

**P-ADIC ANALYTIC GROUPS**  
HARVARD MATH 291Y, FALL 2023

PIOTR PSTRĄGOWSKI

CONTENTS

1. Motivation	2
2. Profinite groups	9
3. Pro- $p$ -groups and the lower $p$ -series	13
4. Topology of finitely generated pro- $p$ groups	19
5. Powerful finite $p$ -groups	22
6. Pro- $p$ -groups of finite rank	26
7. Uniform power	32
8. The $p$ -adic general linear group	36
9. The additive structure of a uniform group	38
10. Formal groups laws	43
11. Lubin-Tate formal group laws	46
12. The Morava stabilizer group	51
13. Normed algebras and power series	59
14. The completed group algebra	66
15. The group algebra of a uniform group	71
16. Baker-Campbell-Hausdorff formula	77
17. The Lie correspondence	83
18. Analytic groups	88
19. Lazard's characterization	92
20. Cohomology of profinite groups	97
21. Cohomological dimension and mod $p$ cohomology	103
22. The derived $\infty$ -category and cup products	109
23. Torsion-free groups and locality of cohomological dimension	116
24. Poincaré duality	122
25. Cohomology of $p$ -adic analytic groups	131
References	140

**Disclaimer:** Use these notes at your own risk - it is likely that there are mistakes. If you find any errors, or if you have any comments or suggestions, contact me at [piotr@math.harvard.edu](mailto:piotr@math.harvard.edu).

ACKNOWLEDGEMENTS

Parts of these notes were adapted from ones taken in class by Thomas Brazelton, Stephen McKean, Natalia Pacheco-Tallaj and Wyatt Reeves. I would like to thank Peter Haine and Ishan Levy for helpful comments and suggestions. I would like to thank Sanath Devalapurkar and Ishan Levy for substituting for me when I was traveling.

1. MOTIVATION

This course is an introduction to the beautiful theory of  $p$ -adic analytic groups. Informally,  $p$ -adic analytic groups are the non-Archimedean analogue of the notion of a real Lie group. As motivation, let us recall the latter.

**Definition 1.1.** A *Lie group*  $G$  is a group together with the structure of a smooth manifold such that the group multiplication  $G \times G \rightarrow G$  is smooth.

Note that this last condition essentially ensures that the group and smooth structures are compatible with each other. One can show that it also follows that the group inverse map  $(-)^{-1}: G \rightarrow G$  is smooth, too.

**Example 1.2.** The basic example of a Lie group is given by  $GL_n(\mathbb{R})$ , the group of invertible  $n \times n$  real matrices. It is a group under multiplication of matrices and a smooth manifold as an open subset of the vector space of all matrices.

**Example 1.3.** Many important Lie groups arise as subgroups of  $GL_n(\mathbb{R})$ . For example, we have

$$O(n) \leq GL_n(\mathbb{R});$$

the subgroup of matrices which are orthonormal; equivalently, which correspond to a linear automorphism of  $\mathbb{R}^n$  which is an isometry. Similarly, we have

$$SO(n) \leq O(n),$$

the subgroup of matrices with positive determinant; equivalently, which correspond to an orientation-preserving linear automorphism.

**Example 1.4.** If  $G$  is a Lie group, then it is not difficult to see that so is its universal cover  $\tilde{G} \rightarrow G$ . For example, for  $n > 2$  the universal cover of  $SO(n)$  is given by the so-called spin group

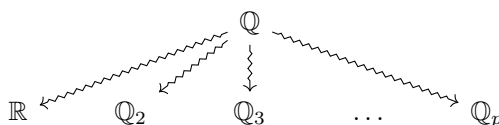
$$\text{Spin}(n) \rightarrow SO(n).$$

Since  $p$ -adic analytic groups are the analogue of Lie groups, one might expect that the theorems we can prove about them would be similar in spirit to the ones we prove about real Lie groups. As motivation, what are the kinds of things one might learn about Lie groups in a graduate course?

- (1) (*The Lie correspondence*) - The tangent space of the identity of a Lie group has a structure of a Lie algebra which completely determines its local structure. Moreover, in the simply-connected case, the group is uniquely determined by its Lie algebra, giving an equivalence of categories.
- (2) (*Analyticity and uniqueness*) - The smooth structure of a Lie group can be uniquely promoted to a structure of an analytic manifold. Continuous group homomorphisms between Lie groups are automatically analytic.
- (3) (*Group-theoretic properties*) - Closed subgroups of Lie groups are again Lie. Moreover, any Lie group  $G$  has a *no small subgroups property*; that is, there exists an open neighbourhood  $U \subseteq G$  of the identity which doesn't contain any subgroups.

In this course, we will undertake a similar study in the  $p$ -adic context. As cohomology of  $p$ -adic analytic groups is often important in applications, we will also prove basic results about their cohomology. In this first lecture, we give an informal overview of the kinds of objects and results we will touch upon throughout the term.

Where do the  $p$ -adics come from? We begin with  $\mathbb{Q}$  and look at different completions:



Completion with respect to the standard Archimidean metric gives the real field  $\mathbb{R}$ , but completions with respect to  $p$ -adic metrics instead yield  $\mathbb{Q}_p$ . The latter can be also easily described using algebra.

**Definition 1.5.** The ring of  $p$ -adic integers is given by

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n.$$

This has a canonical limit topology, where we endow each finite ring  $\mathbb{Z}/p^n$  with the discrete topology, which makes it into a compact Hausdorff ring. The  $p$ -adic field is given by the localization

$$\mathbb{Q}_p := \mathbb{Z}_p[p^{-1}] \simeq \varinjlim (\mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \xrightarrow{p} \dots)$$

which we endow with the colimit topology.

There is a metric on  $\mathbb{Q}_p$  which induces the same topology. Since  $\mathbb{Z}_p$  is a complete discrete valuation ring, any non-zero  $x \in \mathbb{Z}_p$  can be written uniquely in the form  $x = p^n \cdot u$ , where  $u \in \mathbb{Z}_p^\times$  and  $n \geq 0$ . The same works for  $\mathbb{Q}_p$ , where now we need to allow  $n \in \mathbb{Z}$ .

**Definition 1.6.** The  $p$ -adic absolute value  $|\cdot|_p: \mathbb{Q}_p \rightarrow \mathbb{R}$  is given by

- (1)  $|0|_p := 0$ ,
- (2)  $|p^n \cdot u|_p := p^{-n}$  for any  $u \in \mathbb{Z}_p^\times$ .

It is not difficult to see that this really is an absolute value in the sense that it is multiplicative

$$|xy|_p = |x|_p |y|_p$$

and subadditive

$$|x + y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p.$$

This absolute value defines the  $p$ -adic metric

$$d(x, y) := |x - y|_p$$

on  $\mathbb{Q}_p$ . It is a good exercise that this metric induces the colimit-limit topology described before.

As any complete metric field,  $\mathbb{Q}_p$  admits differential calculus; that is, standard notions of convergence or derivatives work in this setting and satisfy the usual formulas. However, we have a host of new phenomena due to the fact that this is the  $p$ -adic metric, unlike the standard metric on  $\mathbb{R}$ , is actually an *ultrametric*. That is, the  $p$ -adic metric satisfies the stronger form of the triangle inequality given by

$$d(x, y) \leq \max(d(x, z), d(z, y))$$

In this course, we will not delve too deeply into  $p$ -adic analysis, but let us give two instructive examples which convey a little bit of the flavour of the field. Among these two examples, the first one highlights that sometimes the non-Archimedean world is much more simple than the real one, while the second one highlights that it can also carry unexpected dangers.

**Example 1.7.** If  $a_i \in \mathbb{Q}_p$  is a sequence of  $p$ -adic numbers, then the following two conditions are equivalent:

- (1)  $\sum_{i \geq 0} a_i$  converges,
- (2)  $a_i \rightarrow 0 \in \mathbb{Q}_p$ ; equivalently,  $|a_i|_p \rightarrow 0 \in \mathbb{R}$ .

Indeed, the ultrametric inequality implies that the  $p$ -adic absolute value of partial sums  $\sum_{m \leq i \leq n} a_i$  is bounded by the maximum of absolute values of their terms, so that they become very small as the terms do. This makes convergence of series much easier in the  $p$ -adic world than in the real world.

**Example 1.8.** We give an example of a smooth function  $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  whose derivative vanishes identically, but which is injective. In particular, it is not constant.

Using the limit description  $\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}_p/p^n$ , it is not difficult to show that any  $a \in \mathbb{Z}_p$  can be uniquely represented as a convergent power series

$$a = \sum a_i p^i,$$

where  $a_i \in \{0, 1, \dots, p-1\}$ . We now define  $f$  by

$$f\left(\sum a_i p^i\right) := \sum a_i p^{2i}.$$

It is a good exercise in getting used to the  $p$ -adic metric to verify that this function satisfies

$$|f(x-y)|_p \leq |x-y|_p^2.$$

Since this function is highly contractive (roughly the same as  $x \mapsto x^2$  is around zero, but at each point), it is continuous and its derivative vanishes identically. However, it is immediate from the formula that this function is injective and hence even a homeomorphism onto its image.

One way to interpret [Example 1.8](#) is that smooth  $p$ -adic functions can be very badly behaved. As a consequence, to define the  $p$ -adic analytic groups, we work with a more restrictive class of functions where such pathological behaviour cannot occur.

**Definition 1.9.** Let  $U \subseteq \mathbb{Q}_p^n$  be an open subset. We say a function  $f: U \rightarrow \mathbb{Q}_p$  is *locally analytic* if it is locally given by a convergent power series.

In more detail,  $f$  is locally analytic if for any  $u \in U$  we can find

- (1) a real  $\epsilon_u > 0$ ,
- (2) a formal power series  $F_u \in \mathbb{Q}_p[[X_1, \dots, X_n]]$

with the properties that

- (1) if we expand the formal power series

$$F_u = \sum_{I=(i_1, \dots, i_n)} a_I X^I$$

in terms of monomials then

$$\epsilon_u^{i_1 + \dots + i_n} |a_I|_p \rightarrow 0$$

as  $|i_1 + \dots + i_n| \rightarrow \infty$ ,

- (2) if  $u' = u + (x_1, \dots, x_n) \in U$  with  $|x_i|_p \leq \epsilon_u$ , then

$$f(u') = F_u(u' - u).$$

Note that the first condition guarantees that in the context of the second, the right hand side of

$$F_u(u' - u) = \sum a_I x^I = \sum a_{(i_1, \dots, i_n)} \cdot x_1^{i_1} \cdot \dots \cdot x_n^{i_n}$$

converges, so that the equation makes sense.

To define  $p$ -adic analytic groups one mimics the definition of Lie groups. This means that we first need an appropriate notion of a manifold which is as follows:

**Definition 1.10.** A  $p$ -adic manifold of dimension  $n$  is a Hausdorff, paracompact topological space  $X$  together with a maximal atlas of charts

$$(U_\alpha, \varphi_\alpha)$$

where  $U_\alpha \subseteq X$  is open and  $\varphi: U_\alpha \rightarrow \mathbb{Q}_p^n$  is a homeomorphism onto an open subset  $V_\alpha \subseteq \mathbb{Q}_p^n$  with the property that for any  $\alpha, \beta$ , the transition function

$$V_\alpha \supseteq \varphi_\alpha^{-1}(U_\alpha \cap U_\beta) \xrightarrow{\varphi_\alpha^{-1}} U_\alpha \cap U_\beta \xrightarrow{\varphi_\beta} \varphi_\beta^{-1}(U_\alpha \cap U_\beta) \subseteq V_\beta$$

is locally analytic.

The basic notions of manifold topology carry over to the setting of  $p$ -adic manifolds. For example, it makes sense to speak of differentiable, smooth or locally analytic functions between  $p$ -adic manifolds. Moreover, any point of a  $p$ -adic manifold has a tangent space, which is a vector space over  $\mathbb{Q}_p$  of dimension the same as the manifold, and differentiable maps induce morphisms between tangent spaces.

However, unlike the theory of (real) manifolds, classification of  $p$ -adic manifolds is very easy, essentially due to the fact that the topology on  $\mathbb{Q}_p$  has too many open sets, so that it is difficult to glue things together in an interesting way:

**Warning 1.11.** One can show that any compact  $p$ -adic manifold  $X$  of dimension  $n$  is isomorphic to a disjoint union

$$X \simeq \mathbb{Z}_p^{\times n} \sqcup \dots \sqcup \mathbb{Z}_p^{\times n}$$

of copies of the closed  $p$ -adic unit disc. In particular, all non-empty compact  $p$ -adic manifolds of positive dimension are homeomorphic.

However, while the theory of  $p$ -adic manifolds is not particularly interesting,  $p$ -adic analytic groups, which we define now, have a beautiful, complex theory.

**Definition 1.12.** A  $p$ -adic analytic group  $G$  is a group together with a structure of a  $p$ -adic manifold such that the multiplication  $m: G \times G \rightarrow G$  and inverse  $(-)^{-1}: G \rightarrow G$  maps are locally analytic.

These are the central objects of study in this course, and we give a few examples.

**Example 1.13.** The general linear group  $\mathrm{GL}_n(\mathbb{Q}_p)$ , which inherits a structure of a  $p$ -adic manifold as an open subset of the  $\mathbb{Q}_p$ -vector space of  $n \times n$  matrices, is a  $p$ -adic analytic group under multiplication of matrices. This is a prototypical example of a  $p$ -adic analytic group.

Note that  $\mathrm{GL}_n(\mathbb{Q}_p)$  has a compact open subgroup given by  $\mathrm{GL}_n(\mathbb{Z}_p)$ , the group of invertible matrices with coefficients in the  $p$ -adic integers. In fact, we have a whole descending chain of compact open subgroups of the form

$$\dots \leq I + p^2 \cdot M_n(\mathbb{Z}_p) \leq I + p \cdot M_n(\mathbb{Z}_p) \leq \mathrm{GL}_n(\mathbb{Z}_p) \leq \mathrm{GL}_n(\mathbb{Q}_p).$$

One can show that these compact open subgroups form a basis of neighbourhoods of the identity matrix  $I$ . This is one crucial way in which  $p$ -adic analytic groups differ from Lie groups: while the latter have no small subgroups,  $p$ -adic analytic groups have *arbitrarily small open subgroups*.

**Example 1.14.** Let  $K$  be a  $p$ -adic local field; that is, a finite extension  $\mathbb{Q}_p \subseteq K$ . The ramified part of the maximal abelian extension  $K^{ab} \subseteq K$  is known as the *Lubin–Tate extension* and is denoted by  $K^{\mathrm{LT}}$ . Local class field theory gives a canonical continuous isomorphism

$$\mathrm{Gal}(K^{\mathrm{LT}}/K) \cong \mathcal{O}_K^\times$$

which shows that the Galois group has a natural structure of a  $p$ -adic analytic group.

**Example 1.15.** Let  $\mathbf{G}_0$  be the Honda formal group law over  $\mathbf{F}_{p^n}$ , which is the unique  $p$ -typical formal group law whose  $p$ -series is given by  $[p]_{\mathbf{G}_0}(x) = x^{p^n}$ . One can show that the endomorphism ring  $\mathrm{End}(\mathbf{G}_0)$  has a natural structure of a free finite rank  $\mathbb{Z}_p$ -algebra, so that the automorphism group

$$\mathbb{G}_n := \mathrm{Aut}(\mathbf{G}_0) = \mathrm{End}(\mathbf{G}_0)^\times$$

inherits a structure of a  $p$ -adic analytic group.

This group (which depends on the choice of a prime  $p$  and a height  $n > 0$ ) is known as the *Morava stabilizer group*. It is extremely important because its cohomology groups form the basic building blocks of the stable homotopy groups of spheres.

As we observed in the discussion following [Example 1.13](#), the group  $\mathrm{GL}_n(\mathbb{Q}_p)$  has a basis of open neighbourhoods of the identity given by compact open subgroups of the form  $I + p^k \cdot M_n(\mathbb{Z}_p)$ . Compact groups with this property are called *profinite*, and it is not difficult to show that  $p$ -adic analytic groups are always locally profinite.

One of the main results in this course is the following beautiful theorem of Lazard, which essentially gives a local characterization of  $p$ -adic analytic groups in purely group-theoretic terms:

**Theorem 1.1** (Lazard, [19.11](#)). *Let  $G$  be a topological group. The following are equivalent:*

- (1)  $G$  admits a structure of a  $p$ -adic analytic group compatible with its topology,
- (2) there exists an open compact subgroup  $F \leq G$  which is a pro- $p$  group of finite subgroup rank; that is, there exists an integer  $d$  such that all closed subgroups  $H \leq F$  can be generated by at most  $d$  elements
- (3) there exists an open compact subgroup  $P \leq G$  which is a finitely generated pro- $p$  group and which is powerful; that is, such that  $P/\overline{P^p}$  (the quotient by the closed subgroup generated by  $p$ -th powers) is abelian<sup>1</sup>,
- (4) there exists an open compact subgroup  $U \leq G$  which is uniformly powerful; that is, finitely generated, powerful and torsion-free.

More informally, condition (2) characterizes  $p$ -adic analytic groups as being locally profinite and with good finiteness properties; while (3) characterizes them as locally profinite and “almost abelian”. Moreover, we will show that the analytic structure is essentially determined by the group structure alone, since:

- (1) continuous maps between  $p$ -adic analytic groups are locally analytic,
- (2) group homomorphisms between compact  $p$ -adic analytic groups are continuous.

In practice, it is characterization (4) of [Theorem 1.1](#) which is most useful, as uniformly powerful pro- $p$ -groups are easy to understand. We will prove the following result describing the theory of uniformly powerful groups in purely linear terms.

**Theorem 1.16** (Lazard, Dixon-Du Sautoy-Mann-Segal, [17.3](#), [17.10](#)). *Let  $U$  be a uniformly powerful group. Then, the group structure of  $U$  induces continuous maps  $+: U \times U \rightarrow U$  and  $(-, -): U \times U \rightarrow U$  such that the pair*

$$(U, +, (-, -))$$

*is a  $\mathbb{Z}_p$ -Lie algebra which as a  $\mathbb{Z}_p$ -module is free of finite rank and whose bracket is abelian modulo  $p^2$ ; that is, such that*

$$(U, U) \subseteq p \cdot U.$$

*This construction gives an equivalence of categories between uniformly powerful groups and continuous group homomorphisms and the category of  $\mathbb{Z}_p$ -Lie algebras with these two properties.*

As any  $p$ -adic analytic group is locally uniform, one can interpret [Theorem 1.16](#) as the  $p$ -adic analogue of the Lie correspondence, describing the local structure of  $p$ -adic analytic groups in linear terms.

Another reason why Lazard’s characterization is useful in practice is that uniformly powerful groups have very favourable group-theoretic properties. In particular, their group algebra is well-behaved.

Recall that if  $G$  is a group, then to give a  $G$ -representation on a  $\mathbf{F}_p$ -vector space is the same as to give a module over the group algebra  $\mathbf{F}_p[G]$ . For topological groups, we have a variant of the group algebra construction which takes the topology into account.

---

<sup>1</sup>When  $p = 2$ , this condition needs to be slightly modified. A pro-2-group is said to be *powerful* if  $P/\overline{P^4}$  is abelian. One intuition about this change is that  $P/\overline{P^2}$  is always abelian, which is not true at odd primes. We will discuss these differences in more detail later in the course.

<sup>2</sup>If  $p = 2$ , then the bracket is abelian modulo 4. This is related to the slightly altered definition of a powerful group when  $p = 2$ .

**Definition 1.17.** Let  $G = \varprojlim G_i$  be a profinite group; that is, a limit of finite groups equipped with its limit topology. The *completed group algebra* is given by

$$\mathbf{F}_p[[G]] := \varprojlim \mathbf{F}_p[G_i].$$

Understanding continuous  $G$ -representations on  $\mathbf{F}_p$ -vector spaces is closely related to understanding the ring-theoretic properties of the completed group algebra. Despite being defined as a limit of such, this ring is often better-behaved than the group algebra of a finite group, as the following example shows.

**Example 1.18.** Consider the completed group algebra  $\mathbf{F}_p[[\mathbb{Z}_p]]$  and if  $a \in \mathbb{Z}_p$ , write  $[a] \in \mathbf{F}_p[[\mathbb{Z}_p]]$  for the corresponding element of the group algebra. A result of Iwasawa shows that the inclusion of  $x := [0] - [1]$  induces an isomorphism of topological rings

$$\mathbf{F}_p[[\mathbb{Z}_p]] \cong \mathbf{F}_p[[x]]$$

This shows that to define a continuous action of the topological group  $\mathbb{Z}_p$  on a finite dimensional  $\mathbf{F}_p$ -vector space is the same as to give a single topologically nilpotent operator. Moreover, it implies that the completed group algebra of the  $p$ -adics is noetherian.

