quotient description above.*

In fact, F_ν is a valued field (field with a valuation). For, if $x = \{x_n\}$ where $x_n \in F$, is an element of F_ν, then we may define

$$\nu(x) = \lim_{n\to\infty} \nu(x_n) \quad \text{and} \quad |x| = \lim_{n\to\infty} |x_n| = c^{-\lim_{n\to\infty} \nu(x_n)} = c^{-\nu(x)},$$

where $c > 1$ is a constant. It should also be noted that $|x| = 0$ (or $\nu(x) = \infty$) if and only if $\{x_n\}$ is a null sequence, i.e., if and only if $x = 0$. Furthermore, if $x \neq 0$, then $\{\nu(x_n)\}$ must be a eventually constant sequence for $\{x_n\}$ to be Cauchy. Therefore, the range of the extended ν is again $r\mathbb{Z} \cup \{\infty\}$. Thus, we may as well define its *discrete valuation ring* $\mathcal{O}_\nu$ of F_ν to be

$$\mathcal{O}_\nu = \{x \in F_\nu : \nu(x) \geq 0\} = \{x \in F_\nu : |x| \leq 1\}$$

with the unique maximal ideal $\mathfrak{m}$ given by

$$\mathfrak{m}_\nu = \{x \in F_\nu : \nu(x) > 0\} = \{x \in F_\nu : |x| < 1\}.$$

Our key result concerning F_ν is the following. Most of the properties listed below, follow from Proposition 1, or are very similar to proofs done in the case of $\mathcal{O}$. We leave these details and prove the others.

Proposition 5. *Let F_ν and $\mathcal{O}_\nu$ be as above. Then we have the following.*

(i) *F is dense in F_ν*

(ii) *The field of fractions of $\mathcal{O}_\nu$ is F_ν.*

(iii) *There is a natural inclusion $\mathcal{O} \hookrightarrow \mathcal{O}_\nu$ by $x \to \{x, x, \cdots\}$. Therefore, there is also a natural inclusion $F \hookrightarrow F_\nu$.*

(iv) *$\mathcal{O}_\nu$ is integrally closed in F_ν.*

(v) *$\mathcal{O}_\nu \cap F = \mathcal{O}$*

(vi) *$\mathcal{O}_\nu$ is a local ring with the unique maximal ideal $\mathfrak{m}_\nu$, generated by π (the uniformizer of F). Thus, $\mathfrak{m}_\nu = \pi\mathcal{O}_\nu$.*

(vii) *Any ideal of $\mathcal{O}_\nu$ is of the form $\pi^n\mathcal{O}_\nu$ where n is nonnegative integer. Moreover $\cap_{n=1}^{\infty}\pi^n\mathcal{O}_\nu = (0)$.*

(viii) *For every $x \in \mathcal{O}_\nu$, there exists a $\{x_n\} \to x$ where x_n is a unique element $\mathcal{O}/\pi^n\mathcal{O}$ (here, we interpret x_n as an element of $\mathcal{O}$), and $x_n \equiv x_{n-1} \pmod{\pi^{n-1}}$. Thus $\mathcal{O}$ is dense in $\mathcal{O}_\nu$.*

(ix) *One has an exact sequence*

$$0 \longrightarrow \mathcal{O}_\nu \xrightarrow{\cdot\pi^n} \mathcal{O}_\nu \xrightarrow{\epsilon_n} \mathcal{O}/\pi^n\mathcal{O} \longrightarrow 0,$$

where $n \geq 1$ and $\epsilon_n(x) = x_n + \pi^n\mathcal{O}$. In particular, we see that

$$\mathcal{O}_\nu/\pi^n\mathcal{O}_\nu \cong \mathcal{O}/\pi^n\mathcal{O} \quad \forall \quad n \geq 1.$$

(x) *The residue fields $\urcorner = \mathcal{O}/\pi\mathcal{O}$ and $\urcorner_\nu = \mathcal{O}_\nu/\pi\mathcal{O}_\nu$ are isomorphic.*

Proof. Most of these are straightforward. We begin with part (vi). Clearly, we have $\pi\mathcal{O} \subseteq \mathfrak{m}_\nu$. Let α be a nonzero element of $\mathfrak{m}_\nu$. As noted earlier, $\nu(\alpha) \in r\mathbb{Z}$ where $r = \nu(\pi)$. Thus, there is an integer k such that $\nu(\alpha) = \nu(\pi^k)$. A routine calculation as before shows that there is a unit $u_\nu \in \mathcal{O}_\nu$ such that $\alpha = u_\nu\pi^k$. Part (vii) follows from Proposition 1.

For part (viii), observe that F is dense in F_ν. Thus, for any $x \in \mathcal{O}_\nu$, and $n \geq 1$, there is an element $a/b \in F$, where a, b are in $\mathcal{O}$, such that

$$\left|x - \frac{a}{b}\right| < \frac{1}{r^n} = \frac{1}{|\pi^n|}.$$

Also, by the noarchimedean property of $|\cdot|$, one has

$$\left|\frac{a}{b}\right| \leq \max\left\{|x|, \left|x - \frac{a}{b}\right|\right\} \leq 1.$$

It follows that $a/b \in \mathcal{O}_\nu$. Since, $\nu(a/b) \geq 0$, we may assume that $\pi \nmid b$. Define x_n to be the unique element $ab^{-1} \pmod{\pi^n\mathcal{O}}$. In particular, we find that $|x_n - a/b| \leq 1/|\pi^n|$. Thus, for all $n \geq 1$, we have

$$|x - x_n| < \max\left\{\left|x - \frac{a}{b}\right|, \left|x_n - \frac{a}{b}\right|\right\} \leq 1/|\pi^n|, \quad \text{i.e.,} \quad x \equiv x_n \pmod{\pi^n}.$$

We have thus gotten hold of a sequence $\{x_n\}$ in $\mathcal{O}_\nu$ that converges to x. The other half follows from the observation that $x_n - x_{n-1} = (x - x_n) - (x - x_n) \equiv 0 \pmod{\pi^{n-1}}$.

For part (ix), we observe that the map $\mathcal{O}_\nu \to \mathcal{O}_\nu$, sending $x \to \pi^n x$ is clearly injective. Also, if $\{x_n\}$ is a sequence of numbers in $\mathcal{O}$ satisfying the conditions in (viii), then one has for any $m \geq n$ that

$$|x_n - x_m| \leq \max\{|x_i - x_{i-1}| : n \leq i \leq m\} \leq \max\{1/p^{i-1} : n \leq i \leq m\} = 1/p^{n-1}$$

Thus, $\{x_n\}$ is Cauchy, and hence has a limit x in F_ν. Since, $x_n \in \mathcal{O}$ for all n, it follows that

$$|x| = \lim_{n\to\infty} |x_n| \geq 1,$$

i.e., $x \in \mathcal{O}_\nu$. Consequently, ϵ_n is onto for every $n \geq 1$. To finish the prove, it thus remains to show that $\ker \epsilon_n = \pi^n \mathcal{O}_\nu$. Suppose, $x = \{x_i\}$ be in the kernel of ϵ_n where $\{x_i\}$ is as in part (ix). It thus follows that $x_n \equiv 0 \pmod{\pi^n}$. If $m \geq n$, then

$$x_m \equiv x_{m-1} \equiv \cdots \equiv x_n \equiv 0 \pmod{\pi^n},$$

while,from $x_{n-1} \equiv x_n \equiv 0 \pmod{\pi^{n-1}}$, we find that $x_{n-1} \equiv 0 \pmod{\pi^{n-1}}$. Proceeding inductively, one obtains that $x_m \equiv 0 \pmod{\pi^m}$ for all $m \leq n$. Thus, the sequence $\{x_i\}$, when considered as a sequence in $\mathcal{O}$, satisfies $x_i = \pi^n y_i$, where $y_i \in \mathcal{O}$ and $y_i = 0$ for all $i \leq n$. Thus

$$x = \lim_{i\to\infty} x_i = \pi^n \lim_{i\to\infty} y_i \in \pi^n \mathcal{O}_\nu.$$

Conversely, if $x \in \pi^n \mathcal{O}_\nu$, then it is easy to see that $x_n = \epsilon_n(x) \equiv 0 \pmod{\pi^n}$.

Part (x) easily follows from (ix) by taking $n = 1$. This finishes the proof of the proposition.

□

We will be particularly interested in *finite extensions* of completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to the absolute value induced by p-adic valuation on $\mathbb{Q}$, which in turn arises from the fundamental theorem of arithmetic. The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$. Our next goal will be to study the relationship between localization of an extension of a number field and the extension of its localization. We begin by constructing a complete valued local field starting with a Noetherian domain $\mathcal{O}$ and a given prime ideal $\mathfrak{p}$ in $\mathcal{O}$. We follow the same steps as one would take to obtain $\mathbb{Q}_p$ starting with $\mathbb{Z}$. That is, first localize $\mathbb{Z}$ at (p) to obtain the local ring

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b \right\}.$$

$\mathbb{Q}$ is still the fraction field of $\mathbb{Z}_{(p)}$. In fact, it is the valuation ring of $\mathbb{Q}$ with respect to the p-adic valuation. Now, complete $\mathbb{Q}$ with respect to the p-adic absolute value to obtain $\mathbb{Q}_p$. Let F denote the field of fractions of $\mathcal{O}$. Localize $\mathcal{O}$ at $\mathfrak{p}$ by inverting all the elements of the multiplicatively closed set $\mathcal{O}\backslash\mathfrak{p}$ to obtain the local ring $\mathcal{O}_{(\mathfrak{p})}$ whose unique maximal ideal is given by $\mathfrak{B} = \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$, and whose field of fractions is F. Next, we give a notion of valuation $\nu = \nu_{\mathfrak{p}}$ on $\mathcal{O}_{(\mathfrak{p})}$ which, we then extend to all of F by setting $\nu(a/b) = \nu(a) - \nu(b)$. In order to look for a valuation on $\mathcal{O}$, we appeal to Krull-intersection theorem and Nakayama's Lemma.

Theorem 12. *(Krull Intersection Theorem) Let R be a commutative Noetherian ring, I be an ideal in R and let M be a finitely generated module over R. Further let $L = \cap_{n=1}^{\infty} I^n M$. Then $IL = L$.*

Theorem 13. *(Nakayama's Lemma) Let R be a commutative ring with unity, and let M be a finitely generated module over R. Further suppose that an ideal J of R is contained in its* Jacobson radical *(intersection of maximal ideals of R). If $JM = M$, then $M = 0$.*

As an immediate consequence, we have the following.

Corollary 3. *In $\mathcal{O}_{(\mathfrak{p})}$, we have $\cap_{n=1}^{\infty} \mathfrak{B}^n = (0)$. Consequently, for every $x \in \mathcal{O}_{(\mathfrak{p})}$ there exists a unique nonnegative integer $n = n(x)$ such that $x \in \mathfrak{B}^n \backslash \mathfrak{B}^{n+1}$ (here, we interpret $\mathfrak{B}^0$ as $\mathcal{O}_{(\mathfrak{p})}$).*

Proof. First, we take $M = R = \mathcal{O}_{(\mathfrak{p})}$ in Theorem 12. Since $\mathcal{O}$ is Noetherian, it follows that so is $\mathcal{O}_{(\mathfrak{p})}$, and as such can be thought as a finitely generated module over itself. We further take $I = \mathfrak{B}$ and $L = \cap_{n=1}^{\infty} \mathfrak{B}^n$. From the conclusion of the theorem, it thus follows that $\mathfrak{B}L = L$. Since, $\mathfrak{B}$ is the only maximal ideal in $\mathcal{O}_{(\mathfrak{p})}$, we deduce that it is the Jacobson radical of $\mathcal{O}_{(\mathfrak{p})}$. Note that L is an ideal in $\mathcal{O}_{(\mathfrak{p})}$, and hence, finitely generated. Now, taking $J = \mathfrak{B}$ in Theorem 13, we deduce that $L = (0)$. Now, let $x \in \mathcal{O}_{(\mathfrak{p})}$. If x is a unit, then $x \in \mathcal{O}_{(\mathfrak{p})} \backslash \mathfrak{B}$. Otherwise, the ideal (x) is either (x) is contained in some maximal ideal in $\mathcal{O}_{(\mathfrak{p})}$. Since $\mathfrak{B}$ is the only maximal ideal in $\mathcal{O}_{(\mathfrak{p})}$, it follows that $x \in \mathfrak{B}$. As $\cap_{n=1}^{\infty} \mathfrak{B}^n = (0)$, we have that

$$\mathfrak{B} = \bigcup_{n=1}^{\infty} (\mathfrak{B}^n \backslash \mathfrak{B}^{n+1}).$$

Therefore, we conclude that there is a unique $n = n(x)$ such that $x \in \mathfrak{B}^n \backslash \mathfrak{B}^{n+1}$. □

Thanks to Corollary 3, we may now define a valuation on $\mathcal{O}_{(\mathfrak{p})}$ by setting

$$\nu(x) = n(x)r \in r\mathbb{Z}$$

where r is positive rational number (we keep r for strategic purposes). If x and y are elements of $\mathcal{O}_{(\mathfrak{p})}$ with corresponding valuation numbers $n(x)$ and $n(y)$, respectively, then

$$\mathfrak{B}^{n(x)}||(x) \quad \text{and} \quad \mathfrak{B}^{n(y)}||(y).$$

Therefore, it follows that $\mathfrak{B}^{n(x)+n(y)}||(xy)$, and consequently, $\nu(xy) = \nu(x)+\nu(y)$ for all x and y in $\mathcal{O}_{(\mathfrak{p})}$. Also, $x+y \in \mathfrak{B}^m$ where $m = \min\{n(x), n(y)\}$. Therefore, it follows that the absolute value induced by ν on F is nonarchimedean. Let $F_{\mathfrak{p}}$ be the completion of F with respect to ν. Thus, $F_{\mathfrak{p}}$ is a complete valued field. Let $\mathcal{O}_{\mathfrak{p}}$ be its valuation ring (in fact, it is a DVR) with the unique maximal ideal $\mathfrak{B}\mathcal{O}_{\mathfrak{p}}$. All the properties of $\mathcal{O}_{\mathfrak{p}}$ and $F_{\mathfrak{p}}$ can be obtained by appealing to Proposition 5. Moreover, it thus turns out that $\mathcal{O}_{(\mathfrak{p})}$ has a uniformizer π (an element with the smallest positive valuation in $\mathcal{O}_{(\mathfrak{p})}$) which also behaves as the uniformizer in $\mathcal{O}_{\mathfrak{p}}$.

