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 ${}^{G}/_{H} := \{g_1H, g_2H, \dots, g_nH\}$ 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 $v\mathcal{L}_{pn}$ is uniquely represented as a linear combination of elements of the basis, $v = \sum_{i=1}^{n} \lambda_i b_i$.

Proposition 1.2.1. *Let p be any prime number, then $L_p < \mathcal{L}_p$*

Proof. Let $B = \{b_1, \ldots, b_n\}$ a basis of $\mathcal{L}_p$, so, for any $v \in \mathcal{L}_p$, we have that $v = \lambda_1 b_1 + \cdots + \lambda_n b_n$, where $r\lambda_1, \ldots, \lambda_n \in \mathbb{Q}_p$. Obviously, for any prime number p, we have that $\mathbb{Z}_p \subset \mathbb{Q}_p$, in other words, $\iota : \mathbb{Z}_p \to \mathbb{Q}_p$ is a monomorphism of rings. This means that the ring $\mathbb{Z}_p$ acts on the left $\mathbb{Q}_p$-module $\mathcal{L}_p$ by restriction of scalars, that is, for every $r \in \mathbb{Z}_p$, and $s \in \mathcal{L}_p$, we have that $rs := \iota(r)s$, which is well defined, because $\iota(r) \in \mathbb{Q}_p$. This means that $\mathcal{L}_p$ inherits the structure of a left $\mathbb{Z}_p$-module. We mark $L_p := \{r_1 b_1, \ldots, r_n b_n\}$, where $r1_, \ldots, r_n \in \mathbb{Z}_p$. B is generating L_p, by the construction, and it is clear that B is $\mathbb{Z}_p$-linearly-independent, since B is $\mathbb{Q}_p$-linearly-independent, and $\mathbb{Z}_p \subset \mathbb{Q}_p$. So, B is a basis also for L_p, and it is clear that any $\mathbb{Z}_p$-linear combination of vectors of B is a $\mathbb{Q}_p$-linear combination of vectors of B, hence $L_p \leq \mathcal{L}_p$. □

Proposition 1.2.2. *Let p be a prime number, and let $L_n(\mathbb{Z}_p)$ be a $\mathbb{Z}_p$-algebra, for any $n \in \mathbb{N}$, then there exists a $\mathbb{Q}_p$-algebra, denoted by $\mathcal{L}_n(\mathbb{Q}_p)$, such that 1.2.2 holds.*

Proof. We construct $\mathcal{L}_n(\mathbb{Q}_p)$ from $L_n(\mathbb{Z}_p)$ by extension of scalars. $\mathbb{Q}_p$ is a $\mathbb{Z}_p$-module, as a trivial fact, so, taking the tensor product $L_n \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, we have, for all $a \in Ł_n(\mathbb{Z}_p)$, and for all $r, r' \in \mathbb{Q}_p$, that $r'(a \otimes r) = a \otimes rr' = rr'(a \otimes 1)$, which is well-defined, because of the multiplication in $\mathbb{Q}_p$, 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 $L_n \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, we denote $\mathcal{L}_n(\mathbb{Q}_p) := L_n \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and we got that $\mathcal{L}_n(\mathbb{Q}_p)$ is a $\mathbb{Q}_p$-algebra, with the same basis, B, but with scalars from $\mathbb{Q}_p$, which proves that $L_n < \mathcal{L}_n$. □

Proposition 1.2.3. *Let $B = \{b_1, \ldots, b_n\}$ be any basis of $\mathcal{L}_p$, and $\varphi \in G(\mathbb{Q}_p)$ any $\mathbb{Q}_p$-automorphism. Then $\varphi(L_p) \subseteq L_p$ iff $\varphi(b_1), \ldots, \varphi(b_n) \in L_p$*

