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

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. □

Proposition 1.1.2. *Let G be a group, and let $\mathcal{N} := \{N \trianglelefteq G\}$ the set of all normal subgroups of G. Let $I \subset \mathbb{N}$ be a set of indices, for which we shall define the following partial order, $\forall i, j \in I$, $i \leq j$ iff $N_j \subseteq N_i$ iff ${}^{G}/_{N_i} \subseteq {}^{G}/_{N_j}$. So, for each $i \leq j$, there exists an epimorphism $\pi_{ji} : {}^{G}/_{N_j} \to {}^{G}/_{N_i}$, which projects ${}^{G}/_{N_j}$ onto ${}^{G}/_{N_i}$. Then,*

- *I is a directed set.*
- *$\{{}^{G}/_{N_k}\}_{k\in I}$ is a projective system.*
- *$\widehat{G} = \varprojlim\{{}^{G}/_{N_k}\}_{k\in I} := \{(h_k)_{k\in I} \in \prod_{k\in I} {}^{G}/_{N_k} : \pi_{ji}(h_j) = h_i, \forall i \leq j\}$ is an inverse limit of $\{{}^{G}/_{N_k}\}_{k\in I}$*

Proof. One checks that all the above is according to the definitions. □

Proposition 1.1.3. *Let G be any group, with $\widehat{G}$ defined as above. Then there is a canonical homomorphism, $\varphi : G \to \widehat{G}$, defined by $\forall g \in G, \varphi(g) := (gN_k)_{k\in I}$, and $ker\varphi = \bigcap_{k\in I} N_k$*

Proof. Easy to verify that φ is a well-defined homomorphism. Let $g \in \bigcap_{k\in I} N_k$. then $\forall k \in I, gN_k = N_k$, then $\varphi(g) = (gN_k)_{k\in I} = (N_k)_{k\in I} = ([e] \in {}^{G}/_{N_k})_{k\in I} = [e] \in \prod_{k\in I} {}^{G}/_{N_k}$ □

Definition 1.1.4. *Let G be any group. a subgroup $H \leq G$ is called **pro-isomorphic**, if $\widehat{H} \cong \widehat{G}$.*

Definition 1.1.5. *Let G be any group, and let $\widehat{a_n}(G) := \#\{H \leq G : \widehat{H} \cong \widehat{G}, [G : H] = n\}$, in words, the number of pro-isomorphic subgroups of G, of index n. The **pro-isomorphic ζ-function** of G is defined by $\widehat{\zeta_G}(s) := \sum_{i=1}^{\infty} \widehat{a_n}(G)n^{-s}$, for some $s \in \mathbb{C}$*

Example 1.1.6. *$G = (\mathbb{Z}, +)$. G is an abelian group, and every $H \leq G$ is of the form $H = n\mathbb{Z} = \langle n \rangle$, for some $n \in \mathbb{N}$, which means that $H \cong G$, as both are infinite cyclic groups. For any $n \in \mathbb{N}$, we can construct a poset of normal subgroups, of the form $\{n\mathbb{Z}, 2n\mathbb{Z}, 3n\mathbb{Z}, \dots\}$, which is naturally in bijection with the poset of all normal subgroups of $\mathbb{Z}$ itself. This construction forms a projective system, for G, and for every $H \leq G$, by taking all the quotient groups of the form ${}^{G}/_{kn\mathbb{Z}}$. From this, it is obvious that $\widehat{H} \cong \widehat{G}$, for every $H \leq G$. Any such $H = n\mathbb{Z}$ is the only subgroup of G, which is of index n, therefore, the pro-isomoprhic ζ-function of G is $\widehat{\zeta_G}(s) = \sum_{i=1}^{\infty} \widehat{a_n}(G)n^{-s}$, where $\widehat{a_n}(G) = 1$, which comes to $\widehat{\zeta_{\mathbb{Z}}} = \sum_{i=1}^{\infty} n^{-s} = \zeta(s)$, the Riemann ζ-function.*