4.2 Finite Extensions of $\mathbb{Q}_p$

In this section, we briefly discuss some algebraic number theory on $\mathbb{Q}_p$. Let us clarify the notations first. We let L denote a finite extension of $\mathbb{Q}_p$ with $[L : \mathbb{Q}_p] = N$, and let $\mathcal{O}_L$ denote the integral closure of $\mathbb{Z}_p$ in L. For $\alpha \in L$, we denote its minimal polynomial in $\mathbb{Q}_p[x]$ by $m_\alpha(x)$. Thus, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \deg m_\alpha = d$ (say) where $d|N$. Let $\sigma_1, \sigma_2, \cdots, \sigma_N$ be the N distinct $\mathbb{Q}_p$-embeddings of L into a normal closure M of L. The *norm* $N_{L/\mathbb{Q}_p}(\alpha)$ of α is defined to be the determinant of the $\mathbb{Q}_p$-linear transformation given by multiplication by α. Alternatively, one has

$$N_{L/\mathbb{Q}_p}(\alpha) = \prod_{i=1}^{N} \sigma_i(\alpha).$$

We recollect a description of the norm thus defined.

Proposition 6. *Let L, $\mathcal{O}_L$ and α be as above. Then $N_{L/\mathbb{Q}_p}(\alpha) = (-1)^N m_\alpha(0)^{N/d} \in \mathbb{Q}_p$.*

We are primarily interested in giving a p-adic absolute value on L. It turns out that the p-adic absolute value $|\cdot| = |\cdot|_p$ extends in a *unique* way and can be given by

$$|\alpha|_p = |N_{L/\mathbb{Q}_p}(\alpha)|_p^{1/N},$$

and that L is *complete* with respect to these equivalent norms. This is established by using the fundamental theorem on finite dimensional normed vector spaces, namely that if V is a finite dimensional vector space over a valued field (such as $\mathbb{Q}_p$), then all vector space norms on V are equivalent and that V is complete with

respect to this norm. We omit the proof and refer the reader to the treatment given in Gouvea's text. It follows that the valuation $\nu(\alpha)$ is thus given by

$$\nu(\alpha) = -\frac{1}{N}\log_p |N_{L/\mathbb{Q}_p}(\alpha)| = \frac{1}{N}\nu(|N_{L/\mathbb{Q}_p}(\alpha)|).$$

Since, $(\mathbb{Z}, +)$ is the value group of $\mathbb{Q}_p^*$, we deduce that the same for L^* is contained in $\frac{1}{N}\mathbb{Z}$. In fact, the value group of L^* is of the form $\frac{1}{e}\mathbb{Z}$ where $e|N$. The number e is called the *ramification index* of L.

Proposition 7. *The image $\nu(L^*) = (1/e)\mathbb{Z}$ for some positive integer $e|N$.*

Proof. It is clear that $H = \nu(L^*)$ is an additive subgroup of $\mathbb{Q}$ contained in $(1/N)\mathbb{Z}$. Also, $\nu(L^*)$ contains $\mathbb{Z}$ as $\mathbb{Q}_p$ is contained in L^*. Let d/e be an element of H with $\gcd(d, e) = 1$ and e is as large as possible. Note that $e|N$. Now, there are integers u and v such that $ud + ve = 1$. Therefore, we find that $1/e = u(d/e) + v \in H$. Now, observe that NH is a subgroup of $\mathbb{Z}$, and therefore, there is a l such that $NH = l\mathbb{Z}$. It follows that $H = (l/N)\mathbb{Z}$. Thus, there is a $k \in \mathbb{Z}$ such that $1/e = kl/N$. But then $l|N$. Now, $l/N \in H$. Since, $1/e = kl/N \geq 1/(N/l)$, and since e was chosen to be as large as possible, it follows that $k = 1$, and hence, $H = (1/e)\mathbb{Z}$. □

As a consequence, we state a theorem of Coleman which he uses to establish the irreducibility of truncated exponential series.

Theorem 14. *Let $f(x) \in \mathbb{Q}[x]$ and let p be a prime. Consider the Newton polygon $NP_p(f)$ of f with respect to p. If d divides the denominator of slopes of all the edges of $NP_p(f)$, then d divides the degree of any factor g of f in $\mathbb{Q}[x]$.*

We will give a proof of this theorem in last chapter.

Our next goal is to determine the valuation ring of L. In fact, $\mathcal{O}_L$ turns out to be the valuation ring of L. We need a little lemma based on an application of the following version of Hensel's lemma regarding lifting factorization of polynomials from $\mathbb{F}_p[x]$ to $\mathbb{Q}_p[x]$.

Theorem 15. *(Hensel's Lemma, second form) Let $f(x) \in \mathbb{Z}_p[x]$, and suppose that there are polynomials g_1 and h_1 in $\mathbb{Z}_p[x]$ satisfying the following conditions.*

a) *g is monic,*

b) *g_1 and h_1 are relatively prime $\pmod p$, i.e., there are polynomials U and V in $\mathbb{F}_p[x]$ such that $Ug_1 + Vh_1 \equiv 1 \pmod p$, and*

c) *$f \equiv g_1 h_1 \pmod p$.*

Then there are polynomials g and h in $\mathbb{Z}_p[x]$ such that

(i) g *is monic,*

(ii) $g \equiv g_1 \pmod{p}$, $h \equiv h_1 \pmod{p}$, *and*

(iii) $f = gh$.

We use this to prove something really interesting about the monic irreducible polynomials in $\mathbb{Q}_p[x]$.

Lemma 7. *Let $f(x)$ be a monic irreducible polynomial in $\mathbb{Q}_p[x]$. If $f(0) \in \mathbb{Z}_p$, then $f(x) \in \mathbb{Z}_p[x]$.*

Proof. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[x], \quad \text{with} \quad a_0 \in \mathbb{Z}_p.$$

Let $m = \min\{\nu(a_i) : 0 \leq i \leq n-1\}$. Note that $m \leq 0$ (as f is monic). If $m = 0$, then we are done. If $m < 0$, then we work with $g(x) = p^{-m}f(x) = \sum_{j=0}^{n} b_j x^j$ where $b_n = p^{-m}$ and $b_j = p^{-m}a_j$ for $j \in \{0, 1, \cdots, n-1\}$. Note that $\nu(b_j) \geq 0$ for all $0 \leq j \leq n$, $\nu(b_0) > 0$ and $\nu(b_n) > 0$, and that there is at least one j such that $\nu(b_j) = 0$. Let k be the smallest positive integer in $\{1, 2, \cdots, n-1\}$ such that $\nu(b_k) = 0$. Thus, we have

$$\nu(b_j) \begin{cases} > 0 & \text{if} \quad 0 \leq j < k \\ = 0 & \text{if} \quad j = k \\ \geq 0 & \text{if} \quad k+1 \leq j \leq n-1 \\ > 0 & \text{if} \quad j = n. \end{cases}$$

Thus, $\pmod{p}$, g factors as

$$g(x) \equiv (b_n x^{n-k} + \cdots + b_k)x^k \pmod{p}.$$

Since, b_k is a unit, it follows that the two factors appearing above are relatively prime $\pmod{p}$. Now, by appealing to Theorem 15, we deduce that g, and hence, f factors in $\mathbb{Q}_p[x]$, a contradiction. Thus, it follows that $m = 0$, and the proposition is proved. □

Immediately, we have what we are seeking here.

Corollary 4. *The integral closure $\mathcal{O}_L$ of $\mathbb{Z}_p$ in L is the valuation ring of L.*

Proof. Let $\alpha \in L$ be a nonzero element. It suffices to show that $|\alpha| \leq 1$ if and only if $\alpha \in \mathcal{O}_L$. If $\alpha \in \mathcal{O}_L$, then its minimal polynomial m_α over $\mathbb{Q}_p$ belongs to $\mathbb{Z}_p[x]$. Thus, $a = m_\alpha(0) \in \mathbb{Z}_p$. Consequently, we have

$$|\alpha| = |N_{L/\mathbb{Q}_p}(\alpha)|^{1/N} = |a^{N/d}|^{1/N} = |a|^{1/d} \leq 1,$$

where $d = \deg m_\alpha$. Conversely, if $|\alpha| \leq 1$, then following the argument above, we find that $|m_\alpha(0)| = |\alpha|^d \leq 1$. Thus, the minimal polynomial m_α of α which is monic, irreducible and has its constant term in $\mathbb{Z}_p$. By Lemma 7, we deduce that $m_\alpha \in \mathbb{Z}_p[x]$, and consequently, $\alpha \in \mathcal{O}_L$. □

We now describe $\mathcal{O}_L$ which apart from being a valuation ring, is also an extension of $\mathbb{Z}_p$. Most of the valuation theoretic properties follow from our discussions in the previous section.

Proposition 8. *Let L and $\mathcal{O}_L$ be as above. Then we have the following:*

(i) *O_L is integrally closed in L.*

(ii) *$\mathcal{O}_L$ is a free $\mathbb{Z}_p$-module of rank $N = [L : \mathbb{Q}_p]$.*

(iii) *The unique maximal ideal $\mathfrak{p}$ (also called valuation ideal) is generated by a uniformizer π satisfying $|\pi|^e = |p| = 1/p$ (Thus, we have $p\mathcal{O}_L = (\pi^e) = \mathfrak{p}^e$) where e is the ramification index of $L/\mathbb{Q}_p$.*

(iv) *The residue field $\ell = \mathcal{O}_L/\pi\mathcal{O}_L$ is a finite extension of $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ of dimension $f \leq N = [L : \mathbb{Q}_p]$. Thus $|l| = p^f$.*

(v) *$N = [L : \mathbb{Q}_p] = ef$.*

Proof. Part (i) follows from the fact that $\mathcal{O}_L$ is a valuation ring in L.

For part (ii), we let $\{\alpha_1, \alpha_2, \cdots, \alpha_N\}$ be a $\mathbb{Q}_p$-basis of L consisting of elements from $\mathcal{O}_L$ (such a basis exists as for every $y \in L$, there is a $n(y) \in \mathbb{Z}_p$ such that $n(y)y \in \mathcal{O}_L$). Let $\beta \in \mathcal{O}_L$. Then there exist elements $x_i \in \mathbb{Q}_p$ such that

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_N\alpha_N = \beta.$$

Applying σ_i to the above for $i = 1$ to $i = N$, we get N equations of the form and noting that $\sigma_i(x_i) = x_i$, we get

$$x_1\sigma_i(\alpha_1) + x_2\sigma_i(\alpha_2) + \cdots + x_N\sigma_i(\alpha_N) = \sigma_i(\beta) \quad i = 1, 2, \cdots N.$$

Expressing this in terms of matrices, we have $AX = B$ where

$$A = [\sigma_i(\alpha_j)]_{1 \leq i,j \leq N}, X = [x_1 x_2 \cdots x_N]^t \quad \text{and} \quad B = [\sigma_1(\beta)\sigma_2(\beta)\cdots\sigma_N(\beta)]^t.$$

Note that $(\det A)^2$ is the discriminant of the basis $\{\alpha_1, \alpha_2, \cdots, \alpha_N\}$ where $\alpha_i \in \mathcal{O}_L$. Thus, $(\det A)^2 \neq 0$ and belongs to $\mathbb{Z}_p$. Let $\Delta = \det A$. Thus, by Cramer's rule, the unique elements $x_i \in \mathbb{Q}_p$ are given by

$$x_i = \Delta_i/\Delta = \Delta_i\Delta/\Delta^2.$$

where Δ_i is the determinant of the matrix obtained by replacing the i-th column in A by the column B^t. Note that Δ_i, being the discriminant of the N algebraic integers $\{\alpha_1, \cdots, \alpha_{i-1}, \beta, \alpha_{i+1}, \cdots, \alpha_N\}$, is in $\mathbb{Z}_p$ (it may be 0). Thus, the quantity $\Delta^2 x_i$, which is already in $\mathbb{Q}_p$, also happens to be an algebraic integer being a product of two algebraic integers Δ and Δ_i. Therefore, it must be that $\Delta^2 x_i \in \mathbb{Z}_p$ for all $i = 1, 2, \cdots, N$. Consequently, we deduce that $\mathcal{O}_L$ is contained in free $\mathbb{Z}_p$-module of rank N given by

$$\overbrace{\frac{1}{\Delta^2}\mathbb{Z}_p \oplus \frac{1}{\Delta^2}\mathbb{Z}_p \oplus \cdots \oplus \frac{1}{\Delta^2}\mathbb{Z}_p}^{N\text{-times}}.$$

Thus, $\mathcal{O}_L$ is a free $\mathbb{Z}_p$-module of rank $\leq N$. But $\mathcal{O}_L$ contains a free $\mathbb{Z}_p$-module of rank N, namely the $\mathbb{Z}_p$-module

$$\{n_1\alpha_1 + n_2\alpha_2 + \cdots + n_N\alpha_N : n_i \in \mathbb{Z}_p\}.$$

The conclusion of part (ii) follows at once.

Part (iii) follows from the discussion in the previous section and the fact that $1/e$ is the generator (smallest positive element) of the value group of L^*. For part (iv), observe that $\mathbb{Z}_p$ has a natural inclusion inside $\mathcal{O}_L$ as $\mathcal{O}_L \cap \mathbb{Q}_p = \mathbb{Z}_p$. Define the map $i : \mathbb{Z}_p/p\mathbb{Z}_p \to \mathcal{O}_L/\pi\mathcal{O}_L$ by $i(a + p\mathbb{Z}_p) = a + \pi\mathcal{O}_L$. The inclusion

$$p\mathbb{Z}_p \subseteq p\mathcal{O}_L = \pi^e\mathcal{O}_L \subseteq \pi\mathcal{O}_L$$

ensures that the map i is well defined. Also, i is clearly a field homomorphism. Furthermore, if $x + p\mathbb{Z}_p \in \ker i$, then $x \in \pi\mathcal{O}_L$. But this means, $|x| < 1$. Since, $x \in \mathbb{Z}_p$, we may then deduce that $x \in p\mathbb{Z}_p$. Thus, i is injective, thereby proving the first half of part (iv). For the other half, we note that if x_1, x_2, $\cdots$, x_t are linearly dependent over $\mathbb{Q}_p$, i,e,. there exist $a_i \in \mathbb{Q}_p$, not all zero, such that

$$a_1x_1 + a_2x_2 + \cdots + a_tx_t = 0,$$

then by multiplying the last equation by a suitable power of 2, we find that all a_i can be assumed to be in $\mathbb{Z}_p$ with at least one of the a_i, say a_s above is a unit in $\mathbb{Z}_p$. Now, reducing the equation $\pmod{\pi}$, we find that

$$\sum_{i=1}^{t}(a_i + \pi\mathcal{O}_L)(x_i + \pi\mathcal{O}_L) = 0 + \mathcal{O}_L,$$

with (crucially) $a_s + \pi\mathcal{O}_L$, a unit in $\mathcal{O}_L/\pi\mathcal{O}_L$ (being nonzero element of a field). Therefore, linearly dependent sets in $\mathcal{O}_L$ remain linearly dependent over $\mathbb{F}_p$ when reduced $(\mathrm{mod}\ \pi)$. Consequently, we have $\dim_{\mathbb{F}_p}(\mathcal{O}_L/\pi\mathcal{O}_L) \leq \dim_{\mathbb{Q}_p} L$.

