Abstract

Let G be any group. For any natural number $n \in \mathbb{N}$, let a_n be the number of subgroups $H \leq G$, such that $[G : H] = n$. Assume G is finitely-generated, then $a_n < \infty$, and we can define a ζ-function of the form $\zeta_G(s) := \sum_{i=1}^{\infty} a_n n^{-s}$, where $s \in \mathbb{C}$. Assume, in addition, that G is also nilpotent and torsion-free, then this function has properties of the Riemann ζ-function, mainly the decomposition of ζ to an Euler product of local factors indexed by primes. Using different variations of the ζ-function and its factorization, we can obtain more information about G and specific subgroups of G. Specifically, we are interested in the number of pro-isomorphic subgroups of G, and in this research, we shall display an approach to the problem of counting them.

1 Scientific Background

1.1 Introduction

We start our discussion with the following proposition, which stands at the very base of our subject.

Proposition 1.1.1. *Let G be any finitely generated group, and let $n \in \mathbb{N}$ any natural number. Then there is a finite number of subgroups $H \leq G$, such that $[G : H] = n$*

Proof. Let $H \leq G$, such that $[G : H] = n$, then ${}^{G}/_{H} := \{g_1H, g_2H, \ldots, g_nH\}$ is the set containing all left cosets of H. We shall define an operation $* : G \times {}^{G}/_{H} \to {}^{G}/_{H}$, in the following way. $\forall g \in G$, and $\forall g_iH \in {}^{G}/_{H}$, the operation is $g * g_iH := (gg_i)H = g_jH$, that is, g maps a left cost to another left coset. But that means that g maps every index $i \in [n]$ to another index, which means that g operates as a permutation on $[n]$, so $*$ defines a homomorphism $f : G \to \mathcal{S}_n$, from G to the symmetric group of order n. H is a subgroup, so $\forall g \in G$, it is clear that $g \in H$ iff $gH = H$. Assume that i_0 is the index of the left coset which identifies with H, i.e. $g_{i_0}H = H$, then $g \in H$ iff $g * g_{i_0}H = H$, which means that the permutation $f(g)$ stabilizes i_0, i.e. $f(g)(i_0) = i_0$. So, we can write $H = \{g \in G : f(g)(i_0) = i_0\}$. From this observation, it is clear that $\#\{H \leq G : [G : H] = n\} \leq \#\{f : G \to \mathcal{S}_n\}$. But all f are homomorphisms from a finitely generated group to a finite group, and since group homomorphisms are uniquely determined by the mapping

of the generators, it is clear that $\#\{f : G \to \mathcal{S}_n\} < \infty$, which proves the proposition. $\square$

This proposition gives rise to an entire subject in group theory, called **Subgroup Growth**. We denote by $a_n(G)$ the number of G-subgroups of index n, and claim, without proving, that the sequence $\{a_n(G)\}$ depends on n, and is monotonically increasing, hence the name, subgroup growth. Several important results have been found, regarding bounds of this n-dependent growth, including polynomial, exponential, and intermediate bounds. These bounds may vary by certain characteristics of the group G. In addition, we can also research the growth of G-subgroups of specific types. This research will concentrate on the growth of **pro-isomorphic** subgroups, which we now define.

Definition 1.1.2. *Let G be any group, and let $\mathcal{N} := \{N \trianglelefteq G\}$ the set of all normal subgroups of G. We define a partial order on $\mathcal{N}$, by inclusion, and assign G an infinite set of indices, $I \subset \mathbb{N}$. $\widehat{G} = \varprojlim\{{}^{G}/_{N_k}\}_{k\in I} := \{(h_k)_{k\in I} \in \prod_{k\in I} {}^{G}/_{N_k} : \pi_{ji}(h_j) = h_i, \forall i \leq j\}$ is an inverse limit of $\{{}^{G}/_{N_k}\}_{k\in I}$, and is called the **Profinite Closure** of G.*

Definition 1.1.3. *Let G be any group. a subgroup $H \leq G$ is called **Pro-Isomorphic**, if $\widehat{H} \cong \widehat{G}$.*

Definition 1.1.4. *Let G be any group, and let $\hat{a_n}(G) := \#\{H \leq G : \widehat{H} \cong \widehat{G}, [G : H] = n\}$, in words, the number of pro-isomorphic subgroups of G, of index n. The **Pro-Isomorphic ζ-Function** of G is defined by $\hat{\zeta}_G(s) := \sum_{n=1}^{\infty} \hat{a_n}(G)n^{-s}$, for some $s \in \mathbb{C}$.*

In this research, we discuss only groups for which $\hat{a_n}(G) < \infty$, for every $n \in \mathbb{N}$. A sufficient condition for this would be that G is finitely-generated, by proposition 1.1.1.

Example 1.1.5. *$G = (\mathbb{Z}, +)$. $\mathbb{Z}$ is an abelian group, and every $H \leq \mathbb{Z}$ is of the form $H = n\mathbb{Z} = \langle n \rangle$, for some $n \in \mathbb{N}$, which means that $H \cong \mathbb{Z}$, as both are infinite cyclic groups, and so, $\widehat{H} \cong \widehat{\mathbb{Z}}$. Since we have only one $\mathbb{Z}$-subgroup of index n, for every $n \in \mathbb{N}$, then $a_n(\mathbb{Z}) = \hat{a_n}(\mathbb{Z}) = 1$, thus, its pro-isomorphic ζ-function is $\hat{\zeta}_{\mathbb{Z}} = \sum_{i=1}^{\infty} n^{-s} = \zeta(s)$, the Riemann ζ-function.*

After establishing the basic definitions, we observe a fact that is a major motivation for this research, which says that the Riemann ζ-function

decomposes to an infinite product of local ζ_p-functions, that is, $\zeta(s) = \prod_p \zeta_p(s) = \prod_p \sum_{k=0}^{\infty} p^{-ks} = \prod_p \frac{1}{1-p^{-s}}$, where the product runs over all the prime numbers. Following this fact, regarding the Riemann *zeta*-function, we observe that for any finitely-generated, nilpotent and torsion-free group, G, we have the same decomposition as above, for the pro-isomorphic ζ-function, $\hat{\zeta_G}(s) = \prod_p \hat{\zeta_{G,p}}(s)$, where $\hat{\zeta_{G,p}}(s) := \sum_{k=0}^{\infty} a_{p^{ks}}(G)p^{-ks}$ We hereby bring several basic definitions of group nilpotency, which are very important for this research.