The following result which we prove later in the course gives a partial extension of Iwasawa's description to the case of an arbitrary uniformly powerful group.

**Theorem 1.2** (Lazard, 15.8, 25.24). *Let  $U$  be uniformly powerful  $p$ -adic analytic group of dimension  $d$ . Let*

$$I := \ker(\mathbf{F}_p[[U]] \rightarrow \mathbf{F}_p)$$

*be the augmentation ideal given by the kernel of the map of group algebras induced by the unique map  $U \rightarrow 0$  into the zero group. Then the associated graded of the  $I$ -adic filtration is isomorphic as a graded ring*

$$\mathrm{gr}_I(\mathbf{F}_p[[U]]) \simeq \bigoplus_{k \geq 0} I^k / I^{k+1} \simeq \mathbf{F}_p[x_1, \dots, x_d]$$

*to a polynomial algebra in  $d$  variables.*

In the course, we will in fact prove a slightly stronger variant of [Theorem 1.2](#) which essentially describes the completed group algebra over  $\mathbb{Z}_p$  rather than the finite field  $\mathbf{F}_p$ .

Informally, [Theorem 1.2](#) says that the completed group algebra of a uniformly powerful group is close to a polynomial ring, despite not being commutative. Since any compact  $p$ -adic analytic group has a finite index uniformly powerful subgroup by [Theorem 1.1](#), and since the property of being noetherian is inherited from the associated graded of a ring, we deduce the following:

**Corollary 1.19.** *If  $G$  is compact  $p$ -adic analytic, then  $\mathbf{F}_p[[G]]$  is both left and right noetherian.*

In both number theory and other subjects, many important invariants can be expressed as group cohomology of a profinite group  $G \simeq \varprojlim G_i$ . If  $M$  is a finite abelian group, the continuous cohomology groups

$$H^*(G; M)$$

can be defined in several equivalent ways, for example

- (1) as cohomology of the continuous group cochain complex

$$M \rightarrow \mathrm{map}_{\mathrm{cts}}(G, M) \rightarrow \mathrm{map}_{\mathrm{cts}}(G \times G, M) \rightarrow \dots,$$

- (2) as extension groups in an appropriate abelian category of abelian groups with a continuous  $G$ -action,
- (3) as the colimit

$$\varinjlim H^*(G_i; M)$$

of cohomology groups of finite quotients of  $G$ .

More generally, one can define cohomology with coefficients in a  $G$ -module, not necessarily finite or with trivial  $G$ -action. We give a few examples of these groups describing important phenomena.

**Example 1.20.** Let  $K$  be a field,  $K^{sep}$  its separable closure and  $\text{Gal} := \text{Gal}(K^{sep}/K)$  the absolute Galois group. The Brauer group of  $K$  which is given by central division  $K$ -algebras up to Morita equivalence, is canonically isomorphic to

$$H^2(\text{Gal}, (K^{sep})^\times),$$

continuous cohomology of the Galois group.

**Example 1.21.** Following up on [Example 1.15](#), let  $\mathbf{G}_0$  be the Honda formal group law of height  $n$  over the finite field  $\mathbf{F}_{p^n}$  and let  $\mathbb{G}_n$  be its automorphism group, the Morava stabilizer group. Associated to  $\mathbf{G}_0$  we have the Lubin-Tate ring  $E$  which parametrizes its deformations, together with a free rank one module  $\omega$  over  $E$  which corresponds to the tangent space of the universal deformation. This ring is non-canonically isomorphic

$$E \simeq W(\mathbf{F}_{p^n})[[u_1, \dots, u_{n-1}]]$$

to a power series algebra over the Witt vectors.

Since this construction is functorial in  $\mathbf{G}_0$ , the Morava stabilizer group  $\mathbb{G}_n$  acts on both  $E$  and  $\omega$  in a compatible manner. One can show that there is a spectral sequence

$$H^s(\mathbb{G}_n, \omega^{\otimes t}) \Rightarrow \pi_{2t-s} S_{K(n)}^0,$$

relating the cohomology of the Morava stabilizer group to the stable homotopy groups of the  $K(n)$ -local sphere. Informally, the latter can be thought of as “stable homotopy groups of height exactly  $n$ ” and so are of central importance in stable homotopy theory.

A combination of fundamental results of Lazard and Serre shows that  $p$ -adic analytic groups have excellent cohomological properties:

**Theorem 1.3** (Lazard, Serre, [25.2](#)). *Let  $G$  be a compact  $p$ -adic analytic group of dimension  $d$ . If  $G$  has no  $p$ -torsion, then  $G$  is a Poincaré group of dimension  $d$ . In particular:*

- (1) *there exists a contravariant equivalence*

$$(-)^{*G} : \text{Mod}_G(\text{Ab}_{(p)}^\omega)^{op} \rightarrow \text{Mod}_G(\text{Ab}_{(p)}^\omega)$$

*from the category of finite abelian  $p$ -groups with a continuous  $G$ -action to itself, called  $G$ -Pontryagin duality,*

- (2) *for any finite abelian  $p$ -group  $A$  with a continuous  $G$ -action the cohomology groups*

$$H^k(G, A)$$

*are finite and vanish for  $k > d$ ,*

- (3) *there's a canonical isomorphism*

$$H^{d-k}(G, A^{*G}) \simeq H^k(G, A)^*$$

*between cohomology with coefficients in the  $G$ -Pontryagin dual  $A^{*G}$  and the Pontryagin dual*

$$H^k(G, A)^* := \text{Hom}_{\text{Ab}}(H^k(G, A), \mathbb{Z}/p^\infty)$$

*of cohomology with coefficients in  $A$ .*

In the context of [Theorem 1.3](#), the  $G$ -Pontryagin duality functor is given by mapping into a certain special  $G$ -module called the *dualizing module*, which can be thought of as playing a role similar to the one played by the orientation bundle in the case of cohomology of manifolds. As an abelian group, the dualizing module is isomorphic to  $\mathbb{Z}/p^\infty$ , so that as an abelian group  $A^{*G}$  can be identified with a Pontryagin dual of  $A$ , but with a possibly twisted  $G$ -action.

Note the surprising part of [Theorem 1.3](#) it is the *group* cohomology of  $p$ -adic analytic groups which behaves very much so like the cohomology algebra of a manifold. This is in stark contrast to the case of compact Lie groups, whose underlying topological space does have finite-dimensional cohomology, but whose group cohomology is almost always infinite-dimensional.

## 2. PROFINITE GROUPS

In previous lecture, we saw a fundamental characterization of  $p$ -adic analytic groups due to Lazard, namely [Theorem 1.1](#). In particular, the result shows that any  $p$ -adic analytic group has an open subgroup which is a particularly nice profinite group. As a beginning of our journey towards Lazard’s theorem, today we define and study profinite groups.

**Remark 2.1.** Another good reason to study profinite groups, besides their ubiquity, is the theory of condensed mathematics due to Clausen and Scholze. Informally, condensed mathematics provides an alternative to the theory of topological spaces where the building blocks are given by profinite sets. This means that a good understanding of profinite objects, for example profinite groups, is helpful when learning condensed mathematics.

The following is our main object of study in this lecture.

**Definition 2.2.** A topological group  $G$  is *profinite* if

- (1) it is compact Hausdorff and
- (2) normal open subgroups  $U \leq G$  form a basis of neighborhoods of the identity  $e \in G$ .

Informally, a profinite group is a topological group with plenty of open subgroups.

**Notation 2.3.** If  $H \subseteq G$  is a subgroup, we write  $H \leq G$ . If it closed as a subset of  $G$ , we write  $H \leq_c G$ . If it is open, we write  $H \leq_o G$ . We denote normal subgroups by  $H \triangleleft G$ , and closed and open ones, respectively, by  $H \triangleleft_c G$  and  $H \triangleleft_o G$ .

The following large proposition collects the basic properties of subgroups of profinite groups.

**Proposition 2.4.** *Let  $G$  be a profinite group.*

- (1) *If  $U \leq_o G$  is open, then it is closed and of finite index.*
- (2) *If  $K \leq_c G$  is closed, then it is open if and only if it is of finite index.*
- (3) *Any open subset is a union of cosets of open normal subgroups.*
- (4) *If  $H \leq G$  is a subgroup, then so is its closure  $\bar{H}$ , and the latter is given as the intersection*

$$\bar{H} = \bigcap_{\substack{U \leq_o G \\ H \leq U}} U$$

*of all open subgroups which contain  $H$ .*

*Proof.* We prove these one by one.

- (1) The set of opens  $Ug$  for  $g \in G$  is an open cover of  $G$ , so since  $G$  is compact there is a finite list  $g_1, \dots, g_n$  such that

$$Ug_1, \dots, Ug_n$$

is an open cover. Two cosets of the same subgroup are either equal or don’t intersect at all, so by making them smaller, we can assume  $Ug_i \cap Ug_j = \emptyset$  if  $i \neq j$ . This implies that the index is finite, in fact  $|U : G| = n$ . To see that  $U$  is closed, notice that without loss of generality we can assume that  $Ug_1 = U$ . In this case the set-theoretic difference

$$G \setminus U = \bigcup_{2 \leq i \leq n} Ug_i$$

is a finite union of open sets hence open, so  $U$  is closed.

- (2) We have seen one direction just above, so instead suppose  $K$  is a closed finite index subgroup. Because it is finite index, there exist elements  $g_2, \dots, g_n$  of  $G$  such that

$$K, Kg_2, \dots, Kg_n$$

is a finite closed cover. It follows that the complement of  $K$  is

$$G \setminus K = \bigcup_{2 \leq i \leq n} Kg_i,$$

so  $K$  is open.

- (3) By assumption, open normal subgroups  $U$  form a basis of neighbourhoods of the identity. Since for every  $g \in G$ , the right multiplication  $(-) \cdot g : G \rightarrow G$  is a homeomorphism,  $Ug$  forms a basis of neighborhoods of  $g$  for any  $g \in G$ , and the claim follows.
- (4) By the first part, the intersection of all open subgroups containing  $H$  is closed and hence contains the closure. To prove the converse, we have to show that if  $g \notin \overline{H}$ , then there exists an open subgroup  $U \leq_o G$  such that  $H \leq U$  and  $g \notin U$ . Since  $g$  is not in the closure, by the third part there exists an open normal subgroup  $V$  such that  $Vg \cap H = \emptyset$ . It easily follows that  $g \notin VH$ , and we are done since  $VH$  is an open subgroup (it is a subgroup since  $V$  is normal, and it is open since it is a union of cosets of  $V$ ) containing  $H$ .

□

Using [Proposition 2.4](#), it is not difficult to show that profinite groups are closed under various operations, such as passing to subgroups and quotient groups.

**Example 2.5.** If  $G$  is profinite, and  $K \leq_c G$  is a closed subgroup, then  $K$  is profinite with respect to its subspace topology. Indeed, it is compact and Hausdorff and it has a basis of neighbourhoods of the identity given by open normal subgroups  $K \cap U$ , where  $U \leq_o G$  is normal.

**Example 2.6.** If  $G$  is profinite and  $K \leq_c G$  is a closed normal subgroup, then  $G/K$  is profinite with respect to the quotient topology induced by the projection  $G \rightarrow G/K$ . Indeed, it is clearly compact. Moreover, it is Hausdorff since  $K$  is intersection of open subgroups which contain it by [Proposition 2.4](#), so that the identity of  $G/K$  is closed and has a basis of open neighbourhoods given by images of open subgroups of  $G$  which contain  $K$ . It then also follows that  $G/K$  is Hausdorff.

**Example 2.7.** Providing a partial converse to [Example 2.5](#) and [Example 2.6](#), if  $G$  is a compact Hausdorff topological group with a closed subgroup  $K \leq_c G$  such that both  $K$  and  $G/K$  are profinite, then  $G$  is profinite. We leave the argument to the interested reader.

The following justifies the terminology *profinite*. Recall that a poset  $P$  is said to be *cofiltered* if for every finite collection  $p_1, \dots, p_n \in P$  there exists a  $p \in P$  such that  $p \leq p_i$  for each  $1 \leq i \leq n$ .

**Theorem 2.8.** *For a topological group  $G$ , the following are equivalent:*

- (1)  $G$  is profinite,
- (2) we can write  $G = \varprojlim G_i$  as a limit in the category of topological groups of diagram of finite groups equipped with the discrete topology indexed by a cofiltered poset,
- (3) we can write  $G = \varprojlim G_i$  as a limit of finite groups in the category of topological groups.

*Proof.* We first show (3  $\Rightarrow$  1), so let  $G := \varprojlim G_i$  be a limit of a diagram of finite groups indexed by a category  $I$ . Let  $I^{disc}$  denote the subcategory with the same objects but only identity morphisms, so that the natural inclusion  $I^{disc} \hookrightarrow I$  induces a canonical map

$$\varprojlim G_i \rightarrow \prod_{i \in I} G_i.$$

This presents the source as a closed subgroup of the target, so using [Example 2.5](#) it is enough to show that the target is profinite. It is clearly compact Hausdorff, by Tychonoff's theorem. Moreover, any open set containing the identity contains an open subgroup of the form

$$\prod_{i \in I \setminus J} G_i \times \prod_{j \in J} \{e_{G_j}\} \subseteq \prod_{i \in I \setminus J} G_i \times \prod_{j \in J} G_j \simeq \prod_{i \in I} G_i$$

for some finite subset  $J \subseteq I$ . Thus, the product is profinite, as needed.

Since  $(2 \Rightarrow 3)$  is immediate, we move to  $(1 \Rightarrow 2)$ . Let  $P$  be the poset of normal open subgroups of  $G$ . Since open normal subgroups are stable under finite intersections, this poset is cofiltered. We have a natural comparison map

$$G \rightarrow \varprojlim_{U \in P} G/U$$

and we claim it is a bijective homeomorphism. Note that the target is also profinite, by what we have shown above. The comparison map is continuous since each of the quotients  $G \rightarrow G/U$  is continuous as  $U$  is open. Since the identity is the intersection of all open normal subgroups, the comparison map is injective. Thus, it is enough to show that the image is dense.

Since the image is a closed subgroup, it is enough to show that if  $V \leq \varprojlim_{U \in P} G/U$  is an open subgroup containing the image of  $G$ , then it is the whole thing. Any such subgroup is a preimage of a subgroup of  $G/U_0$  along the projection

$$\varprojlim_{U \in P} G/U \rightarrow G/U_0.$$

Since the composite  $G \rightarrow \varprojlim_{U \in P} G/U \rightarrow G/U_0$  is surjective, we deduce the subgroup is the whole thing, as needed.  $\square$

**Example 2.9.** If  $\Gamma$  is a group, the profinite group

$$\widehat{\Gamma} := \varprojlim_{\substack{N \triangleleft G \\ [N:\Gamma] < \infty}} \Gamma/N$$

given by the limit of finite quotients of  $\Gamma$ , is profinite. It is called the *profinite completion* of  $\Gamma$ .

**Example 2.10.** The profinite completion of the free group  $\mathbb{Z}$  on one generator arises naturally as the absolute Galois group

$$\widehat{\mathbb{Z}} \simeq \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$$

of any finite field. The generator corresponding to  $1 \in \widehat{\mathbb{Z}}$  is given by the Frobenius  $x \mapsto x^q$ .

**Warning 2.11.** Beware that the profinite completion map  $\Gamma \rightarrow \widehat{\Gamma}$  is in general neither injective nor surjective.

Note that a profinite group is either finite or at least of cardinality of continuum. Despite this, there is a good theory of finite generation in the setting of profinite (more generally, topological) groups.

**Definition 2.12.** Let  $G$  be a topological group. We say that elements  $g_1, \dots, g_d$  generate  $G$  if

$$\overline{\langle g_1, \dots, g_n \rangle} = G;$$

that is, if the closure of the subgroup generated by them is the whole group. We say  $G$  is *finitely generated* if it admits a finite list of generators.

As we have seen, any profinite group  $G$  is a limit of finite groups. Almost as if by magic, in the profinite setting it is possible to verify that a group is finitely generated by verifying the same about its finite quotients. To prove this, we will need the following lemma.

**Lemma 2.13.** *Let  $X_\alpha$  be a diagram of nonempty compact Hausdorff topological spaces indexed by a cofiltered poset  $P$ . Then the limit  $\varprojlim_{\alpha \in P} X_\alpha$  is also nonempty.*

*Proof.* As in the proof of [Theorem 2.8](#), forgetting the poset structure of  $P$  yields a natural map

$$\varprojlim_{\alpha \in P} X_\alpha \rightarrow \prod_{\alpha} X_\alpha$$

which exhibits the limit as a closed subspace of the product. To be more precise, it is the subspace of those families  $(x_\alpha)$  such that  $f_{\alpha,\beta}(x_\alpha) = x_\beta$  for every  $\alpha \leq \beta$ . In particular, both are compact Hausdorff: the product by Tychonoff's theorem, and the limit as a closed subspace.

For every finite subposet  $P' \subseteq P$ , let

$$\left(\prod_{\alpha} X_\alpha\right)^{P'} \subseteq \prod_{\alpha} X_\alpha$$

denote the subspace of those families  $(x_\alpha)$  which satisfy  $f_{\alpha,\beta}(x_\alpha) = x_\beta$  if both  $\alpha, \beta \in P'$ . Since  $P$  is cofiltered, for every such  $P'$  we can find an  $\alpha_0$  such that  $\alpha_0 \leq \alpha$  for each  $\alpha \in P$ . Since  $X_{\alpha_0}$  is non-empty, we can choose a point  $x_{\alpha_0}$ . Then, any family  $(x_\alpha)$  such that  $x_\alpha = f_{\alpha_0,\alpha}(x_{\alpha_0})$  lies in  $\left(\prod_{\alpha} X_\alpha\right)^{P'}$ . We deduce that the latter is non-empty.

As from the explicit description of the limit we have

$$\varprojlim_{\alpha \in P} X_\alpha = \bigcap_{P' \subseteq P} \left(\prod_{\alpha} X_\alpha\right)^{P'},$$

where the intersection is taken over all finite subsets of  $P$ . Since it is an intersection of non-empty closed subsets of a compact Hausdorff topological space, it is itself non-empty, ending the argument.  $\square$

**Remark 2.14.** More generally, there is a notion of a *cofiltered category*, see [[Lur09](#), 5.3.1.7], generalizing that of cofiltered posets. Since any cofiltered category admits a final map from a cofiltered poset by [[Lur09](#), 5.3.1.16], [Lemma 2.13](#) also holds for limits of nonempty compact Hausdorff topological spaces taken over cofiltered categories.

**Proposition 2.15.** *Let  $G$  be a profinite group such that for each open normal subgroup  $U$ ,  $G/U$  can be generated by at most  $d$  elements. Then  $G$  can be generated by at most  $d$  elements; in particular, it is finitely generated.*

*Proof.* As in the proof of [Theorem 2.8](#), we can write

$$G \simeq \varprojlim_{U \triangleleft_o G} G/U$$

as a limit of quotients by its open normal subgroups. If  $H$  is a finite group, we write

$$\text{Gen}_d(H) \subseteq H^{\times d}$$

for the subset of  $d$ -tuples of elements which generate  $H$ . This is a functor on the category of finite groups and epimorphisms. By assumption, for each open normal  $U \leq G$ ,  $\text{Gen}_d(G/U)$  is nonempty. By [Lemma 2.13](#), the limit

$$\varprojlim \text{Gen}_d(G/U) \subseteq \varprojlim (G/U)^{\times d} \simeq G^d$$

is nonempty. A point of the limit can be identified with a tuple  $(g_1, \dots, g_d)$  of elements of  $G$  with the property their images generate  $G/U$  for every open normal  $U$ . We deduce that the only open subgroup which contains  $g_1, \dots, g_d$  is all of  $G$ , so  $\langle g_1, \dots, g_d \rangle = G$  as needed.  $\square$

**Warning 2.16.** In the context of [Proposition 2.15](#), beware that the uniform upper bound on the number of generators of  $G/U$  cannot be dispensed with! In fact, all of  $G/U$  are finite, so they definitely admit *some* finite number of generators. However, not all profinite groups are finitely generated. For a specific example, consider

$$\prod_{n \in \mathbb{Z}} \mathbf{F}_2,$$

the product of infinitely many copies of the field with two elements. This is abelian and any element is of order 2, so that any finitely generated subgroup is finite hence closed. However, the product is uncountable, so this profinite group is not finitely generated.

As we now show, in finitely generated profinite groups, the structure of their open subgroups is somewhat constrained.