For part (v), we use (ii) first to deduce that

$$\mathcal{O}_L/\pi^e\mathcal{O}_L = \mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{Z}_p^N/p\mathbb{Z}_p^N \cong (\mathbb{Z}_p/p\mathbb{Z}_p)^N.$$

Thus, we have $|\mathcal{O}_L/\pi^e\mathcal{O}_L| = p^N$. Next, observe that the map $\phi_i(:\pi^i)/(\pi^{i+1}) \to \mathcal{O}_L/(\pi)$, sending $\pi x + (p^{i+1}) \to x + (\pi)$ sets up an isomorphism for $i = 1, 2, \cdots, e-1$. Thus, each of the quotients $(\pi^i)/(\pi^{i+1})$ is isomorphic to residue field $\ell = \mathcal{O}_L/(\pi)$. Since, $\mathcal{O}_L \supset (\pi) \supset \cdots \supset (\pi^e)$, we have a natural projective sequence

$$\mathcal{O}_L/(\pi^e) \to (\pi)/(\pi^e) \to \cdots (\pi^{e-1})/(\pi^e) \to 0.$$

Set $\mathcal{O}_L = (\pi^0)$. By quotient of quotient isomorphism theorem for modules, one has

$$(\pi^i)/(\pi^e) \Big/ (\pi^{i+1})/(\pi^e) \cong (\pi^i)/(\pi^{i+1}) \cong \ell \quad \text{as} \quad \mathcal{O}_L - \text{modules}$$

for all $i = 1, 2, \cdots, e-1$. By induction on i above, one can show that $|\mathcal{O}_L/(\pi^e)| = |\ell|^e = p^{ef}$. For, at the base step $i = 1$, one has

$$(\pi^{e-1})/(\pi^e) \cong \ell$$

Therefore, one has

$$|(\pi^{e-1})/(\pi^e)| = |\ell|^1.$$

Thus, proceeding inductively, we get at the $i+1$-st step that

$$(\pi^{e-i-1})/(\pi^e) = |\ell||(\pi^{e-i})/(\pi^e)| = |\ell||\ell|^i = |\ell|^{i+1},$$

proving the formula. Comparing the two values obtained for $|\mathcal{O}_L/(\pi^e)|$, we deduce that $N = ef$. □

We next take up the Galois group $\mathrm{Gal}(L/\mathbb{Q}_p)$. In what follows, we assume that $L/\mathbb{Q}_p$ is Galois. We will require some knowledge of the Galois theory of finite extensions of finite fields. We state and prove the main theorem in this context.

Theorem 16. *Let $\urcorner$ be a finite field of cardinality q where q is power of a prime. Let ℓ be a finite extension of $\urcorner$ of degree f. Then $\ell/\urcorner$ is Galois with $\mathrm{Gal}(\ell/\urcorner)$ is the cyclic subgroup of order f generated by the Frobenius automorphism ψ of ℓ given by $\psi(\alpha) = \alpha^q$ for $\alpha \in \ell$.*

Proof. Since ℓ is a $\digamma$-vector space of dimension f, it follows that $|\ell| = p^f$. Note that every $\alpha \in \ell$ satisfies $\alpha^{q^f} = \alpha$. Thus, the polynomial $f(x) = x^{q^f} - x \in \digamma[x]$, being separable, has all its roots in ℓ. Since, any element of ℓ is a root of f, it follows that ℓ is the splitting field of $f(x)$, and hence, $\ell/\digamma$ is Galois. Now consider the Frobenius map ψ given by $\psi(\alpha) = \alpha^q$. Let $q = p^m$. Since, ℓ has characteristic p, it follows that

$$\psi(\alpha+\beta) = (\alpha+\beta)^q = \alpha^q + \beta^q = \psi(\alpha) + \psi(\beta) \quad \text{and} \quad \psi(\alpha\beta) = (\alpha\beta)^q = \alpha^q\beta^q$$

for all α and β in ℓ. Furthermore, $\psi(\alpha) = 0$ implies $\alpha = \alpha^q = 0$. Thus ψ is injective. Since, ℓ is finite, it follows that ψ is onto, and as such, an automorphism. Finally, if $a \in \digamma$, then $\psi(a) = a^q = a$. Therefore, $\psi \in \mathrm{Gal}(\ell/\digamma)$. Now, observe that if ψ^t is identity, then for any $\alpha \in \ell$, one has

$$\alpha = \psi^t(\alpha) = \alpha^{q^t}.$$

In particular, if α is the primitive element of ℓ, then we find that $\alpha^{q^t-1} = 1$. Since, the multiplicative order of α is $q^f - 1$, we deduce that $t \geq f$. Thus, 1, ψ, ψ^2, $\cdots$, ψ^{f-1} are all distinct elements of $\mathrm{Gal}(\ell/\digamma)$, and $|\mathrm{Gal}(\ell/\digamma)| = f$, the result follows. □

We get back to $\mathrm{Gal}(L/\mathbb{Q}_p)$. The key result in this direction is that there is a canonical surjective homomorphism $\phi : \mathrm{Gal}(L/\mathbb{Q}_p) \to \mathrm{Gal}(\ell/\mathbb{F}_p)$ where ℓ and $\mathbb{F}_p$ are the respective residue fields $\mathcal{O}_L/p\mathcal{O}_L$ and $\mathbb{Z}_p/p\mathbb{Z}_p$. For a $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$, define $\overline{\sigma} : \ell \to \ell$ as

$$\overline{\sigma}(\alpha + p\mathcal{O}_L) = \sigma(\alpha) + p\mathcal{O}_L.$$

Since $\sigma(p\mathcal{O}_L)$ is a prime ideal and $p\mathcal{O}_L$ is the only prime ideal in $\mathcal{O}_L$, it follows that $\sigma(p\mathcal{O}_L) = p\mathcal{O}_L$. Consequently, $\overline{\sigma}$ is well defined. It is easy to see that $\overline{\sigma}$ is a field homomorphism. Again from our discussion above and the fact σ is an automorphism it follows that

$$\sigma(\alpha - \beta) \in p\mathcal{O}_L \quad \Longrightarrow \quad \alpha - \beta \in p\mathcal{O}_L.$$

Thus, $\overline{\sigma}$ is an automorphism of ℓ. Finally, if $\bar{a} = a + p\mathbb{Z}_p \in \mathbb{F}_p$, i.e., $a \in \mathbb{Z}_p$, we recall that $\bar{a}$ sits inside ℓ as $a + p\mathcal{O}_L$. Since σ fixes a, we thus have

$$\overline{\sigma}(a + p\mathcal{O}_L) = \sigma(a) + p\mathcal{O}_L = a + p\mathcal{O}_L.$$

Thus, we obtain the promised map $\phi : \mathrm{Gal}(L/\mathbb{Q}_p) \to \mathrm{Gal}(\ell/\mathbb{F}_p)$ by defining $\phi(\sigma) = \overline{\sigma}$. It is easy to see that ϕ is in fact a group homomorphism.

Proposition 9. *The map ϕ defined above is surjective.*

Proof. Let a be a primitive element of ℓ, i.e., $\ell^* =< a >$, and let α be its pre-image in $\mathcal{O}_L$ under the canonical surjective map $\mathcal{O}_L \to \mathcal{O}_L/p\mathcal{O}_L$. Let

$$f(x) = \prod_{\rho \in \mathrm{Gal}(\ell/\mathbb{Q}_p)} (x - \rho(a)) \in \mathbb{F}_p[x]$$

be the minimal polynomial of a over $\mathbb{F}_p$. Now, consider the set $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)\}$. This set is partitioned into equivalence classes under 'is equal to' relation. We pick a representative from each of these classes and let G' denote the set of these representatives and define

$$g(x) = \prod_{\sigma \in G'} (x - \sigma(\alpha)).$$

It follows that g is the minimal polynomial of α over $\mathbb{Q}_p$. Since $\alpha \in \mathcal{O}_L$, we have that $g \in \mathbb{Z}_p[x]$. Now, consider $\bar{g} = g \pmod{p} \in \mathbb{F}_p[x]$. Now, we note that

$$\bar{g}(x) = \prod_{\sigma \in G'} (x - \sigma(\alpha) + p\mathcal{O}_L) = \prod_{\sigma \in G'} (x - \overline{\sigma}(\alpha + p\mathcal{O}_L)) \prod_{\sigma \in G'} (x - \overline{\sigma}(a)).$$

Thus, $\bar{g}(a) = 0$, and consequently, $f | \bar{g}$ in $\mathbb{F}_p[x]$. Let $\rho \in \mathrm{Gal}(\ell/\mathbb{F}_p)$, then it thus follows that there is a $\sigma \in G'$ such that $\rho(a) = \overline{\sigma}(a)$. Since, a is a primitive element of ℓ^*, hence, ρ and σ agree on ℓ, and hence, are equal. Consequently, one has $\rho = \overline{\sigma} = \phi(\sigma)$ where $\sigma \in G' \subseteq \mathrm{Gal}(L/\mathbb{Q}_p)$. This finishes the proof of the proposition. □

The kernel of the map ϕ which is thus a normal subgroup of $\mathrm{Gal}(L/\mathbb{Q}_p)$ is called the *inertia group* of L and denoted by $I(L/\mathbb{Q}_p)$. Thus,

$$\mathrm{Gal}(L/\mathbb{Q}_p)/I(L/\mathbb{Q}_p) \cong \mathrm{Gal}(\ell/\mathbb{F}_p).$$

From $|\mathrm{Gal}(L/\mathbb{Q}_p)| = [L : \mathbb{Q}_p] = ef$, it therefore follows that $|I(L/\mathbb{Q}_p)| = e$. If $e = 1$, then

$$\mathrm{Gal}(L/\mathbb{Q}_p) \cong \mathrm{Gal}(\ell/\mathbb{F}_p),$$

and hence, cyclic. In this case, we say that $L/\mathbb{Q}_p$ is *unramified*.

4.3 Local Global Galois Principal

In this section, our main goal is to find a connection between the Galois group of a number field and that of its localization. This study, along with the theory of Newton polygons, give us substantial amount of information regarding the Galois groups of number fields in many interesting cases.

Let $K/\mathbb{Q}$ be a Galois extension with $[K : \mathbb{Q}] = n$. Let $\mathcal{O}_K$ be its ring of integers. Let p be a prime in $\mathbb{Z}$, and let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ be all the primes in $\mathcal{O}_K$ lying over p, i.e., $\mathfrak{p}_i \cap \mathbb{Q} = p\mathbb{Z}$. In fact, these are also the primes appearing in the prime factorization of p. Since $K/\mathbb{Q}$ is Galois, its Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r\}$, and hence, their *ramification index* are the same, say e. Consequently, one has

$$p\mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r)^e.$$

Let $\urcorner = \mathcal{O}_K/p\mathcal{O}_K$ denote the *residue field*. The residue field $\urcorner$ is a finite extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and its degree f is called the *residual degree*. The numbers r, e, f and n are related by the formula $n = ref$. Let $\mathfrak{p} \in \{\mathfrak{p}_i : 1 \leq i \leq r\}$. We will be particularly interested in the stabilizer of $\mathfrak{p}$ under the action of $\mathrm{Gal}(K/\mathbb{Q})$, called the *decomposition group* of $\mathfrak{p}/p$ and denoted by $D(\mathfrak{p}/p)$, i.e.,

$$D(\mathfrak{p}/p) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Thus, the decomposition groups of different $\mathfrak{p}_i$ are conjugates of each other.

Note that $\mathcal{O}_K$ is a Dedekind domain, and hence is Noetherian. Like was done in a previous section, we localize $\mathcal{O}_K$ at $\mathfrak{p}$ to obtain $\mathcal{O}_{K,(\mathfrak{p})}$ whose field of fractions is still K. Now we give a valuation to $\mathcal{O}_{K,(\mathfrak{p})}$, extend it to K and then complete K with respect to the norm induced by the valuation. Let $K_\mathfrak{p}$ be completion of K and let $\mathcal{O}_\mathfrak{p}$ denote its valuation ring. Note that in $\mathcal{O}_{K,(\mathfrak{p})}$, all other $\mathfrak{p}_i$ except $\mathfrak{p}$ be comes unital. Thus, in $\mathcal{O}_{K,(\mathfrak{p})}$, one has

$$p\mathcal{O}_{K,(\mathfrak{p})} = \mathfrak{p}^e\mathcal{O}_{K,(\mathfrak{p})}.$$

Thus, if π is the uniformizer of $\mathcal{O}_{K,(\mathfrak{p})}$, then we have $p = u\pi^e$ where u is a unit in $\mathcal{O}_{K,(\mathfrak{p})}$. By our construction, the value group to be assigned to $\mathcal{O}_{K,(\mathfrak{p})}$ is $r\mathbb{Z}$ where $r \in \mathbb{Q}$. Note that $r = \nu(\pi)$. We take $r = 1/e$ and take $|x| = p^{-\nu(x)}$ for all $x \in \mathcal{O}_{K,(\mathfrak{p})}$). Therefore, $|\pi| = p^{-1/e}$, and consequently, $|p| = p^{-1}$. Thus, the norm $|\cdot|$ thus assigned to $\mathcal{O}_{K,\mathfrak{p}}$ coincides with the usual p-adic norm on $\mathbb{Q}_p$. Consequently, we have

$$\mathbb{Q}_p = \text{completion of } \mathbb{Q} \text{ w.r.t. } |\cdot| \subseteq \text{completion of } K \text{ w.r.t. } |\cdot| = K_\mathfrak{p}.$$

Since, the p-adic absolute value extends uniquely to an extension of $\mathbb{Q}_p$, we deduce that $|\cdot|$ is the unique extension in this case. It further follows that the ramification index of $K_\mathfrak{p}/\mathbb{Q}_p$ is indeed e, the same as that of $\mathfrak{p}/p$. Furthermore, from the isomorphisms

$$\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}, \quad \text{and} \quad \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z},$$

it follows that the residual degree of $\mathfrak{p}\mathcal{O}_\mathfrak{p}/p$ is is equal to that of $\mathfrak{p}/p$ which is taken to be f. Therefore, we find that $K_\mathfrak{p}/\mathbb{Q}_p$ is a finite extension of degree ef. Our final task will be establish that $K_\mathfrak{p}/\mathbb{Q}_p$ is in fact, a Galois extension. This is achieved in the proposition below. But, we will need a result on decomposition group $D(\mathfrak{p}/p)$ which can be proved in an exact similar manner as in Proposition 9. The result states that there is a surjective group homomorphism

$$D(\mathfrak{p}/p) \to \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}).$$

It now follows that $|D(\mathfrak{p}/p)| = ef$. We use this fact along with the proposition below to show that $K_\mathfrak{p}/\mathbb{Q}_p$ is Galois.