Definition 1.1.6. *Let G be any group, then the **Lower Central Series** of G is a sequence of subgroups of G, defined by the recursive rule, $G_n := [G, G_{n-1}]$, for every $n \in \mathbb{N}$, where $G_0 := G$. We recall that $[G, G_n] \leq G$ is the subgroup of commutators, $\{gg_ng^{-1}g_n^{-1} : g \in G, g_n \in G_n\}$*

Definition 1.1.7. *Let G be any group. the **Nilpotency Class** of G is $min\{n \in \mathbb{N} : G_n = [G, G_{n-1}] = \{e\}\}$, in words, the smallest natural number, such that the subgroup of commutators of the form $[G, G_n]$ is the trivial group. We can extend this definition, and say that the trivial group nilpotency class is 0.*

Definition 1.1.8. *Let G be a group. If G if of a finite nilpotency class, $n \in \mathbb{N}$, then G is said to be a **Nilpotent** group.*

1.2 Linearization

For finitely-generated torsion-free nilpotent groups, we associate nilpotent Lie algebras over $\mathbb{Z}_p$, the ring of p-adic integers. We show here the basic properties of $\mathbb{Z}_p$-algebras, as subalgebras of $\mathbb{Q}_p$-algebras, where $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$. In the part that describes the goals of this research, we present a specific structure of nilpotent groups, and their associated Lie algebras over the p-adic integers. We begin this part of our discussion by a very basic fact, which says that the group of automorphisms of $\mathcal{L}_{p,n}$, namely $G_n(\mathbb{Q}_p)$, where p is a prime number, and $n = dim\mathcal{L}_{p,n}$, is a subgroup of $GL_n(\mathbb{Q}_p)$, which means that $G_n(\mathbb{Q}_p)$ is a group of invertible $n \times n$ matrices over $\mathbb{Q}_p$, which is actually true for any field. This basic fact comes immediately from choosing a basis for $\mathcal{L}_{p,n}$, $\mathcal{B} = \{b_1, \ldots, b_n\}$, and showing that for every $\mathcal{L}_{p,n}$-automorphism, $\varphi \in G_n(\mathbb{Q}_p)$, and for every $v \in \mathcal{L}_{p,n}$, the image $\varphi(v)$ can be uniquely determined by one invertible linear transformation,

This obviously comes from the fact that every $v \in \mathcal{L}_{pn}$ is uniquely represented as a linear combination of elements of the basis, i.e. $v = \sum_{i=1}^{n} \lambda_i b_i$, then the image $\varphi(v) = \varphi(\sum_{i=1}^{n} \lambda_i b_i) = \sum_{i=1}^{n} \varphi(\lambda_i b_i) = \sum_{i=1}^{n} \lambda_i \varphi(b_i)$. Clearly, $\{\varphi(b_1), \ldots, \varphi(b_n)\}$ itself forms a basis of $\mathcal{L}_{p,n}$, and so, φ can be represented as a basis transition matrix, which proves the above. After establishing the basic fact, regarding the structure of $\mathcal{L}_p, n$-automorphisms as invertible matrices over $\mathbb{Q}_p$, we observe that $\mathcal{L}_{p,n}$ can be restricted to an algebra over the ring of p-adic integers, which we denote as $L_{p,n} < \mathcal{L}_{p,n}$. This comes from the fact that $\mathbb{Z}_p < \mathbb{Q}_p$, so if $\mathcal{B}_n = \{b_1, \ldots, b_n\}$ is a basis for for $\mathcal{L}_{p,n}$, and if $v = \sum_{i=1}^{n} \alpha_i b_i$, and $u = \sum_{i=1}^{n} \beta_i b_i$, where $\alpha_i, \beta_i \in \mathbb{Z}_p$, then clearly, $v + u, vu \in L_{p,n}$. For the construction of the algebras we shall study, in this research, we need to show the opposite direction of the above claim. Suppose we have $\mathcal{A}_n$, a $\mathbb{Z}$-algebra, with a basis $\mathcal{B}_n = \{b_1, \ldots, b_n\}$. We observe that $\mathbb{Z}_p$, as an abelian group, has a natural structure of $\mathbb{Z}$-module, and therefore, we can take the tensor product $\mathcal{A}_n \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and so we have, for all $a \in \mathcal{A}_n$, and for all $r, s \in \mathbb{Z}_p$, that $s(a \otimes r) = a \otimes rs = rs(a \otimes 1)$, which is well-defined, because of the multiplication in $\mathbb{Z}_p$, and so, given $B = \{b_1, b2, \ldots, b_n\}$, a basis for $L_n(\mathbb{Z}_p)$, we have a natural bijection between b_i and $b_i \otimes 1$, for $1 \leq i \leq n$, which means that $\{b_1 \otimes 1, b_2 \otimes 1, \ldots, b_n \otimes 1\}$ is a basis for $\mathcal{A}_n \otimes_{\mathbb{Z}} \mathbb{Z}_p$, we denote $L_{p,n} := \mathcal{A}_n \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and we got that $L_{p,n}$ is a $\mathbb{Z}_p$-algebra, with the same basis, $\mathcal{B}_n$, but with scalars from $\mathbb{Z}_p$, which proves that $L_n < \mathcal{L}_n$. The same construction exactly extends $L_{p,n}$ to $\mathcal{L}_{p,n}$.

The above discussion brings us closer to the essence of our research background, for now we are able to observe the following important fact. If $\mathcal{B}_n$ is a basis for $\mathcal{L}_{p,n}$, then, for every $\varphi \in G_n(\mathbb{Q}_p)$, we have that $\varphi(L_{p,n}) \subseteq L_{p,n}$ iff $\varphi(b_1), \ldots, \varphi(b_n) \in L_{p,n}$, in words, the image of every vector in $L_{p,n}$ is in $L_{p,n}$ itself if and only if the coefficients of the $\mathbb{Q}_p$-linear transformation φ, i.e., the rows of the $n \times n$ matrix that represents φ, are in $\mathbb{Z}_p$ itself. The less obvious direction comes from the fact that if $v = \sum_{i=1}^{n} \lambda_i b_i$, where $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}_p$, then $\varphi(v) = \varphi(\sum_{i=1}^{n} \lambda_i b_i) = \sum_{i=1}^{n} \varphi(\lambda_i b_i) = \sum_{i=1}^{n} \lambda_i \varphi(b_i)$, but $\varphi(b_1), \ldots, \varphi(b_n) \in L_p$, so $\sum_{i=1}^{n} \lambda_i \varphi(b_i)$ is a $\mathbb{Z}_p$-linear combination, hence $\varphi(v) \in L_p$.

Another important step in the direction of our research would be to introduce the following object. $G_n^+(\mathbb{Q}_p) := G_n(\mathbb{Q}_p) \cap \mathcal{M}_n(\mathbb{Z}_p)$, in words, all the $\mathcal{L}_{p,n}$-automorphisms, which are matrices over $\mathbb{Z}_p$. We immediately observe that $G_n^+(\mathbb{Q}_p)$ is a monoid, since $G_n(\mathbb{Q}_p)$ is a group, thus a monoid, and $\mathcal{M}_n(\mathbb{Z}_p)$ is a monoid, so, their intersection is a monoid.