Proof. Clearly, if $\varphi(v) \in L_p$, for every $v \in L_p$, then also $\varphi(b_1), \ldots, \varphi(b_n) \in L_p$. We prove the opposite by taking $v = r_1 b_1 + \cdots + r_n b_n$, then $\varphi(v) = \varphi(\sum_{i=1}^n r_i b_i) = \sum_{i=1}^n \varphi(r_i b_i) = \sum_{i=1}^n r_i \varphi(b_i)$, but $\varphi(b_1), \ldots, \varphi(b_n) \in L_p$, so $\sum_{i=1}^n r_i \varphi(b_i)$ is a $\mathbb{Z}_p$-linear combination, hence $\varphi(v) \in L_p$ □

Proposition 1.2.4. *Let $G^+(\mathbb{Q}_p) := G(\mathbb{Q}_p) \cap \mathcal{M}_n(\mathbb{Z}_p) = \{\varphi \in Aut_{\mathbb{Q}_p}(\mathcal{L}_p) : \varphi \in \mathcal{M}_n(\mathbb{Z}_p)\}$, in words, all the $\mathcal{L}_p$-automorphisms, which are matrices over $\mathbb{Z}_p$. Then, $G^+(\mathbb{Q}_p)$ is a monoid.*

Proof. $G(\mathbb{Q}_p)$ is a group, thus a monoid, and $\mathcal{M}_n(\mathbb{Z}_p)$ is a monoid, so, their intersection is a monoid. □

Proposition 1.2.5. *Let $g \in G^+(\mathbb{Q}_p)$, then, the right coset $G(\mathbb{Z}_p)g \subseteq G^+(\mathbb{Q}_p)$*

Proof. Let $h \in G(\mathbb{Z}_p)$. We proved in 1.2.2 that $L_p \leq \mathcal{L}_p$, so $h \in G(\mathbb{Q}_p)$. But, $h(L_p) \subseteq L_p$, and from 1.2.4, we know that h is a $\mathbb{Z}_p$-linear combination of vectors in L_p, which means that h is a matrix with coefficients in $\mathbb{Z}_p$, that means, $h \in \mathcal{M}_n(\mathbb{Z}_p)$, so $h \in G(\mathbb{Q}_p) \cap \mathcal{M}_n(\mathbb{Z}_p)$, which means that $hg \in G(\mathbb{Q}_p) \cap \mathcal{M}_n(\mathbb{Z}_p)$. □

Corollary 1.2.6. *$G^+(\mathbb{Q}_p) = \bigsqcup_{i=1}^n G(\mathbb{Z}_p)g_i$, where $[G(\mathbb{Q}_p) : G(\mathbb{Z}_p)] = n$*

Proposition 1.2.7. *There is a bijection between $G(\mathbb{Z}_p)\backslash G^+(\mathbb{Q}_p)$ and $\{M \leq L_p : M \cong L_p\}$*

Proof. Let $\varphi \in G(\mathbb{Z}_p)g| \in G(\mathbb{Z}_p)\backslash G^+(\mathbb{Q}_p)$, and let $M = \varphi(L_p)$. But, from 1.2.6, we have that $\varphi \in G^+(\mathbb{Q}_p)$, so $M = \varphi(L_p) \subseteq L_p$. Choose a different representative $\psi \in G(\mathbb{Z}_p)g$, we have that $\tau = \psi\varphi^{-1} \in G(\mathbb{Z}_p)$, which means that $\tau(L_p) = L_p$. But $\tau\varphi = \psi\varphi^{-1}\varphi = \psi$, which means that $\psi(L_p) = \tau\varphi(L_p) = \varphi(\tau(L_p)) = \varphi(L_p) = M$, so we have that M is the image of any representative of $G(\mathbb{Z}_p)g$. Let $\varphi|_{L_p} : L_p \to M$ be the restriction of φ to L_p. Obviously, $\varphi|_{L_p}$ is onto M, and is one-to-one, as a restriction of an automorphism. So we have that $\varphi|_{L_p}$ is an isomorphism, which means that $L_p \cong M$. So, we conclude that every right coset of the form $G(\mathbb{Z}_p)g$ defines an isomomorphism of the form $L_p \cong M$. For the opposite direction, we show that for every isomorphism $L_p \cong M$, we can find some $\varphi \in G^+(\mathbb{Q}_p)$, for which $\varphi(L_p) = M$. Choose another automoprhism, $\psi \in G^+(\mathbb{Q}_p)$, such that $\psi(L_p) = M$, and let $\tau = \varphi\psi^{-1}$. But $\tau(L_p) = \varphi\psi^{-1}(L_p) = \psi^{-1}(\varphi(L_p)) = \psi^{-1}(M) = L_p$, which means that $\tau \in G(\mathbb{Z}_p)$. But $\tau\psi = \varphi\psi^{-1}\psi = \varphi \in G(\mathbb{Z}_p)\psi$, and, obviously, $\tau^{-1}\varphi = \tau^{-1}\tau\psi = \psi$ means that also $\psi \in G(\mathbb{Z}_p)\varphi$, so φ andf ψ are in the same right coset of $\mathbb{Z}_p$, so we have that every isomorphism $L_p \cong M$ is common to all representatives of the same right coset of $G(\mathbb{Z}_p)$, proving the bijection. □