Proposition 1.1.7. *The Riemann ζ-function is decomposing to an infinite product of ζ_p-functions, that is, $\zeta(s) = \prod_p \zeta_p(s) = \prod_p \sum_{k=0}^{\infty} \frac{1}{p^{ks}} = \prod_p \frac{1}{1-p^{-s}}$, where p is prime, and the product consists of all the prime number existing.*

Proof. $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = 1 + \frac{1}{2^{-s}} + \frac{1}{3^{-s}} + \dots$, but every $n \in \mathbb{N}$ is decomposing to a finite product of powers of primes, $n = 2^{k_2}3^{k_3}5^{k_5}\dots$, so, taking this product, $\prod_p \sum_{k=0}^{\infty} \frac{1}{p^{ks}} = (1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^s} + \dots)(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \frac{1}{3^s} + \dots)(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \frac{1}{5^s} + \dots)\cdots = \prod_p (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^s} + \dots)$, we have every expression of the form $\frac{1}{2^{k_2 s}3^{k_3 s}5^{k_5 s}\dots}$, where the denominator is a finite product of powers of primes, and each expression is uniquely existing in this product. From this, it is obvious that this product forms an infinite sum of expressions of the form $\frac{1}{n^s}$, where every $n \in \mathbb{N}$ is uniquely existing. This means that $\prod_p \sum_{k=0}^{\infty} \frac{1}{p^{ks}} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{5^s} + \dots = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$. This decomposition is called **Euler Decomposition**. One checks that if $Re(s) > 0$, then the sum of the geometric series is $\sum_{k=0}^{\infty} \frac{1}{p^{ks}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \dots = \frac{1}{1-p^{-s}}$, so $\prod_p \sum_{k=0}^{\infty} \frac{1}{p^{ks}} = \prod_p \frac{1}{1-p^{-s}} = \prod_p \zeta_p(s)$, which completes the proof. □

Proposition 1.1.8. *Let G be any finitely-generated, nilpotent and torsion-free group, then we have the same decomposition as above, for the pro-isomorphic ζ-function, $\widehat{\zeta_G}(s) = \prod_p \widehat{\zeta_{G,p}}(s)$*

Definition 1.1.9. *Let G be any group, then the **lower central series** of G is series 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 1.1.10. *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.*

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 $\mathbb{Z}_p$.

Proposition 1.2.1. *Let $\mathcal{L}_p$ be any $\mathbb{Q}_p$-algebra, with $n = dim\mathcal{L}_p$. Then $G(\mathbb{Q}_p) \leq GL_n(\mathbb{Q}_p)$. This is true for any field $\mathbb{F}$ and $\mathbb{F}$-algebra $\mathcal{L}_\mathbb{F}$.*