A very important attribute of this object is that it absorbs $L_{p,n}$-automorphisms

by multiplication from right, i.e., for every $g \in G_n^+(\mathbb{Q}_p)$, the right coset $G_n(\mathbb{Z}_p)g \subseteq G_n^+(\mathbb{Q}_p)$. This comes from the fact that if $\varphi \in G_n(\mathbb{Z}_p)$, then clearly $\varphi \in G(\mathbb{Q}_p)$, but on the other hand, $\varphi(L_{p,n)} \subseteq L_{p,n}$, as we saw earlier, which means that φ is a $n \times n$ matrix with coefficients from $\mathbb{Z}_p$, so $\varphi \in \mathcal{M}_n(\mathbb{Z}_p)$, as well, and the two inclusions give us that $\varphi \in G(\mathbb{Q}_p) \cap \mathcal{M}_n(\mathbb{Z}_p)$, hence, $\varphi g \in G(\mathbb{Q}_p) \cap \mathcal{M}_n(\mathbb{Z}_p)$. This gives way to the following result, $G^+(\mathbb{Q}_p) = \bigsqcup_{i=1}^m G(\mathbb{Z}_p)g_i$, where $[G(\mathbb{Q}_p) : G(\mathbb{Z}_p)] = m$, in words, the monoid $G_n^+(\mathbb{Q}_p)$ is a disjoint union of right-cosets of $G_n(\mathbb{Z}_p)$ in $G_n(\mathbb{Q}_p)$.

The discussion above reveals the construction we base our research upon. We observe that there is a bijection between $G(\mathbb{Z}_p)\backslash G^+(\mathbb{Q}_p)$ and $\{M \leq L_{p,n} : M \cong L_{p,n}\}$, in words, we have a bijective map between each right-coset of $G_n(\mathbb{Z}_p)$ in $G_n^+(\mathbb{Q}_p)$ and each $L_{p,n}$-subalgebra which is isomorphic to $L_{p,n}$ itself. The general idea behind this observation is that if we take an automorphism in a right-coset of $G_n(\mathbb{Z}_p)$, namely $\varphi \in G_n(\mathbb{Z}_p)g \in G_n(\mathbb{Z}_p)\backslash G_n^+(\mathbb{Q}_p)$, and denote $M = \varphi(L_{p,n})$, since $\varphi \in G_n^+(\mathbb{Q}_p) = G_n(\mathbb{Q}_p) \cap \mathcal{M}_n(\mathbb{Z}_p)$, we have that $M = \varphi(L_{p,n}) \subseteq L_{p,n}$, as we saw earlier. If we choose a different representative of the same right-coset, namely $\psi \in G(\mathbb{Z}_p)g$, we have that $\tau = \psi\varphi^{-1} \in G(\mathbb{Z}_p)$, which means that $\tau(L_{p,n}) = L_{p,n}$. But $\tau\varphi = \psi\varphi^{-1}\varphi = \psi$, which means that $\psi(L_{p,n}) = \tau\varphi(L_{p,n}) = \varphi(\tau(L_{p,n})) = \varphi(L_{p,n}) = M$, so we have that M is the image of any representative of $G(\mathbb{Z}_p)g$. We further observe that the restriction $\varphi|_{L_{p,n}}$ is a one-to-one map from $L_{p,n}$ onto $L_{p,n}$ itself, and therefore, it is an isomorphism. If we take $M = \varphi_{L_{p,n}}(L_{p,n})$, we have that $M \cong L_{p,n}$, as the image of the restriction of any choice of representative of $G(\mathbb{Z}_p)g$, which generally shows where this bijection comes from.

We end this part, as a preparation for the final part of this technical background review, with the following result, which says that for each right-coset of $G_n(\mathbb{Z}_p)$ in $G_n^+(\mathbb{Q}_p)$, namely, $G_n(\mathbb{Z}_p)g$, taking any representative of this coset $\varphi \in G_n(\mathbb{Z}_p)g$, and taking the image $M = \varphi(L_{p,n}) \leq L_{p,n}$, then $[L_{p,n} : M] = |det(g)|_p^{-1}$.

1.3 p-adic Integration

In this final part of the technical background review, we finally get to the motivation for all the construction we have presented in the first parts. We start with a basic observation about topological groups, which says that if Γ is a topological group, and $U \subseteq \Gamma$, is an open subset of Γ, then $\gamma U := \{\gamma u : \gamma \in \Gamma, u \in U\}$ is also an open subset of Γ. To show this is true, We define a map $f = f_{\gamma^{-1}} : \Gamma \to \Gamma$, by $f(g) := \gamma^{-1}g$, for any $g \in \Gamma$. Clearly, f is

continuous, as a composition of the group inverse and multiplication maps, both continuous in Γ, therefore, taking, for every open set $U \subseteq \Gamma$, the inverse image $f^{-1}(U) = \{g \in G : f(g) = \gamma^{-1}g \in U\} = \{\gamma h : f(\gamma h) = \gamma^{-1}\gamma h = h \in U\} = \{\gamma h : h \in U\} = \gamma U$, proves that γU is also an open subset in Γ.

We shall now define a very central object for our research. Prior to defining this object, we actually claim, without proving, that it does exist, under the prerequisites of the definition.

Definition 1.3.1. *Let Γ be a locally compact topological group, i.e., $\forall \gamma \in \Gamma$, there is an open environment U_γ of γ, and a compact subset K_γ, such that $\gamma \in U_\gamma \subset K_\gamma$. Then there is a measure μ, with the following property: for any measurable subset, $U \subseteq \Gamma$, and any $\gamma \in \Gamma$, $\mu(U\gamma) = \mu(U)$, where $U\gamma := \{u\gamma : u \in U\}$, and μ is unique up to multiplication in constant. μ is called a* ***Right Haar Measure***

Equipped with the newly-defined right Haar measure, we can finally make use of the construction from above. We start by claiming, without proof, that if p be a prime number, then $G_n(\mathbb{Q}_p)$, that is, the group of automoprhisms, for any n-dimensional $\mathbb{Z}_p$-algebra, $L_{p,n}$, is a locally compact topological group.

We continue to claim that $G_n(\mathbb{Q}_p)$, the group of $\mathcal{L}_{p,n}$-automorphisms, has a unique right Haar measure μ, with the property that $\mu(G(\mathbb{Z}_p)) = 1$.