Proposition 1.2.8. *Let $G(\mathbb{Z}_p)g \in G(\mathbb{Z}_p)\backslash G^+(\mathbb{Q}_p)$ be a right coset, and $M \leq L_p$ the image of this coset, as constructed in 1.2.8, then $[L_p : M] = |detg|_p^{-1}$.*

1.3 p-adic Integration

Proposition 1.3.1. *Let Γ be a topological group, and let $U \subseteq \Gamma$, be an open subset in Γ. Then $\gamma U := \{\gamma u : \gamma \in \Gamma, u \in U\}$ is also an open subset of Γ.*

Proof. 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 continuous maps, that is, the inverse map $\gamma \mapsto \gamma^{-1}$, and the multiplication map $(\gamma^{-1}, g) \mapsto \gamma^{-1}g$, so any inverse image f^{-1} of an open subset is an open subset. But $f^{-1}(U) = \{g \in G : f(g) = \gamma^{-1}g \in U\} = \{\gamma h : f(\gamma h) = \gamma^{-1}\gamma h = h \in U\} = \{\gamma h : h \in U\} = \gamma U$, which proves that γU is an open subset in Γ. $\square$

Proposition 1.3.2. *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***

Proposition 1.3.3. *Let p be a prime number, then $G(\mathbb{Q}_p)$ is a locally compact topological group.*

Proposition 1.3.4. *Let p be a prime number, then $G(\mathbb{Q}_p)$ has a unique right Haar measure μ, with the following property: $\mu(G(\mathbb{Z}_p)) = 1$.*

Corollary 1.3.5. *For every $g \in G(\mathbb{Q}_p)$, we have that $\mu(G(\mathbb{Z}_p)g) = \mu(G(\mathbb{Z}_p)) = 1$*

Proposition 1.3.6. *Let p be a prime number, $s \in \mathbb{C}$, and let $g \in G^+(\mathbb{Q}_p)$, then $|det(g)|_p^s = \int_{h \in G^+(\mathbb{Q}_p)} |det(h)|_h^s d\mu$.*

Proof. We saw in 1.2.9 that for every $g \in G(\mathbb{Z}_p)h$, we have that $|det(g)|_p^{-1}$ does not depend on the choice of representative, which means that $|det(g)|_p$ is constant on the entire coset, which means that $|det(g)|_p = |det(h)|_p$. so, $|det(g)|_p^s = \int_{h \in G^+(\mathbb{Q}_p)} |det(h)|_p^s d\mu = \int_{h \in G^+(\mathbb{Q}_p)} |det(g)|_p^s d\mu = |det(g)|_p^s \int_{h \in G^+(\mathbb{Q}_p)} d\mu$. But, $\mu = \mu(G(\mathbb{Z}_p)h)$, and we saw in 1.3.5 that $\mu(G(\mathbb{Z}_p)h) = \mu(G(\mathbb{Z}_p)) = 1$, so $\int_{h \in G^+(\mathbb{Q}_p)} |det(h)|_p^s d = |det(g)|_p^s \int_{h \in G^+(\mathbb{Q}_p)} d\mu = |det(g)|_p^s \cdot 1 = |det(g)|_p^s$ $\square$

