1 Technical Background

Notations 1.1. ,

- $\mathbb{Z}_p$, *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* $\mathcal{L}_p$.

Proposition 1.2. *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 1.3. *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 1.4. *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 1.5. *Let G be any group. a subgroup $H \leq G$ is called **pro-isomorphic**, if $\widehat{H} \cong \widehat{G}$.*

Definition 1.6. *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 1.7. *$G = (\mathbb{Z}, +)$. 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 1.8. *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 $\frac{1}{2^{k_2s}3^{k_3s}5^{k_5s}\dots}$, 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 1.9. *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 1.10. *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 1.11. *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.*

Proposition 1.12. *Let $\mathcal{L}_p$ be any $\mathbb{Q}_p$-algebra, with $n=dim\mathcal{L}_p$. Then $G(\mathcal{L}_p)\leq GL_n(\mathcal{L}_p)$. This is true for any field $\mathbb{F}$ and $\mathbb{F}$-algebra $\mathcal{L}_{\mathbb{F}}$.*

Proof. Choose a basis $B=\{b_1,\dots,b_n\}$ of $\mathcal{L}_p$. Let $\varphi\in G(\mathcal{L}_p)$, and $v\in\mathcal{L}_p$. B is a basis, so there are $\lambda_1,\dots,\lambda_n\in\mathbb{Q}_p$, such that $v=\lambda_1b_1,\dots,\lambda_nb_b$. Then, $\varphi(v)=\varphi(\sum_{i=1}^n\lambda_ib_i)=\sum_{i=1}^n\varphi(\lambda_ib_i)=\sum_{i=1}^n\lambda_i\varphi(b_i)$. Mark $B_\varphi=\{\varphi(b_1),\dots,\varphi(b_n)\}$. 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 $\rho_1,\dots,\rho_n\in\mathbb{Q}_p$. But $u=\sum_{i=1}^n\tau_ib_i$, φ is an automoprhism, so $u=\varphi\varphi^{-1}(u)=\varphi(\varphi^{-1}(\sum_{i=1}^n\tau_ib_i))=\varphi(\sum_{i=1}^n\varphi^{-1}(\tau_ib_i))=\varphi(\sum_{i=1}^n\tau_i\varphi^{-1}(b_i))=\sum_{i=1}^n\varphi(\tau_i\varphi^{-1}(b_i))=\sum_{i=1}^n\tau_i\varphi(\varphi^{-1}(b_i))=\sum_{i=1}^n\tau_ib_i$, 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 1.13. *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 1.14. *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 1.15. *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 1.16. *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 1.13 that $L_p \leq \mathcal{L}_p$, so $h \in G(\mathbb{Q}_p)$. But, $h(L_p) \subseteq L_p$, and from 1.14, 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 1.17. *$G^+(\mathbb{Q}_p) = \bigsqcup_{i=1}^{n} G(\mathbb{Z}_p)g_i$, where $[G(\mathbb{Q}_p) : G(\mathbb{Z}_p)] = n$*

Proposition 1.18. *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 1.16, 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, obviosuly, $\tau^{-1}\varphi = \tau^{-1}\tau\psi = \psi$ 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 isomoprhism $L_p \cong M$ is common to all representatives of the same right coset of $G(\mathbb{Z}_p)$, proving the bijection. □