Moreover, we claim that for every $g \in G_n(\mathbb{Q}_p)$, we also have that $\mu(G(\mathbb{Z}_p)g) = \mu(G(\mathbb{Z}_p)) = 1$. With this observation, we go directly to the calculation of the p-adic valuation of the determinant as an integral, and say that if p is a prime number, $s \in \mathbb{C}$, and $g \in G_n^+(\mathbb{Q}_p)$, then $|det(g)|_p^s = \int_{h \in G_n^+(\mathbb{Q}_p)} |det(h)|_h^s d\mu$.

This comes from the above claim, that for every right-coset of $G_n(\mathbb{Z}_p)$ in $G_n^+(\mathbb{Q}_p)$, we have that for every $L_{p,n}$-automorphism, $g \in G(\mathbb{Z}_p)h$, the inverse of the p-adic valuation of the determinant, $|det(g)|_p^{-1}$, does not depend on the choice of representative, which means that $|det(g)|_p$ is constant on the entire right-coset, so we have that $|det(g)|_p = |det(h)|_p$, hence, $|det(g)|_p^s = \int_{h \in G^+(\mathbb{Q}_p)} |det(h)|_p^s d\mu = \int_{h \in G^+(\mathbb{Q}_p)} |det(g)|_p^s d\mu = |det(g)|_p^s \int_{h \in G^+(\mathbb{Q}_p)} d\mu$. But, $\mu = \mu(G(\mathbb{Z}_p)h)$, and we saw earlier that $\mu(G(\mathbb{Z}_p)h) = \mu(G(\mathbb{Z}_p)) = 1$, so $\int_{h \in G^+(\mathbb{Q}_p)} |det(h)|_p^s d = |det(g)|_p^s \int_{h \in G^+(\mathbb{Q}_p)} d\mu = |det(g)|_p^s \cdot 1 = |det(g)|_p^s$

Now we can conclude all this construction by the following observation, that if p is a prime number, and $s \in \mathbb{C}$, then $\hat{\zeta_{L,p}}(s) = \sum_{G(\mathbb{Z})g \in G(\mathbb{Z}_p)\backslash G^+(\mathbb{Q}_p)} |det(g)|_p^s =$

$\sum_{G(\mathbb{Z})g\in G(\mathbb{Z}_p)\backslash G^+(\mathbb{Q}_p)} \int_{h\in G(\mathbb{Z}_p)g} |det(h)|_p^s d\mu = \int_{h\in G^+(\mathbb{Q}_p)} |det(h)|_p^s d\mu$, which brings us back to our initial quest, which is, finding a way to calculate the local pro-isomorphic $\hat{\zeta}_{G,p}$-function, for every prime number p. We end this technical background review by a theorem, brought with no proof,

Theorem 1.3.2. *Let p be a prime number, $s \in \mathbb{C}$, then there exists a rational function, $w_p(s) := \frac{f(x)}{g(x)}$, where $f, g \in \mathbb{Z}_p[x]$, which satisfies $\hat{\zeta_{L,p}}(s) = w_p(p^{-s})$.*

2 Research Goals and Methodology

2.1 The group $U_n(\mathbb{Z}_p)$

We start by this following definition.

Definition 2.1.1. *Let $\mathcal{R}$ be a commutative ring. Let $U_n(\mathcal{R}) \leq GL_n(\mathcal{R})$ be the subgroup of upper triangular matrices, i.e. $U_n(\mathcal{R}) = \left\{ \begin{pmatrix} 1 & a_{12} & & \\ & \ddots & \ddots & \\ & & & 1 \end{pmatrix} \right\}$*

Looking deeper into the structure of $U_n(\mathbb{Z}_p)$, we observe that $U_n(\mathbb{Z}_p)$ can be generated by matrices of the form $E_{ij} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ & \ddots & 1 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}$, where besides the elements on the main diagonal, only the element in row i and column j, satisfying the condition that $i < j$, is 1, and all the other elements are 0. It is easy to observe that $E_{ij}^m = \begin{pmatrix} 1 & 0 & \dots & 0 \\ & \ddots & m & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}$, for every $m \in \mathbb{Z}$, by simple induction.

Now we introduce a fact that is very basic to our research and will come in handy when we move from the group $U_n(\mathbb{Z}_p)$ to the appropriate Lie algebra. Taking any two such elementary matrices, E_{ij}, E_{kl}, and calculating their commutator, $[E_{ij}, E_{kl}] = E_{ij}E_{kl}E_{ij}^{-1}E_{kl}^{-1}$, we can easily check that $E_{ij}E_{kl} = E_{il}$ iff $j = k$, and $E_{ij}E_{kl} = -E_{kj}$ iff $i = l$, and $E_{ij}E_{kl} = I_n$ in any other

case. For example, $\left[\begin{pmatrix}1 & 1 & 0\\ & 1 & 0\\ & & 1\end{pmatrix}, \begin{pmatrix}1 & 0 & 0\\ & 1 & 1\\ & & 1\end{pmatrix}\right] = \begin{pmatrix}1 & 0 & 1\\ & 1 & 0\\ & & 1\end{pmatrix}$ This fact puts $U_n(\mathbb{Z}_p)$ in the category of nilpotent groups, since, taking $\mathcal{E}(\mathbb{Z}_p) : \{E_{ij} : i < j\}$, the set of $U_n(\mathbb{Z}_p)$ generators from the set of $U_n(\mathbb{Z}_p)$ generators, and observing its lower central series, we see that $\mathcal{E}_{n-1} = \{I_n\}$, which says that $U_n(\mathbb{Z}_p)$ is of nilpotency class $n-1$.

Considering the behavior of this said set of generators, we observe that we need a significantly smaller set, because, if we start only with elementary matrices of the form $E_{i,i+1}$, where $1 \leq i \leq n-1$, we can obtain any matrix E_{ij} of the wider set, by taking any chain of commutators of the form $[E_{i,i+1}, [E_{i+1,i+2}, [\ldots, [E_{i+k,j}]]]]$, where $i+k+1 = j$. We end this $U_n(\mathbb{Z}_p)$ review by stating another important fact, that $U_n(\mathbb{Z}_p)$ is torsion-free. Again, we show this by looking at the set of generators, $\mathcal{E}$, and we observe that for any $E_{ij} \in \mathcal{E}$, since E_{ij}^m, for any $m \in \mathbb{Z}$, has one element equals to m, as we saw above, clearly, $m \neq 0$, which means that there is no $m \in \mathbb{N}$, for which $E_{ij}^m = I_n$. These facts $U_n(\mathbb{Z}_p)$ place it as a group of our interest, for this research, and bring us next to its associated Lie algebra.

2.2 The algebra $L_{p,n}$

We start with E_{ij} from above and define matrices of the form $e_{ij} = E_{ij} - I_n$, in words, e_{ij} is obtained by replacing all the 1 on the main diagonal with 0. Then clearly, $e_{ij}e_{kl} = e_{il}$ where $j = k$, $e_{ij}e_{kl} = -e_{kj}$ where $i = j$, and $e_{ij}e_{kl} = 0$ in any other case.