**Proposition 2.17.** *Let  $G$  be profinite and finitely generated. Then for every  $m \geq 0$ , there's only finitely open subgroups  $H \leq_o G$  of index  $m$ .*

*Proof.* Let  $H \leq_o G$  be an open subgroup of finite index  $m$ . Then  $H$  is the stabilizer of its own coset in the  $G$ -set

$$G/H,$$

on which  $G$  acts continuously since  $H$  is closed. It follows that each such  $G$  arises as a preimage of some subgroup of the symmetric group  $S_m$  along a continuous homomorphism  $G \rightarrow S_m$ . As any such homomorphism is determined by the images of the generators, there are only finitely many such homomorphisms. We deduce that there are only finitely many such  $H$ , as needed.  $\square$

**Corollary 2.18.** *If  $G$  is profinite and finitely generated, then any open subgroup  $H \leq_o G$  contains  $N \leq_o H$  which is open and topologically characteristic in  $G$ ; that is, preserved by all continuous automorphisms of  $G$ .*

*Proof.* If  $H$  is of index  $m$ , then we can take

$$N := \bigcap_{H \leq_o G, |H:G|=m} H,$$

the intersection of all open subgroups of the same index. This is again open, because the intersection is finite by [Proposition 2.17](#). Clearly,  $N$  is topologically characteristic.  $\square$

Recall the classical fact, most easily proven using covering spaces by reducing to the case of free groups, that if  $\Gamma$  is a finitely generated group and  $\Gamma' \leq \Gamma$  is a finite index subgroup, then  $\Gamma'$  is also finitely generated. In fact, if  $\Gamma$  can be generated by  $d$  elements and  $\Gamma$  is of index  $m$ , then the Schreier index formula tells us that  $\Gamma'$  can be generated by  $d' = 1 + d(m - 1)$  elements. We now show that the same is true in the setting of profinite groups and topological finite generation.

**Proposition 2.19.** *If  $G$  is profinite and finitely generated, then any open subgroup  $H \leq_o G$  is again finitely generated.*

*Proof.* Suppose that  $G$  can be generated by  $d$  elements and that  $H$  is of index  $m$ . Using [Proposition 2.15](#), it is enough to show that there exists some  $d'$  such that any quotient  $H/V$  by an open normal subgroup is generated by  $d'$  elements.

By making  $V$  smaller if necessary, using [Corollary 2.18](#) we can assume that  $V$  is normal in  $G$ . In this case,  $U/V$  can be identified with a subgroup of index  $m$  inside  $G/V$ . Since the latter can be generated by  $d$  elements, the Schreier index formula tells us that  $U/V$  can be generated by at most  $d' = 1 + d(m - 1)$  elements. This ends the argument.  $\square$

### 3. PRO- $p$ -GROUPS AND THE LOWER $p$ -SERIES

Before we move on to  $p$ -groups, let us say a little bit more about finite generation. In the theory of rings, an important notion is that of a Jacobson radical, which is given by the intersection of all maximal left ideals (equivalently, all maximal right ideals). Informally, the elements of the Jacobson radical are “small” and can often be safely ignored.

In the theory of profinite groups, the role of the Jacobson radical is played by the following important subgroup.

**Definition 3.1.** Let  $G$  be a profinite group. The *Frattini subgroup* is given by

$$\Phi(G) := \bigcap_{\substack{H \text{ maximal proper} \\ \text{open subgroup of } G}} H,$$

the intersection of maximal proper open subgroups; that is, those  $H \triangleleft_o G$  such that if  $H < K \leq G$  for some subgroup  $K$ , then  $K = G$ .

**Remark 3.2.** It is immediate from the definition that the Frattini subgroup is topologically characteristic; that is, preserved by all continuous automorphisms of  $G$ . In particular, it is normal. Moreover, it is closed as an intersection of closed subgroups.

Importantly, the Frattini subgroup is well-behaved with respect to passing to quotient groups.

**Lemma 3.3.** *Let  $K \triangleleft_c G$ . Then  $\Phi(G)K/K \leq \Phi(G/K)$ . If moreover  $K \leq \Phi(G)$ , then  $\Phi(G)K/K = \Phi(G/K)$ .*

*Proof.* We have to show that  $\Phi(G)K$  is contained in every maximal proper open subgroup  $H \leq G/K$ . For each such  $H$ , its preimage  $p^{-1}(H) \leq G$  is a maximal proper open subgroup of  $G$ , so that  $\Phi(G) \leq p^{-1}(H)$  and thus  $\Phi(G)K \leq H$ .

For the second part, suppose that  $K \triangleleft_c \Phi(G)$ . Suppose that  $gK \in \Phi(G/K)$ , so that  $gK \leq M$  for all maximal proper open subgroups which contain  $K$ . However, all maximal proper open subgroups contain  $K$  by assumption, so  $g \in M$  and thus  $g \in \Phi(G)$  as needed.  $\square$

The importance of the Frattini subgroup stems from the fact that its elements are “non-generators” in the following sense:

**Proposition 3.4.** *Let  $G$  be a profinite group. For a tuple  $g_1, \dots, g_d \in G$ , the following are equivalent:*

- (1)  $g_i$ 's generate  $G$ ,
- (2) the cosets  $g_i\Phi(G)$  generate  $G/\Phi(G)$ .

*Proof.* The forward direction is clear. For the backward one, assume by contradiction that

$$\overline{\langle g_1, \dots, g_n \rangle} \neq G.$$

Since a closed subgroup is an intersection of open subgroups which contain it, and any proper open subgroup is contained in a maximal one, it follows that

$$\overline{\langle g_1, \dots, g_n \rangle} \leq U$$

for  $U$  some maximal proper open subgroup. Since  $\Phi(G) \leq U$ , we deduce that

$$\overline{\langle g_1, \dots, g_n \rangle} \Phi(G) \leq U \neq G,$$

which contradicts the hypothesis that the cosets  $g_i\Phi(G)$  generate  $G/\Phi(G)$ .  $\square$

The theory of finite groups is quite complicated, but a particular class of groups which is much easier to understand is that of  $p$ -groups; that is, of those finite groups whose order is a power of a prime. Finite  $p$ -groups have many favourable properties which do not hold for a general finite group: for example, they are always nilpotent.

The profinite analogue of a finite  $p$ -group is given by the following notion.

**Definition 3.5.** A profinite group  $G$  is *pro- $p$*  if for every open subgroup  $U \leq_o G$ , the index  $|G : U|$  is a power of  $p$ .

The following analogue of [Theorem 2.8](#) is proven in the same way and we leave it to the interested reader.

**Proposition 3.6.** *For a topological group  $G$ , the following are equivalent:*

- (1)  $G$  is profinite and pro- $p$ ,
- (2) we can write  $G = \varprojlim G_i$  as a limit of finite  $p$ -groups equipped with the discrete topology.

**Remark 3.7.** If  $G$  is pro- $p$  and  $K \triangleleft_c G$  is a closed subgroup, then both  $K$  and  $G/K$  are also pro- $p$ . Conversely, if  $G$  is compact Hausdorff and  $K$  and  $G/K$  are pro- $p$ , then so is  $G$ .

We observe that, similarly to finite groups, profinite groups have *maximal* pro- $p$ -subgroups.

**Lemma 3.8.** *Let  $G$  be a profinite group. Then there exists a closed subgroup  $S \leq G$  with the following properties:*

- (1)  $S$  is pro- $p$ ,
- (2) for any open normal  $U \triangleleft_o G$ ,  $SU/U \leq G/U$  is a Sylow subgroup of the finite group  $G/U$ .

*In particular,  $S$  is maximal among all closed subgroups of  $G$  which are pro- $p$ . Moreover, any two such subgroups are conjugate.*

*Proof.* For each open normal subgroup  $U \triangleleft G$ , write  $\text{Syl}(G/U)$  for the set of Sylow subgroups of  $G/U$ . Since the image of a Sylow subgroup of a finite group in a quotient is again a Sylow subgroup,  $\text{Syl}(-)$  forms a contravariant functor into sets indexed by the poset of open normal subgroups.

By Sylow's theorem for finite groups,  $\text{Syl}$  takes value in non-empty finite sets, and we conclude from [Lemma 2.13](#) that its limit

$$\text{Syl}(G) := \varprojlim_{U \triangleleft G} \text{Syl}(G/U)$$

is non-empty. An element of this limit can be identified with a compatible family of Sylow subgroups of  $G/U$  whose limit is the needed subgroup  $S \leq G$ .

To see that any two such subgroups  $S_1, S_2$  are conjugate, one applies the same argument to the functor sending  $U$  to the set of elements of  $G/U$  that conjugate the images of  $S_1$  and  $S_2$  in  $G/U$ .  $\square$

**Definition 3.9.** If  $G$  is a profinite group, then a subgroup  $S \leq G$  satisfying the conditions of [Lemma 3.8](#) is called a  *$p$ -Sylow subgroup*.

We now go back to the Frattini subgroup. Our goal is to show that in the case of pro- $p$ -groups, it can be identified very explicitly. This rests on the following simple result:

**Lemma 3.10.** *If  $G$  is pro- $p$ , then every maximal proper open subgroup  $U \triangleleft_o G$  is normal and has index  $p$ .*

*Proof.* Since  $U$  is open, it contains an open normal subgroup  $V \leq U$ . Then,  $U$  is determined by its image in  $G/V$ , which is a maximal proper subgroup of the finite  $p$ -group  $G/V$ . It follows by induction on the nilpotence index of  $G/V$  that  $UV \leq G/V$  is normal and of index  $p$ , as needed.  $\square$

**Proposition 3.11.** *If  $G$  is pro- $p$ , then*

$$\Phi(G) = \overline{G^p [G, G]},$$

*the closed subgroup generated by  $p$ -th powers and commutators.*

*Proof.* We begin with  $(\supseteq)$  containment, where we have to show that if  $U \triangleleft_o G$  is a maximal proper open subgroup, then  $G^p [G, G] \leq U$ . By assumption, [Lemma 3.10](#),  $U$  is normal and  $G/U \simeq C_p$  is a cyclic group with  $p$  elements, so that it is abelian and of exponent  $p$ , as needed.

We now move on to  $(\subseteq)$ . We have to show that if  $U$  is an open subgroup containing  $G^p [G, G]$ , then  $\Phi(G) \leq U$ . Observe that  $G/U$  is a finite elementary abelian  $p$ -group; in other words, we have  $G/U \simeq \mathbf{F}_p^{\oplus n}$  for some  $n$ . It follows that  $\Phi(G/U) = 0$  and since

$$\Phi(G)U/U \leq \Phi(G/U) = 0$$

by [Lemma 3.3](#), we deduce that  $\Phi(G) \leq U$  as needed.  $\square$

**Corollary 3.12.** *If  $G$  is pro- $p$  and  $K \triangleleft_c G$  is a closed subgroup, then*

$$\Phi(G)K/K = \Phi(G/K).$$

*as subgroups of  $G/K$ .*

*Proof.* Since both subgroups are closed, it is enough to show that they have the same image in  $G/H$  where  $H$  is any open normal subgroup containing  $K$ . However, since both  $G$  and  $G/K$  are  $p$ -groups, in both cases the image consists of

$$(G/U)^p [G/U, G/U] \leq G/U$$

by [Proposition 3.11](#), as needed. □

**Warning 3.13.** Beware that [Corollary 3.12](#) is not true without the assumption that  $G$  is pro- $p$ , even in the setting of finite groups. As an explicit example, consider the cyclic group  $C_5$  with five elements. Multiplication by three  $3: C_5 \rightarrow C_5$  is a group automorphism of order four, and we can consider the associated semidirect product

$$F_5 := C_5 \rtimes C_4.$$

Explicitly,  $F_5$  has a presentation

$$F_5 = \langle a, b \mid a^5 = e, b^4 = e, b^{-1}ab = a^3 \rangle$$

It is not difficult to check that the subgroup generated by  $b$  and its conjugate generated by  $aba^{-1} = ba^2$  are both maximal and do not intersect, so that  $\Phi(F_5) = 0$ . However,  $F_5$  has  $C_4$  as a quotient, and  $\Phi(C_4) = 2C_4 \neq 0$ .

As we now show, in the case of pro- $p$  groups, not only is the Frattini subgroup quite easy to describe, it also essentially controls whether a given pro- $p$ -group is finitely generated.

**Theorem 3.14.** *If  $G$  is pro- $p$ , then the following are equivalent:*

- (1)  $G$  is finitely generated,
- (2)  $\Phi(G) \leq G$  is open. ‘

*Proof.* We first show the forward implication, so suppose that  $G$  can be generated by  $d < \infty$  elements. Let  $U \triangleleft_o G$  be an open normal subgroup containing  $\Phi(G) = \overline{G^p [G, G]}$ . Then  $G/U$  is an abelian  $p$ -group of exponent  $p$ , so that  $G/U \simeq \mathbf{F}_p^{\oplus n}$  for some  $n$ .

Since  $G/U$  is also generated by  $d$  elements, we must have  $n \leq d$ . We deduce that  $|U : G| \leq p^d$ . Since  $G$  is finitely generated, there is at most finitely many open subgroups with this property by [Proposition 2.17](#). We deduce that  $\Phi(G)$  is an intersection of finitely many open subgroups, hence it is open.

The backward implication is immediate from [Proposition 3.4](#), since if  $\Phi(G)$  is open, then  $G/\Phi(G)$  is finite and hence finitely generated. □

**Warning 3.15.** Beware that [Theorem 3.14](#) fails spectacularly for general profinite groups. For example, if we consider the free profinite group on one generator

$$\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p,$$

then its Frattini subgroup is given by

$$\Phi(\widehat{\mathbb{Z}}) = \prod_p p\mathbb{Z}_p.$$

This is a closed subgroup which is not open.

The construction of the Frattini subgroup can be refined to become a first step of an important canonical filtration on any pro- $p$ -group.

**Definition 3.16.** Let  $G$  be a pro- $p$  group. The *lower  $p$ -series* of  $G$  is the sequence of closed subgroups defined inductively by

- (1)  $P_1(G) = G$
- (2)  $P_{i+1}(G) = \overline{P_i(G)^p [P_i(G), G]}$ .

**Example 3.17.** For any  $G$ , we have  $P_2(G) = \Phi(G)$ . More generally,

$$\Phi(P_i(G)) \leq P_{i+1}(G),$$

but beware that in general this inclusion is strict. We will later show that for “nice” pro- $p$ -groups, such as small open subgroups of  $p$ -adic analytic groups, this is an equality for all  $i$ .

By induction, it is easy to see that each of the subgroups  $P_i(G)$  is normal. Moreover, by construction they have the property that for each  $i \geq 1$ , the subgroup

$$P_i(G)/P_{i+1}(G) \triangleleft G/P_{i+1}(G)$$

of the quotient is central and of exponent  $p$ . In fact, the lower  $p$ -series is the “fastest descending” filtration with this property in the following sense:

**Proposition 3.18.** *Let  $G$  be a pro- $p$ -group and let*

$$\dots \leq G_3 \leq G_2 \leq G_1 = G$$

*be a descending filtration by normal closed subgroups such that for each  $i \geq 1$ ,*

$$G_i/G_{i+1} \leq G/G_{i+1}$$

*is central and of exponent  $p$ . Then we have  $P_i(G) \leq G_i$  for each  $i \geq 1$ .*

*Proof.* We prove this by induction on  $i$ , the case of  $P_1(G) = G_1 = G$  being clear. If  $i > 1$ , then by inductive assumption  $P_{i-1} \leq G_{i-1}$ . To show that  $P_i \leq G_i$ , it is enough to show that the composite

$$P_i := \overline{P_{i-1}^p [P_{i-1}(G), G]} \rightarrow P_{i-1} \rightarrow G_{i-1} \rightarrow G_{i-1}/G_i$$

is zero. However, the elements of  $P_{i-1}^p$  go to zero since  $G_{i-1}/G_i$  is of exponent  $p$ , and the elements of  $[P_{i-1}(G), G]$  go to zero since they factor through  $[G_{i-1}, G]$  and  $G_{i-1}/G_i$  is assumed central in  $G/G_i$ . □

**Corollary 3.19.** *If  $G$  is a finite  $p$ -group, then  $P_i(G) = 0$  for all  $i$  large enough.*

*Proof.* By [Proposition 3.18](#), it is enough to show that there exists *some* finite filtration

$$0 = G_{n+1} \leq G_n \leq G_{n-1} \leq \dots \leq G_1 = G$$

where each group is central and of exponent  $p$  relative to the previous one. We prove this by induction on the order  $\#G = p^n$ .

If  $n = 0$ , there is nothing to be proven. Otherwise,  $G$  has a non-zero center which contains some cyclic group of order  $p$ . Taking  $G_n := C_p \leq Z(G)$  and applying the inductive assumption to  $G/C_p$  finishes the argument. □

**Proposition 3.20.** *Let  $G$  be pro- $p$ .*

- (1) *If  $K \leq_c G$ , then  $P_i(G)K/K = P_i(G/K)$*
- (2) *We have  $\bigcap_i P_i(G) = \{e\}$ .*
- (3) *If  $G$  is finitely generated, then all of the  $P_i(G)$  are open and hence a basis of neighbourhoods of the identity.*

*Proof.* We begin with (1). Since each of  $P_i(G)/P_{i+1}(G) \leq G/P_{i+1}$  is central and of exponent  $p$ , and both of these properties are stable under taking quotients, the same is true about their images in  $G/K$ . We deduce from [Proposition 3.18](#) that  $P_i(G/K) \leq P_i(G)K/K$  for each  $i \geq 1$ .

To see that  $P_i(G)K/K \leq P_i(G/K)$ , we argue by induction. The base case is clear, and the inductive step follows from the inductive formula for the lower  $p$ -series.

To show (2), it is enough to verify that  $\bigcap_i P_i(G)$  is contained in any open normal subgroup  $U$ . Since  $G$  is a finite  $p$ -group, by [Corollary 3.19](#) we have

$$P_i(G)U/U = P_i(G/U) = 0$$

for  $i$  large enough, where the first equality is part (1). It follows that  $P_i(G) \leq U$  for  $i$  large enough, as needed.

To show (3), we argue by induction, starting with  $G_1 = G$  which is open. If  $G_{i-1}$  is open, it is also finitely generated by [Proposition 2.19](#). Since  $\Phi(G_{i-1}) \leq G_i$  is open by [Theorem 3.14](#), we deduce that so is  $G_i$ , as needed.  $\square$

The last property we show, which is a little bit more involved, is that the lower  $p$ -series filtration is compatible with the commutator:

**Theorem 3.21.** *Let  $G$  be a pro- $p$ -group. Then*

$$[P_i(G), P_j(G)] \leq P_{i+j}(G).$$

This requires a little bit of work, so before delving into the proof, let us discuss a little bit of the motivation. Associated to any filtration by normal subgroups we have the associated graded

$$\text{gr}_i(G) := P_i(G)/P_{i+1}(G).$$

In the case of a lower  $p$ -series, the quotients are abelian and of exponent  $p$ , hence the associated graded is in fact a graded  $\mathbf{F}_p$ -vector space. As a consequence of [Theorem 3.21](#), the commutator of  $G$  induces a function

$$[-, -] : \text{gr}_i(G) \times \text{gr}_j(G) \rightarrow \text{gr}_{i+j}(G).$$

One can show that this function is in fact a  $\mathbf{F}_p$ -Lie algebra structure. For particularly nice pro- $p$  groups this Lie algebra structure remembers a whole deal about  $G$ , and can be thought of as a form of “linearization”.