Proposition 10. *We have* $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \cong D(\mathfrak{p}/p)$.

Proof. We begin by showing that there is a canonical homomorphism $\eta : \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \to \mathrm{Gal}(K/\mathbb{Q})$ whose image is contained in the decomposition group $D(\mathfrak{p}/p)$. Let $\sigma \in \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ and $\alpha \in K$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α. Since, σ is identity on $\mathbb{Q}_p$, and hence on $\mathbb{Q}$, one has that $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$. Thus, $\sigma(\alpha)$ is a root of $f(x)$ and since, $K/\mathbb{Q}$ is Galois and $K \hookrightarrow K_\mathfrak{p}$, we deduce that $\sigma(\alpha) \in K$. Thus, the restriction $\sigma\big|_K$ of σ is in $\mathrm{Gal}(K/\mathbb{Q})$. We thus define $\eta(\sigma) = \sigma\big|_K$. Next, we observe that

$$\sigma(\mathfrak{p}) = \sigma(p\mathcal{O}_\mathfrak{p} \cap K) = \sigma(p\mathcal{O}_\mathfrak{p}) \cap \sigma(K) = \sigma(p\mathcal{O}_\mathfrak{p}) \cap K.$$

Since, $\sigma(p\mathcal{O}_\mathfrak{p})$ is a prime ideal of $\mathcal{O}_\mathfrak{p}$, and we know that $p\mathcal{O}_\mathfrak{p}$ is the only prime ideal in the local ring $\mathcal{O}_\mathfrak{p}$, we deduce that $\sigma(p\mathcal{O}_\mathfrak{p}) = p\mathcal{O}_\mathfrak{p}$. Consequently, we find that $\sigma(\mathfrak{p}) = \mathfrak{p}$, and as such, $\eta(\sigma) \in D(\mathfrak{p}/p)$. Conversely, suppose $\rho \in D(\mathfrak{p}/p)$. We would like to extend ρ to a $\mathbb{Q}_p$-automorphism of $K_\mathfrak{p}$. Let $x \in K_\mathfrak{p}$, then there exists a sequence $\{x_n\} \in K$ such that $x = \lim_n x_n$. We define $\gamma(\rho) : K_\mathfrak{p} \to K_\mathfrak{p}$ as

$$\gamma(\rho)(x) = \lim_{n\to\infty} \rho(x_n).$$

Since ρ is an isometry on L, $\gamma(\rho)$ is well defined. It is also easy to see that $\gamma(\rho)$ is a field homomorphism. Moreover, from the isometric property of ρ. we find that

$$\gamma(\rho)(x) = 0 \iff \lim_{n\to\infty} \rho(x_n) = 0 \iff \lim_{n\to\infty} x_n = \iff x = 0.$$

Thus, $\gamma(\rho)$ is an automorphism of $K_\mathfrak{p}$. Lastly, we have that if $a \in \mathbb{Q}_p$, then $a = \lim_n a_n$ where $a_n = a$ for all $n \geq 1$, so that one has

$$\gamma(\rho)(a) = \lim_{n\to\infty} a_n = \lim_{n\to\infty} a = a.$$

Thus $\gamma(\rho)$ is indeed an element of $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$. We note that the restriction of $\gamma(\rho)$ to K is simply, ρ, i.e., we have that $\eta\gamma(\rho) = \rho$ for any $\rho \in D(\mathfrak{p}/p)$. This

means that $\eta\gamma : D(\mathfrak{p}/p) \to D(\mathfrak{p}/p)$ is the identity map. It follows that η is onto and γ is $1-1$. This in turn implies that η is $1-1$ and γ is onto. Thus, η and γ are the respective inverses of each other, and consequently we have the desired result. $\square$

Thus, we have following local global Galois principle.

Corollary 5. *The Galois group* $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ *can be realized as a subgroup of* $\mathrm{Gal}(K/\mathbb{Q})$.

Chapter 5

Galois group of $L_n^{(\alpha)}(x)$ where $\alpha \in \mathbb{N} \cup \{0\}$

In this chapter, we investigate the Galois group associated with GLP $L_n^{(\alpha)}(x)$ over $\mathbb{Q}$ and also find when the determinant of this polynomial be square, where

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \binom{n+\alpha}{n-j} \frac{(-x)^j}{j!}.$$

We restrict ourselves to the case that α be an integer. In the late 1920's and early 1930's, I.Schur established the irreducibility of these polynomials in the case $\alpha \in \{0, 1, -n-1\}$ and then obtain the following results associated with their Galois groups over the rationals;

(1) $L_n^{(0)}(x)$ has Galois group S_n for each n.

(2) $L_n^{(1)}(x)$ has Galois group S_n for each even n with $n+1$ is not square.

(3) $L_n^{(1)}(x)$ has Galois group A_n for each odd n each even n with $n+1$ square.

(4) $L_n^{(-n-1)}(x)$ has Galois group S_n for each $n \not\equiv (\mod 4)$.

(5) $L_n^{(-n-1)}(x)$ has Galois group A_n for each $n \equiv (\mod 4)$.

He also gave the remarkable formula for the discriminant $Disc(n, \alpha)$ of the monic integral polynomials $\mathcal{L}_n^{(\alpha)}(x) = (-1)^n n! L_n^{(\alpha)}(x)$ namely

$$Disc(n, \alpha) = \prod_{j=2}^{n} j^j (\alpha + j)^{j-1}.$$

5.1 A Criteria For Having Large Galois Group

In this section, we will consider an application of Corollary 5 from the previous chapter to computing Galois groups of polynomials via the use of Newton polygons. Let $f(x) \in \mathbb{Q}[x]$ be irreducible, p be a prime and let $NP_p(f)$ denote the Newton polygon of f with respect to the prime p. Let $\mathcal{V} = \{(x_i, y_i) : i = 0, 1, \cdots l\}$ be the vertices of $NP_p(f)$ and $m_i = (y_i - y_{i-1})/(x_i - x_{i-1})$ be the slope of the i-th edge for $i \in \{1, 2, \cdots, l\}$. Lastly, we let n_i denote the positive integer $x_i - x_{i-1}$ where $i \in \{1, 2, \cdots, l\}$. The fundamental theorem of Newton polygons states that

Theorem 17. *Let the notations be as above. Then there exist l polynomials f_1, f_2, $\cdots$, f_l in $\mathbb{Q}_p[x]$ such that*

(i) $f = f_1 f_2 \cdots f_l$ *in* $\mathbb{Q}_p[x]$,

(ii) $\deg f_i = n_i$, *and*

(iii) if β is a root of f_i in $\overline{\mathbb{Q}_p}$, then the p-adic valuation (unique extension of the usual valuation on $\mathbb{Q}$) of β is m_i.

If $K/\mathbb{Q}$ is the splitting field of f and. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ lying over p. Let $K_\mathfrak{p}$ be the completion of K under the p-adic norm. We have seen that $K_\mathfrak{p}/\mathbb{Q}_p$ is Galois extension of degree ef where e and f are respectively the ramification index and residual degree of $\mathfrak{p}/p$. Let α be a root of f in $\overline{\mathbb{Q}_p}$. Let $g \in \mathbb{Q}_p[x]$ be its minimal polynomial. Now, α is also a root of f_i for some $i \in \{1, 2, \cdots, l\}$. Thus, $\nu(\alpha) = m_i$. On the other hand, we also have that $\nu(\alpha) \in (1/e)\mathbb{Z}$. Let d_i be the denominator of m_i. Then it follows that $d_i | e$. But e divides $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$ which in turn divides $[K_\mathfrak{p} : \mathbb{Q}_p] = |\operatorname{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)|$. Therefore, d_i divides the order of the Galois group $\operatorname{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$.

Definition 4. *(Newton Index) Let $\mathcal{N}_p(f)$ be defined to be the* lcm *of the denominators of slopes m_i of $NP_p(f)$. The* Newton index *$\mathcal{N}(f)$ of f is defined as*

$$\operatorname{lcm}_{p-prime}(\mathcal{N}_p(f)).$$

Since, $m_i = 1$ for all but finitely many primes p, we can see that $\mathcal{N}(f)$ is well defined. Here is the main theorem on the Newton index.

Theorem 18. *Let $f \in \mathbb{Q}[x]$ be irreducible of degree n. Let $K/\mathbb{Q}$ be the splitting field of f. Then $\mathcal{N}(f)$ divides $|\operatorname{Gal}(K/\mathbb{Q})|$. Moreover, if there is a prime divisor $l \in (n-2, n/2)$ of $\mathcal{N}(f)$, then $\operatorname{Gal}(K/\mathbb{Q})$ contains A_n, the alternating group on n letters (i.e., as large as possible).*

Proof. Let d be a divisor of $\mathcal{N}(f)$, then by definition, d divides the denominator of some slope of $NP_p(f)$ for some prime p. From the discussion preceding the theorem, we then find that d divides $|\operatorname{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)|$, which by Corollary 5, divides $|\operatorname{Gal}(K/\mathbb{Q})|$. Thus, d divides $|\operatorname{Gal}(K/\mathbb{Q})|$, proving the first half of the theorem. For the second part, we note that if $d = l$ is a prime in the interval $(n-2, n/2)$, then l dividing $|\operatorname{Gal}(K/\mathbb{Q})|$ implies that $\operatorname{Gal}(K/\mathbb{Q})$ contains a l-cycle. It now follows from Jordan's criteria that $\operatorname{Gal}(K/\mathbb{Q})$ contains A_n. □

Now we will state the main result of this section.

Theorem 19. *Suppose α is a fixed non negative integer. Then for all but finitely many integers n , the Galois group of $L_n^{\alpha}(x)$ is A_n if Δ_n^{α} is square and S_n otherwise.*

To prove this theorem , we mainly use the following lemma.

Lemma 8. *Suppose a prime $p \in (n/2, n-2)$ and $f(x) = \sum_{j=0}^{n} \binom{n}{j} c_j\, x^j \in \mathbb{Q}[x]$ is an irreducible polynomial of degree n over $\mathbb{Q}$ with p-integral coefficients , i.e., $\nu_p(c_j) \geq 0$ for $j = 0, 1, \cdots, n$. Suppose further that*

(i) $\nu_p(c_0) = 1$,

(ii) $\nu_p(c_j) \geq \nu_p(c_0)$ *for* $1 \leq j \leq n-p$,

(iii) $\nu_p(c_p) = 0$.

Then p divides the order of the Galois group of f over $\mathbb{Q}$. Indeed , this Galois group is A_n if $disc(f) \in \mathbb{Q}^{*2}$ and S_n otherwise.

Proof. Clearly, $\binom{n}{j}$ is divisible by p if and only if $n-p+1 \leq j \leq p-1$. Then given assumption guarantees that $(0, \nu_p(c_0))$ and $(p, 0)$ are the first two corners of $NP_p(f)$. This implies that the slope of the left most edge is $\frac{-\nu_p(c_0)}{p}$. Then from the first condition, it follows that $p \mid \mathcal{N}_f$. Then using the theorem 18, we get the result. □

Remark 1. *One can easily show that the Lemma 8 holds for $p \in (1+n/2, n-2)$ if we replace i) with i') $1 \leq \nu_p(c_0) \leq p/(2p-n-1)$.*

Now we are ready to prove the main theorem of this chapter.
Proof of theorem 19:

Let us take α be a positive integer. Let

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)!}{(j+\alpha)!(n-j)!} \frac{(-x)^j}{j!}$$

and

$$\mathcal{L}_n^{(\alpha)}(x) = (-1)^n n! L_n^{(\alpha)}(x)$$
$$= \sum_{j=0}^{n} (-1)^{n+j} \binom{n}{j} (n+\alpha)\cdot(n+\alpha-1)\cdots(j+1+\alpha)\, x^j.$$

We want to work with the normalized (monic, integral) polynomial

$$f(x) = \sum_{j=0}^{n} \binom{n}{j} (n+\alpha)\cdot(n+\alpha-1)\cdots(j+1+\alpha)\, x^j.$$

We wish to apply Lemma 8 to it, so we let

$$c_j = \prod_{k=j+1}^{n} (k+\alpha), \quad 0 \le j \le n. \tag{5.1}$$

and seek a appropriate prime p, i.e., one satisfying the condition of Lemma. By suitably strong form of Dirichlet's theorem on primes in arithmetic progression, there exist an effective constant $D(\alpha)$ such that if $x \ge D(\alpha)$ and $h(x) \ge \frac{x}{2\log^2(x)}$, the interval $[x-h, x]$ contains a prime. Taking $x = n-3 \ge D(\alpha)$, we find that for some integer $l \in [1, n], p = l+\alpha$ is a prime satisfying

$$\frac{n+1+\alpha}{2} \le p \le n-3 \tag{5.2}$$

as long as

$$\frac{n-3}{n2\log^2(n-3)} + \frac{3}{n} + \frac{1+\alpha}{2n} \le 1/2 \tag{5.3}$$

i.e.,

$$\frac{n-3}{2\log^2(n-3)} + 3 + \frac{1+\alpha}{2} \le n/2.$$

Which clearly holds for all n large enough with respect to α. Let us now fix a prime $p = l+\alpha$ satisfying equation 5.2 . Since, we have $(n+1+\alpha)/2 > n/2$. It is obvious because $1+\alpha > 0$. Then this implies that

$$n/2 < (n+1+\alpha)/2 \le p \le n-3 < n-2.$$

So, our c_j are integral. This implies that $f(x)$ is p-integral for every prime p.

Since $j \in [0, n]$, then there exist a prime in $[j+1+\alpha, n+\alpha]$ such that p divides $c_j = (j+1+\alpha)\cdots(n+\alpha)$. Since , we take $p = l+\alpha$. Hence

$$p/c_j \quad \forall j \in \{0, 1, \cdots l-1\}$$

Again from equation 5.2

$$p \geq (n+1+\alpha)/2$$

i.e.,

$$2p \geq (n+1+\alpha)$$

This implies that p exactly divides c_j i.e., $\nu_p(c_j) = 1 \quad \forall j \in \{0, 1, \cdots, l-1\}$
Since , we already take $p = l + \alpha$, this implies that $p \nmid c_j \quad \forall j \in l, \cdots, n$ i.e., $\nu_p(c_j) = 0$ for $l \leq j \leq n$.