Corollary 2.2.1. *Let $\mathcal{B}_n$ be the set $\{e_{ij} : i < j\}$, of all the matrices of the form described in 2.2.1. Then $\mathcal{B}_n$, with the standard matrix addition, and a multiplication operation $*$, defined by $e_{ij} * e_{jk} = e_{ij}e_{jk} - e_{jk}e_{ij}$, is a basis for a Lie algerba over $\mathbb{Z}_p$, which shall be denoted by $L_n(\mathbb{Z}_p)$, or L_n, for abbreviation, which is the $\mathbb{Z}_p$-algebra of all the matrices $A \in \mathcal{M}_n(\mathbb{Z}_p)$, with 0 on the main diagonal. The multiplication operation $*$ shall be denoted by Lie Brackets, that is, $e_{ij} * e_{jk} = [e_{ij}, e_{jk}]$.*

Proof. Since we have defined the multiplication operation as the standard Lie brackets, for matrix Lie algebras, i.e., $[A, B] = AB - BA$, for all the matrices A, B in the algebra, one easily checks that all the axioms of a Lie algebra hold for this definition. Obviously, L_n is a $\mathbb{Z}_p$-span of $\mathcal{B}_n$, since every

matrix of the form $A = \begin{pmatrix} 0 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 0 & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_{n-1n} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ is a linear combination of matrices of $\mathcal{B}_n$, i.e., $A = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} a_{ij} e_{ij}$. We can observe that if $B = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} b_{ij} e_{ij} = 0_n$, then clearly all the b_{ij} are 0. We conclude that $\mathcal{B}_n$ is a basis for L_n. □

Proposition 2.2.2. *Let p be a prime number, and let $n \in \mathbb{N}$ be any natural number, then dim $L_n(\mathbb{Z}_p) = \binom{n}{2}$*

Proof. From 2.2.2, we have that a basis for $L_n(\mathbb{Z}_p)$ is the set of all e_{ij}, where $i < j$. For each row $1 \leq i \leq n-1$, we have $n - i$ elements of the form e_{ij}, which gives, in total, $\frac{n(n-1)}{2} = \frac{n!}{2!(n-2)!} = \binom{n}{2}$ elements of the the basis. □

Proposition 2.2.3. *Let p be a prime number, and let $n \in \mathbb{N}$ be any natural number, then $L_n(\mathbb{Z}_p)$ is a nilpotent Lie algebra.*

Proof. It is followed directly from 2.2.1, and from 2.1.9, since $[e_{ij}, e_{jk}] = [E_{ij}, E_{jk}] - I_n = E_{ik} - I_n = e_{ik}$, where the first brackets are Lie Brackets of $L_n(\mathbb{Z}_p)$, and the second brackets are a group commutator of $U_n(\mathbb{Z}_p)$. □

By considering the behavior of $\mathcal{L}_n(\mathbb{Q}_p)$ under the Lie brackets, we can learn about the structure of $Aut_{\mathbb{Q}_p}(\mathcal{L}_n)$. As a basic fact, every $\mathcal{L}_n(\mathbb{Q}_p)$-automorphism φ must obey the $\mathcal{L}_n$ Lie brackets, meaning that for all $x, y \in \mathcal{L}_n$, we must have that $\varphi([x, y]) = [\varphi(x), \varphi(y)]$. Let $B = \{b_1, b_2, \dots, b_m\}$ be a basis for $\mathcal{L}_n$, we have that $x = \sum_{i=1}^{m} \lambda_i b_i$, and $y = \sum_{i=1}^{m} \rho_i b_i$, so $\varphi([x, y]) = [\varphi(\sum_{i=1}^{m} \lambda_i b_i), \varphi(\sum_{i=1}^{m} \rho_i b_i)] = [\sum_{i=1}^{m} \varphi(\lambda_i b_i), \sum_{i=1}^{m} \varphi(\rho_i b_i)] = [\sum_{i=1}^{m} \lambda_i \varphi(b_i), \sum_{i=1}^{m} \rho_i \varphi(b_i)] = \sum_{i=1}^{m} \sum_{j=1}^{m} [\lambda_i \varphi(b_i), \rho_j \varphi(b_j)] = \sum_{i=1}^{m} \sum_{j=1}^{m} \lambda_i \rho_j [\varphi(b_i), \varphi(b_j)]$. This technique can be demonstrated in the most simple case, which is the Heisenberg group.

2.3 The Heisenberg group

Definition 2.3.1. *The **Heisenberg group** is the unipotent group of 3×3 matrices, over $\mathbb{Q}_p$, namely $U_3(\mathbb{Q}_p)$. Every matrix $A \in U_3$ is of the form*

$$\begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix}$$

where $a_1, a_2, a_3 \in \mathbb{Q}_p$.

The $\mathbb{Q}_p$-algebra associated with U_3 consists of matrices of the form

$$A - I_3 = \begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} = a_{12}e_{12} + a_{13}e_{13} + a_{23}e_{23}$$

. Let $\varphi \in Aut_{\mathbb{Q}_p}(\mathcal{L}_p)$ be an $\mathcal{L}_{p,n}$-automorphism. The image of every $A \in \mathcal{L}_{p,n}$, as a linear combination of elements of the basis, is a linear combination of the images of these elements. So, let $v = (x, y, z) = xe_{12} + y_{23} + z_{13}$, where $x, y, z \in \mathbb{Q}_p$, we have that $\varphi(v) = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} =$
$\begin{pmatrix} a_{11}x + a_{12}x + a_{13}x & a_{21}y + a_{22}y + a_{23}y & a_{31}z + a_{32}z + a_{33}z \end{pmatrix} =$
$\begin{pmatrix} (a_{11} + a_{12} + a_{13})x & (a_{21} + a_{22} + a_{23})y & (a_{31} + a_{32} + a_{33})z \end{pmatrix} = \begin{pmatrix} \varphi(x) & \varphi(y) & \varphi(z) \end{pmatrix}$,
which means that