To prove [Theorem 3.21](#), we will need some basic formulas from group theory, which we recall. If  $a, b, c \in G$  are elements of a group, we write

$$a^b := b^{-1}ab$$

for the conjugation and

$$[a, b] := a^{-1}a^b = a^{-1}b^{-1}ab$$

for the commutator. This can be extended to three elements by declaring that

$$[a, b, c] := [[a, b], c].$$

**Recollection 3.22** (Hall-Witt identity). The celebrated *Hall-Witt identity* says that

$$[a, b^{-1}, c]^b \cdot [b, c^{-1}, a]^c \cdot [c, a^{-1}, b]^a = e$$

for any group  $G$  and  $a, b, c \in G$ . With enough patience, this can be verified by expanding the left hand side out. As a consequence, we have the *three subgroup lemma* which says that if  $A, B, C \triangleleft G$  are the normal subgroups, then

$$[A, B, C] \leq [B, C, A][C, A, B].$$

Note that for subgroups we have

$$[A, B] = [B, A]$$

and similarly

$$[A, [B, C]] = [[A, B], C].$$

**Recollection 3.23** (Conjugate-linearity of the commutator). In any group, the commutator is linear up to conjugation in the sense that

$$[a, bc] = [a, c][a, b]^c.$$

and

$$[ab, c] = [a, c]^b[a, b].$$

Again, the proof is given by expanding both sides out. This is most useful when, for example, we know that the commutators we're interested are contained in the center, in which case the conjugation can be omitted. Iterating these identities, we deduce that for any  $n \geq 0$  we have

$$[a, b^n] = [a, b] \cdot [a, b]^b \cdot [a, b]^{b^2} \cdot \dots \cdot [a, b]^{b^{n-1}}$$

and similarly

$$[a^n, b] = [a, b]^{a^{n-1}} \cdot \dots \cdot [a, b]^a \cdot [a, b].$$

*Proof of Theorem 3.21:* For brevity, we write  $G_i := P_i(G)$  for the lower  $p$ -series. We want to show that

$$[G_m, G_n] \leq G_{m+n},$$

and we argue by induction on  $n$ . For the base case of  $n = 1$ , we observe that

$$[G_m, G] \leq \overline{G_m^p [G_m, G]} = G_{m+1}.$$

We now assume that  $n > 1$ . Since  $G_{n+m}$  is closed, it is enough to show that  $[G_m, G_n] \leq N$  for any open subgroup of  $G$  which contains  $G_{n+m}$ . Since the lower  $p$ -series filtration is compatible with passing to quotients by part (1) of Proposition 3.20, we can replace  $G$  by  $G/N$  and thus assume that

- (1)  $G$  is finite and
- (2)  $G_{n+m} = 0$ .

It follows from the second property that  $G_{n+m-1}$  is central and of exponent  $p$ . If  $x \in G_m$  and  $y \in G_{n-1}$ , then by induction we have  $[x, y] \in G_{n+m-1}$ . Using the conjugate-linearity of the commutator of Recollection 3.23, where we can ignore the conjugations since these commutators are central, we see that

$$(3.1) \quad [x, y^p] = [g, x]^p = e.$$

Moreover, using the three subgroup lemma of Recollection 3.22 we have that

$$(3.2) \quad [G_m, [G_{n-1}, G]] \leq [G_{n-1}, [G, G_m]] [G, [G_m, G_{n-1}]] = [G_{n+m-1}, G] [G, G_{n+m-1}] = \{e\},$$

where we apply the inductive assumption that

$$[G_{n-1}, G_m] = [G_m, G_{n-1}] \leq G_{n+m-1}$$

which is central. Combining (3.1), (3.2) with another application of the linearity of the commutator, we see that

$$[G_m, G_n] = [G_m, G_{n-1}^p [G_{n-1}, G]] \leq \{e\}$$

which is what we wanted to show. □

#### 4. TOPOLOGY OF FINITELY GENERATED PRO- $p$ GROUPS

The goal of this lecture is to prove the following striking result of Serre.

**Theorem 4.1** (Serre). *Let  $G$  be a finitely generated pro- $p$  group. Then any finite index subgroup  $H \leq G$  is open.*

Since the topology of a profinite group is completely determined by which of its subgroups are open, Theorem 4.1 implies that for finitely generated pro- $p$  groups, their topology is completely determined by the group structure. In fact, we have the following strong consequence:

**Corollary 4.2.** *Let  $G$  be a finitely generated pro- $p$  group and  $G'$  be a profinite group. Then any abstract group homomorphism  $G \rightarrow G'$  is continuous.*

*Proof.* We can write  $G' \simeq \varprojlim G'_\alpha$  as a limit of finite groups. To show that an abstract group homomorphism  $G \rightarrow G'$  is continuous, it is enough to verify that each of the composites

$$G \rightarrow G' \rightarrow G'_\alpha$$

is; that is, has an open kernel. But the kernel is a finite index subgroup, hence the result follows from [Theorem 4.1](#).  $\square$

Before we prove [Theorem 4.1](#), we will need a few preliminary results.

**Lemma 4.3.** *Let  $G$  be pro- $p$  and  $H \leq G$  be a finite index subgroup, not necessarily closed. Then the index  $|G : H|$  is a power of  $p$ .*

*Proof.* By replacing  $H$  by the intersection of its conjugates, we can assume that  $H$  is normal. If  $n \geq 1$ , we write

$$G^{\{n\}} := \{g^n \mid g \in G\}$$

for the set of  $n$ -th powers. This is the image of the  $n$ -th power map  $G \rightarrow G$  and hence is a closed subset. Let  $m = |G : H|$  be the order, which we can write as

$$m = qp^r$$

where  $q$  is coprime to  $p$ . We will show that

$$(4.1) \quad G^{\{p^r\}} \subseteq G^{\{m\}},$$

which since  $G^{\{m\}} \subseteq H$  will imply that  $G/H$  is of exponent  $p^r$  and hence a  $p$ -group, as needed.

Let  $N$  be an open normal subgroup. Since  $G/N$  is a  $p$ -group by assumption, we can find  $e \geq r$  such that the  $|N : G|$  divides  $p^e$  and so  $G^{\{p^e\}} \subseteq N$ . Since  $q$  is coprime to  $p$ , we can find  $a, b \in \mathbb{Z}$  such that

$$p^r = am + bp^e$$

and thus for any  $g \in G$  we have

$$g^{p^r} = (g^a)^m (g^b)^{p^e} \in G^{\{m\}} N.$$

Since this holds for any  $N$  and  $G^{\{m\}}$  is closed, we deduce that  $g^{p^r} \in G^{\{m\}}$ . This shows (4.1) and hence the needed statement.  $\square$

The second result we will need is slightly more involved, and its proof requires a little bit of theory of nilpotent groups which we now recall.

**Recollection 4.4.** A finite group  $G$  is said to be *nilpotent* if there exists a finite filtration

$$0 = G_{c+1} \leq G_c \leq \dots \leq G_1 = G$$

such that for each  $i \geq 1$ ,  $G_i/G_{i+1} \leq G/G_{i+1}$  is central. It follows by induction that each of  $G_i \leq G$  is a normal subgroup. If a group is nilpotent, then its *lower central series* defined inductively by

- (1)  $\gamma_1(G) := G$ ,
- (2)  $\gamma_{i+1}(G) := [\gamma_i(G), G]$

terminates at a finite stage in the trivial subgroup. If  $\gamma_c(G) \neq 0$  but  $\gamma_{c+1}(G) = 0$ , we say that  $G$  is of *nilpotence index  $c$* .

**Example 4.5.** Finite  $p$ -groups are nilpotent (for example, by [Corollary 3.19](#)).

**Lemma 4.6.** *Let  $G$  be a finite nilpotent group generated by  $a_1, \dots, a_d \in G$ . Then any element  $x \in [G, G]$  of the derived subgroup can be written as a product of  $d$  commutators*

$$x = [g_1, a_1] \cdot \dots \cdot [g_d, a_d]$$

for some  $g_i \in G$ .

*Proof.* We prove this by induction on the nilpotence index  $c$  of  $G$ . If  $c \leq 1$ , then  $G$  is abelian and there is nothing to prove.

Now suppose that  $G$  is of nilpotence index  $c > 1$  and that the needed statement holds for all nilpotent groups of smaller nilpotence index. For brevity, we write  $G_i := \gamma_i(G)$  for the lower central series. Observe that  $G_c = [G_{c-1}, G]$  is in the center. Using the conjugate-linearity of the commutator of [Recollection 3.23](#), which is simple linearity here as all of these commutators are in the center, we deduce that the map

$$[-, -] : G_{c-1} \times G \rightarrow Z(G)$$

is multiplicative in each variable. As the target is abelian, we deduce that it factors through a linear map

$$G_{c-1}^{ab} \otimes G^{ab} \rightarrow Z(G)$$

from the tensor product of the abelianizations. Since  $G^{ab}$  is an abelian group generated by the images of the  $a_i$ , any of elements can be written in the form  $x_1 \otimes a_1 + \dots + x_d \otimes a_d$  for some  $x_i \in G_{c-1}$ . Thus, any element  $w \in G_c$  can be written in the form

$$w = [x_1, a_1] \cdot \dots \cdot [x_d, a_d].$$

for some  $x_i \in G_{c-1}$ .

By inductive assumption, the result holds for  $G/G_c$ , so that any element of the derived group can be written as

$$[g_1, a_1] \cdot \dots \cdot [g_d, a_d] w$$

where  $w \in G_c$ . Using the previous paragraph, we deduce that any element of  $[G, G]$  can be written as

$$[g_1, a_1] \cdot \dots \cdot [g_d, a_d] \cdot [x_1, a_1] \cdot \dots \cdot [x_d, a_d]$$

with  $x_i \in G$ . Since the commutators  $[x_i, a_i]$  are in the center, using conjugate-linearity we can rewrite this product as

$$[g_1 x_1, a_1] \cdot \dots \cdot [g_d x_d, a_d]$$

which is what we wanted to show. □

**Proposition 4.7.** *Let  $G$  be a finitely generated pro- $p$  group. Then the derived subgroup  $[G, G]$  is closed.*

*Proof.* Let  $a_1, \dots, a_d$  be generators of  $G$ , and consider the continuous map

$$[-, a_1] \cdot \dots \cdot [-, a_d] : G^d \rightarrow G$$

whose image  $X \subseteq G$  is closed and contained in  $[G, G]$ . We claim that  $X = \overline{[G, G]}$  which implies that  $[G, G] = \overline{[G, G]}$  as needed. Since both  $X$  and the closure of the derived group are closed, it is enough to verify that they have the same image in the quotient  $G/N$  for any open normal subgroup  $N \triangleleft_o G$ , which is an immediate consequence of [Lemma 4.6](#) as  $G/N$  is a nilpotent group generated by the images of the  $a_i$ . □

We are now ready to prove Serre's theorem.

*Proof of Theorem 4.1:* Let  $H$  be a finite index subgroup of  $G$ , which we can assume to be normal. By Lemma 4.3,  $G/H$  is a  $p$ -group, so that  $|G : H| = p^n$ . We prove the result by induction on  $n \geq 1$ , since the case of  $n = 0$  is trivial.

We first tackle the case of  $n = 1$ , in which we have  $G/H \simeq C_p$ , a cyclic group of order  $p$ . Since  $G$  is finitely generated pro- $p$ , we can rewrite the Frattini subgroup as

$$\Phi(G) = \overline{G^p[G, G]} = \overline{G^{\{p\}}[G, G]} = G^{\{p\}}[G, G],$$

where the first equality is Proposition 3.11, the second is the fact that in  $G/[G, G]$  the  $p$ -th powers form a subgroup, and the last one is a consequence of the fact the derived subgroup is closed by Proposition 4.7. Since  $G/H$  is abelian of exponent  $p$ , we deduce that we have  $\Phi(G) \leq H$ . Since the Frattini subgroup is open by Theorem 3.14, we deduce that so is  $H$  as needed.

Now assume that  $|G : H| = p^n$  with  $n > 1$ . Since  $G/H$  is a  $p$ -group, by iteratively choosing a subgroup isomorphic to  $C_p$  in the center of the quotient we can construct a sequence of normal subgroups

$$H = H_n \leq H_{n-1} \leq \dots \leq H_0 = G$$

where each one is of index  $p$  in the next one. By what we've shown in the previous paragraph,  $H_1$  is open inside  $G$ . It follows from Proposition 2.19 that  $H_1$  is also finitely generated and pro- $p$ . Since  $|H_n : H_1| = p^{n-1}$ , from inductive assumption we deduce that  $H_n$  is open in  $H_1$ , and thus also in  $G$ . This ends the argument.  $\square$

### 5. POWERFUL FINITE $p$ -GROUPS

In this lecture, we will study a very important class of finite  $p$ -groups which are known as *powerful*. This class has the advantage of being quite general (for example, we will prove later in the course that any  $p$ -adic analytic group has an open subgroup which is a limit of powerful finite  $p$ -groups) and at the same time sharing some favourable properties of abelian groups.

Continuing from previous lectures, if  $G$  is a group, we write

$$G^{\{p\}} := \{g^p \mid g \in G\}$$

for the subset of  $p$ -th powers and

$$G^p := \langle G^{\{p\}} \rangle$$

for the subgroup they generate. Two important properties of abelian groups which we will show are shared by all powerful  $p$ -groups are that

- (1)  $G^{\{p^k\}} = G^{p^k}$ ; that is, the  $p^k$ -th powers form a subgroup,
- (2) the map  $x \rightarrow x^p$  defines a group homomorphism  $G^{p^k}/G^{p^{k+1}} \rightarrow G^{p^{k+1}}/G^{p^{k+2}}$ <sup>3</sup>.

Informally, powerful  $p$ -groups are those which are “abelian up to  $p$ -th powers”. The precise definition, which is different at odd and even primes, is as follows:

**Definition 5.1.** A finite  $p$ -group  $G$  is said to be *powerful* if

- (1)  $[G, G] \leq G^p$  and  $p > 2$ ,
- (2)  $[G, G] \leq G^4$  and  $p = 2$ .

**Warning 5.2** (The even prime). As we see, the definition of a powerful  $p$ -group is slightly different when  $p = 2$ . An adjustment is in some sense necessary, since if  $G$  is a group of exponent 2, then for any  $x, y \in G$  we have

$$e = (xy)^2 = xyxy = x^{-1}y^{-1}xy = [x, y]$$

and thus the group is abelian. Thus, for any finite group we have  $[G, G] \leq G^2$ , and the obvious analogue of the definition of being powerful at odd primes has no teeth when  $p = 2$ .

<sup>3</sup>Of course, if  $G$  is abelian, then  $x \mapsto x^p$  is an endomorphism of  $G$ , even before passing to quotients. In the powerful case, this is in general only true if we consider this as a map between the quotients  $G^{p^k}/G^{p^{k+1}}$ .

Thus unfortunately means that some of the proofs of basic properties of powerful groups need to be slightly adjusted when  $p = 2$ . In these notes, we take the convention of only stating results which are true at all primes (or otherwise being specific as to what is true at what prime), but we will usually only give the proof in the case of  $p > 2$ . The arguments for  $p = 2$  are minor variations; a reader interested in seeing the details should consult [DDSMS03].

**Example 5.3.** Abelian  $p$ -groups are powerful.

**Example 5.4.** Let  $p > 2$  and consider group of order  $p^3$  given by the semi-direct product  $G := (C_{p^2}) \rtimes C_p$  with respect to some non-trivial homomorphism  $C_p \rightarrow \text{Aut}(C_{p^2}) \simeq (\mathbb{Z}/p^2)^\times$ . Then  $G/G^p$  can be identified with

$$(C_{p^2}/pC_{p^2}) \rtimes C_p \simeq C_p \rtimes C_p \simeq C_p \times C_p,$$

which is abelian. Thus,  $G$  is a powerful, non-abelian  $p$ -group.

**Warning 5.5.** Not all  $p$ -groups are powerful. For example, if  $p > 2$ , then the group of order  $p^3$  with explicit presentation

$$\langle x, y, z \mid x^p = y^p = z^p = e, [x, z] = [y, z] = e, [x, y] = z \rangle$$

is not powerful, since it is of exponent  $p$  but it is not abelian. This group can be equivalently described as  $(C_p \times C_p) \rtimes C_p$  or as unitriangular  $3 \times 3$  matrices over the field  $\mathbf{F}_p$ .

When working with powerful groups, a relative notion is often useful.

**Definition 5.6.** Let  $G$  be a finite  $p$ -group and let  $N \leq G$  be a subgroup. We say that  $N$  is *powerfully embedded in  $G$* , which we denote by  $N$  *p.e.*  $G$ , if

- (1)  $[N, G] \leq N^p$  and  $p > 2$  or
- (2)  $[N, G] \leq N^4$  and  $p = 2$ .

**Remark 5.7.** A finite  $p$ -group  $G$  is powerful if and only if it is powerfully embedded in itself.

**Remark 5.8.** Observe that if  $N$  *p.e.*  $G$ , then  $N$  is a normal subgroup of  $G$ .

The following stability under quotients follows straight from the definitions:

**Lemma 5.9.** *If  $N \leq G$  and  $K \triangleleft G$  are subgroups, the following hold:*

- (1) *if  $N$  *p.e.*  $G$ , then  $NK/K$  *p.e.*  $G/K$ ,*
- (2) *if  $K \leq N^p$ , then the converse holds: if  $NK/K$  *p.e.*  $G/K$ , then also  $N$  *p.e.*  $G$ .*

The following technical lemma, while strange-looking at first sight, is useful in inductive arguments.

**Lemma 5.10.** *Let  $G$  be a finite  $p$ -group with  $p > 2$ . Let  $N \triangleleft G$  be a normal subgroup and suppose that  $N$  is not powerfully embedded in  $G$ . If  $p > 2$ , then there exists a normal  $J \triangleleft G$  such that*

$$N^p[N, G, G] \leq Y < N^p[N, G]$$

and  $|Y : N^p[N, G]| = p$ .

*Proof.* If  $N$  is not powerfully embedded, then  $N^p < N^p[N, G]$ . Since both are normal subgroups of a  $p$ -group  $G$ , we can find a normal  $J \triangleleft G$  such

$$N^p \leq J < N^p[N, G]$$

and such that the second inclusion is of index exactly  $p$  (for example, by taking the preimage of a maximal proper subgroup of  $[N, G]N^p/N^p$ , which is necessarily normal since  $[N, G]$  is). We claim that  $J$  has the needed properties, of which the only remaining is that  $[N, G, G] \leq J$ . This is equivalent to saying that  $[N, G]J/J$  is central in  $G/J$ , which is clear since it is a normal subgroup of order  $p$ , and  $p$ -groups cannot act trivially on cyclic groups of order  $p$ .  $\square$

**Remark 5.11.** [Lemma 5.10](#) has a variant at  $p = 2$ , namely one can show in the same situation there exists a normal  $J$  such that

$$N^4[N, G]^2[N, G, G] \leq J < N^4[N, G],$$

where the second inclusion is of index exactly 2. This turns out to be enough to also prove [Proposition 5.13](#) at  $p = 2$ , which in these notes we only prove at odd primes.

**Remark 5.12.** The usefulness of [Lemma 5.10](#) is as follows: suppose we have a subgroup  $N \triangleleft G$  which we want to show is powerfully embedded. Arguing by contradiction, we can assume that it is not, and we can find a subgroup  $J$  as in [Lemma 5.10](#). Writing  $\tilde{G} := G/J$  and  $\tilde{N} := NJ/J$  for the image of  $N$ , we see that

- (1)  $\tilde{N}$  is of exponent  $p$ ,
- (2)  $[\tilde{N}, \tilde{G}]$  is central in  $\tilde{G}$  and is of order exactly  $p$ .

These two properties guarantee that  $\tilde{P}$  is also not powerfully embedded in  $\tilde{G}$ . This allows one to only study the possible failure to be powerfully embedded in the restrictive class of examples satisfying these two properties.

**Proposition 5.13.** *Let  $G$  be a finite  $p$ -group and  $N$  p.e.  $G$ . Then we also have  $N^p$  p.e.  $G$ .*

*Proof.* Suppose for contradiction that  $N^p$  is not powerfully embedded. Replacing  $G$  by a quotient by a suitable subgroup produced by [Lemma 5.10](#) as in [Remark 5.12](#), we can assume that

- (1)  $(N^p)^p = 0$  and
- (2)  $[N^p, G]$  is of order exactly  $p$  and is central in  $G$ .

Pick elements  $n \in N$  and  $g \in G$ . Since  $N$  p.e.  $G$ , we deduce that  $[N, G, G] \leq [N^p, G] \leq Z(G)$ , where the last subgroup is the center. Using the conjugate-linearity of the commutator of [Recollection 3.23](#), which is ordinary linearity here as the relevant commutators are central, we deduce that the map

$$w \mapsto [n, g, w]$$

defines a group homomorphism  $G \rightarrow Z(G)$ . It follows that we have

$$(5.1) \quad \prod_{j=0}^{p-1} [n, g, n^j] = \prod_{j=0}^{p-1} [n, g, n]^j = ([n, g, n]^p)^{p-1/2} = e,$$

where the last equality follows from the fact that  $[N, G, G] \leq [N^p, G]$  and the latter is of order  $p$ . We now consider the bracket

$$[n^p, g] = [n, g]^{n^{p-1}} \cdot [n, g]^{n^{p-2}} \cdot \dots \cdot [n, g]^{n^0}$$

which we can rewrite as

$$[n, g] \cdot [n, g, n^{p-1}] \cdot [n, g] \cdot [n, g, n^{p-2}] \cdot \dots \cdot [n, g] \cdot [n, g, n^0].$$

Since all of the triple commutators are central, we can collect them together and moreover their product vanishes by (5.1). It follows that we have

$$[n^p, g] = [n, g]^p$$

which necessarily vanishes since  $[N, G]^p \leq (N^p)^p = 0$ . This shows that  $[N^p, G] = 0$ , which implies that  $N^p$  p.e.  $G$ , as needed.  $\square$

Recall that associated to a finite  $p$ -group  $G$  we have the lower  $p$ -series of [Definition 3.16](#). This is a descending filtration of  $G$  by subgroups defined inductively by

- (1)  $P_1(G) := G$  and
- (2)  $P_{i+1}(G) := P_i(G)^p [P_i(G), G]$  for  $i \geq 1$ .