Since, α is not a negative integer and $p = n + \alpha$, this implies $p > l - 1$ and

$$2p \geq n+1+\alpha \Rightarrow l+2p \geq n+1+l+\alpha = n+1+p \Rightarrow l+p \geq n+1 \Rightarrow n-p < l,$$

i.e., condition ii) and iii) of Lemma 8 hold. In chapter 3, we already shown that there is an effectively computable constant n_0 dependent on α such that $f(x)$ is irreducible for $n \geq n_0$. Thus, all the conditions of Lemma 8 hold, and the proof of the theorem is complete.

The next corollary can be viewed as improvements of the above Hajir's results. (see [6]).

Corollary 6. *Fix a nonnegative integer $\alpha \notin \{1, 3, 5\}$. Then for all but finitely many positive integers n, the Galois group associated with $L_n^{(\alpha)}(x)$ over the rationals is S_n.*

Chapter 6

Irreducibilty of $L_n^{(\alpha)}(x)$ where $\alpha \in \mathbb{Z}^-$

6.1 Reducibility of $L_n^{(-\alpha)}(x)$ for all integers $\alpha \in [1, n]$

Let $\alpha \in [1, n]$, then $L_n^{(-\alpha)}(x) \in \mathbb{Z}[x]$ defined as

$$L_n^{(-\alpha)}(x) = \sum_{j=0}^{n} \frac{(n-\alpha)\cdot(n-\alpha-1)\cdot(n-\alpha-2)\cdots(j+1-\alpha)}{(n-j)!j!}(-x)^j$$

i.e.,

$$L_n^{(-\alpha)}(x) = \sum_{j=0}^{n} \binom{n-\alpha}{j-\alpha}\frac{(-x)^j}{j!}.$$

We know that

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \binom{n+\alpha}{j+\alpha}\frac{(-x)^j}{j!}.$$

First we show that $L_n^{(-\alpha)}(x) =$ is reducible for $\alpha \in [1, n]$. Now,

$$L_{n-\alpha}^{(\alpha)}(x) = \sum_{j=0}^{n-\alpha} \binom{n}{j+\alpha}\frac{(-x)^j}{j!}.$$

Now, we deduce that

$$(-x)^{(\alpha)}(n-\alpha)!L_{n-\alpha}^{(\alpha)}(x)$$

$$= \sum_{j=0}^{n-\alpha} \binom{n}{j+\alpha} (n-\alpha)! \frac{(-x)^{(j+\alpha)}}{j!}$$

$$= \sum_{j=0}^{n-\alpha} \frac{(n-\alpha)!\, n!}{(n-j-\alpha)!\, (j+\alpha)!} \frac{(-x)^{(j+\alpha)}}{j!}$$

$$= \sum_{i=\alpha}^{n} \frac{(n-\alpha)!\, n!}{(n-i)!\, (i)!} \frac{(-x)^{(i)}}{(i-\alpha)!} \text{ (replacing } j \text{ by } i-\alpha)$$

$$= n! \sum_{i=\alpha}^{n} \frac{(n-\alpha)(n-\alpha-1)\cdots(i-\alpha+1)}{(n-i)!} \frac{(-x)^{(i)}}{(i)!}$$

$$= n! \cdot \sum_{i=0}^{n} \frac{\{(n-\alpha)(n-\alpha-1)\cdots(i-\alpha+1)\}}{(n-i)!} \frac{(-x)^{(i)}}{(i)!}$$

(since if we put the value $i = 0, 1, \cdots, \alpha-1$ then the quantity in the above $\{\}$ be 0)

$$= n! \sum_{j=0}^{n} \binom{n-\alpha}{j-\alpha} \frac{(-x)^j}{j!}$$

$$= n! L_n^{(-\alpha)}(x).$$

Therefore, we get

$$n! L_n^{(-\alpha)}(x) = (-x)^{(\alpha)}(n-\alpha)! L_{n-\alpha}^{(\alpha)}(x).$$

From the above equation, it is clearly shows that $L_n^{(-\alpha)}(x)$ is reducible for all integers $\alpha \in [1, n]$.

6.2 Irreducibilty of $L_n^{(\alpha)}(x)$ where α is a negative integers and $\alpha < -n$

In this section, we will discuss about irreducibility of $L_n^{(\alpha)}(x)$, where α is a negative integer, and $\alpha < -n$. Now, we can replace the parameter α by a parameter r via the translation $\alpha = -1-n-r$, and consider instead

$$L_n^{<r>}(x) = L_n^{(-1-n-r)}(x) = \sum_{j=0}^{n} \binom{n-j+r}{n-j} \frac{(x)^j}{j!}. \tag{6.1}$$

It is also useful to note that

$$\mathcal{L}_n^{<r>}(x) = n!L_n^{<r>}(x) = \sum_{j=0}^{n} \binom{n}{j}(r+1)\cdot(r+2)\cdots(r+n-j)x^j \qquad (6.2)$$

is monic and has a positive integer coefficients as r is a non negative integer. If $r = 0$, then let us say as

$$E_n(x) := L_n^{<0>}(x) = \sum_{j=0}^{n} \frac{x^j}{j!}, \qquad (6.3)$$

and if $r = n$ then we define

$$z_n(x) := \mathcal{L}_n^{<n>}(x) = \sum_{j=0}^{n} \frac{(2n-j)!}{j!(n-j)!}x^j. \qquad (6.4)$$

In (see[18]), we find the following.

Conjecture 1. *For integers $r, n \geq 0$, $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$.*

In the same paper (see[18]), Hajir settles the following.

Theorem 20. *For a fixed integer $r \geq 0$, all but finitely many $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$.*

6.2.1 Irreducibility criteria

Take a prime p and $z \in \mathbb{Q}^*(= \mathbb{Q}\backslash\{0\})$, we write $\nu_p(z) = u$ where $z = p^u m/n$ with integers m and n not divisible by p. It is convenient to put that $\nu_p(0) = \infty$. We use two results which follow from the main theorem of Newton polygons (theorem 21 stated below); these are state below as corollary 7 and Lemma 13. We review the definition of Newton Polygons below.

Definition 5. *The $p-$Newton Polygon $NP_p(f)$ of a polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Q}[x]$ is the lower convex hull of the set of points*

$$S_p(f) = \{(j, \nu_p(a_j)); \quad 0 \leq j \leq n\}.$$

It is the highest polygonal line passing on or below the points in $S_p(f)$. The vertices $(x_0, y_0), (x_1, y_1), \cdots, (x_v, y_v)$, i.e., the points where the slope of Newton Polygon changes (including the rightmost and leftmost points) are called the corners $NP_p(f)$; their x co-ordinates ($0 = x_0 < x_1 < \cdots < x_v = n$) are the breaks of $NP_p(f)$. For the i-th edge , joining (x_{i-1}, y_{i-1}) to (x_i, y_i), we put $m_i = \frac{y_i - y_{i-1}}{x_i - x_{i-1}}$ and is called the i-th slope of $NP_p(f)$.

The main theorem of Newton polygons is stated below.

Theorem 21. *Let* $(x_0, y_0), (x_1, y_1),$
$\cdots (x_r, y_r)$*, denote the successive vertices of* $NP_p(f)$*. Then there exist a polynomial* $f_1, f_2, \cdots f_r$ *in* $\mathbb{Q}_p[x]$ *such that*

(1) $f(x) = f_1(x)f_2(x)\cdots f_r(x)$

(2) for $i = 1 \cdots r$*, the degree of* f_i *is* $x_i - x_{i-1}$

(3) for $i = 1 \cdots r$*, and* α_i *any root of* f_i *in* $\mathbb{Q}_p$ *. We have* $\nu_p(\alpha_i) = -m_i$*.*

The main irreducibility criteria in this case is due to Coleman (see[9]).

Corollary 7. *(Coleman) Suppose* $f \in \mathbb{Q}[x]$ *and* p *is a prime. If an integer* d *divides the denominator (lower terms) of every slope of* $NP_p(f)$*, then* d *divides the degree of each factor* $g \in \mathbb{Q}[x]$ *of* $f(x)$*.*

Proof. Note that a factor $f(x)$ of degree k in $\mathbb{Q}[x]$ induces a factor of degree k in $\mathbb{Q}_p[x]$, and since, every polynomial in factors into irreducible factors in $\mathbb{Q}_p[x]$, it suffices to prove the theorem for $\mathbb{Q}_p$-factors of f. Let g be an irreducible factor of f in $\mathbb{Q}_p$, and let α be a root of g in some normal closure of $\mathbb{Q}_p$. By the fundamental theorem of Newton polygons (see Theorem 17 below), $\nu_p(\alpha)$ is equal to the slope of some edge of $NP_p(f)$. By the hypothesis of the theorem, d divides the denominator of $\nu_p(\alpha)$. On the other hand, by the last proposition, $\nu_p(\alpha)$ also belongs to $(1/e)\mathbb{Z}$ where e divides $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \deg g$. It follows that $d|e$, and hence, $d|\deg g$. □

We have following two lemmas stated below.

Lemma 9. *Let* m *be a non negative integer, and* p *is a prime. If we write* m *in the base* p *as*

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_t p^t, \quad 0 \leq a_i \leq p - 1.$$

Then

$$\nu_p(m!) = \frac{m - \sigma_p(m)}{p - 1},$$

where $\sigma_p(m) = a_0 + a_1 + a_2 + \cdots + a_t$*.*

Lemma 10. *Let* m, r *be non negative integers and* p *is a prime. Let* $b = \binom{m+r}{r}$*, where* m, r *are non negative integers. For any prime* $p, \nu_p(b)$ *is the number of carries in the base* p *addition of* m *and* r*.*

Proof. Now

$$\begin{aligned}\nu_p(b) &= \nu_p\left(\binom{m+r}{r}\right)\\ &= \nu_p\Big((m+r)! \mid (m!r!)\Big)\\ &= \nu_p((m+r)!) - \nu_p(m!) - \nu_p(r!)\\ &= \frac{\sigma_p(m)+\sigma_p(r)-\sigma_p(m+r)}{p-1} \qquad \text{(by lemma (9)).}\end{aligned}$$

The latter expression is precisely the number of carries in the base p addition of m and r. □

Let us take a positive integer n and a prime p. We will define $s+1$ non negative integers $0 = k_0 < k_1 < \cdots < k_s = n$ (where s is the number of nonzero p-adic digits of n) called the pivotal indices associated to (n, p). Write n in the base p, labeling only the non zero digits

$$n = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_s p^{e_s}, \tag{6.5}$$

where $0 < b_1, b_2, \cdots, b_s < p$, and $e_1 > e_2 > \cdots > e_s \geq 0$.
Now, let $k_0 = 0$ and $k_s = n$, we define

$$k_i = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_i p^{e_i} \quad i = 0, 1, 2, \cdots, s. \tag{6.6}$$

The above partial sums are the pivotal indices associated to (n, p). This definition is motivated by coleman's calculation of $NP_p(E_n)$. We will discuss a fundamental fact about the GLP $L_n^{<r>}(x)$ for $r \geq 0$ that the p Newton polygon lies on or above $NP_p(E_n)$. Now, we discuss some more terminology.

Definition 6. *Let p be a prime number and consider a polynomial $f(x) = \sum_{j=0}^{n} a_j \frac{x^j}{j!} \in \mathbb{Q}[x]$. We say that f is p-Hurtwitz integral if $\nu_p(a_j) \geq 0$ for $j = 0, \cdots, n$. We say it is Hurtwitz integral if it is p-Hurtwitz integral for all primes p i.e., if the Hurtwitz co-efficients $a_j \in \mathbb{Z}$ for all $j = 0, \cdots, n$. We say f is $p-$Coleman if f is p-Hurtwitz integral and $\nu_p(a_j) = 0$ for $j = k_i, 0 \leq i \leq s$ where k_i is defined in (6.6).*

We now prove the earlier stated fact about p-Coleman polynomials.

Lemma 11. *If $f \in \mathbb{Q}(x)$ is p-Coleman integral of degree n, then*

(1) $NP_p(f) = NP_p(E_n)$;

(2) the breaks of $NP_p(f)$ are precisely the pivotal indices associated to(n,p);

(3) the slopes of $NP_p(f)$ all have denominator divisible by $p^{\nu_p(n)}$.

Proof. Part-(1): Here

$$f(x) = \sum_{j=0}^{n} a_j \frac{x^j}{j!},$$

and

$$E_n(x) := L_n^{<0>}(x) = \sum_{j=0}^{n} \frac{x^j}{j!}.$$

As f is Hurtwitz integral at p, the vertices of $NP_p(f)$ lies on or above of vertices $NP_p(E_n)$. Again since f is $p-$Coleman integral, then $\nu_p(a_j) = 0$, where $j = k_i$ and $0 \leq i \leq s$. Now, j'th vertices of $NP_p(f)$ is $(j, \nu_p(a_j/j!)) = (j, \nu_p(1/j!))$. This implies that the vertices are in fact same. So, $NP_p(f) = NP_p(E_n)$.

Part-2: We know from Coleman [9] that the breaks of $NP_p(E_n)$ are the pivotal points associated to (n,p).

Part-3:Let the slopes of $NP_p(E_n)$ be m_i, then

$$\begin{aligned} m_i &= \frac{\nu_p(1/k_i!) - \nu_p(1/k_{i-1}!)}{k_i - k_{i-1}} \\ &= \frac{k_{i-1} - \sigma_p(k_{i-1}) - k_i + \sigma_p(k_i)}{(p-1)(k_i - k_{i-1})} \quad \text{(by lemma (9))} \\ &= \frac{b_i - b_i p^{e_i}}{b_i p^{e_i}(p-1)} \quad \text{(from the equation (6.6))} \\ &= \frac{1 - p^{e_i}}{p^{e_i}(p-1)}. \end{aligned}$$

□

We have the following.