Corollary 1.3.7. *Let p be a prime number, $s \in \mathbb{C}$, then* $\widehat{\zeta_{L,p}}(s) = \sum_{G(\mathbb{Z})g \in G(\mathbb{Z}_p) \backslash G^+(\mathbb{Q}_p)} |det(g)|_p^s = \sum_{G(\mathbb{Z})g \in G(\mathbb{Z}_p) \backslash G^+(\mathbb{Q}_p)} \int_{h \in G(\mathbb{Z}_p)g} |det(h)|_p^s d\mu = \int_{h \in G^+(\mathbb{Q}_p)} |det(h)|_p^s d\mu$

Theorem 1.3.8. *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 $\widehat{\zeta_{L,p}}(s) = w_p(p^{-s})$.*

2 Research Goals and Methodology

2.1 The group U_n

Proposition 2.1.1. *Let $A \in \mathcal{M}_n(\mathbb{Z}_p)$, then $A \in GL_n(\mathbb{Z}_p)$ iff $det(A) = \pm 1$*

Proof. We shall prove only one direction. Assume $det(A) = \pm 1$. For A, we calculate the adjoint matrix, $Adj(A)$, by calculating minors for all the elements of A, and create the cofactor matrix of A, then take the transpose of the cofactor matrix. With this calculation, $A^{-1} = \frac{Adj(A)}{det(A)}$, and, since calculating minors requires multiplication and subtraction between elements of the A. But $\mathbb{Z}_p$ is a ring, so closed under multiplication and subtraction, hence all the minors are also in the ring, which means that $Adj(A) \in \mathcal{M}_n(\mathbb{Z}_p)$. But $det(A) = \pm 1$, so $A^{-1} = \frac{Adj(A)}{det(A)} = \pm 1 \cdot Adj(A) \in \mathcal{M}_n(\mathbb{Z}_p)$, which means that $A, A^{-1} \in GL_n(\mathbb{Z}_p)$. □

Corollary 2.1.2. *Let A be a $n \times n$ matrix, with 1 on the main diagonal, and $a_{ij} \in \mathbb{Z}_p$, where $i < j$, and all the other elements, namely, the elements below the main diagonal, are 0. Then every matrix A of this form has an inverse matrix, A^{-1}, of the same form.*

Proof. One checks that all the minors of the elements on the main diagonal are 1, all the minors of the elements above the main diagonal are 0, and all the minors of the elements below the main diagonal can be any p-adic integers. constructing the cofactor matrix and transposing it, gives a matrix of the form described above, which is the inverse matrix of A, as we prove in 2.1.1. □

Corollary 2.1.3. *Let U_n be the set of all matrices of the form described in 2.1.2, then $(U_n, \cdot)$ is a group, where $\cdot$ is the standard matrix multiplication.*

Proof. One checks that multiplying two matrices in U_n gives a product matrix of the same form. Associativity comes from the standard matrix multiplication, and clearly, the standard unit matrix, I_n, is also in U_n. By 2.1.2, we know that A has an inverse matrix, A^{-1}, which is of the same form, hence $A^{-1} \in U_n$, which completes the proof. □

Proposition 2.1.4. *Let $E_{ij} \in U_n$, where $1 \leq i < j \leq n$, be a $n \times n$ matrix, with 1 on the main diagonal, and $a_{ij} = 1$, and 0 anywhere else. Then, E_{ij}^m is a matrix of the same form, except that $a_{ij} = m$.*