We now show that the lower  $p$ -series of a *powerful*  $p$ -group is exceptionally well-behaved, and in many ways resembles the filtration by  $p$ -th powers one has on any abelian  $p$ -group. The following two theorems establish crucial properties of powerful  $p$ -groups which we alluded to at the beginning of the lecture.

**Theorem 5.14.** *Let  $G$  be a powerful finite  $p$ -group and write  $G_i := P_i(G)$  for its lower  $p$ -series. Then*

- (1)  $G_i$  *p.e.*  $G$  for all  $i$ ,
- (2)  $G_{i+1} = G_i^p = \Phi(G_i)$ ,
- (3) the map  $x \mapsto x^p$  defines an onto group homomorphism

$$G_i/G_{i+1} \rightarrow G_{i+1}/G_{i+2}$$

for any  $i \geq 1$ .

*Proof.* We prove (1) and (2) together by induction on  $i$ . For the beginning of the induction, observe that since  $G$  is powerful, we have  $G_1$  *p.e.*  $G_1$ . Now suppose inductively that we know that  $G_i$  *p.e.*  $G$ . Then, we have  $[G_i, G] \leq G_i^p$ , so that

$$\Phi(G_i) \leq P_{i+1}(G) = G_i^p [G_i, G] \leq G_i^p \leq \Phi(G_i)$$

and thus all of these groups are equal to each other. Moreover,  $G_{i+1} = G_i^p \leq G$  is powerful by the inductive assumption and [Proposition 5.13](#).

We now move on to (3). Since we had already shown that for powerful  $p$ -groups the lower  $p$ -series is just the sequence of subgroups of  $p^k$ -th powers, by reindexing we can take  $G = G_i$  and thus assume that  $i = 1$ . We then have to show that  $x \mapsto x^p$  defines a group homomorphism

$$G_1/G_2 \rightarrow G_2/G_3.$$

Since this property doesn't depend on  $G_3$ , we can assume that  $G_3 = 0$ . In this case, we have  $G_2^p = 0$ ,  $[G, G] \leq G_2$  and  $G_2 \triangleleft G$  is central, since  $G$  is powerful and  $G_2$  *p.e.*  $G$ . If  $x, y \in G$ , then we have

$$(xy)^p = x^p y^p [x, y]^{\frac{p-1}{2}} = x^p y^p$$

where the first equality follows from the fact that to commute the  $x$ -s past the  $y$ -s we need to insert the commutators  $[x, y]$ , all of which are central and hence be grouped together, and the second from the fact that  $[x, y] \in G_2$  hence  $[x, y]^p = e$ . This ends the argument.  $\square$

**Lemma 5.15.** *If  $N$  *p.e.*  $G$  and  $x \in G$ , then the subgroup  $H = \langle N, x \rangle$  generated by  $N$  and  $x$  is powerful.*

*Proof.* We claim that we have  $[N, H] = [H, H]$ . To see this, notice that  $H/[N, H]$  has the image of  $N$  in its center, and is generated over its centre by a single element. Since any element commutes with itself and the center,  $H/[N, H]$  is abelian, which gives the claim. Then

$$[H, H] = [N, H] \leq N^p \leq H^p,$$

where the first inequality is the assumption that  $N$  *p.e.*  $G$ , which is what we wanted to show.  $\square$

**Warning 5.16.** In the context of [Lemma 5.15](#), beware that  $\langle N, x \rangle \leq G$  need not be powerfully embedded. The conclusion is only that  $\langle N, x \rangle$  is powerful as a group on its own.

**Theorem 5.17.** *If  $G$  is powerful, then*

$$G^p = G^{\{p\}} = \{g^p \mid g \in G\};$$

that is, the subset of  $p$ -th powers forms a subgroup.

*Proof.* We prove this by induction on the order  $\#G = p^n$ . If  $n = 0$ , then the group is trivial and there is nothing to prove.

Suppose that  $n > 0$  and let  $g \in G^p$ . Since the homomorphism in part (3) of [Theorem 5.14](#) is onto, we know we can write

$$g = x^p y$$

for  $x \in G$  and  $y \in G_3$ . Let's write  $H = \langle G_2, x \rangle$  for the subgroup generated by  $G_2$  and  $x$ , which is powerful by [Lemma 5.15](#). We have  $g \in H^p$ , since  $y$  is in  $G_3 = G_2^p$ . We now have two cases:

- (1) If  $H \neq G$ , then since  $H$  has smaller order than  $G$ , the inductive hypothesis gives that  $g = h^p$  for some  $h \in H$ , so that  $g$  is also a  $p$ -th power in  $G$ .
- (2) If  $H = G$ , then since  $G/G_2$  is a cyclic group generated by an element  $x$ , and since  $G_2 = \Phi(G)$  is the Frattini subgroup,  $G$  itself is generated by  $x$ . It follows that  $G$  is abelian, which also gives the needed claim.

□

## 6. PRO- $p$ -GROUPS OF FINITE RANK

In the last lecture, we introduced the notion of a powerful finite  $p$ -group. The condition of being powerful naturally extends to the profinite context in the following way:

**Definition 6.1.** A pro- $p$ -group  $G$  is *powerful* if

- (1)  $[G, G] \leq \overline{G^p}$  and  $p > 2$  or
- (2)  $[G, G] \leq \overline{G^4}$  and  $p = 2$ .

We say an open subgroup  $N \leq_o G$  is *powerfully embedded*, denoted by  $N$  *p.e.*  $G$ , if

- (1)  $[G, N] \leq \overline{N^p}$  and  $p > 2$  or
- (2)  $[G, N] \leq \overline{N^4}$  and  $p = 2$ .

As we will see, in the pro- $p$  context the notion of being powerful arguably is even more important than in the finite case, as it turns out to be closely related to a very natural finiteness condition known as being *finite rank*. Since all finite  $p$ -groups are finite rank, this condition does not naturally arise in the finite context.

We first collect basic properties of powerful pro- $p$ -groups, all of which follow immediately from the case of finite groups.

**Proposition 6.2.** *Let  $N \leq_o G$  be an open subgroup. Then  $N$  p.e.  $G$  if and only if for each open normal  $O \triangleleft_o G$  we have  $NO/O$  p.e.  $G/O$ .*

*Proof.* This is immediate from the formula

$$\overline{G^p} = \bigcap G^p O,$$

where the intersection is taken over all open normal subgroups of  $G$ , and similarly for  $\overline{G^4}$ . □

**Corollary 6.3.** *A pro- $p$ -group  $G$  is a powerful if and only if it can be written as a cofiltered limit of powerful finite  $p$ -groups and surjections.*

*Proof.* If  $G$  is powerful, then  $G \simeq \varprojlim G/O$ , where the limit is taken over the poset of open normal subgroups.

Conversely, suppose that  $G \simeq \varprojlim G_\alpha$  can be written as a cofiltered limit of powerful finite  $p$ -groups and surjections. If  $N \leq_o G$  is an open subgroup, then it contains the kernel of the surjection  $G \rightarrow G_\alpha$  for some  $\alpha$ , so that  $G/K$  is a quotient of  $G_\alpha$ . It follows that  $G/K$  is also powerful. □

Recall that in [Definition 3.16](#) we introduced the lower  $p$ -series, which is a filtration of a pro- $p$ -group  $G$  by subgroups defined inductively by

- (1)  $P_1(G) = G$

$$(2) P_{i+1}(G) = \overline{P_i(G)^p [P_i(G), G]}.$$

We now observe that, as in the finite case, for powerful pro- $p$ -groups the lower  $p$ -series has a particularly simple form.

**Theorem 6.4.** *Let  $G$  be a powerful pro- $p$ -group. Then for any  $i \geq 1$  we have*

- (1)  $P_{i+1}(G) = \overline{G^{p^i}} = \{g^{p^i} \mid g \in G\}$  and
- (2)  $P_{i+1}(G)$  is powerfully embedded in  $G$ .

*Proof.* Both  $P_{i+1}(G)$  and  $\overline{G^{p^i}}$  are stable under passing to finite quotients (in the sense that their image in a finite quotient is the corresponding subgroup of the quotient group), so the first equality is true as it is true when  $G$  is a finite  $p$ -group by [Theorem 5.14](#). Similarly, as the condition of being powerfully embedded is also detected in finite quotients by [Proposition 6.2](#), conclusion (2) also follows from the finite case.

We are left with showing that  $\overline{G^{p^i}} = \{g^{p^i} \mid g \in G\}$ . Since both subsets are closed, the latter as an image of a continuous self-map of  $G$ , it is enough to verify that they have the same image in  $G/O$  for any open normal  $O$ , which is a consequence of [Theorem 5.17](#).  $\square$

We now move to the discussion of rank, which we first do in the finite case.

**Definition 6.5.** Let  $G$  be a finite group. Then we write

- (1)  $d(G) = \inf\{|X| \mid X \subseteq G, \langle X \rangle = G\}$  for the *minimal number of generators* of  $G$  and
- (2)  $\text{rk}(G) = \sup\{d(H) \mid H \leq G\}$  for the *rank* of  $G$ ; that is, the smallest number  $d$  such that all subgroups of  $G$  can be generated by  $d$  elements.

**Warning 6.6** (Important!). In most of group theory literature, what we call in [Definition 6.5](#) the minimal number of generators would be called *rank* and what we call rank would be instead called *subgroup rank*. Our non-standard convention follows that of [\[DDSMS03\]](#), on which this lecture is based.

We will be mainly interested in groups of *finite rank*, and “groups of finite subgroup rank”, while unambiguous and consistent with the literature, does not quite have the same ring to it.

**Remark 6.7.** For any finite group  $G$ , we have

$$d(G) = d(G/\Phi(G))$$

as a consequence of [Proposition 3.4](#).

It is clear from the definitions that we always have

$$d(G) \leq \text{rk}(G).$$

If  $G$  is abelian, these two quantities are in fact the same<sup>4</sup>. This is not true in general, even for  $p$ -groups, as the following example shows.

**Example 6.8.** Let  $\mathbf{F}_3^3$  be a 3-dimensional vector space over  $\mathbf{F}_3$ , the field with three elements. This admits a linear cyclic action of  $C_3$  defined by

$$(1, 0, 0) \mapsto (0, 1, 0), (0, 1, 0) \mapsto (0, 0, 1), (0, 0, 1) \mapsto (1, 0, 0).$$

It is not difficult to see that the semi-direct product  $G := \mathbf{F}_3^3 \rtimes C_3$  is generated by two elements  $((1, 0, 0), 0)$  and  $((0, 0, 0), 1)$ . However, it has  $\mathbf{F}_3^3$  as a normal subgroup which cannot be generated by two elements. It follows that  $\text{rk}(G) > d(G)$ .

The following beautiful result gives another piece of evidence that powerful  $p$ -groups are “morally abelian”.

<sup>4</sup>For example, because any finite abelian group  $A$  is (non-canonically) isomorphic to its Pontryagin dual  $\text{Hom}(A, \mathbb{Q}/\mathbb{Z})$ . Since Pontryagin duality takes monomorphisms to epimorphisms, it follows that any subgroup of  $A$  is isomorphic to some quotient of  $A$ , and so can be generated by the same number of elements.

**Theorem 6.9.** *If  $G$  is a finite powerful  $p$ -group, then  $\text{rk}(G) = d(G)$ .*

*Proof.* For brevity, we write  $G_2 := P_2(G) = G^p$  and  $G_3 := P_3(G) = G_2^p$ , where the second equality is [Theorem 5.14](#). By induction on the order of  $G$ , we can assume the result holds for  $G_2$ , since the latter is also powerful. If we write  $r := d(G)$  and  $m := d(G_2)$ , then since  $x \mapsto x^p$  defines an onto homomorphism

$$\pi: G/G_2 \rightarrow G_2/G_3,$$

of  $\mathbf{F}_p$ -vector spaces, we have  $m \leq r$ .

We have to show that if  $H \leq G$  be a subgroup, then  $d(H) \leq r$ . We write  $e = d(HG_2/G_2)$ , which means we can choose  $h_1, \dots, h_e \in H$  such that

$$HG_2 = \langle h_1, \dots, h_e \rangle G_2.$$

We have that  $\dim_{\mathbf{F}_p}(\ker(\pi)) = r - m$ , and thus

$$\dim(HG_2/G_2 \cap \ker(\pi)) \leq r - m$$

and therefore

$$(6.1) \quad \dim(\pi(HG_2/G_2)) \geq e - r - m = m - (r - e).$$

Let  $K := H \cap G_2$ . Since  $\Phi(K) \leq \Phi(G_2) \leq G_3$ , it follows from (6.1) that the subspace of  $K/\Phi(K)$  spanned by  $h_1^p, \dots, h_e^p$  is of dimension at least  $m - (r - e)$ . But  $\dim(K/\Phi(K)) \leq m$  since the inductive assumption holds for  $G_2$  and  $K \leq G_2$ . Thus there exist  $k_1, \dots, k_{r-e}$  such that

$$K = \langle h_1^p, \dots, h_e^p, k_1, \dots, k_{r-e} \rangle \Phi(K) = \langle h_1^p, \dots, h_e^p, k_1, \dots, k_{r-e} \rangle$$

We then have

$$H = H \cap HG_2 = H \cap \langle h_1, \dots, h_e \rangle G_2 = \langle h_1, \dots, h_e \rangle K = \langle h_1, \dots, h_e, k_1, \dots, k_{r-e} \rangle,$$

which shows that  $d(H) \leq r$ , as needed. □

Let's move to the context of profinite groups. We had previously defined a profinite group  $G$  to be finitely generated if there exists a finite subset  $x_1, \dots, x_n$  such that  $G = \overline{\langle x_1, \dots, x_n \rangle}$  is equal to the closure of the subgroup they generate. Thus, we have a notion of a minimal number of generators, given by

$$d(G) := \inf\{ |X| \mid X \leq G, \overline{\langle X \rangle} = G \}.$$

One would expect that there is also an analogue of rank in this context, but there are several possible variations: one could try to look at the number of generators of closed subgroups, of open subgroups, or perhaps at the ranks of finite quotients. Luckily, all of these are equal:

**Lemma 6.10.** *Let  $G$  be a profinite group. Then*

$$\sup\{d(H) \mid H \leq_c G\} = \sup\{d(O) \mid O \leq_o G\} = \sup\{\text{rk}(G/O) \mid O \triangleleft_o G\}$$

*Proof.* Clearly the left hand term is greater than or equal to the middle one.

We now show that the middle term is greater than or equal to the right one. Assume that  $d(O) \leq d$  for all open normal subgroups  $O \triangleleft_o G$ . We have to show that if  $O$  is open normal and  $K \leq G/O$ , then  $d(K) \leq d$ . Since  $K$  is a quotient of its preimage, which is also an open normal subgroup of  $G$  and so generated by  $d$  elements, we deduce that  $K$  is also generated by  $d$  elements.

Finally, we show that the right term is greater or equal to the left one. Assume that  $\text{rk}(G/O) \leq d$  for all open normals  $O$ ; we have to show that if  $H \leq_c G$  is a closed subgroup, then  $d(H) \leq d$ . As a closed subgroup,  $H$  is a limit of its images in the finite quotients  $G/O$ . Since all of these images are generated by at most  $d$  elements by the assumption about the rank, we deduce that so is  $H$  by [Proposition 2.15](#). □

**Definition 6.11.** Let  $G$  be a profinite group. The *rank* of  $G$ , denoted by  $\text{rk}(G)$ , is given by any of the three equivalent expressions of [Lemma 6.10](#).

Note that unlike for finite groups, the rank of a profinite group might very well be infinite. For example, it is always infinite if  $G$  is not finitely generated, as is the case for the profinite group described in [Warning 2.16](#). The following fundamental result characterizes finite rank pro- $p$ -groups.

**Theorem 6.12** (Lubotzky-Mann). *For a pro- $p$  group  $G$ , the following are equivalent:*

- (1)  $G$  has an open subgroup  $P \triangleleft G$  which is finitely generated and powerful,
- (2)  $G$  is of finite rank.

We encourage the reader to take a moment to marvel at the beauty of [Theorem 6.12](#). This fundamental result relates a natural finiteness condition on a pro- $p$ -group, namely of being of finite rank, to the condition of being powerful, which is of very different, equational nature. It also clearly demonstrates the importance and centrality of the theory of powerful groups. In fact, considering how natural the latter notion turns out to be, and how well  $p$ -groups are understood overall, it is quite surprising that powerful groups were not introduced until 1987<sup>5</sup>!

The rest of this lecture will be devoted to the proof of [Theorem 6.12](#). Note that in the finite setting, we already established a relationship between being powerful and rank in [Theorem 6.9](#). To begin with, we need a partial converse to the latter; that is, we show that a finite  $p$ -group of a specified rank is not “not too far” from being powerful in a quantitative way.

**Notation 6.13.** If  $r \geq 0$ , we write  $\text{GL}_r(\mathbf{F}_p) := \text{Aut}(\mathbf{F}_p^r)$  for the general linear group over the field with  $p$  elements. We write  $\text{U}_r(\mathbf{F}_p) \leq \text{GL}_r(\mathbf{F}_p)$  for the subgroup of upper unitriangular matrices; that is, those which are upper triangular and have 1s on the diagonal.

Equivalently,  $\text{U}_r(\mathbf{F}_p)$  is the subgroup of those automorphisms of  $\mathbf{F}_p$  which preserve the standard complete flag

$$0 \leq \mathbf{F}_p \leq \mathbf{F}_p^2 \leq \dots \leq \mathbf{F}_p^r$$

of subspaces and which act by the identity on the associated graded. As an upper unitriangular matrix is uniquely determined by the entries above the diagonal, which are arbitrary, we see that

$$|\text{U}_r(\mathbf{F}_p)| = p^{(r-1)+(r-2)+\dots+1} = p^{r(r-1)/2}.$$

As we have

$$|\text{GL}_r(\mathbf{F}_p)| = (p^r - 1) \cdot (p^r - p) \cdot \dots \cdot (p^r - p^{r-1})$$

by a standard argument of choosing the images of basis elements, we see that  $\text{U}_r(\mathbf{F}_p) \leq \text{GL}_r(\mathbf{F}_p)$  is a  $p$ -Sylow subgroup.

**Definition 6.14.** Let  $G$  be a finite  $p$ -group and  $r \geq 0$ . The subgroup  $V(G, r) \triangleleft G$  is the intersection

$$V(G, r) := \bigcap_{\phi: G \rightarrow \text{GL}_r(\mathbf{F}_p)} \ker(\phi),$$

of kernels of all homomorphisms  $G \rightarrow \text{GL}_r(\mathbf{F}_p)$ . Equivalently, it is the intersection

$$V(G, r) := \bigcap_{\phi: G \rightarrow \text{U}_r(\mathbf{F}_p)} \ker(\phi),$$

of kernels of all homomorphisms  $G \rightarrow \text{U}_r(\mathbf{F}_p)$ .

**Remark 6.15.** Note that the equivalence of the two variants of [Definition 6.14](#) follows from the fact that  $\text{U}_r(\mathbf{F}_p) \leq \text{GL}_r(\mathbf{F}_p)$  is  $p$ -Sylow, hence is conjugate to all other  $p$ -Sylow subgroups. As  $G$  is a  $p$ -group, its image is contained in some  $p$ -Sylow subgroup, and the equivalence follows.

<sup>5</sup>In the celebrated work of Lubotzky and Mann, see [\[LM87a\]](#) and [\[LM87b\]](#).

**Remark 6.16.** It is clear from the definition that  $V(G, r) \triangleleft G$  can be characterized as follows: it is the subgroup of those elements  $g \in G$  which act trivially on any  $G$ -representations over  $\mathbf{F}_p$  of dimension at most  $r$ .

**Remark 6.17.** If  $G$  is a finite  $p$ -group and  $N \triangleleft G$  is a normal subgroup, then we have

$$V(G, r)N/N \leq V(G/N, r),$$

since homomorphisms  $G/N \rightarrow \mathrm{GL}_r(\mathbf{F}_p)$  can be identified with a subset of homomorphisms  $G \rightarrow \mathrm{GL}_r(\mathbf{F}_p)$ . If  $N \leq V(G, r)$ , then

$$V(G, r)/N = V(G/N, r),$$

as in this case such homomorphisms are in bijection.