Proof. Choose a basis $B = \{b_1, \ldots, b_n\}$ of $\mathcal{L}_p$. Let $\varphi \in G(\mathcal{L}_p)$, and $v \in \mathcal{L}_p$. B is a basis, so there are $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}_p$, such that $v = \lambda_1 b_1, \ldots, \lambda_n b_b$. Then, $\varphi(v) = \varphi(\sum_{i=1}^n \lambda_i b_i) = \sum_{i=1}^n \varphi(\lambda_i b_i) = \sum_{i=1}^n \lambda_i \varphi(b_i)$. Mark $B_\varphi = \{\varphi(b_1), \ldots, \varphi(b_n)\}$. B_φ must span $\mathcal{L}_p$, otherwise, there exists a vector $u \in \mathcal{L}_p$, such that $\sum_{i=1}^n \rho_i \varphi(b_i) \neq u$, for any $\rho_1, \ldots, \rho_n \in \mathbb{Q}_p$. But $u = \sum_{i=1}^n \tau_i b_i$, φ is an automoprhism, so $u = \varphi\varphi^{-1}(u) = \varphi(\varphi^{-1}(\sum_{i=1}^n \tau_i b_i)) = \varphi(\sum_{i=1}^n \varphi^{-1}(\tau_i b_i)) = \varphi(\sum_{i=1}^n \tau_i \varphi^{-1}(b_i)) = \sum_{i=1}^n \varphi(\tau_i \varphi^{-1}(b_i)) = \sum_{i=1}^n \tau_i \varphi(\varphi^{-1}(b_i)) = \sum_{i=1}^n \tau_i b_i$, in contradiction to the assumed. B_φ is also linearly-independent, because, supposed that $\sum_{i=1} \rho_i \varphi(bi) = 0$, then, since φ is an automorphism, must be that $\varphi^{-1}(\sum_{i=1} \rho_i \varphi(bi)) = 0$, which means that $\sum_{i=1} \varphi^{-1}(\rho_i \varphi(bi)) = \sum_{i=1} \rho_i \varphi^{-1}(\varphi(bi)) = \sum_{i=1} \rho_i b_i = 0$, which contradicts to thew fact that B is a basis. So, B_φ is also a basis of $\mathcal{L}_p$. It is immediate to conclude that the matrix representing φ is an inverse $n \times n$ matrix, which means that $\varphi \in GL_n(\mathbb{Q}_p)$, and that $\forall \varphi, \psi \in G(\mathbb{Q}_p)$, their compositions $\varphi\psi$, and $\psi\varphi$ are also in $G(\mathbb{Q}_p)$, which means that $G(\mathbb{Q}_p) \leq GL_n(\mathbb{Q}_p)$. □

Proposition 1.2.2. *Let p be any prime number, then $L_p \leq \mathcal{L}_p$*

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 1.2.3. *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 1.2.3, 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 1.2.5, 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 1.2.7, 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. □

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 1.2.8 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 $\int_{h \in G^+(\mathbb{Q}_p)} |det(h)|_p^s d = |det(g)|_p^s \int_{h \in G^+(\mathbb{Q}_p)} d\mu = |det(g)|_p^s \cdot 1 = |det(g)|_p^s$ □

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

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 $m = 1$, $E_{ij}^1 = E_{ij}$, so, trivially, $a_{ij} = 1 = m$. For $m+1$, we have that $E_{ij}^{m+1} = E_{ij}^m E_{ij}$. But E_{ij}^m has that $a_{ij} = m$, by the assumption, and one checks that $E_{ij}^m E_{ij} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & m & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} =$

$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & m+1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, which proves the induction step, and the proposition. □

Corollary 2.1.5. *Let $A = E_{ij}^m$, and $B = E_{ij}^r$. Then, $D = AB = E_{ij}^m E_{ij}^r$ 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_{ij}^{-m} is a matrix of the same form, but with $a_{ij} = -m$.*

Proof. From 2.1.4, we have that $E_{ij}^m = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & m & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$. From 2.1.2, we

know that $B = (E_{ij}^m)^{-1} \in U_n$, 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. □

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. □

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 $a_{12}, a_{23}, \dots, a_{n-1n}$, i.e., on the diagonal above the main diagonal. Then the set $\mathcal{E}_n = \{E_1, E_2, \dots, E_{n-1}\}$ 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 $[E_i, [E_{i+1}, [\dots [E_{j-2}, E_{j-1}]]]]$. 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. □

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^{-1}_{1n-1}, but $[E_{1n-1}, E^{-1}_{1n-1}] = [E^{-1}_{1n-1}, E_{an-1}] = I_n$. One can check that this holds for the unipotent group U_n itself, as generated by $\mathcal{E}_n$. □

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 $E^m_i = I_n$. But by 2.1.4, we know that E^m_i is the matrix with $a_{ii+1} = m$, which means that $m = 0$, which is a contradiction. □

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. □

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. □

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 $\mathcal{L}_p$.