Lemma 12. *(Coleman criterion) Suppose $f \in \mathbb{Q}[x]$ has degree n and p is a prime number. If f is $p-$coleman then $p^{\nu_p(n)}$ divides the degree of any factor $g \in \mathbb{Q}[x]$ of f. If f is a p-coleman integral for all primes p dividing n. Then f is irreducible in $\mathbb{Q}[x]$.*

Proof. Let $n = b_1 p_1^e + b_2 p_2^e + \cdots + b_s p_s^e$ and $p^{\nu_p(n)}$ divides n. The slopes of $NP_p(E_n)$ are

$$m_i = \frac{-(p^{e_i} - 1)}{p^{e_i}(p-1)}.$$

Then by lemma (11), $p^{\nu_p(n)}$ divides the denominator of each m_i. Then by corollary (7), $p^{\nu_p(n)}$ divides the degree of each factor of f over $\mathbb{Q}$. Let $n = \prod p^{n_p}$ (where $n_P = \nu_p(n)$) be the prime factorization of p then p^{n_p} divides the degree of each factor of f in $\mathbb{Q}$. Since this is true for all $p \mid n$. Hence, n divides the degree of each factor of f over $\mathbb{Q}$. Therefore, f is irreducible over $\mathbb{Q}[x]$. □

Example 4. *The classical Laguerre polynomial*

$$L_n^{(0)}(x) = \sum_{j=0}^{n} \binom{n}{j} \frac{(-x)^j}{j!}$$

is $p-$coleman integral for every prime p. Since from 6.6, we have

$$k_i = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_i p^{e_i} \quad i = 0, 1, 2, \cdots, s.$$

Let $j = k_i$, then

$$j = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_i p^{e_i},$$

and

$$n - j = b_{i+1} p^{e_{i+1}} + b_{i+2} p^{e_{i+2}} + \cdots + b_s p^{e_s}$$

are completely disjoint. So, there is no carry in the base p addition of this numbers. Then by lemma 9, implies that $\nu_p\binom{n}{j} = 0$ for such j. Then by lemma 11,

$$NP_p(L_n^{(0)}(x)) = NP_p(L_n^{<0>}(x))$$

for all primes p. Then by lemma 12, $L_n^{(0)}(x)$ is irreducible over $\mathbb{Q}[x]$.

The following lemma due to Filaseta.

Lemma 13. *(Filaseta criteria) Suppose*

$$f(x) = \sum_{j=0}^{n} b_j \frac{x^j}{j!} \in \mathbb{Q}[x]$$

is Hurwitz integral, and $\mid b_0 \mid = 1$. Let k be a positive integer $\leq n/2$. Suppose there exist a prime $p \geq k+1$ such that

$$\nu_p(n(n-1)(n-2)\cdots(n-k+1)) > \nu_p(b_n).$$

Then, $f(x)$ cannot have a factor of degree k in $\mathbb{Q}[x]$.

We have the following.

Lemma 14. *If p is a prime number which divides n, then $L_n^{<r>}(x)$ is $p-$Coleman integral if and only if $\binom{n+r}{r} \not\equiv 0$ mod p.*

Proof. We know that

$$L_n^{<r>}(x) = \sum_{j=0}^{n} \binom{n-j+r}{n-j} \frac{(-x)^j}{j!}.$$

Let

$$L_n^{<r>}(x) = \sum_{j=0}^{n} a_j \frac{x^j}{j!}.$$

Then $a_j = \binom{n-j+r}{n-j}$. Clearly, $\nu_p(a_j) \geq 0$ for all primes p. So, this is Hurwitz integral. Suppose that p divides $\binom{n+r}{r}$. Also, $k_0 = 0$. Now,

$$a_0 = \binom{n+r}{n} = \binom{n+r}{r}.$$

Therefore, $p \mid a_0$ and this implies $\nu_p(a_0) > 0$. So,

$$\nu_p(a_{k_i}) \neq 0, \quad 0 \leq i \leq s.$$

Therefore, $L_n^{<r>}(x)$ is not $p-$Coleman. Now, suppose if

$$p \nmid \binom{n+r}{r} = a_0,$$

this implies $\nu_p(a_0) = 0$. Since, $\nu_p(a_0)$ is the number of carries in the base p addition of n and r, then there is no carry in the base p in the addition of n and r. Since, from the equation (6.5)

$$n = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_s p^{e_s}$$

and from the equation (6.6),

$$k_i = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_i p^{e_i} \quad i = 0, 1, 2, \cdots, s.$$

Then

$$n - k_i = b_{i+1} p^{e_{i+1}} + b_{i+2} p^{e_{i+2}} + \cdots + b_s p^{e_s}.$$

The base p expansion of $n - k_i$ is simply truncation of that of n. Therefore, there cannot be a carry in the addition of $n - k_i$ and r. This shows that

$$\nu_p(a_{k_i}) = 0, (0 \leq i \leq s).$$

This implies $L_n^{<r>}(x)$ is $p-$Coleman integral .

□

We have following theorems.

Theorem 22. *If* $gcd(n, \binom{n+r}{r}) = 1$*, then* $L_n^{<r>}(x)$ *is irreducible over* $\mathbb{Q}$.

Proof. Let p be a prime which divides n. Since, n and $\binom{n+r}{r}$ is relatively prime, then $p \nmid \binom{n+r}{r}$. Using lemma (14) we get $L_n^{<r>}(x)$ is $p-$coleman. Since, $L_n^{<r>}(x)$ is $p-$Coleman for all prime p divides n, then by (Coleman criteria) lemma (12), $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$. □

Theorem 23. *If* $gcd(n, r!) = 1$*, then* $L_n^{<r>}(x)$ *is irreducible over* $\mathbb{Q}$.

Proof. Given $gcd(n, r!) = 1$. Clearly, $L_n^{<r>}(x)$ is Hurtwitz integral at p. Since, p be prime which divides n then $p \nmid r!$. We want to show that

$$\nu_p(a_{k_i}) = 0, (1 \leq i \leq s) \quad where \quad a_{k_i} = \binom{n - k_i + r}{r}.$$

Now,

$$\begin{aligned}
&\nu_p(a_{k_i}) \\
&= \nu_p((n - k_i + 1) \cdots (n - k_i + r)) - \nu_p(r!) \\
&= \nu_p(n - k_i + 1) + \nu_p(n - k_i + 2) + \cdots + \nu_p(n - k_i + r), (i = 0, 1, \cdots s - 1).
\end{aligned}$$

We know

$$n - k_i = b_{i+1}p^{e_{i+1}} + b_{i+2}p^{e_{i+2}} + \cdots + b_s p^{e_s}.$$

So, $p \mid n - k_i$. Again

$$\begin{aligned}
&p \nmid r! \\
&\Rightarrow p > r \\
&\Rightarrow p \nmid n - k_i + t, (1 \leq t \leq r).
\end{aligned}$$

So, we get $\nu(a_{k_i}) = 0$ where $0 \leq i \leq s - 1$. Since, $a_{k_s} = 1$, this implies $\nu(a_{k_s}) = 0$. Therefore,

$$\nu(a_{k_i}) = 0 \quad (0 \leq i \leq s).$$

Therefore, $L_n^{<r>}(x)$ is p-Coleman, i.e., $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$.

□

6.2.2 Primes in Short Intervals

We want to prove of Theorem 20. Before going to prove we need to establish the existence of primes of appropriate size, namely primes for which the Newton polygon of $L_n^{<r>}(x)$ precludes the existence of factors of certain degrees. Now we state important result here to use next section.

This theorem is a well known consequences of the Prime Number Theorem, generalizing Chebyshev's theorem on the theorem on the existence of a prime in $(n, 2n)$.

Theorem 24. *Given $h \geq 2$, there exist a constant $C(h)$ such that whenever $N \geq C(h)$, the interval $[N(1-1/h), N]$ contains a prime . We may take $C(h) = e^{h+1/2}(1-1/h)^{-h}$.*

Corollary 8. *If $n + r \geq 48$ and and $n \geq 8 + 5r/3$, then there exist a prime p in the interval $(n + r)/2 < p < n - 2$.*

We have the following theorem.

Theorem 25 (Harborth-Kemnith)**.** *If $n \geq 48683$, then the interval $(n, 1.001n]$ contains a prime.*

6.2.3 Irreducibility of $L_n^{<r>}(x)$ for Large n

First we fix $r \geq 0$, and let $n = n_0 n_1 = n_2 n_3$, where

$$n_1 = \prod_{p \mid \gcd(n, \binom{n+r}{r})} p^{\nu_p(n)},$$

$$n_3 = \prod_{\substack{p \mid n \\ \nu_p(n) \leq \nu_p(r!)}} p^{\nu_p(n)}.$$

Note that, n_0 is the largest divisor of n which is co -prime to $\binom{n+r}{r}$. Also, it is clear that $n_2 \mid n_0$. So, $n_1 \mid n_3 \mid \gcd(n, r!)$. It follows that

$$n_1 \leq r!. \tag{6.7}$$

We can improve it slightly.

We know that a prime p divides $\binom{n+r}{r}$ iff there is a carry in the base p addition of n and r. Thus if p^a divides n and $r < p^a$, then $p \nmid \binom{n+r}{r}$. So $p \nmid n_1$; as an

example primes exceeding r do not divide n_1. Therefore, for a given fixed r, we get

$$\begin{aligned} n_1 &\leq \prod_{\substack{p|r! \\ \nu_p(n)\leq\nu_p(r!)}} p^{\nu_p(n)} \\ &\leq \prod_{\substack{p|r! \\ \nu_p(r!)\leq\lfloor\log_p(r)\rfloor}} p^{\nu_p(n)} \quad \text{since } p^{\nu_p(n)} < r \Rightarrow \nu_p(n)\log p < \log r \Rightarrow \nu_p(n) < \log_p(r) \\ &\leq \prod_{p|r!} p^{\lfloor\log_p(r)\rfloor} \end{aligned}$$

(Since $p \mid \binom{n+r}{r} \Rightarrow \nu_p(n) < \log_p(r)$. Suppose if $\log_p(r) < \nu_p(n) \Rightarrow r < p^{\nu_p(n)}$, a contradiction.)

Again $r \geq 4, \quad \nu_p(r!) \geq \lfloor \log_p r \rfloor$ and also

$$p = 2, \quad \nu_2(r!) \geq 1 + \lfloor \log_2 r \rfloor \quad \text{holds.}$$

$$\begin{aligned} r! &= \prod_{p|r!} p^{\nu_p(r!)} \\ &= 2^{\nu_2(r!)} \cdot \prod_{\substack{p|r! \\ p\neq 2}} p^{\nu_p(r!)} \\ &\geq 2 \cdot 2^{\lfloor \log_2 r \rfloor} \cdot \prod_{p\neq 2} p^{\lfloor \log_p r \rfloor} \\ &= 2 \cdot \prod_{p|r!} p^{\lfloor \log_p r \rfloor} \\ &\geq 2n_1. \end{aligned}$$

This shows that

$$\text{if} \quad r \geq 4, \quad \text{then} \quad n_1 \leq r!/2. \tag{6.8}$$

We remark that for any prime p satisfying $p \leq r/2$, $\lfloor \log_p r \rfloor < \nu_p(r!)$.
We have the following lemma.

Lemma 15. *If there is a prime p satisfying $\max(\frac{n+r}{2}, n - n_0) < p \leq n$, then $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Every $\mathbb{Q}[x]$ factor of $L_n^{<r>}(x)$ has degree divisible by n_0 (by Lemma (14), and (12)). If $n_1 = 1$, then $n = n_0$. So, we are done. Let $n_1 > 1$. Let us assume that $L_n^{<r>}(x)$ has a $\mathbb{Q}[x]$ factor of positive degree $k \leq n/2$. We know $k \in \{n_0, 2n_0, 3n_0, \cdots (n_1 - 1)n_0\}$. To eliminate this possibilities, we apply Filaseta criteria. So, we require $b_0 = 1$. We set

$$f(x) = a_0^{-1} L_n^{<r>}(a_0 x) = \sum_{j=0}^{n} b_j \frac{x^j}{j!},$$

where

$$b_j = a_0^{-1} a_0^j a_j = a_0^{j-1} a_j,$$

and $a_0 = \binom{n+r}{r}$ and $a_j = \binom{n-j+r}{n-j}$. Clearly, b_j is Hurtwitz coefficients, and $b_n = a_0^{n-1} a_n = a_0^{n-1}$. Of course the factorization over $\mathbb{Q}$ of $f(x)$ mirrors exactly that of $L_n^{<r>}(x)$. With the hypothesis on p, we have $p \geq k + 1$ (since $k \leq n/2$). Moreover, $p \geq n - k + 1$, since $k \geq n_0$ and

$$a_0 = \frac{(n+1)(n+2)\cdots(n+r)}{r!},$$

and also $(n + r)/2 < p < n + 1$, then $p \nmid b_n = a_0^{n-1}$. Now, by apply Filaseta criteria as $f(x)$ is Hurtwitz integral with $\mid b_0 \mid = 1, k \leq n/2$ and there exist a prime $p \geq k + 1$ such that

$$\nu_p(n(n-1)(n-2)\cdots(n-k+1)) > \nu_p(b_n).$$

Then, $f(x)$ cannot have a factor of degree k in $\mathbb{Q}[x]$. Therefore, $L_n^{<r>}(x)$ cannot have a factor of degree k. So, we arrived at a contradiction . Then, $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$. □

Definition 7. *For an integer $r \geq 0$, we define*

$$B(r) = \begin{cases} 48 & \text{if} \quad r = 0, 1, 2, 3. \\ e^{r!+1/2}(1 - 1/r!)^{-r!} & \text{if} \quad r \geq 4. \end{cases}$$

We have the following lemma.

Lemma 16. *Given $r \geq 0$ for every integer $n \geq B(r)$, there exist a prime p satisfying*

$$\max(\frac{n+r}{2}, n - n_0) < p \leq n,$$

where n_0 is the largest divisor of n, co prime to $\binom{n+r}{r}$.

Proof. First let us take $r \geq 4$. It is clear that from definition (7) if $r \geq 4$, then $B(r) > r(r!)/(r! - 2)$ holds. Thus,

$$\begin{aligned} & n > B(r) \\ & \Rightarrow n > r(r!)/(r! - 2) \\ & \Rightarrow n(r! - 2)/r! > r \\ & \Rightarrow \frac{n(r! - 2)}{r!} + n > n + r \\ & \Rightarrow \frac{2n(r! - 1)}{r!} > n + r \\ & \Rightarrow (n + r)/2 < n(1 - 1/r!). \end{aligned}$$

Since, $r \geq 4$, from the equation (6.8), we get $n_1 \leq r!/2$.
Now,

$$\begin{aligned} n - n_0 &= n - n/n_1 \\ &\leq n(1 - 2/h) \quad \text{taking } h = r! \\ &< n(1 - 1/h). \end{aligned}$$

Therefore, we get

$$\max(\frac{n + r}{2}, n - n_0) < n(1 - 1/h).$$

We also have $n > e^{h+1/2}(1 - 1/h)^{-h}$. Hence by using Theorem (24), there exist a prime p satisfying $\max(\frac{n+r}{2}, n - n_0) < p \leq n$. Now, let us take $r \in [0, 3]$ and $n \geq 48$. Then, by using the equation (6.7), we get $n_1 \leq 3!$, this implies $n - n_0 \leq 5n/6$. On the other hand, we get

$$(n + r)/2 \leq (n + 3)/2 \leq 5n/6.$$

This implies that

$$\max(\frac{n + r}{2}, n - n_0) < 5n/6.$$

Now, by applying Theorem (24) with $h = 7$, we find that $[6n/7, n] \subset (5n/6, n]$ contains a prime for $n > 5320$. One can direct check for $n \in [48, 5320]$, find that $(5n/6, n]$ contains a prime for all $n \geq 48$. So, we are done. □

Combining the above lemmata gives the proof of the Theorem 20.
More precisely, we have proved the following.