We now show that  $V(G, r)$  differs from  $G$  itself by a relatively small number of elementary abelian subquotients.

**Notation 6.18.** For  $r > 0$ , we write

$$\lambda(r) := \lceil \log_2(r) \rceil,$$

the ceiling of the logarithm. In other words,  $\lambda(r)$  is the unique integer such that

$$2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}.$$

**Lemma 6.19.** *The group  $U_r(\mathbf{F}_p)$  can be built as an iterated extension of  $\lambda(r)$  elementary abelian groups.*

*Proof.* We prove this by induction on  $r$ , the case  $r = 1$  being trivial. If  $r > 1$ , let  $s = \lceil r/2 \rceil$  and  $s' = r - s$ . If  $\phi: \mathbf{F}_p^r \rightarrow \mathbf{F}_p^r$  be an automorphism preserving the standard complete flag of subspaces, let  $\phi_1, \phi_2$  be the unique linear automorphisms which make the following diagram commute

$$\begin{array}{ccccc} \mathbf{F}_p^s & \longrightarrow & \mathbf{F}_p^r & \longrightarrow & \mathbf{F}_p^{s'} \\ \downarrow \phi_1 & & \downarrow \phi & & \downarrow \phi_2 \\ \mathbf{F}_p^s & \longrightarrow & \mathbf{F}_p^r & \longrightarrow & \mathbf{F}_p^{s'} \end{array},$$

where we identify  $\mathbf{F}_p^{s'} \simeq \mathbf{F}_p^r/\mathbf{F}_p^s$ . In other words,  $\phi_1$  is the restriction of  $\phi$  to  $\mathbf{F}_p^s$  and  $\phi_2$  is the induced map on the quotient. The association  $\phi \rightarrow \phi_1 \times \phi_2$  defines a map

$$(6.2) \quad U_r(\mathbf{F}_p) \rightarrow U_s(\mathbf{F}_p) \times U_{s'}(\mathbf{F}_p)$$

whose kernel is by group of linear automorphisms which act by identity on both  $\mathbf{F}_p^s$  and the quotient.

Any automorphisms with this property is of the form  $1 + v$ , where  $v: \mathbf{F}_p^r \rightarrow \mathbf{F}_p^r$  acts by zero on the subspace  $\mathbf{F}_p^s$  and the quotient. Any two such  $v_1, v_2$  compose to zero by a diagram chase using the diagram above, hence

$$(1 + v_1) \cdot (1 + v_2) = 1 + v_1 + v_2 + v_1v_2 = 1 + v_1 + v_2.$$

This shows that the kernel of (6.2) is elementary abelian. Since the inductive assumption applies to the product  $U_s(\mathbf{F}_p) \times U_{s'}(\mathbf{F}_p)$ , we see that  $U_r$  can be built as an iterated extension of

$$\lambda(s) + 1 = \lambda(2s)$$

If  $r$  is even, then  $2s = r$  and we are done. If  $r$  is odd, then we have  $2s = r + 1$ , but in this case we also have  $\lambda(2s) = \lambda(r)$  since  $\lambda$  is lower semicontinuous and only jumps at powers of two.  $\square$

**Corollary 6.20.** *Let  $G$  be a  $p$ -group of rank  $r$ . Then  $|G : V(G, r)| \leq p^{r\lambda(r)}$ .*

*Proof.* Since by construction  $G/V(G, r)$  embeds as a subgroup of a product of  $U_r(\mathbf{F}_p)$ , it follows from [Lemma 6.19](#) that it can be built using iterated extensions out of  $\lambda(r)$  elementary abelian groups. Since the groups which appear in this way are subquotients of  $G$ , they are of rank at most  $r$ , and hence each is of order at most  $p^r$ . Combining these two claims we obtain the needed bound.  $\square$

**Proposition 6.21.** *Let  $G$  be a finite  $p$ -group and let  $N \triangleleft G$  be a normal subgroup such that  $d(N) \leq r$  and  $W$  an arbitrary subgroup. Suppose that either*

- (1)  $p > 2$  and  $N \leq W \leq V(G, r)$  or
- (2)  $p = 2$  and  $N \leq W \leq V(G, r)^2$ .

*Then  $N$  p.e.  $W$ .*

*Proof.* We only prove the case of an odd prime. When  $p = 2$ , the obtained statement is slightly different, since in the basic reduction step one has to use the variant of [Lemma 5.10](#) outlined in [Remark 5.11](#), which takes a slightly different form.

We argue by induction on the order of  $N$ . Assume by contradiction that  $N$  is not powerfully embedded in  $V(G, R)$ . Using [Lemma 5.10](#), we can pass to a suitable quotient of  $G$  and by replacing  $N$  and  $W$  by their images in the quotient assume that

- (1)  $N^p = 0$ ,
- (2)  $|[N, W]| = p$ .

Note that in the quotient we still have  $W \leq V(G, r)$  by [Remark 6.17](#). We can find a normal subgroup  $M \triangleleft G$  such that

- (1)  $[N, W] \leq M < G$

and where the second inclusion is of index exactly  $p$ . Since  $N/[N, W]$  is elementary abelian and generated by at most  $r$  elements and  $M/[N, W]$  is a proper subgroup, we have  $d(M/[N, W]) \leq r - 1$ . Since  $[N, W]$  is cyclic, we deduce that  $d(M) \leq r$ . As  $M$  is of strictly smaller order than  $N$ , applying the inductive hypothesis we deduce that  $M$  p.e.  $W$ ; that is,

$$[M, W] \leq M^p \leq N^p = 0,$$

so that  $M$  is central in  $W$ . Since  $M \leq N$  is then also central with a quotient cyclic, we deduce that  $N$  is abelian, necessarily elementary abelian of rank at most  $r$ . From the definition of  $V(G, r)$ , it necessarily acts trivially on  $N$  by conjugation, so that  $N$  is central in  $V(G, r)$  and hence  $W$ . This is a contradiction to  $[N, W]$  being of order exactly  $p$ , ending the argument.  $\square$

**Corollary 6.22.** *Let  $G$  be a finite  $p$ -group of rank  $r$ . Then*

- (1) if  $p > 2$ , then  $V(G, r)$  is powerful,
- (2) if  $p = 2$ , then  $V(G, r)^2$  is powerful.

*Proof.* This is an application of [Proposition 6.21](#) to either  $N = V(G, r)$  or  $N = V(G, r)^2$ .  $\square$

Combining the above results, we obtain the following useful statement.

**Proposition 6.23.** *Let  $G$  be a finite  $p$ -group of rank  $r$ . Then  $G$  has a characteristic subgroup  $P \leq G$  which is powerful and of index at most*

- (1)  $p^{r\lambda(r)}$  if  $p > 2$ ,
- (2)  $p^{r\lambda(r)+r}$  if  $p = 2$ .

*Proof.* At odd primes,  $V(G, r) \triangleleft G$  has the needed properties by a combination of [Corollary 6.20](#) and [Corollary 6.22](#). When  $p = 2$ , we can take  $V(G, r)^2$ , which is of index at most

$$2^{r\lambda(r)+r} = 2^{r(\lambda(r)+1)}$$

since  $V(G, r)/V(G, r)^2$  is elementary abelian and hence of order at most  $2^r$ .  $\square$

We are now ready to prove the main result of this lecture.

*Proof of Theorem 6.12:* Suppose first that  $G$  has an open subgroup  $P \triangleleft G$  which is finitely generated and powerful. Since for any closed  $K \triangleleft_o G$ , the index  $|K : K \cap P|$  is bounded by  $|G : P|$ , it is enough to show that  $P$  itself is of finite rank. If  $P$  is generated by  $r$  elements, then so can all of its finite quotients, which are thus of rank at most  $r$  by Theorem 6.9 as they are also powerful. We deduce that  $P$  is also of rank  $r$ .

Conversely, suppose that  $G$  is of finite rank  $r$ . Consider

$$V(G, r) := \bigcap_{\phi: G \rightarrow \mathrm{GL}_r(\mathbf{F}_p)} \ker(\phi),$$

where the intersection is taken over all continuous homomorphisms. Since  $G$  is finitely generated, there are only finitely many such homomorphisms so that  $V(G, r)$  is open. We can write  $G$  as

$$\varprojlim_{O \triangleleft_o G, O \leq V(G, r)} G/O,$$

the limit of quotients indexed by the poset of open subgroups contained in  $V(G, r)$ . Since  $V(G, r)$  is closed, we have

$$V(G, r) \simeq \varprojlim V(G, r)/O \simeq \varprojlim V(G/O, r),$$

where the second equivalence is Remark 6.17. If  $p > 2$ , then each of  $V(G/O, r)$  is powerful by Corollary 6.22, and hence so is  $V(G, r)$  as their limit. If  $p = 2$ , we can take  $V(G, r)^2$  instead.  $\square$

**Remark 6.24.** Using Proposition 6.23, one can give Theorem 6.12 a more quantitative form: if  $G$  is a pro- $p$ -group of rank  $r$ , then it has an open characteristic powerful subgroup of index at most  $p^{r\lambda(r)}$  (or  $2^{r\lambda(r)+r}$  when  $p = 2$ ).

## 7. UNIFORM POWER

In the previous lecture, we have proven the remarkable Theorem 6.12, which shows that a pro- $p$ -group is of finite rank if and only if it has an open subgroup which is powerful and finitely generated. Today, we will show that such groups always have open subgroups which exhibit strong self-similarity.

**Definition 7.1.** We say that a pro- $p$  group  $G$  is *uniformly powerful* (or simply *uniform*) if

- (1)  $G$  is finitely generated,
- (2)  $G$  is powerful,
- (3) for all  $i \geq 1$  we have

$$|G_i : G_{i+1}| = |G_{i+1} : G_{i+2}|,$$

where  $G_i := P_i(G)$  is the lower  $p$ -series.

Note that the first two conditions are equivalent to being of finite rank; we will use this equivalence freely in what follows. Informally, Definition 7.1 can be summarized as saying that a group is uniform when it is "not too large" and its lower  $p$ -series "moves at a constant pace".

**Remark 7.2.** Note that a finite  $p$ -group is uniform if and only if it is zero. Indeed, for finite groups we have  $G_i = 0$  for  $i$  large enough, which forces all of  $G_i$  to be zero by uniformity.

We will need the following slightly more elaborate form of Theorem 6.12:

**Lemma 7.3.** *Let  $G$  be a pro- $p$ -group of finite rank. Then, there exists a characteristic open subgroup  $V \leq G$  such that if  $N \triangleleft_c G$  is normal closed and  $N \leq V$ , then  $N$  is powerful.*

*Proof.* If  $G$  is of rank  $r$ , we write  $V(G, r)$  for the intersection of the kernels of all continuous homomorphisms  $G \rightarrow \mathrm{GL}_r(\mathbf{F}_p)$ . We can then take

- (1)  $V := V(G, r)$  if  $p > 2$ ,
- (2)  $V := V(G, r)^2$  if  $p = 2$ .

The needed property then follows from Proposition 6.21.  $\square$

**Proposition 7.4.** *If  $G$  is a pro- $p$ -group of finite rank, then  $G_i$  is uniform for all  $i$  large enough.*

*Proof.* Since  $G_i$  form a basis of open neighbourhoods of the identity by Proposition 3.20, they are powerful for  $i$  large enough as a consequence of Lemma 7.3. Since  $x \mapsto x^p$  defines an epimorphism  $G_i/G_{i+1} \rightarrow G_{i+1}/G_{i+2}$  for all  $i$  by Theorem 5.14, the sequence of numbers

$$|G_1 : G_2| \geq |G_2 : G_3| \geq \dots$$

is decreasing. Since they are non-negative, this sequence must eventually stabilize, at which point  $G_i$  become uniform.  $\square$

Uniform groups have the following beautiful characterization.

**Theorem 7.1.** *If  $G$  is a powerful pro- $p$  group, then the following are equivalent:*

- (1)  $G$  is uniform,
- (2)  $G$  is torsion-free; that is, if  $g^n = e$  for  $n > 0$ , then  $g = e$ .

*Proof.* (1  $\Rightarrow$  2): We show that if  $G$  is not torsion-free, then it's not uniform. Since  $G$  is pro- $p$ , this means there exists some  $g \neq e$  such that  $g^p = e$ . Choose an  $i$  such that  $g \in G_i \setminus G_{i+1}$ . It follows that  $g$  defines a non-zero element in the kernel of the map

$$G_i/G_{i+1} \rightarrow G_{i+1}/G_{i+2}$$

defined by  $x \mapsto x^p$ . Since this map is surjective, we deduce that  $|G_i : G_{i+1}| > |G_{i+1} : G_{i+2}|$ , so that  $G$  is not uniform.

(2  $\Rightarrow$  1): We show that if  $G$  is not uniform, then  $G$  is not torsion-free. By assumption, one of the maps  $G_i/G_{i+1} \rightarrow G_{i+1}/G_{i+2}$  has non-zero kernel, so that there exists  $x \in G_i \setminus G_{i+1}$  such that  $x^p \in G_{i+2}$ . By replacing  $G_i$ , we can assume that  $i = 1$ .

We will inductively construct a sequence  $x_2, x_3, \dots$  such that

- (1)  $x_2 = x$ ,
- (2)  $x_{k+1} \equiv x_k \pmod{G_k}$
- (3)  $x_k^p \in G_{k+1}$ .

The base case is determined by the first condition, so suppose that  $x_n$  has been chosen. Since  $G_n/G_{n+1} \rightarrow G_{n+1}/G_{n+2}$  is an epimorphism, we can find  $z_n \in G_n$  such that  $z_n^p \equiv x_n^p \pmod{G_{n+2}}$ . We can then set  $x_{n+1} := x_n z_n^{-1}$ .

Finally, let  $x := \lim_{k \rightarrow \infty} x_k$ ; this limit exists as this sequence is Cauchy by the second condition above and  $G$  is compact. Then

$$x^p = \lim_{k \rightarrow \infty} x_k^p \in \bigcap G_i = 0,$$

so that  $G$  is not torsion-free, since  $x \in G_1 \setminus G_2$ .  $\square$

**Corollary 7.5.** *Any pro- $p$  group  $G$  of finite rank has an open characteristic subgroup  $U \triangleleft_o G$  such that any open normal closed subgroup  $N \triangleleft_c G$  satisfying  $N \leq U$  is uniform.*

*Proof.* First, let  $V$  be an open subgroup as in Lemma 7.3. Then  $V_i \leq V$  is uniform for some  $i$  by Proposition 7.4 and hence torsion-free by Theorem 7.1. All of its closed subgroups are also torsion-free, and hence uniform since they're powerful by the choice of  $V$ .  $\square$

The following will be needed to define the dimension of a pro- $p$ -group of finite rank.

**Lemma 7.6.** *Let  $G$  be a pro- $p$  group of finite rank, and  $A, B \leq G$  be uniform open subgroups. Then  $d(A) = d(B)$ .*

*Proof.* Since  $B$  is open and  $P_i(A)$  is a system of open neighborhoods, for some  $i \gg 0$  we know  $P_i(A) \leq B$ . Since the minimal number of generators and rank coincide for powerful pro- $p$ -groups

by [Theorem 6.9](#) and the fact that a rank of a profinite group is the supremum of ranks of its finite quotients, this gives

$$d(A) = d(A/P_2(A)) = d(P_i(A)/P_{i+1}(A)) = d(P_i(A)) \leq d(B),$$

where the second equality is the uniformity of  $A$ . By symmetry, we deduce that also  $d(B) \leq d(A)$ , as needed.  $\square$

**Definition 7.7.** Let  $G$  be pro- $p$  group of finite rank. The *dimension* of  $G$  is given by

$$\dim(G) := d(A)$$

where  $A \leq_o G$  is any uniform open subgroup.

**Remark 7.8.** To motivate [Definition 7.7](#), observe that for real Lie groups one shows that a small neighbourhood of the identity is diffeomorphic to an open subset of the tangent space through the exponential map, and the dimension of a Lie group is the same as the dimension of the tangent space. For  $p$ -adic analytic groups, the role of such a small neighbourhood is played by uniform open subgroups.

Again, notice the curious feature that in the  $p$ -adic case, the dimension can be defined in purely group-theoretic terms. Even the topology plays no role, as long as they're compact, as by [Serre's Theorem 4.1](#) all finite index subgroups are open.

The following is a basic consistency check of [Definition 7.7](#).

**Proposition 7.9.** Let  $G$  be pro- $p$  of finite rank and let  $N \triangleleft_c G$  be a closed normal subgroup. Then

$$\dim(G) = \dim(N) + \dim(G/N).$$

*Proof.* We first show this in the special case when  $G$ ,  $N$ , and  $G/N$  are all uniform. Then  $\dim(G) = \dim_{\mathbf{F}_p}(G/G^p)$  and similarly for  $N$  and  $G/N$ . We have

$$\dim(G) = \dim_{\mathbf{F}_p}(G/G^p) = \dim_{\mathbf{F}_p}(NG^p/G^p) + \dim_{\mathbf{F}_p}(G/NG^p).$$

Since  $G/N$  is torsion-free by [Theorem 7.1](#), we necessarily have  $N^p = G^p \cap N$ , so that we can rewrite the above as

$$\dim_{\mathbf{F}_p}(N/(G^p \cap N)) + \dim_{\mathbf{F}_p}(G/NG^p) = \dim_{\mathbf{F}_p}(N/N^p) + \dim_{\mathbf{F}_p}(G/NG^p) = \dim(N) + \dim(G/N),$$

which is the needed claim.

We now tackle the general case. By [Corollary 7.5](#), we can find an open characteristic subgroup  $G' \leq G$  such that if  $K \triangleleft_c G$  and  $K \leq G'$ , then  $K$  is uniform. Similarly, we can choose such subgroups  $N' \leq N$  and  $H/(G' \cap N') \leq G'/G' \cap N'$ . Since  $N/(G' \cap N')$  is finite and  $H/(G' \cap N')$  is uniform and thus torsion-free, we necessarily have  $N \cap H = G' \cap N'$ . Thus, all three of  $H \leq_o G$ ,  $N \cap H \leq_o N$  and  $H/(N \cap H) \leq_o G/N$  are uniform and by the first part we have

$$\dim(G) = \dim(H) = \dim(H \cap N) + \dim(H/H \cap N) = \dim(N) + \dim(G/N).$$

$\square$

**Remark 7.10.** Observe that in the context of [Proposition 7.9](#), both  $N$  and  $G/N$  are automatically of finite rank, as this property is clearly closed under taking quotients and closed subgroups. Conversely, it is not difficult to show that if  $N$  and  $G/N$  are finite rank, then so is  $G$ .

We will now describe how a choice of generators of a uniform group induces a coordinate system on the whole group. This can be seen as the first solid piece of evidence towards [Lazard's Theorem 1.1](#) which characterizes  $p$ -adic analytic groups as those topological groups which are locally uniform. In this case, we will see that uniform groups (and hence all pro- $p$  groups of finite rank, locally) are homeomorphic to  $\mathbb{Z}_p^n$  in a semi-canonical way. This requires some preparation.

**Lemma 7.11.** *Let  $G$  be a powerful finite  $p$ -group generated by  $a_1, \dots, a_d$ . Then any element of  $G$  can be written in the form*

$$a_1^{\lambda_1} \cdot a_2^{\lambda_2} \cdot \dots \cdot a_d^{\lambda_d}$$

for some  $\lambda_i \in \mathbb{Z}$ .

*Proof.* We prove this by induction on the length of the  $p$ -series. If  $G_2 = 0$ , then  $G$  is abelian, and the result is clear. If we have  $n \geq 2$  with  $G_n \neq 0$  and  $G_{n+1} = 0$ , then by inductive assumption the result applies to  $G/G_n$ . It follows that any element  $g \in g$  can be written as

$$g = a_1^{\lambda_1} \cdot a_2^{\lambda_2} \cdot \dots \cdot a_d^{\lambda_d} x$$

with  $x \in G_n$ . As  $G_n$  is generated by  $b_i := a_i^{p^{n-1}}$  by repeated application of part (3) of [Theorem 5.14](#) and  $G_n$  is central, the result follows by writing  $x$  as a product of  $b_i$  and moving things around.  $\square$

In any group, one can make sense of expressions of the form  $g^\lambda$  where  $g \in G$  and  $\lambda \in \mathbb{Z}$ . We now show that if  $G$  is pro- $p$ , then  $\lambda$  can even be a  $p$ -adic integer.