$$\varphi(e_{12}) = a_{11}e_{12} + a_{12}e_{23} + a_{13}e_{13}$$

$$\varphi(e_{23}) = a_{21}e_{12} + a_{22}e_{23} + a_{23}e_{13}$$

$$\varphi(e_{13}) = a_{31}e_{12} + a_{32}e_{23} + a_{33}e_{13}$$

. We want to find relations between the elements of φ. Considering the fact that $[\varphi(x), \varphi(y)] = \varphi([x, y]) =$, we observe that the Lie brackets on images of any two commuting elements of the basis give 0, as they are images of 0, i.e., for every $x, y \in \mathcal{L}_n$, such that $[x, y] = 0$, we have that $[\varphi(x), \varphi(y)] = \varphi([x, y]) = \varphi(0) = 0$. Hence, the only images that do not vanish under Lie brackets are $[\varphi(e_{12}), \varphi(e_{23})] = [a_{11}e_{12} + a_{12}e_{23} + a_{13}e_{13}, a_{21}e_{12} + a_{22}e_{23} + a_{23}e_{13}] = a_{11}a_{21}[e_{12}, e_{12}] + a_{11}a_{22}[e_{12}, e_{23}] + \cdots + a_{13}a_{23}[e_{13}, e_{13}] = \varphi([e_{12}, e_{23}]) = \varphi(e_{13}) = a_{31}e_{12} + a_{32}e_{23} + a_{33}e_{13}$. Considering again only the non-vanishing Lie brackets, we have that $[\varphi(e_{12}), \varphi(e_{23})] = a_{11}a_{22}[e_{12}, e_{23}] + a_{12}a_{21}[e_{23}, e_{12}] = a_{11}a_{22}e_{13} - a_{12}a_{21}e_{13} = (a_{11}a_{22} - a_{12}a_{21})e_{13} = a_{31}e_{12} + a_{32}e_{23} + a_{33}e_{13} = \varphi(e_{13})$. Comparing the scalars, for the three elements of the basis, gives the following relations,

$$a_{31} = 0$$

$$a_{32} = 0$$

$$a_{33} = (a_{11}a_{22} - a_{12}a_{21}) \neq 0$$

which gives the following matrix,

$$\varphi(v) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & det(A) \end{pmatrix}$$

where A is the minor

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

We can observe that for every $v \in \mathcal{L}_{p,n}$, writing $M = \varphi(v)$ lines in the following way,

$$M = \begin{pmatrix} \varphi(e_{12}) \\ \varphi(e_{23}) \\ \varphi(e_{n-1n}) \\ \varphi(e_{13}) \\ \vdots \\ \varphi(e_{n-1n}) \\ \vdots \\ \varphi(e_{1n}) \end{pmatrix}$$

where $m = \binom{n}{2}$, divides M to a block matrix,

$$M = \left(\begin{array}{c|c|c|c|c} M_{11} & M_{12} & \dots & M_{1n-1} & M_{1n} \\ \hline M_{21} & M_{22} & \dots & M_{2n-1} & M_{2n} \\ \hline \vdots & \vdots & \dots & \vdots & \vdots \\ \hline M_{n1} & M_{n2} & \dots & M_{nn-1} & M_{nn} \end{array}\right)$$

where $M_{ij} \in \mathcal{M}_{k\times l}(\mathbb{Q}_p)$, k =dim$(\gamma_i\mathcal{L}), l$ =dim$(\gamma_j\mathcal{L})$. From this, we can understand that the blocks on the main diagonal of M are squared matrices, $A_{ii} \in \mathcal{M}_{n-i}$. From the calculation on $\mathcal{L}_{p,3}$, we understand also that any element $e_{ii+k} \in \gamma_k\mathcal{L}_{p,n}$ must vanish in the images of elements from higher nilpotency classes, i.e. $\varphi(e_{i,i+l})$, where $l > k$, which means that all the elements under every squared block on the main diagonal must be zero, so M has the form,

$$M = \left(\begin{array}{c|c|c|c|c|c} M_{11} & M_{12} & M_{13} & \dots & M_{1m-1} & M_{1m} \\ \hline 0 & M_{22} & M_{23} & \dots & M_{2m-1} & M_{2m} \\ \hline \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ \hline 0 & 0 & 0 & \dots & M_{2m-1} & M_{2m} \\ \hline 0 & 0 & 0 & \dots & 0 & M_{mm} \end{array}\right)$$

We observe that the matrix M_{ij} blocks represent quotients of the form ${}^{\gamma_i\mathcal{L}_{p,n}}/_{\gamma_{i+1}\mathcal{L}_{p,n}}, {}^{\gamma_j\mathcal{L}_{p,n}}/_{\gamma_{j+1}\mathcal{L}_{p,n}}$. We shall state, as a fact, that the block M_{11} is either diagonal or anti-diagonal, i.e.,

$$M_{11} = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}$$

or

$$M_{11} = \begin{pmatrix} & & & \lambda_1 \\ & & \lambda_2 & \\ & \iddots & & \\ \lambda_n & & & \end{pmatrix}$$

In the case of an anti-diagonal block, we have the following proposition,

Proposition 2.3.2. *Let p be a prime number, and let $n \in \mathbb{N}$. $B_n = \{e_1, \ldots, e_{m-1}\}$, where $m = \binom{n}{2}$. Then, the map $\eta_n : B_n \to B_n$, defined by $\eta_n(e_i) := e_{m-i}$ is a $\mathcal{L}_{p,n}$-automorphism, which is also an involution.*

Proof. Clearly, η_n is the anti-diagonal $m \times m$ matrix,

$$\eta_n = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{pmatrix}$$

η_n is an invertible matrix, which operates on any vector

$$v = (a_1, a_2, \ldots, a_{m-1}) = \sum_{i=1}^{m-1} a_i e_i$$

in the following way,

$$\eta_n(v) = \eta_n\left(\sum_{i=1}^{m-1} a_i e_i\right) = \begin{pmatrix} a_1 & a_2 & \ldots & a_{m-1} \end{pmatrix} \begin{pmatrix} & & & 1 \\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{pmatrix} = \begin{pmatrix} a_{m-1} & a_{m-2} & \ldots & a_1 \end{pmatrix} =$$

$$\begin{pmatrix}\eta_n(a_1) & \eta_n(a_2) & \dots & \eta_n(a_{m-1})\end{pmatrix} = \sum_{i=1}^{m-1} \eta_n(a_i e_i) = \sum_{i=1}^{m-1} a_i \eta_n(e_i)$$

And, $\eta_n^2(v) = \eta_n(\eta_n(v)) = \eta_n\left(\eta_n\left(\sum_{i=1}^{m-1} a_i e_i\right)\right) = \eta_n\left(\sum_{i=1}^{m-1} a_i \eta_n(e_i)\right) = \sum_{i=1}^{m-1} a_i \eta_n^2(e_i) = \sum_{i=1}^{m-1} a_i \eta_n(e_{n-i}) = \sum_{i=1}^{m-1} a_i e_i$ □

From this proposition, we realize that if M_{11} is anti-diagonal, then $\eta_n\varphi$ is the automorphism which has that M_{11} is diagonal.