Theorem 26. *For $r \geq 0$, if $n \geq B(r)$, then $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$.*

6.3 Partial answer of Hajir's Conjecture

In this section, Our goal is to prove that n is sufficiently large , then every admissible modification of $L_n^{<r>}(x)$ is irreducible over $\mathbb{Q}$. The main result of this section stated below.

Theorem 27. *For a fixed integer $r \geq 0$, then there exist an effectively computable constant N_r such that every admissible modification of $L_n^{<r>}(x)$ is either irreducible or if it is reducible, then it has at most one linear factor over $\mathbb{Q}$ for all $n \geq N_r$.*

Our use of Filaseta criteria for obtaining above result is summarized by the following lemma.

Lemma 17. *Let n be a positive integer. Suppose that p is a prime, that k and α are positive integers and that l be a non-negative integer for which*

$$p^{\alpha} \parallel (n-l), \tag{6.9}$$

$$p \geq \max\{2r+1, 2l+1\}, \tag{6.10}$$

$$\frac{\log(n+r)}{p^{\alpha}\log p} + \frac{1}{p-1} \leq \frac{1}{k}. \tag{6.11}$$

Then $f(x) = \sum_{j=0}^{n} b_j x^j$, where $b_j = \binom{n}{j}\frac{(n+r-j)!}{r!}$ cannot have a factor with degree $\in [l+1, k]$.

Proof. Let $b_j = \binom{n}{j}\frac{(n+r-j)!}{r!}$ where $j \in \{0, 1, \cdots, n\}$.
We first observe that $b_n = 1$. So that $p \nmid b_n$.
Since

$$b_j = \binom{n}{j}\frac{(n+r-j)!}{r!} = \frac{n!}{j!}\frac{(n+r-j)!}{r!(n-j)!} = \binom{n+r-j}{r} n \cdot (n-1)\cdots(n-j+1),$$

Therefore, $p/b_j \forall j \in \{0, 1, \cdots n-l-1\}$

Next we need to show the right most edge of Newton polygon of $f(x)$ with respect to p has slope $< 1/k$. The right most edge has slope $= \max_{0\le j\le n} \frac{\nu(b_0)-\nu(b_j)}{j}$. So that by the equation 6.11, it is sufficient to show that

$$\frac{\nu(b_0)-\nu(b_j)}{j} < \frac{\log(n+r)}{p^\alpha \log p} + \frac{1}{p-1} \tag{6.12}$$

Now

$$\begin{aligned}
&\nu(b_0)-\nu(b_j)\\
&= \nu\{\binom{n}{0}\frac{(n+r)!}{r!}\} - \nu\binom{n}{j}\frac{(n+r-j)!}{r!}\\
&= \nu(n+r)! - \nu\binom{n}{j} - \nu(n+r-j)!\\
&= \nu\{\frac{(n+r)!}{(n+r-j)!}\} - \nu\{\frac{(n)!}{(n-j)!}\} + \nu(j!)
\end{aligned}$$

Note that

$$\nu((j)!) = \sum_{i=1}^{\infty}\left[\frac{j}{p^i}\right] < \sum_{i=1}^{\infty}\frac{j}{p^i} = \frac{j}{p-1}.$$

To handle the remaining terms, we introduce the notation

$$a(n+r,i) = \left[\frac{n+r}{p^i}\right] - \left[\frac{n+r-j}{p^i}\right]$$

$$a(n,i) = \left[\frac{n}{p^i}\right] - \left[\frac{n-j}{p^i}\right]$$

so that

$$\nu\left\{\frac{(n+r)!}{(n+r-j)!}\right\} - \nu\left\{\frac{(n)!}{(n-j)!}\right\} = \sum_{i=1}^{\infty}\{a(n+r,i)-a(n,i)\}$$

We note that $a(n+r,i)$ is the number of multiplies of p^i in the interval $(n+r-j, n+r]$. Moreover the sum may be truncated at $i = \left[\frac{\log(n+r)}{\log p}\right]$. Since $a(n+r,i) = a(n,i) = 0$ when $p^i > n+r$. To complete the proof it therefore suffices to show that $a(n+r,i) - a(n,i) \le j/p^\alpha$ for $i \ge 1$.
we distinguish three cases.

(i) $i \leq \alpha$,

(ii) $i > \alpha$ and $j \leq l + r$,

(ii) $i > \alpha$ and $j > l + r$.

Case (i): $i \leq \alpha$. By condition 6.9 there exist some m such that $n = p^{\alpha}m + l$.

$$\begin{aligned} a(n+r,i) &= \left[\frac{n+r}{p^i}\right] - \left[\frac{n+r-j}{p^i}\right] \\ &= \left[\frac{p^{\alpha}m+l+r}{p^i}\right] - \left[\frac{p^{\alpha}m+l+r-j}{p^i}\right] \\ &= \left[\frac{l+r}{p^i}\right] - \left[\frac{l+r-j}{p^i}\right] \end{aligned}$$

$$\begin{aligned} a(n,i) &= \left[\frac{n}{p^i}\right] - \left[\frac{n-j}{p^i}\right] \\ &= \left[\frac{p^{\alpha}m+l}{p^i}\right] - \left[\frac{p^{\alpha}m+l-j}{p^i}\right] \\ &= \left[\frac{l}{p^i}\right] - \left[\frac{l-j}{p^i}\right] \end{aligned}$$

$$\begin{aligned} \therefore a(n+r,i) - a(n,i) &= \left[\frac{l+r}{p^i}\right] - \left[\frac{l+r-j}{p^i}\right] - \left[\frac{l}{p^i}\right] + \left[\frac{l-j}{p^i}\right] \\ &= \left[\frac{l-j}{p^i}\right] - \left[\frac{l+r-j}{p^i}\right] \\ &\leq 0. \end{aligned}$$

So, the condition 6.11 follows in this case.

Case (ii): $i > \alpha$ *and* $j \leq l + r$.

We observe that

$$j \leq l + r \Rightarrow -j \geq -l - r \Rightarrow n + r - j \geq n - l.$$

Since, $n - l$ is the multiple of p and $p > \max\{2r, 2l\}$, so $(n + r - j, n + r]$ has no multiple of p and so $a(n + r, i) = 0$. So, the condition 6.11 follows.

Case (iii): $i > \alpha$ and $j > l + r$.

In this case, we observe that

$$j > l + r \Rightarrow -j < -l - r \Rightarrow n + r - j < n - l < n + r.$$

$$\therefore n + r - j < n - l < n + r.$$

The number of multiple of p^α in $(n + r - j, n + r]$ is $[j/p^\alpha] + 1$. Again since $i > \alpha, n - l$ is not divisible by p^i.

$$\therefore a(n + r, i) \leq a(n + r, \alpha) - 1 \leq [j/p^\alpha].$$

Since $a(n, i) \geq 0$, then the inequality 6.11 holds in this case.
This completes the proof.

□

Proof of the theorem 27: Let us take

$$\mathcal{L}_n^{<r>}(x) = n! L_n^{<r>}(x) = \sum_{j=0}^{n} \binom{n}{j} (r+1) \cdot (r+2) \cdots (r+n-j) x^j. \quad (6.13)$$

Let $f(x) = \mathcal{L}_n^{<r>}(x)$. Then we can write $f(x)$ as

$$\begin{aligned} f(x) &= \sum_{j=0}^{n} \binom{n}{j} (r+1) \cdot (r+2) \cdots (r+n-j) x^j \\ &= \sum_{j=0}^{n} \binom{n}{j} \frac{(n+r-j)!}{r!} x^j \\ &= \sum_{j=0}^{n} \binom{n+r-j}{r} \frac{n!}{j!} x^j \\ &= \sum_{j=0}^{n} b_j x^j, \quad where \quad b_j = \binom{n+r-j}{r} \frac{n!}{j!}. \end{aligned}$$

It is easy to understand that $f(x)$ is monic and has a positive integer coefficients as r is a non negative integer. Let us assume that $f(x)$ is reducible, then it has a factor with degree in $[1, n/2]$. Since $f(x)$ is reducible over $\mathbb{Q}$, it is also reducible over $\mathbb{Z}$. Therefore, we deduce that if $f(x)$ is reducible, then it has a factor with integer coefficients and degree $\leq n/2$. Let k denote the smallest degree of an irreducible factor of $f(x)$, then $k \leq n/2$.

$$b_j = \binom{n+r-j}{r}\frac{n!}{j!}$$
$$= \binom{n+r-j}{r}c_j \text{ (say)}.$$

If $i < j$

$$\frac{c_i}{c_j} = \frac{n!}{i!}\cdot\frac{j!}{n!} = \frac{j!}{i!} = j\cdot(j-1)\cdots(i+1).$$

This implies if $i < j$ then c_j/c_i. Therefore, if we are to show that f does not have a factor of degree k, it is sufficient to show that there exist a prime p such that p satisfies the both condition

(i) p/b_j for all $j \in \{0, 1, \cdots, n-k\}$,

(ii) p satisfied the lemma 17

We will give different arguments for various sizes of k with respect to n.

Case (i): $2n/\log n < k \leq n/2$.

For k in the indicated range, we will show that there is a prime p in the interval $(n-k, n]$. First of all, any prime $p \in (n-k, n]$ divides

$$c_{n-k} = n(n-1)(n-2)\cdots(n-k+1)$$

and hence, p divides c_j for all $j \in \{0, 1, \cdots, n-k\}$. Now observe that this prime p satisfies

$$p > n-k = n-n/2 = n/2.$$

Thus, $2p > n$. Consequently, $\nu(c_j) = 1$ for all $j \in \{0, 1, \cdots, n-k\}$ (i.e., p divides c_j exactly once for all $j \in \{0, 1, \cdots, n-k\}$). Next, let us try to figure out if p divides any other c_j. Note that, since $2p > n$, p divides $c_j = (n)(n-1)(n-2)\cdots(j+1)$ if and only if p appears as one of the factors in the product formula for c_j. That is, $p|c_j$ if and only if $p \in [j+1, n]$, i.e., if and only if $j \leq p-1$. Therefore, we have

$$\nu(c_j) = \begin{cases} 1 & \text{if} \quad 0 \leq j \leq p-1 \\ 0 & \text{if} \quad j \geq p. \end{cases}$$

It is easy to understand that the Newton polygon $NP_p(f)$ has only two edges, one joining $(0,0)$ and $(n-p,0)$; and the other edge joining $(n-p,0)$ and $(n,1)$. Thus, the slope of the rightmost edge of $NP_p(f)$ is $1/(p)$. Now, we observe that

$$p > n-k \geq k \quad (\text{since, } n \geq 2k).$$

Therefore, we may now conclude that the slope of the rightmost edge of $NP_p(f)$ is $< 1/k$. By appealing to Lemma 2, we deduce that $f(x)$ does not have a factor of degree k in this cases.
Thus, it remains to show that there is a prime p in the interval $(n-k, n]$ for $2n/\log n < k \leq n/2$ By explicit gap estimates on primes [3], we already have

$$\pi(x) > \frac{x}{\log x - 0.5} \quad \text{for} \quad x \geq 67, \tag{6.14}$$

and

$$\pi(x) < \frac{x}{\log x - 1.5} \quad \text{for} \quad x \geq e^{1.5}. \tag{6.15}$$

Note that it suffices to show that $\pi(n) - \pi(n - 2n/\log n) > 0$. Set $u = (\log n)/2$. Then, we have

$$\pi(n) - \pi(n(1-1/u)) > \frac{n}{\log n - 0.5} - \frac{n(1-1/u)}{\log n + \log(1-1/u) - 1.5},$$

provided, $n \geq 67$ and $n(1-1/u) \geq e^{1.5}$. Since $67(1-2/\log 67) > e^{1.5}$, we just have to take $n \geq 67$. The expressions on the right hand side above upon simplification yields

$$\frac{\log n((\log n)/u + \log(1-1/u) - 1 - 1/2u)}{(\log n - 0.5)(\log n + \log(1-1/u) - 1.5)}.$$

For $n \geq 67$, the factors in the denominator above are > 0, and $\log n > 0$. Thus, the expression above is positive if and only if

$$\log n > u + 1/2 - u\log(1-1/u).$$

Observe that

$$\begin{aligned} -u\log(1-1/u) =& 1 + \frac{1}{2u} + \frac{1}{3u^2} + \cdots \\ &< \frac{1}{2} + \frac{1}{2}\left(1 + \frac{1}{u} + \frac{1}{u^2} + \cdots\right) \\ &= \frac{1}{2}\left(1 + \frac{u}{u-1}\right) < 1.5. \end{aligned}$$

Therefore, it suffices to have $\log n > u + 2$, i.e., $\log n > 4$ which is equivalent to have $n > e^4$. Since $67 > e^4$, our assertion follows for $n \geq 67$. A quick search with SAGE (a mathematical open source software), it follows that the interval $(n - 2n/\log n, n]$ contains a prime for each $n \in [8, 66]$. So, we are done in case (i) for every $n \geq 8$.

Case (ii): $n^{2/3} < k \leq 2n/\log n$.

Recall that in this case $k > n^{2/3}$ and n is large. We show that there is some prime $p > 3k > 3n^{2/3}$ that divides $n(n-1)\cdots(n-k+1)$ so that

$$\frac{\log(n+r)}{p^{\alpha}\log p} + \frac{1}{p-1} < \frac{\log(n+r)}{p\log(n^{2/3})} + \frac{1}{3k} < \frac{2}{3k} + \frac{1}{3k} < \frac{2}{3k} + \frac{1}{3k} = 1/k$$

It only remaining to show that such prime exist.

To prove such prime exist , We mainly use (the next case as well) the lemma 4 due to Erdós, .