**Construction 7.12.** Let  $G$  be a pro- $p$  group. We claim that there is a unique continuous mapping

$$G \times \mathbb{Z}_p \rightarrow G$$

written as

$$(g, \lambda) \mapsto g^\lambda$$

which restricted to  $G \times \mathbb{Z}$  gives the usual  $n$ -th power mapping  $g^n := g \cdot g \cdot \dots \cdot g$ .

Since  $\mathbb{Z} \subseteq \mathbb{Z}_p$  is dense, it is enough to show existence, as uniqueness will be automatic. We can write  $G \simeq \varprojlim G_\alpha$  as a limit of finite  $p$ -groups, and thus it is enough to construct such an extension to

$$G \times \mathbb{Z} \rightarrow G_\alpha.$$

However, for any  $g_\alpha \in G_\alpha$  we have  $g_\alpha^n = g_\alpha^{n+p^d}$ , where  $p^d = |G_\alpha|$  is the order. It follows that we have a commutative diagram

$$\begin{array}{ccc} G \times \mathbb{Z}_p & & \\ \uparrow & \searrow & \\ G \times \mathbb{Z} & \longrightarrow & G \times \mathbb{Z}/p^d \longrightarrow G_\alpha \end{array}$$

which provides the needed extension.

**Remark 7.13.** Explicitly, the  $p$ -adic powers of [Construction 7.12](#) can be calculated as follows: if  $g \in G$  and  $\lambda \in \mathbb{Z}_p$ , then

$$g^\lambda = \lim_{i \rightarrow \infty} g^{\lambda_i}$$

where on the right hand side we have the standard powers and  $\lambda_i \in \mathbb{Z}$  is a sequence of integers converging  $\lambda_i \rightarrow \lambda$  in  $\mathbb{Z}_p$ . This follows from continuity, and such a sequence can always be chosen by density of ordinary integers inside the  $p$ -adics.

**Theorem 7.14.** *Let  $G$  be a uniform pro- $p$  group and let  $a_1, \dots, a_d$  be a minimal system of generators. Then the map*

$$\mathbb{Z}_p^d \rightarrow G$$

given by

$$(\lambda_1, \dots, \lambda_d) \mapsto a_1^{\lambda_1} \cdot \dots \cdot a_d^{\lambda_d},$$

the  $p$ -adic powers of [Construction 7.12](#), is a homeomorphism.

*Proof.* Since  $U/pU \simeq U/U_2$  as groups as a consequence of For any  $k \geq 1$ ,  $G/G_{k+1}$  is a finite  $p$ -group of exponent  $p^k$ . It follows from the construction that the above mapping fits into a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p^d & \longrightarrow & G \\ \downarrow & & \downarrow \\ (\mathbb{Z}/p^k)^d & \longrightarrow & G/G_{k+1} \end{array} .$$

The bottom arrow is surjective by [Lemma 7.11](#). As  $G$  is uniform of rank  $d$ , the quotient  $G/G_{k+1}$  has exactly  $p^{kd}$  elements and we deduce that the bottom arrow is a bijection. As the map  $\mathbb{Z}_p^d \rightarrow G$  can be identified with the inverse limit of these maps, we deduce that it is a bijection, too, and hence a homeomorphism as it is continuous.  $\square$

### 8. THE $p$ -ADIC GENERAL LINEAR GROUP

In this lecture, we will verify that the archetypical example of a  $p$ -adic analytic group  $\mathrm{GL}_d(\mathbb{Z}_p)$ , is virtually a pro- $p$  group of finite rank; that is, it has an open subgroup which is a pro- $p$  group of finite rank.

**Definition 8.1.** If  $n \geq 1$ , the  $n$ -th congruence subgroup  $\Gamma_n \triangleleft \mathrm{GL}_d(\mathbb{Z}_p)$  is the open subgroup given by the kernel

$$\Gamma_n := \ker(\mathrm{GL}_d(\mathbb{Z}_p) \rightarrow \mathrm{GL}_d(\mathbb{Z}/p^n)).$$

Explicitly,  $\Gamma_n$  is the subgroup of matrices of the form

$$\Gamma_n = \{1 + p^n a \mid a \in M_d(\mathbb{Z}_p)\},$$

where  $1$  is the identity matrix and  $M_d(\mathbb{Z}_p)$  is the set of all  $p$ -adic matrices. From this description, it is clear that  $\Gamma_n$  is a basis of open neighbourhoods of the identity element. In particular,  $\mathrm{GL}_d(\mathbb{Z}_p)$  is profinite.

**Lemma 8.2.** *We have*

$$|\mathrm{GL}_d(\mathbb{Z}_p) : \Gamma_1| = (p^d - 1) \cdot (p^d - p) \cdot \dots \cdot (p^d - p^{d-1})$$

and

$$|\Gamma_n : \Gamma_{n+1}| = p^{d^2}$$

for each  $n \geq 1$ .

*Proof.* Since any invertible matrix over  $\mathbf{F}_p$  can be lifted to a matrix over  $\mathbb{Z}_p$ , which is then automatically invertible, too, the first index is equal to  $|\mathrm{GL}_d(\mathbf{F}_p)|$ , which we observed is equal to the given expression in [§6](#). The second index is equal to  $|\ker(\mathrm{GL}_d(\mathbb{Z}/p^{n+1}) \rightarrow \mathrm{GL}_d(\mathbb{Z}/p^n))|$ , which is  $p^{d^2}$  since any matrix over  $\mathbb{Z}/p^n$  has exactly  $p^{d^2}$  lifts to  $\mathbb{Z}/p^{n+1}$ .  $\square$

**Corollary 8.3.** *The profinite group  $\mathrm{GL}_d(\mathbb{Z}_p)$  is virtually pro- $p$ ; that is, it has a pro- $p$  open subgroup.*

*Proof.* This follows from the second part of [Lemma 8.2](#), since  $\Gamma_1$  is open and pro- $p$ .  $\square$

We now study the basic relationships between the congruence subgroups.

**Lemma 8.4.** *Let  $a \in \mathrm{GL}_d(\mathbb{Z}_p)$  and  $x \in M_d(\mathbb{Z}_p)$ . Then for any  $n \geq 1$ , we have*

$$a \equiv (a + p^n x) \pmod{\Gamma_n}.$$

*Proof.* Since the images of  $a$  and  $a + p^n x$  in  $\mathrm{GL}_d(\mathbb{Z}/p^n)$  are the same, they generate the same coset with respect to the kernel, which is  $\Gamma_n$ .  $\square$

**Lemma 8.5.** *For any  $n \geq 1$ , we have  $[\Gamma_n, \Gamma_n] \leq \Gamma_{2n}$ .*

*Proof.* Let  $1 + p^n a$  and  $1 + p^n b$  be elements of  $\Gamma_n$ . Then

$$(1 + p^n a)(1 + p^n b) \equiv (1 + p^n a + p^n b + p^{2n} ab) \equiv (1 + p^n a + p^n b) \pmod{\Gamma_{2n}},$$

where the second equivalence is [Lemma 8.4](#). The result follows since  $p^n a + p^n b = p^n b + p^n a$ .  $\square$

**Lemma 8.6.** *For any  $n \geq 1$ , we have  $\Gamma_n^p \leq \Gamma_{n+1}$ .*

*Proof.* If  $1 + p^n a \in \Gamma_n$ , then the binomial formula gives

$$(8.1) \quad (1 + p^n a)^p = 1 + \binom{p}{1} p^n a + \sum_{2 \leq k \leq p} \binom{p}{k} p^{nk} a^k$$

which we can rewrite as

$$1 + \binom{p}{1} p^n a + \sum_{2 \leq k \leq p} \binom{p}{k} p^{nk} a^k = 1 + p^{n+1} (a + \sum_{2 \leq k \leq p} \binom{p}{k} p^{n(k-1)-1} a^k)$$

as needed.  $\square$

**Proposition 8.7.** *Assume that either  $n \geq 1$  and  $p > 2$  or  $n \geq 2$  and  $p = 2$ . Then every element of  $\Gamma_{n+1}$  is a  $p$ -th power of an element in  $\Gamma_n$ .*

*Proof.* Let  $1 + p^{n+1} a \in \Gamma_{n+1}$ , we have to solve the equation

$$f(x) = \frac{(1 + p^n x)^p - 1 - ap^{n+1}}{p^{n+1}} = 0$$

for a matrix  $x \in M_d(\mathbb{Z}_p)$ . Note that this equation has  $p$ -adic integral coefficients by [Lemma 8.6](#). We will show that such a matrix exists using Newton's method. More precisely, we will inductively construct a Cauchy sequence  $x_1, x_2, \dots$  of matrices in the subring generated by  $a$  such that

$$f(x_i) \equiv 0 \pmod{p^i}$$

We claim that we can take  $x_1 := a$ . To see this, note that the binomial expansion of the  $p$ -th power gives

$$f(x) = (x - a) + \sum_{2 \leq k \leq p} \binom{p}{k} p^{nk-n-1} x^k,$$

so that

$$f(a) = \sum_{2 \leq k \leq p} \binom{p}{k} p^{nk} a^k.$$

This is divisible by  $p$  as needed since

- (1)  $p = 2$ , in which case  $n \geq 2$ , so that  $nk - n - 1 \geq 1$ ,
- (2)  $p > 2$ , in which case  $\binom{p}{2}$  is divisible by  $p$  for  $k = 2$ , and  $nk - n - 1 \geq 1$  when  $k > 2$ .

Note that this is the only place where the distinction between  $p = 2$  and  $p > 2$  comes into play. We also calculate that

$$f'(x) = (1 + p^n x)^{p-1},$$

so that  $f'(a)$  is invertible. Since the subring of matrices generated by  $a$  is a finite  $\mathbb{Z}_p$ -algebra, it is  $p$ -complete, and applying Hensel's lemma<sup>6</sup>, we see that inductively defining

$$x_{r+1} := x_r - \frac{f(x_r)}{f'(x_r)}$$

yields a Cauchy sequence which converges to the needed solution.  $\square$

<sup>6</sup>Hensel's lemma is often stated only for local rings, see [[Sta18](#), [Tag 04GM](#)], but since  $\mathbb{Z}_p$  is henselian, the subalgebra of matrices generated by  $a$  is a finite product of  $p$ -complete local rings. Thus, the convergence of the series produced by the Newton's method can be checked in each of these local rings separately. Moreover, it is common to assume that  $f$  is monic, but this is not necessary in the case of complete local rings.

**Theorem 8.8.** *Assume that either  $n \geq 1$  and  $p > 2$  or  $n \geq 2$  and  $p = 2$ . Then  $\Gamma_n$  is a uniformly powerful pro- $p$  group of dimension  $d^2$ .*

*Proof.* By a combination of [Proposition 8.7](#) and [Lemma 8.6](#), we see that

$$\Gamma_n/\Gamma_n^p = \Gamma_n/\Gamma_{n+1}$$

If  $p > 2$ , then the right hand side is abelian by [Lemma 8.5](#). If  $p = 2$ , then we deduce that

$$\Gamma_n/\Gamma_n^4 = \Gamma_n/\Gamma_{n+2}$$

which is similarly abelian since  $n \geq 2$ . We deduce that  $\Gamma_n$  is powerful. Moreover, by [Lemma 8.2](#), for any  $k \geq 1$  we have

$$|P_i(\Gamma_n)/P_{i+1}(\Gamma_n)| = |\Gamma_{n+i-1}/\Gamma_{n+i}| = p^{d^2}$$

from which we deduce at once that  $\Gamma_n$  is finitely generated and uniform. □

**Corollary 8.9.** *The general linear group  $\mathrm{GL}_d(\mathbb{Z}_p)$  is virtually a uniform pro- $p$  group.*

*Proof.* By [Theorem 8.8](#),  $\Gamma_1$  for  $p > 2$  and  $\Gamma_2$  for  $p = 2$  are open subgroups which are uniformly powerful pro- $p$ . □

## 9. THE ADDITIVE STRUCTURE OF A UNIFORM GROUP

In [Theorem 7.14](#), we had seen that if  $U$  is a uniform group of dimension  $d$ , then any choice of generators determines a homeomorphism

$$\mathbb{Z}_p^{\oplus d} \simeq G.$$

Using this homeomorphism, the abelian group structure of the left hand side can be transferred to  $G$ , but this is not a good idea, as this new abelian multiplication of  $G$  depends on the choice of generators. In this lecture, we will see that a uniform group instead supports an *intrinsic* abelian multiplication, which we will refer to as *addition*, which is defined in terms of and related in interesting ways to the original multiplication of  $G$ .

**Remark 9.1.** If  $G$  is a real Lie group, then the behaviour of its multiplication in an infinitesimal neighbourhood of the identity (up to first order) is encoded by the induced multiplication

$$T_e G \times T_e G \rightarrow T_e G.$$

on the tangent space. It is not difficult to show (using the Eckmann-Hilton argument) that the induced multiplication on the tangent space coincides with its addition coming from the structure of a vector space. In this sense, the multiplication of any real Lie group is abelian up to first order.

The main idea behind today's construction is to replace the multiplication of a uniform group  $G$  by multiplication induced from its small subgroups. One then hopes that as in the case of real Lie groups discussed in [Remark 9.1](#), in the limit the multiplication becomes abelian.

The restriction to the case of uniform groups comes from the fact that they can be canonically identified (as topological spaces) with their subgroups appearing in the lower  $p$ -series, which we show now.

**Lemma 9.2.** *Let  $G$  be a pro- $p$  group and write  $G_i := P_i(G)$  for its lower  $p$ -series. Then for any  $n, k$ , the map  $x \mapsto x^{p^n}$  induces a function of sets*

$$G/G_{k+1} \rightarrow G_{n+1}/G_{n+k+1}.$$

*If  $G$  is powerful, this map is a surjective, and bijective if  $G$  is moreover uniform.*

*Proof.* It's enough to do the case  $n = 1$ , as the other cases are obtained by iterating the statement. Suppose that

$$x \equiv y \pmod{G_{k+1}}$$

so that  $x = yz$  for  $z \in G_{k+1}$ . Then

$$x^p \equiv y^p z^p \pmod{[G, G_{k+1}]}$$

which since  $[G, G_{k+1}] \leq G_{k+2}$  and  $z^p \in G_{k+2}$  gives

$$x^p \equiv y^p \pmod{G_{k+2}},$$

which is what we wanted to show. If  $G$  is powerful, then every element of  $G_{n+1}$  is a  $p^n$ -th power by [Theorem 6.4](#) and surjectivity follows. If  $G$  is uniform, then both sets are of the same order  $p^{d(G)k}$ , and hence the surjection must be a bijection.  $\square$

**Warning 9.3.** We have shown in [Theorem 5.14](#) that if  $G$  is powerful and  $k = 1$ , then  $x \mapsto x^p$  not only defines a function of sets  $G/G_{k+1} \rightarrow G_2/G_{k+2}$ , but even a group homomorphism. Beware that this is not in general true for  $k > 1$ , even if  $G$  is powerful.

**Corollary 9.4.** *Let  $U$  be uniform. Then for any  $n$ , the map  $x \mapsto x^{p^n}$  defines a homeomorphism*

$$U \rightarrow U_{n+1}.$$

*Proof.* This map can be identified with the limit of bijections between finite sets of [Lemma 9.2](#) as  $k \rightarrow \infty$ , and hence is a homeomorphism.  $\square$

Note that the homeomorphism of [Corollary 9.4](#) is not in general a group homomorphism. However, using this map we can transfer the group structure of  $U_{n+1}$  onto  $U$  in the following way:

**Construction 9.5.** Let  $U$  be a uniform pro- $p$  group. If  $x, y \in U$ , we write

$$x +_n y := (x^{p^n} y^{p^n})^{p^{-n}},$$

where  $p^{-n}: U_{n+1} \rightarrow U$  is the inverse to the  $p^n$ -th power map.

**Remark 9.6.** Note that the map  $+_n$  makes  $U$  into a topological group with respect to its usual topology. This is the unique group structure such that  $x \mapsto x^{p^n}$  defines a group isomorphism  $(U, +_n) \simeq (U_{n+1}, \cdot)$ , where  $\cdot$  is the standard multiplication of  $U_{n+1}$ .

**Lemma 9.7.** *If  $U$  is uniform and  $x, y \in U$ , then*

$$x +_n y \equiv x +_{n-1} y \pmod{U_n}.$$

Moreover, for any  $u, v \in U_n$  we have

$$ux +_n vy \equiv x +_n y \pmod{U_n}.$$

*Proof.* Since  $[U_n, U_n] \leq U_{2n}$  by [Theorem 3.21](#), we have

$$\left(x^{p^{n-1}} y^{p^{n-1}}\right)^p \equiv \left((xy)^{p^{n-1}}\right)^p \pmod{U_{2n}}.$$

Taking  $p^n$ -th roots, this yields

$$x +_{n-1} y \equiv x +_n y \pmod{U_n}.$$

as needed. For the second statement, we want to show that

$$ux +_n vy \equiv \left((ux)^{p^n} (vy)^{p^n}\right)^{p^{-n}} \equiv \left(x^{p^n} y^{p^n}\right)^{p^{-n}} \pmod{U_n}.$$

Taking  $p^n$ -th powers shows that the above is equivalent to

$$(ux)^{p^n} (vy)^{p^n} \equiv x^{p^n} y^{p^n} \pmod{U_{2n}},$$

which follows from [Lemma 9.2](#).  $\square$

Observe that as a consequence of the first part of [Lemma 9.7](#), for any  $x, y \in U$ , the sequence

$$x +_1 y, x +_2 y, \dots$$

is Cauchy and hence has a unique limit in  $U$ . Thus, the following makes sense.

**Definition 9.8.** If  $U$  is uniform, the *addition* is a function  $U \times U \rightarrow U$  defined by

$$(x, y) \mapsto x + y := \lim_{n \rightarrow \infty} x +_n y.$$

Informally, each of  $+_n$  spreads out the multiplication of  $U_{n+1}$  onto the whole group  $U$ . As  $U_{n+1}$  become smaller as  $n$  grows, the case of real Lie groups leads us to expect that  $+_n$  should become more and more simple. Thus, we would expect that in the limit, as in [Definition 9.8](#), the resulting map has a particularly simple form. We now verify that this is indeed the case.

**Proposition 9.9.** *The map  $+$ :  $U \times U \rightarrow U$  together with the original topology makes  $U$  into an abelian topological group with identity  $e \in U$  and inverse given by  $(-)^{-1}: U \rightarrow U$ .*

*Proof.* We first check that  $e$  is the identity. Since  $e^{p^n} = e$ , we have  $x +_n e = x$  for all  $x \in U$ , so that

$$x + e = \lim x +_n e = \lim x = x.$$

For inverse, we similarly observe that  $x +_n x^{-1} = e$  for all  $n$ , so that

$$x + x^{-1} = \lim x +_n x^{-1} = \lim e = e.$$

Continuity of addition follows from the second part of [Lemma 9.7](#).

For associativity, we again use [Lemma 9.7](#) to observe that

$$\begin{aligned} (x + y) + z &\equiv (x +_n y) + z \pmod{U_{n+1}} \\ &\equiv (x +_n y) +_n z \pmod{U_{n+1}} \\ &\equiv x +_n (y +_n z) \pmod{U_{n+1}} \\ &\equiv x + (y + z) \pmod{U_{n+1}}. \end{aligned}$$

Since this is true for all  $n$ , we get associativity.

We are left with showing that addition is commutative. Since  $[U_{n+1}, U_{n+1}] \leq U_{2n+2}$  by [Theorem 3.21](#), we have

$$\left( x^{p^n} y^{p^n} \right) \equiv y^{p^n} x^{p^n} \pmod{U_{2n+2}}.$$

Taking  $p^n$ -th roots, we get that

$$x +_n y \equiv y +_n x \pmod{U_{n+2}}.$$

Passing to the limit as  $n \rightarrow \infty$ , we get  $x + y = y + x$ .  $\square$

By [Proposition 9.9](#), a uniform pro- $p$  group  $U$  admits a *second* group structure on the same set of elements. To keep the two group structures apart, we continue to write the original multiplication of a uniform group  $U$  using juxtaposition or  $\cdot$  and use  $+$  to denote the addition of [Definition 9.8](#). These two are related in interesting ways, as we now show.

**Lemma 9.10.** *Let  $U$  be a uniform group and  $x, y \in U$ . Then*

- (1) if  $[x, y] = e$ , then  $x + y = xy$ ,
- (2)  $x^m = mx$ ,
- (3)  $p^k U = U_{k+1}$ .