Proof. By induction on m. For $m = 1$, $E^1_{ij} = E_{ij}$, so, trivially, $a_{ij} = 1 = m$. For $m+1$, we have that $E^{m+1}_{ij} = E^m_{ij} E_{ij}$. But E^m_{ij} has that $a_{ij} = m$, by the assumption, and one checks that $E^m_{ij} E_{ij} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & m & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} =$ $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & m+1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, which proves the induction step, and the proposition. □

Corollary 2.1.5. *Let $A = E^m_{ij}$, and $B = E^r_{ij}$. Then, $D = AB = E^m_{ij} E^r_{ij}$ is the matrix with 1 on the main diagonal, $d_{ij} = m + r$, and all the other elements are 0.*

Proof. One checks that the product matrix has also 1 on the main digonal, and all the other elements are 0, except for $d_{ij} = 1 \cdot r + m \cdot 1 = m + r$ □

Proposition 2.1.6. *Let $E_{ij} \in U_n$ be a matrix of the form described in 2.1.4. then E^{-m}_{ij} is a matrix of the same form, but with $a_{ij} = -m$.*

Proof. From 2.1.4, we have that $E^m_{ij} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & m & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$. From 2.1.2, we know that $B = (E^m_{ij})^{-1} \in U_n$, that is, $B = \begin{pmatrix} 1 & b_{12} & \dots & \dots & b_{1n} \\ 0 & 1 & b_{23} & \dots & b_{2n} \\ 0 & 0 & 1 & bij & b_{in} \\ 0 & 0 & 0 & 1 & b_{n-1n} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, which means that $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & m & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_{12} & \dots & \dots & b_{1n} \\ 0 & 1 & b_{23} & \dots & b_{2n} \\ 0 & 0 & 1 & b_{ij} & b_{in} \\ 0 & 0 & 0 & 1 & b_{n-1n} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

Easy to check that all the elements b_{kl} must be 0, but for the element in row i and column j, we must have that $1 \cdot b_{ij} + m \cdot 1 = 0$, which means that $b_{ij} = -m$. One checks that the same calculation holds for $(E_{ij}^{-1})^m$, and so, $E_{ij}^{-m} = (E_{ij}^m)^{-1} = (E_{ij}^{-1})^m$ is of the form described above. $\square$

Proposition 2.1.7. *Let $A = E_{ij}, B = E_{kl} \in U_n$ be two matrices of the form described in 2.1.2, i.e., 1 on the main diagonal, and all the other elements are 0, except for a_{ij} and b_{kl}, which are 1. Then the commutator,* $[E_{ij}, E_{kl}] =$
$$\begin{cases} E_{il}, & j = k \\ E_{kj}^{-1}, & i = l \\ 0, & j \neq k \wedge i \neq l \end{cases}$$

Proof. There are two cases, The first, is where $j = i + 1$, or $l = k + 1$, and the second is where $j > i + 1$, and $l > k + 1$. One checks that the proposition is true in both cases. $\square$

Corollary 2.1.8. *Let $A = E_i = E_{ii+1} \in U_n$, be a matrix of the form described in 2.1.4, where the only 1 which is outside the main diagonal is one of the elements $a_{12}, a_{23}, \ldots, a_{n-1n}$, i.e., on the diagonal above the main diagonal. Then the set $\mathcal{E}_n = \{E_1, E_2, \ldots, E_{n-1}\}$ is a set of generators for the unipotent group U_n.*

Proof. By proposition 2.1.7, we can create any matrix $E_{ij} \in U_n$ by composition of commutators of the form $[E_i, [E_{i+1}, [\ldots [E_{j-2}, E_{j-1}]]]$. From 2.1.4, we know that $A = E_{ij}^m$ has that $a_{ij} = m \in \mathbb{Z}_p$, and by 2.1.5, we know that $D = AB = E_{ij}^m E_{ij}^r$ is the matrix with 1 on the main diagonal, and all the other elements are 0, except for $d_{ij} = m + r$. Checking further gives that if $A = E_{ij}^m$ and $B = E_{jk}^r$, then the commutator $[E_{ij^m}, E_{kl}^r]$ is the matrix with 1 on the main diagonal, and all the other elements are 0, except for $d_{ik} = mr$. Easy to see how to apply the above calculations also for the inverse matrices. This means that we can generate any matrix in U_n, by multiplying matrices that come from commutators on the set $\mathcal{E}_n = \{E_1, E_2, \ldots, E_n - 1\}$, which means that $\mathcal{E}_n$ generates the unipotent group U_n. $\square$