Proposition 2.3.3. *Let p be a prime number, and let $n \in \mathbb{N}$, and let $M = \varphi \in \mathcal{L}_{p,n}$. Then, all the blocks on the main diagonal, $M_{ii}, \dots, M_{n-1n-1}$, are diagonal, of the form,*

$$M = \varphi = \begin{pmatrix} \lambda_1 & & & & & & & & & & \\ & \lambda_2 & & & & & & & & & \\ & & \ddots & & & & & & & & \\ & & & \lambda_n & & & & & & & \\ & & & & \lambda_1\lambda_2 & & & & & & \\ & & & & & \lambda_2\lambda_3 & & & & & \\ & & & & & & \ddots & & & & \\ & & & & & & & \lambda_{n-1}\lambda_n & & & \\ & & & & & & & & \ddots & & \\ & & & & & & & & & \lambda_1\lambda_2\cdots\lambda_n \end{pmatrix}$$

Proof. By simple induction. We have already assumed that M_{11} is diagonal. Every sequential block M_{ii} contains the coefficients of elements of ${}^{\gamma_i\mathcal{L}_{p,n}}/_{\gamma_{i+1}\mathcal{L}_{p,n}}$ as summands in images of elements of the same quotient algebra. So, $\varphi(e_{ii+2}) = \sum_{i=1}^{n-2} a_{ii+2} e_{ii+2}$, but $e_{ii+2} = [e_{ii+1}, e_{i+1i+2}]$, so $\varphi(e_{ii+2}) = [\varphi(e_{ii+1}), \varphi(e_{i+1i+2})]$, hence, $\lambda_{i+2} = a_{ii+2} = a_{ii+1}a_{i+1i+2} = \lambda_i\lambda_{i+1}$, which proves the proposition. □

Proposition 2.3.4. *Let $n \in \mathbb{N}$, and let*

$$A_n = \begin{pmatrix} \lambda_1 & & & & & & & & & & \\ & \lambda_2 & & & & & & & & & \\ & & \ddots & & & & & & & & \\ & & & \lambda_n & & & & & & & \\ & & & & \lambda_1\lambda_2 & & & & & & \\ & & & & & \lambda_2\lambda_3 & & & & & \\ & & & & & & \ddots & & & & \\ & & & & & & & \lambda_{n-1}\lambda_n & & & \\ & & & & & & & & \ddots & & \\ & & & & & & & & & \lambda_1\lambda_2\cdots\lambda_n \end{pmatrix}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Q}_p$, then, $det(A_n) = \prod_{i=1}^{n} \lambda_i^{i(n+1-i)}$.

Proof. We observe that the determinants, for $n = 1, 2, 3, \ldots$, form a recursive sequence,

$$\begin{aligned} det(A_1) &= \lambda_1 \\ det(A_2) &= det(A_1)\lambda_1\lambda_2^2 \\ det(A_3) &= det(A_2)\lambda_1\lambda_2^2\lambda_3^3 \\ &\vdots \\ det(A_n) &= det(A_{n-1})\lambda_1\lambda_2^2\lambda_3^3\cdots\lambda_n^n \end{aligned}$$

Calculating the general element, $a_n = det(A_n)$, we see that we have n times λ_1, $n-1$ times λ_2^2, $n-2$ times λ_3^3, and so forth. In general, we have $n-i+1$ times λ_i^i, which means that we have $i(n-i+1)$ times λ_i, and in total, $a_n = det(A_n) = \prod_{i=1}^{n} \lambda_i^{i(n+1-i)}$. □

This means that every $M = \varphi \in \mathcal{L}_{p,n}$ is of the form,

$$M = \varphi = \left(\begin{array}{c|c|c|c|c} \begin{matrix}\lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n\end{matrix} & M_{12} & M_{13} \quad \dots & M_{1m-1} & M_{1m} \\ \hline \begin{matrix}0\end{matrix} & \begin{matrix}\lambda_1\lambda_2 & & & \\ & \lambda_2\lambda_3 & & \\ & & \ddots & \\ & & & \lambda_{n-1}\lambda_n\end{matrix} & M_{23} \quad \dots & M_{2m-1} & M_{2m} \\ \hline \vdots & \vdots & \vdots \quad \dots & \vdots & \vdots \\ \hline 0 & 0 & 0 \quad \dots & M_{2m-1} & M_{2m} \\ \hline 0 & 0 & 0 \quad \dots & 0 & \lambda 1 \lambda 2 \cdots \lambda_n \end{array}\right)$$

The above discussion gives rise to the decomposition of each $\varphi \in \mathcal{L}_{p,n}$ to two matrices, one is the diagonal matrix

$$h = \begin{pmatrix} \lambda_1 & & & & & & & & & \\ & \lambda_2 & & & & & & & & \\ & & \ddots & & & & & & & \\ & & & \lambda_n & & & & & & \\ & & & & \lambda_1\lambda_2 & & & & & \\ & & & & & \lambda_2\lambda_3 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & \lambda_{n-1}\lambda_n & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & \lambda_1\lambda_2\cdots\lambda_n \end{pmatrix}$$

and the other matrix is

$$n = \begin{pmatrix} 1 & * & * & * & * & * & * & * \\ & 1 & * & * & * & * & * & * \\ & & \ddots & * & * & * & * & * \\ & & & 1 & * & * & * & * \\ & & & & 1 & * & * & * \\ & & & & & 1 & * & * \\ & & & & & & \ddots & * \\ & & & & & & & 1 \end{pmatrix}$$

So, we have the following proposition,

Proposition 2.3.5. *Let p be a prime number, and let $n \in \mathbb{N}$, and let $M = \varphi \in \mathcal{L}_{p,n}$. Then, $M = \varphi = nh$, where n and h are of the above form.*

Proof. Trivially, h is an invertible matrix, and its inverse is the matrix

$$h^{-1} = \begin{pmatrix} \lambda_1^{-1} & & & & & & & & & & & \\ & \lambda_2^{-1} & & & & & & & & & & \\ & & \ddots & & & & & & & & & \\ & & & \lambda_n^{-1} & & & & & & & & \\ & & & & (\lambda_1\lambda_2)^{-1} & & & & & & & \\ & & & & & (\lambda_2\lambda_3)^{-1} & & & & & & \\ & & & & & & \ddots & & & & & \\ & & & & & & & (\lambda_{n-1}\lambda_n)^{-1} & & & & \\ & & & & & & & & \ddots & & & \\ & & & & & & & & & (\lambda_1\lambda_2\cdots\lambda_n)^{-1} \end{pmatrix}$$

Easy to check that $n = Mh^{-1}$ is also an invertible matrix, with 1 on the main diagonal, and 0 below it. □

We observe that all the matrices with non-zero elements on the main diagonal, and 0 everywhere else form an abelian subgroup of $G_n(\mathbb{Q}_p)$, since multiplying such matrices yields a matrix of the same specification. Let

$$h_\alpha = \begin{pmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_m \end{pmatrix}, h_\beta = \begin{pmatrix} \beta_1 & & & \\ & \beta_2 & & \\ & & \ddots & \\ & & & \beta_m \end{pmatrix}$$