For our purposes, we take $u = n-k+1$, $C = 3$ and $\theta = 2/3$ in Lemma 4, so that,

$$p = P(\Delta(n-k+1,k)) > 3k \quad \text{for all} \quad k \geq k_0.$$

where

$$k_0 = 1 + e^{4e^{5.625}}.$$

Since, we have $p > 3k$, also note that $k \leq 2n/\log n$ and $n > k$, it follows that

$$\log n > \log k \Rightarrow \frac{1}{\log n} < \frac{1}{\log k} \Rightarrow \frac{2n}{\log n} < \frac{2n}{\log k} \Rightarrow k < \frac{2n}{\log k},$$

$k < 2n/\log k$. Accordingly, we take $n \geq (k\log k)/2 \geq (k_0 \log k_0)/2$.

Since $p > 3k > 3n^{2/3}$ and $p \geq 2r+1$. Then $3n^{2/3} > 2r \Rightarrow n > (2r/3)^{3/2}$ holds in this case.

For these values of n, we deduce that $f(x)$ does not have a factor of degree k where k is in the range $(n^{2/3}, 2n/\log n]$.

Case(iii): ($k_2 < k \leq n^{2/3}$) Here k_2 is fixed, and will be specified later. The treatment in this case is similar to that in case(ii). We even use the same sets $\mathcal{T}$ and $\mathcal{S}$. As before, we take $C = 3$ and $\theta = 2/3$. Only in the last step in the proof of Lemma 4, we make a small adjustment. Here, we replace

the upper bound $2n/\log n$ of k by $n^{2/3}$. We further note that for $k \geq e^{\frac{(12.5)(3)}{2}}$, i.e, $k \geq e^{18.75}$ one has

$$1 - 1.25(4)/\log k > 0.8.$$

So, we take $k_2 = e^{18.75}$, and after making these changes, we have that

$$n^{2/3} > \left(\frac{n}{2}\right)^{0.8}.$$

The last inequality clearly does not hold for $n \geq 2^6$. Since, we have taken $k \geq k_2$, we must take $n \geq k^{3/2} \geq k_2^{3/2}$. Thus, for $n \geq k_2^{3/2}$, the polynomial $f(x)$ does not have factor of degree in $(k_2, n^{2/3}]$. This settles case (iii).

Case(iv): $1 < k \leq k_2$. The arguments in this section are based on effective versions of Thúe's theorem due to Baker [1].

We begin by proving a lemma concerning the largest prime factor of $n(n-1)$.

Lemma 18. *If $P(\cdot)$ denotes the largest prime factor of a number, then*

$$\lim_{n\to\infty} P(n(n-1)) = \infty.$$

Proof. We will proof the lemma by contradiction. Let us assume that for any $K > 0$, and any $M > 0$, there is a $n > M$ such that $P(n(n-1)) \leq K$. Fixing $K > 0$, and let us define

$$\mathcal{P} = \{p \leq K : p, \text{a prime}\} \quad \text{and} \quad P(K) = \prod_{p\leq K} p.$$

Now, we define a new set

$$\mathcal{A} = \{p : P(n(n-1)) \leq K.\}$$

We assume that $|\mathcal{A}| = \infty$. Now by using the fundamental theorem of arithmetic, we can express every integer l as

$$l = l_1 l_2^3,$$

where l_1 is cub-free. Thus, there exist integers $X = X_n$, $Y = Y_n$, and cube-free integers $A = A_n$ and $B = B_n$ such that

$$n = AX^3 \quad \text{and} \quad n-1 = BY^3; \quad n \quad \text{be an positive integer.}$$

Therefore, we get the equation

$$AX^3 - BY^3 + 1 = 0. \tag{6.16}$$

Since, our assumption that $|\mathcal{A}| = \infty$, it clearly implies that at least one of the following sets is infinite:

$$\mathcal{A}_1 = \{X_n : n \in \mathcal{A}\}, \quad \mathcal{A}_2 = \{Y_n : n \in \mathcal{A}\}.$$

For fixed cube-free positive integers A and B, (6.16) is absolutely irreducible. Now, we prove it by proving the following lemma.

Lemma 19. *For fixed cube-free positive integers A and B, $Ax^3 - By^3 + 1$ is absolutely irreducible.*

Proof. Let A, B are fixed cube free. Let

$$u(x,y) = Ax^3 - By^3 + 1. \tag{6.17}$$

We want to show that $u(x,y)$ is absolutely irreducible. We will prove it by contradiction. Let us assume that $u(x,y)$ is reducible over $\mathbb{C}$.
Let

$$u(x,y) = v(x,y)w(x,y). \tag{6.18}$$

Then

$$\deg u = \deg v + \deg w.$$

Let

$$v(x,y) = a_1x + a_2y + a_3,$$

and

$$w(x,y) = b_1x^2 + b_2y^2 + b_3xy + b_4x + b_5y + b_6.$$

$$\begin{aligned} v(x,y)w(x,y) = a_1b_1x^3 + a_2b_1x^2y + a_1b_3x^2y + a_1b_5xy + a_2b_4xy + a_3b_3xy \\ +a_1b_2xy^2 + a_2b_3xy^2 + a_2b_2y^3 + a_1b_6x + a_3b_4x \\ +a_2b_6y + a_3b_5y + a_3b_1x^2 + a_1b_4x^2 + a_3b_2y^2 \\ +a_2b_5y^2 + a_3b_6. \end{aligned}$$

Now, comparing the coefficients in the above equation with those in the equation (6.17), we get

$$a_1b_1 = A, \tag{6.19}$$

$$a_2b_2 = -B, \tag{6.20}$$

$$a_3b_6 = 1, \tag{6.21}$$

$$a_2b_1 + a_1b_3 = 0, \tag{6.22}$$

$$a_1b_2 + a_2b_3 = 0, \tag{6.23}$$

$$a_1b_6 + a_3b_4 = 0, \tag{6.24}$$

$$a_1b_4 + a_3b_1 = 0, \tag{6.25}$$

$$a_2b_6 + a_3b_5 = 0, \tag{6.26}$$

$$a_3b_2 + a_2b_5 = 0, \tag{6.27}$$

$$a_1b_5 + a_2b_4 + a_3b_3 = 0. \tag{6.28}$$

Now, solving the equations ((6.22) and (6.23)), ((6.24) and (6.25)), and ((6.26) and (6.27)), we get

$$b_3^2 = b_1b_2, \tag{6.29}$$

$$b_4^2 = b_1 b_6, \tag{6.30}$$

$$b_5^2 = b_6 b_2. \tag{6.31}$$

From equations ((6.29), (6.30) and (6.31)), we can say that b_1, b_2, b_6 must have the same sign. Now from equation (6.19) , it is clear that a_1 and b_1 have same sign. Also from equation (6.20), it is clear that a_2 and b_2 have same sign. Again from equation 6.21, it is clear that a_3 and b_6 have same sign. Since b_2, b_6 have same sign, then a_2, a_3 have same sign. Again from the equation (6.24), we get $b_4 = -a_1 b_6/a_3$, this implies b_4, a_1 has opposite sign. Again from the equation (6.27), we get $b_5 = -a_3 b_2/a_2$, this implies b_5, b_2 have same sign. Again from the equation (6.22) we get $b_3 = -a_2 b_1/a_1$, this implies b_3, b_1 have same sign. From the above observation we conclude that $b_1, b_2, b_3, b_5, b_6, a_1, a_3$ has same sign, and a_2, b_4 has same sign. Therefore, we get the result that a_1, b_5 have same sign. a_2, b_4 and a_3, b_3 also have same sign. Therefore, the sign of $a_1 b_5, a_2 b_4, a_3 b_3$ are all positive. Then this cannot satisfy the equation (6.28), if it is satisfied, then all are zeros. So, we arrive at a contradiction. Therefore, our original assumption was wrong. This implies $u(x, y)$ is absolutely irreducible.

□

Hence, by Theorem 10, we deduce that any integral solution (X, Y) of (6.16) must satisfy

$$\max\{X, Y\} < \exp\exp\exp\left((2H)^{10^{3^{10}}}\right), \quad \text{where} \quad H = \max\{A, B\}.$$

Since $P(n(n-1)) \leq K$, we deduce that n and $n-1$ are made up of primes $\leq K$. Since A is a cube-free divisor of n, we have $A|P(K)^2$. Similarly, $B|P(K)^2$. Thus, one has

$$\max\{A, B\} \leq P(K)^2 = \exp(2\sum_{p \leq K} \log p) \leq e^{2.04K}.$$

But this then implies that

$$\max\{X, Y\} < \exp\exp\exp\left((2e^{2.04K})^{10^{3^{10}}}\right) = n_K, \text{ a fixed number.}$$

But this implies both $\mathcal{A}_1$ and $\mathcal{A}_2$ to be finite, and therefore, we arrive a contradiction. So our original assumption is wrong. Thus $|\mathcal{A}| < \infty$, and the lemma follows. □

Let us now get back to the polynomial $f(x)$. Since, we are trying to show that $f(x)$ does not have a factor with degree in $(1, k_2]$. We take $K = \max\{3k_2, 2r\}$ in Lemma 18. We further take $n = \deg f$ to be

$$n > P(K)^2 n_K^3.$$

Then from Lemma 18, we deduce that $P(n(n-1)) > K = \max\{3k_2, 2r\}$. Next, we note that for any $2 \leq k \leq k_2$, one has that

$$n(n-1)|c_j \quad \text{for all} \quad j \in \{0, 1, \cdots, n-k\}.$$

Let $p = P(n(n-1))$. Thus, we have for any $2 \leq k \leq k_2$ that

$$p|n(n-1)|c_j \quad \forall j \in \{0, 1, \cdots, n-k\},$$

and

$$p > K = \max\{3k_2, 2r\} \geq \max\{3k, 2r\}.$$

Our conclusion in case (iv) now follows from Lemma 17.

Let N_r be the maximum of all the lower bounds on n in cases (i) through (iv), i.e., n_r is largest among the following:

- 8 from case (i)
- $\max\{(2r/3)^{3/2}, (k_0 \log k_0)/2\}$, where $k_0 = 1 + e^{4e^{5.625}}$ from case (ii)
- $\max\{(2r/3)^{3/2}, \exp((18.75)^{3/2}$ from case (iii)
- $P(K)^2 n_K^3$ from case (iv) where

$$P(K) = \prod_{p \leq K} p, n_K = \quad \exp\exp\exp\left((2e^{2.04K})^{10^{3^{10}}}\right),$$

and

$$K = \{3\exp((18.75), 2r\}.$$

Clearly, the fourth item gives the maximum value, and this gives us an explicit estimate for N_r (albeit too large).

Bibliography

[1] Alan Baker *Transcendental Number Theory*, Cambridge University Press (1975).

[2] M. Filaseta and T. Y. Lam *On the irreducibility of generalized Laguerre polynomials*, Acta Arith. **105** (2002), 177–182.

[3] Rosser and Schoenfeld, *Approximate formulas for some functions of prime numbers*,

[4] I. Schur, *Gleichungen ohne Affekt*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse (1930), 443–449.

[5] P. Banerjee, *On Galois groups of Laguerre polynomials whose discriminants are squares*, J. Number Theory **141** (2014), 36–58.

[6] P. Banerjee, M. Filaseta, C. Finch and J. Leidy, *On classifying Laguerre polynomials which have Galois group the alternating group*, J. Théor. Nombres Bordeaux **25** (2013), 1–30.

[7] Chao, H. (1974). *A generalization of Eisenstein's criterion. Math. Mag. 47,158-159*

[8] H. Cohen, Number Theory Vol. I (2007) (New York: Springer Science+Business Media, LLC).

[9] R. F. Coleman, *On the Galois groups of exponential Taylor polynomials*, Ensein. Math. (2) **33** (1987), no. 3–4, 183–189.

[10] Dowart.H.L(1935b) *Irreducibility of polynomials. Amer. Math. Monthly 42, 369-381*

[11] G. Dumas, *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, Journal de Math. Pure et Appl. **2** (1906), 191–258.

[12] M. Filaseta, S. Laishram and N. Saradha, *Solving* $n(n+d)\cdots(n+(k-1)d) = by^2$*, with* $P(b) \leq Ck$. Int. Jour. of Number theory **8** (2012), 161–173.

[13] M. Filaseta and T. Y. Lam *On the irreducibility of generalized Laguerre polynomials*, Acta Arith. **105** (2002), 177–182.

[14] M. Filaseta and O. Trifonov, *The irreducibility of the Bessel polynomials*, J. Reine Angew. Math. 550 (2002), 125–140.

[15] M. Filaseta, T. Kidd and O. Trifonov, *Laguerre Polynomials with Galois group* A_m *for each* m, . J. Number Theory **132** (2012), 776–805.

[16] R. Gow, *Some generalized Laguerre polynomials whose Galois groups are the alternating groups*, J. Number Theory **31** (1989), 201–207.

[17] F. Hajir, *Some* A_n*-extensions obtained from generalized Laguerre polynomials*, J. Number Theory **50** (1995), 206–212.

[18] F. Hajir, *Algebraic properties of a family of generalized Laguerre polynomials*, Canad. J. Math. **61** (2009), no. 3, 583–603.

[19] F. Hajir, *On the Galois group of generalized Laguerre polynomials*, J. Théor. Nombres Bordeaux **17** (2005), no. 2, 517–525.

[20] F. Hajir and S. Wong, *Specializations of one parameter family of polynomials*, Ann. Inst. Fourier (Grenoble) **56** (2006), no. 4, 1127–1163.

[21] S. Laishram and T. N. Shorey, *Irreducibility of generalized Hermite-Laguerre polynomials III*, preprint, http://arxiv.org/abs/1306.0736. .

[22] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[23] N. Saradha and T. N. Shorey, *Squares in blocks from an arithmetic progression and Galois groups of Laguerre polynomials*, International Journal of Number Theory, to appear.

[24] I. Schur, *Einege Satže über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen, I*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys-Math. Kl. **14** (1929), 125–136.

[25] I. Schur, *Einege Satže über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen, I*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys-Math. Kl. **14** (1929), 125–136.

[26] I. Schur, *Einege Satz̈e über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen, II*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys-Math. Kl. **14** (1929), 370–391.

[27] I. Schur, *Gleichungen ohne Affekt*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys-Math. Kl. **14** (1929), 443–449.

[28] I. Schur, *Affectlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, Journal für die reine und angewandte Mathematik **165** (1931), 52–58.

[29] I. Schur, *Gesammelte Abhandlungen. Band III*, Springer-Verlag, Berlin, 1973, Herausgegeben von Alfred Brauer und Hans Rohrbach.

[30] E. A. Sell, *On a certain family of generalized Laguerre polynomials*, J. Number Theory **107** (2004), 266–281.

[31] Weiss, E. (1963). *Algebraic Number Theory. New York: Chelsea*