Proposition 2.1.9. *The unipotent group U_n is nilpotent, of nilpotency class n.*

Proof. Easy to observe that for the set of generators, $\mathcal{E}_n$, the longest composition of commutators, $[E_{i_1}, [E_{i_2}, [\ldots [E_{i_k}]]]$ has that $i_1 = 1, i_2 = 2, \ldots, i_k =$

$n-1$, or $i_1 = n-1, i_2 = n-2, \ldots, i_k = 1$, which means that composing $n-1$ commutators of elements in $\mathcal{E}_n$ leaves only E_{1n-1} and E_{1n-1}^{-1}, but $[E_{1n-1}, E_{1n-1}^{-1}] = [E_{1n-1}^{-1}, E_{an-1}] = I_n$. One can check that this holds for the unipotent group U_n itself, as generated by $\mathcal{E}_n$. $\square$

Proposition 2.1.10. *The unipotent group U_n is torsion free.*

Proof. Again, we show the proposition for the set of generators, $\mathcal{E}_n$. Let $A = E_i \in \mathcal{E}_n$, and suppose it has a finite order, which means that there exists a $m \in \mathbb{N}$, such that $E_i^m = I_n$. But by 2.1.4, we know that E_i^m is the matrix with $a_{ii+1} = m$, which means that $m = 0$, which is a contradiction. $\square$

2.2 The algebra L_n

Proposition 2.2.1. *Let $E_{ij} \in \mathcal{E}_n$. Let $e_{ij} = E_{ij} - I_n$, in words, e_{ij} is obtained by replacing all the 1 on the main diagonal with 0. Then $e_{ij}e_{jk} = e_{ik}$, and $e_{jk}e_{ij} = 0_n$, where 0_n is the $n \times n$ zero matrix.*

Proof. Clearly, since $A = e_{ij}$ has a single non-zero element, $a_{ij} = 1$, and $B = e_{jk}$ has that $b_{jk} = 1$, then the product matrix $D = AB = e_{ij}e_{jk}$ has a single element, $d_{ik} = a_{ij}b_{jk} = 1 \cdot 1 = 1$, but in the product $BA = e_{jk}e_{ij}$, we observe that b_{jk} is multiplied by all the elements of the kth row of A, which is all zeros, and a_{ij} is being multiplied by the ith column of B, which is all zeros, thus the product matrix, BA, is all zeros. $\square$

Corollary 2.2.2. *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 2.2.3. *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 2.2.4. *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,

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

We observe that the matrix M_{ij} blocks represent quotients of the form ${}^{\gamma_i\mathcal{L}_{p,n}}\!\big/_{\gamma_{i+1}\mathcal{L}_{p,n}}, {}^{\gamma_j\mathcal{L}_{p,n}}\!\big/_{\gamma_{j+1}\mathcal{L}_{p,n}}$. 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 $n \in \mathbb{N}$. $B_n = \{e_1, \dots, e_{m-1}\}$, 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

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

in the following way,

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

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

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

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. $\square$

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,

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

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,

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

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. $\square$

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, $\displaystyle\int_{N \rtimes H}$. 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 1.2.4, 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 $\displaystyle\int\int\cdots\int\int_{D_1 \times D_2 \cdots \times D_{n-1} \times D_n} f(h_1, h_2, \ldots, h_{n-1}, h_n) d(\mu_1, \mu_2, \ldots, \mu_{n-1}, \mu_n)$, 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

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

. 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 $\mathcal{L}_p$.