Then,

$$h_\alpha h_\beta = \begin{pmatrix} \alpha_1\beta_1 & & & \\ & \alpha_2\beta_2 & & \\ & & \ddots & \\ & & & \alpha_m\beta_m \end{pmatrix} = \begin{pmatrix} \beta_1\alpha_1 & & & \\ & \beta_2\alpha_2 & & \\ & & \ddots & \\ & & & \beta_m\alpha_m \end{pmatrix} = h_\beta h_\alpha$$

Obviously, this subgroup, which we shall denote as $H < G_n(\mathbb{Q}_p)$ is not normal, as we observe by taking the n matrix described above, and multiplying $A = nhn^{-1}$, clearly $A \notin H$. On the other hand, the set of all n matrices if a normal subgroup of $G_n(\mathbb{Q}_p)$, because if

$$n_\alpha = \begin{pmatrix} 1 & \alpha_{12} & \alpha_{13} & \dots & \alpha_{1m} \\ & 1 & \alpha_{23} & \dots & \alpha_{2m} \\ & & \ddots & \vdots & \vdots \\ & & & 1 & \alpha_{m-1m} \\ & & & & 1 \end{pmatrix}, n_\beta = \begin{pmatrix} 1 & \beta_{12} & \beta_{13} & \dots & \beta_{1m} \\ & 1 & \beta_{23} & \dots & \beta_{2m} \\ & & \ddots & \vdots & \vdots \\ & & & 1 & \beta_{m-1m} \\ & & & & 1 \end{pmatrix}$$

Then

$$n_\alpha n_\beta = \begin{pmatrix} 1 & \alpha_{12}+\beta_{12} & * & \dots & * \\ & 1 & * & \dots & * \\ & & \ddots & \vdots & \vdots \\ & & & 1 & \alpha_{m-1m}+\beta_{m-1m} \\ & & & & 1 \end{pmatrix}$$

which proves that all the n matrices form a subgroup, which we shall denote by $N \in G_n(\mathbb{Q}_p)$. taking any matrix, $g \in G_n(\mathbb{Q}_p)$, and taking the product $A = gng^{-1}$, if we look at the main diagonals, we see that the product is of the general form

$$gng^{-1} = \begin{pmatrix} \lambda_1 & a_{12} & \dots & a_{1m} \\ 0 & \lambda_2 & \dots & a_{2m} \\ & & \ddots & * \\ & & & \lambda_m \end{pmatrix} \begin{pmatrix} 1 & b_{12} & \dots & b_{1m} \\ 0 & 1 & \dots & b_{2m} \\ & & \ddots & * \\ & & & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^{-1} & c_{12} & \dots & c_{1m} \\ 0 & \lambda_2^{-1} & \dots & c_{2m} \\ & & \ddots & * \\ & & & \lambda_m^{-1} \end{pmatrix} =$$

$$\begin{pmatrix} 1 & d_{12} & \dots & d_{1m} \\ 0 & 1 & \dots & d_{2m} \\ & & \ddots & * \\ & & & 1 \end{pmatrix} \in N$$

So, $N \lhd G_n(\mathbb{Q}_p)$ is a normal subgroup. This discussion gives rise to the decomposition of $G_n(\mathbb{Q}_p)$. Since only N is a normal subgroup of $G_n(\mathbb{Q}_p)$, we decompose $G_n(\mathbb{Q}_p)$ to a semi-direct product, $G \cong N \rtimes H$, where the map $\phi : H \to Aut(N)$, given by $\phi(h)(n) := hnh^{-1}$, for every $h \in H$, and $n \in N$, is a homomorphism, as we can see by the fact that for every $h_1, h_2 \in H$, and for every $n \in N$, $\phi(h_1)\phi(h_2)(n) = h_1 n(h_2 n h_2^{-1})h_1^{-1} = h_1 h_2 n h_2^{-1} h_1^{-1} = (h_1 h_2)n(h_1 h_2)^{-1} = \phi(h1h2)(n)$ This means that calculating the integral, for $G_n(\mathbb{Q}_p)$, reduces to calculating a double integral, $\int_{N \rtimes H}$. We mean to show in the research that the normal subgroup N can itself be decomposed to a semi-direct product of several subgroups, thus simplyifing the integration.

By **??**, we have that any $L_p(\mathbb{Z}_p)$-automorphism must be in $G_n(\mathbb{Z}_p)$, in words, any $\varphi \in G(\mathbb{Z}_p)$ is an invertible matrix with elements in $\mathbb{Z}_p$. Our goal is to find a way to compute $G(\mathbb{Z}_p)$, the automorphism group of $L_n(\mathbb{Z}_p)$, for any $n \in \mathbb{N}$. After finding a general formula for this calculation, we shall be able to show a way to compute the n-multiple p-adic integral of the form $\int \int \cdots \int \int_{D_1 \times D_2 \cdots \times D_{n-1} \times D_n} f(h_1, h_2, \ldots, h_{n-1}, h_n) d(\mu_1, \mu_2, \ldots, \mu_{n-1}, \mu_n)$, where D_i is the set of $G(\mathbb{Z}_p)$-cosets, for $G(\mathbb{Z}_p)$, the group of $\mathbb{Z}_p$-automorphisms on the algebra $L_i(\mathbb{Z}_p)$, and h_i is any element of this group, and μ_i is the Haar measure on this group. By Fubini, this multiple integral can be calculated as the iterated integral

$$\int_{D_n} \left(\int_{D_{n-1}} \ldots \left(\int_{D_2} \left(\int_{D_1} f(h_1, h_2, \ldots, h_{n-1}, h_n) d\mu_1 \right) d\mu_2 \right) \ldots d\mu_{n-1} \right) d\mu_n$$

. Alternatively, if we do not find an explicit formula for this calculation, we will show the general approach for this calculation, and prove the necessary conditions for its validity.

3 Notations

- $\mathbb{Z}_p$, the ring of p-adic integers.
- $\mathbb{Q}_p$, the fraction field of $\mathbb{Z}_p$.
- L_p, a $\mathbb{Z}_p$-algebra over the ring of p-adic integers.
- $\mathcal{L}_p$, a $\mathbb{Q}_p$-algebra, over the fraction field of $\mathbb{Z}_p$.

- $G(L_p) := Aut_{\mathbb{Z}_p}(L_p)$, the group of $\mathbb{Z}_p$-automorphisms of L_p.
- $G(\mathcal{L}_p) := Aut_{\mathbb{Q}_p}(\mathcal{L}_p)$, the group of $\mathbb{Q}_p$-automorphisms of $\mathcal{L}_p$.