*Proof.* For the first part, we have

$$x +_n y = \left( x^{p^n} y^{p^n} \right)^{p^{-n}}.$$

Since  $x$  and  $y$  commute, this is equal to

$$\left( (xy)^{p^n} \right)^{p^{-n}} = xy.$$

As this holds for all  $n$ , we deduce that  $x + y = xy$ . The second part follows from the first one by induction, since  $x$  commutes with all of its powers. The third part is a consequence of the second one and the fact that all elements of  $U_{k+1}$  are  $p^k$ -th powers, as proven in [Theorem 6.4](#).  $\square$

Note that as consequence of the third part of [Lemma 9.10](#),  $U_n \leq U$  is a normal subgroup with respect to either multiplication or addition. We now verify that with respect to either it determines the same division into cosets.

**Lemma 9.11.** *The additive cosets of  $U_n \subseteq U$  coincide with the multiplicative cosets. That is, for any  $a \in U$  we have*

$$a + U_n = aU_n.$$

*Proof.* If  $v \in U_n$ , then

$$a + v \equiv a + (ve) \equiv a + e \equiv a \pmod{U_n}.$$

So  $a + v = au$  for some  $u \in U_n$  and  $a + U_n \subseteq aU_n$ . Conversely,

$$au - a \equiv a - a \equiv e \pmod{U_n}.$$

Thus  $au - a = v$  for some  $v \in U_n$ , and therefore  $au = a + v$ , showing that  $aU_n \subseteq a + U_n$ .  $\square$

It follows from [Lemma 9.11](#) that for any  $n$  and  $k$ , the two quotients

$$(U_n, +)/(U_{n+k}, +) \simeq (U_n, \cdot)/(U_{n+k}, \cdot)$$

can be canonically identified as *sets*. When  $k = 1$ , they even coincide as groups:

**Lemma 9.12.** *For any  $n$ ,  $+$  and  $\cdot$  induce the same group structure on  $U_n/U_{n+1}$ .*

*Proof.* By [Theorem 5.14](#),  $x \mapsto x^{p^k}$  defines a group isomorphism  $U_n/U_{n+1} \rightarrow U_{n+k}/U_{n+k+1}$ . It follows that  $+_k$  define the same group structure on  $U_n/U_{n+1}$  as standard multiplication and hence so does their limit  $+$ .  $\square$

**Proposition 9.13.** *The addition makes  $U$  into a uniform group of dimension  $\dim(U)$ .*

*Proof.* Since  $p^n U = U_{n+1}$  form a basis of neighborhoods of the identity and

$$(9.1) \quad [(U, +) : p^n U] = [(U, \cdot) : U_{n+1}]$$

by [Lemma 9.11](#), we see that  $(U, +)$  is a pro- $p$  group. Since  $U/pU \simeq U/U_2$  is finite, we deduce that  $(U, +)$  is finitely generated. It is powerful since it is abelian. It is also uniform of the same dimension as  $U$  by [9.1](#), ending the argument.  $\square$

By virtue of [Proposition 9.13](#), the additive structure of a uniform group is not entirely dissimilar from the multiplicative one. However, it is much more simple as it is abelian, using which we can describe it completely. Recall from [Construction 7.12](#) that in a pro- $p$  group one can take powers of elements by  $p$ -adic integers, which defines an action of  $\mathbb{Z}_p$ .

**Theorem 9.14.** *Let  $U$  be uniform pro- $p$  group of dimension  $d$ . Then for any set  $a_1, \dots, a_d$  of generators,  $(U, +)$  is a free  $\mathbb{Z}_p$ -module generated by  $a_1, \dots, a_d$ , so that we have a topological group isomorphism*

$$(U, +) \simeq \mathbb{Z}_p^d.$$

*Proof.* By Lemma 9.12, addition and multiplication define the same group structure on  $U/U_2$ , so that any set of generators for  $U$  under multiplication is also a set of generators for  $U$  under addition. By Theorem 7.14, the map  $\mathbb{Z}_p^d \rightarrow U$  defined by

$$(\lambda_1, \dots, \lambda_d) \rightarrow \lambda_1 a_1 + \dots + \lambda_d a_d$$

is a homeomorphism. Since it is also a group homomorphism as  $(U, +)$  is abelian, the claim follows.  $\square$

Since the addition of a uniform group was defined by looking at its multiplication in smaller and smaller subgroups, informally one can interpret Theorem 9.14 as saying that in an infinitesimal neighbourhood of the identity, the multiplication is essentially linear.

**Remark 9.15.** One can think of  $(U, +)$  as the Lie algebra of  $U$ . In line with this heuristic, we will later show that the commutator of  $U$  induces a Lie bracket on the  $\mathbb{Z}_p$ -module  $(U, +)$ . Using the fact that any pro- $p$  group of finite rank has an open uniform subgroup, one can use this construction to associate a Lie algebra to any pro- $p$  group of finite rank (which in this case is defined only over  $\mathbb{Q}_p$ , essentially since we have to make a choice of a uniform subgroup and there might not be a canonical one).

One can obtain several pleasant consequences of Theorem 9.14 by observing that since addition is defined purely in terms of the group structure and the topology, the construction

$$U \mapsto (U, +) \in \text{Mod}_{\mathbb{Z}_p}$$

is clearly functorial in continuous group homomorphisms between uniform groups. This yields the following:

**Corollary 9.16.** *Any continuous automorphism of  $U$  acts linearly on  $(U, +)$ . Thus, any choice of a basis of  $(U, +)$  induces an identification*

$$\text{Aut}(U) \leq_c \text{GL}_d(\mathbb{Z}_p)$$

*of the group of continuous automorphisms of  $U$  with a closed subgroup of the general linear group.*

Using the fact that any group acts on itself by conjugation, we can prove the following elegant result.

**Theorem 9.17.** *Let  $G$  be a pro- $p$  group of finite rank and dimension  $\dim(G) = d$ . Then there exists an exact sequence of topological groups*

$$0 \rightarrow \mathbb{Z}_p^e \rightarrow G \rightarrow \text{GL}_d(\mathbb{Z}_p) \times F,$$

*where  $F$  is a finite  $p$ -group and  $e \leq d$ .*

*Proof.* By Proposition 7.4,  $G$  has a normal open uniform subgroup  $U \triangleleft_o G$ . We look at the map

$$G \rightarrow \text{Aut}(U) \times G/U$$

which is a product of the conjugation action of  $G$  on  $U$  and the quotient map. By Corollary 9.16,  $\text{Aut}(U)$  can be identified with a closed subgroup of  $\text{GL}_d(\mathbb{Z}_p)$ . We are left with identifying the kernel of this map, which is the center  $Z(U)$ . Since the kernel is abelian, of finite rank and torsion-free as  $U$  is, by Theorem 7.1 it is uniform and hence isomorphic to a free module over the  $p$ -adics by Theorem 9.14. This ends the argument.  $\square$

**Corollary 9.18.** *A profinite group is virtually a finite rank  $p$ -group if and only if it is an extension of closed subgroups of  $\text{GL}_d(\mathbb{Z}_p)$ .*

*Proof.* We have shown in Corollary 8.9 that the general linear group is virtually a uniform pro- $p$  group; in particular, virtually pro- $p$  of finite rank. This property is clearly closed under extensions, providing one direction. The converse follows from Theorem 9.17, since both the  $p$ -adics and any finite group can be embedded as a subgroup of the general linear group.  $\square$

**Remark 9.19.** The linear action of  $U$  on  $(U, +)$  through conjugation can be thought of as the  $p$ -adic analogue of the adjoint representation from the theory of Lie groups. In the latter case, if  $G$  is a Lie group, conjugation induces a map  $G \rightarrow \text{Aut}(\mathfrak{g})$  into the automorphisms of the Lie algebra. The kernel of this group homomorphism is the center  $Z(G) \triangleleft G$ . Following the same argument as in [Theorem 9.17](#), this proves that any Lie group of dimension  $d$  is an extension of a subgroup of  $\text{GL}_d(\mathbb{R})$  (necessarily closed if  $G$  is compact) and an abelian Lie group.

## 10. FORMAL GROUPS LAWS

Informally, formal group laws are a formal analogue of algebraic groups, where instead of remembering the whole variety one remembers the multiplication only in an infinitesimal neighbourhood of the identity. They arise naturally, in either the real or  $p$ -adic context, from the Taylor series expansion of the multiplication, and are an important refinement of the Lie algebra.

We will discuss more general formal group laws, as well as their relationship with  $p$ -adic analytic groups, later in the course. Today, we will focus on a particularly nice class of formal group laws, namely those which are 1-dimensional and commutative. These beautiful objects naturally arise in stable homotopy theory, and their automorphism groups are often  $p$ -adic analytic, as we will show in the next lecture.

**Definition 10.1.** A (1-dimensional, commutative) *formal group law* over a commutative ring  $R$  is a power series  $F(x, y) \in R[[x, y]]$  such that

- (1)  $F(x, 0) = x$  (*right unitality*),
- (2)  $F(0, y) = y$  (*left unitality*),
- (3)  $F(F(x, y), z) = F(x, F(y, z))$  (*associativity*),
- (4)  $F(x, y) = F(y, x)$  (*commutativity*).

**Warning 10.2.** Beware that in addition to the notion of a *formal group law*, there is also a more geometric notion of a *formal group*. These are closely related, but are not quite the same; roughly, the latter is a coordinate-free version of the former, at least locally. In this course, we will be content with only discussing formal group laws, since the additional complication is not needed for our applications.

**Remark 10.3.** For a more thorough exposition of formal group laws in a language similar to ours, including their underlying geometry, we recommend notes from the previous course [[Pst21](#)].

**Notation 10.4.** If  $F(x, y)$  is a formal group law, it is common to write

$$x +_F y := F(x, y).$$

In this notation, the above axioms take the form

- (1)  $x +_F 0 = x$ ,
- (2)  $0 +_F y = y$ ,
- (3)  $(x +_F y) +_F z = x +_F (y +_F z)$ ,
- (4)  $x +_F y = y +_F x$ .

In other words,  $+_F$  (considered, for example, as an operation on power series with no constant term) behaves like an ordinary addition: the sum of any finite number of objects doesn't depend on their order or the order of multiplication itself.

As discussed in the introduction, a natural source of formal group laws is given by algebraic groups.

**Construction 10.5** (Formal group laws from varieties). Let  $k$  be a field and let  $A$  be an abelian group object in  $k$ -varieties which is of dimension one as a variety. Any such variety is smooth, and using this fact one can show that the completion of the local ring

$$\widehat{\mathcal{O}}_{A,e} \simeq k[[x]]$$

at the identity  $e \in A$  is non-canonically isomorphic to the ring of formal power series<sup>7</sup>. The multiplication of  $A$  induces a continuous map

$$\phi: k[[x]] \simeq \widehat{\mathcal{O}}_{A,e} \rightarrow \widehat{\mathcal{O}}_{A,e} \widehat{\otimes}_k \widehat{\mathcal{O}}_{A,e} \simeq k[[x_1, x_2]]$$

which is determined by the image  $F(x_1, x_2) := \phi(x)$  of the generator. The commutativity and associativity of the group multiplication of  $A$  imply that  $F(x_1, x_2)$  is a formal group law.

**Example 10.6** (The additive and multiplicative formal group law). Let  $\mathbb{G}_a \simeq \mathbb{A}_k^1$  be the additive group of a field  $k$ ; that is, the affine one-space considered as a group under addition. In this case, [Construction 10.5](#) yields the *additive formal group law*

$$F_a(x, y) = x + y.$$

If we instead take the multiplicative group  $\mathbb{G}_m \simeq \mathbb{A}_k^1 \setminus \{0\}$ , then we obtain the *multiplicative formal group law*

$$F_m(x, y) = x + y + xy.$$

Formal group laws informally encode multiplication on some geometric object. Because of that, they naturally form a category, with morphisms a natural analogue of maps of geometric objects they correspond to.

**Definition 10.7.** Let  $F, G$  be formal group laws over a ring  $R$ . Then a *morphism of formal group laws*  $\phi: F \rightarrow G$  is a power series  $\phi \in R[[x]]$  with no constant term such that we have an equality

$$\phi(F(x, y)) = G(\phi(x), \phi(y))$$

of power series in two variables.

Note that if given a ring homomorphism  $\phi: R \rightarrow R'$  and a formal group law

$$F = \sum a_{i,j} x^i y^j \in R[[x, y]],$$

applying  $\phi$  to each coefficient separately we obtain a new formal group law

$$\phi^* F := \sum \phi(a_{i,j}) x^i y^j \in R'[[x, y]]$$

over the target ring. Similarly, we can apply  $\phi$  to coefficients of an endomorphism, so that it actually assembles into a functor

$$\phi^*: \{\text{Formal groups laws over } R\} \rightarrow \{\text{Formal groups laws over } R'\}$$

between the corresponding categories.

**Remark 10.8** (The moduli stack of formal groups). Restricting to formal group laws and isomorphisms, to each ring we can functorially associate a groupoid, which we can identify with a 1-truncated anima. This yields a covariant functor of  $\infty$ -categories

$$\{\text{Formal groups laws over } -\}: \mathcal{CRing} \rightarrow \mathcal{S},$$

where the target is the  $\infty$ -category of anima. The Zariski sheafification of this functor is known as the *moduli stack of formal groups* and often denoted by  $\mathcal{M}_{fg}$ .

The functor  $\mathcal{M}_{fg}$  is not far from being an algebraic stack, as one can show that it is a quotient of an affine scheme by a flat action of an affine group scheme. This moduli stack is deeply related to patterns in homotopy theory, as first discovered by Quillen, and an often used informal slogan is that

“The behaviour of stable homotopy theory is controlled by the geometry of the moduli stack of formal groups.”

---

<sup>7</sup>It is this non-canonical choice of a coordinate that distinguishes between formal group laws and formal groups. We will not discuss the latter, but we mention here that the choice of a coordinate is not needed when one works with formal groups instead.

Note that this moduli stack is just a convenient way of packaging information about formal group laws and their isomorphisms, so this is just saying that many phenomena in stable homotopy theory can be directly related to formal groups. This is one piece of motivation to understand this beautiful subject.

An interesting example of an isomorphism of formal group laws is provided by the classical exponential function.

**Example 10.9.** Let  $k$  be a field of characteristic zero and consider the power series

$$\phi(x) := e^x - 1 = \sum_{n \geq 1} \frac{1}{n!} x^n.$$

Then

$$\phi(x + y) = e^{x+y} - 1 = e^x e^y - 1 = (e^x - 1) + (e^y - 1) + (e^x - 1)(e^y - 1),$$

so that  $\phi: F_a \rightarrow F_m$  is an isomorphism between the additive and multiplicative formal group laws of [Example 10.6](#).

Note that in the context of [Example 10.9](#), it is crucial that we work in characteristic zero, or else the exponential power series is not well-defined, as it involves division by factorials. In fact, this is an instance of general phenomena: in characteristic zero, (one-dimensional, commutative) formal group laws are not particularly interesting, as the following result shows.

**Theorem 10.10** (Lazard). *Let  $k$  be a field of characteristic zero. Then:*

- (1) *any formal group law over  $k$  is isomorphic to the additive one,*
- (2) *all automorphisms of the additive formal group law are of the form  $\phi(x) = \lambda x$  for some  $\lambda \in k$ ; that is,  $\text{End}(F_a/k) \simeq k$  as rings.*

*Proof.* This is not difficult, see [[Rav03](#), A.2.1.6]. □

In positive characteristic, the situation is more complex; in particular, the additive and multiplicative formal group laws are not isomorphic. To distinguish between them, it is helpful to look at the analogue of multiplication by  $p$ .

**Definition 10.11.** Let  $F \in R[[x, y]]$  be a formal group law. The  $p$ -series of  $F$  is given by

$$[p]_F(x) := x +_F \dots +_F x.$$

**Remark 10.12.** Since  $F$  is commutative, the  $p$ -series is in fact an endomorphism of  $F$ , corresponding to the element  $p$  in the endomorphism ring  $\text{End}(F/R)$ .

**Remark 10.13.** Moreover, if  $\phi: F \rightarrow G$  is an isomorphism of formal group laws, then

$$\phi \circ [p]_F \circ \phi^{-1} = [p]_G,$$

so that their  $p$ -series differ only by a conjugation by an invertible power series.

The unitality axiom of the formal group laws forces the  $p$ -series to be of the form

$$[p]_F(x) = px + \text{higher order terms.}$$

Since a power series is invertible under composition if and only if the leading term is, we deduce that the  $p$ -series is invertible if and only if  $p \in R$  is invertible. In particular, over a field, the  $p$ -series is an isomorphism when and only when we're working outside of characteristic  $p$ .

This suggests that one measure of complexity of a formal group law in positive characteristic would be *how badly* does it  $p$ -series fail to be invertible, leading to the notion of a *height*.

**Lemma 10.14.** *Let  $F$  be a formal group law over a field  $k$  of characteristic  $p$ . Then either  $[p]_F = 0$  or the  $p$ -series can be written as*

$$[p]_F(x) = \phi(x^{p^n})$$

for an invertible power series  $\phi$  and a unique  $n > 0$ .

*Proof.* This follows from [Lemma 12.10](#), proven in a subsequent lecture. For now, we recommend the reader take this result on faith.  $\square$

**Definition 10.15.** Let  $F$  be a formal group law over a field of characteristic  $p$ . If

$$[p]_F(x) = \phi(x^{p^n})$$

with  $\phi$  invertible, then we say that  $F$  is of *height*  $n$ . If instead  $[p]_F(x) = 0$ , then we say that  $F$  is of *infinite height*.

**Example 10.16.** Let's calculate the heights of the additive and multiplicative formal group laws of [Example 10.6](#) in positive characteristic. In the additive case, we have

$$[p]_{F_a}(x) = px = 0,$$

so that the height is infinite. In the multiplicative case, we have

$$[p]_{F_m}(x) = (x + 1)^p - 1 = x^p,$$

so that height is equal to one.

Since the  $p$ -series of isomorphic formal group laws differ by a conjugation an invertible series as observed in [Remark 10.13](#), a corollary of the calculation of [Example 10.16](#) is that the additive and multiplicative formal group laws are not isomorphic in positive characteristic.

A fundamental result of Lazard shows that locally in the étale topology, height is a complete invariant.

**Theorem 10.17** (Lazard). *Let  $k$  be a separably closed (for example, algebraically closed) field of positive characteristic. Then:*

- (1) *two formal group laws over  $k$  are isomorphic if and only if they are of the same height,*
- (2) *formal group laws of any height  $1 \leq n \leq \infty$  exist.*

Note that [Theorem 10.17](#) does not say anything about automorphisms of formal group laws. In fact, these behave quite differently in the case of infinite height, where the automorphism group depends on the field and is quite enormous, and in the case of finite height, where the automorphism group depends on the base field only very mildly and has favourable properties: it is a  $p$ -adic analytic group. We will discuss this in more detail in the next two lectures, where we also sketch the construction of formal group laws of arbitrary finite height.

## 11. LUBIN-TATE FORMAL GROUP LAWS

In this lecture, we will use a technique due to Lubin-Tate to construct formal group laws of arbitrary finite height, as well as some of their endomorphisms. In the next lecture, we will then describe their endomorphism ring explicitly.

The axioms of a formal group law, which we described in [Definition 10.1](#), look deceptively simple, but when expanded out in terms of the coefficients of the power series in question become quite complicated. Because of that, it is in general difficult to write down a formal group law explicitly by hand, except where it comes from an algebraic group as in [Construction 10.5](#).

An insight due to Lubin and Tate is that formal group laws in positive characteristic can be written down essentially inductively, and the key observation is that this is easier to do in mixed characteristic rather than positive one. We are mostly interested in the situation of perfect fields, where a canonical lift to mixed characteristic is provided by the construction of Witt vectors which we now recall.

**Recollection 11.1.** We say that a commutative ring  $W$  is a *ring of Witt vectors* if it satisfies the following three properties:

- (1)  $W$  is  $p$ -complete; that is,  $W \simeq \varprojlim W/p^n$ ,
- (2)  $W$  is flat over  $\mathbb{Z}_p$ ,

(3) the  $\mathbf{F}_p$ -algebra  $W/pW$  is perfect; that is, the Frobenius  $x \mapsto x^p$  is an isomorphism.

The construction  $W \mapsto W/pW$  provides a functor

$$(11.1) \quad \mathrm{CAlg}^{\mathrm{Witt}} \rightarrow \mathrm{CAlg}_{\mathbf{F}_p}^{\mathrm{perf}}$$

from the full subcategory of rings spanned by rings of Witt vectors to the full subcategory of rings spanned by perfect  $\mathbf{F}_p$ -algebras. One can show using obstruction theory that (11.1) is an equivalence of categories, and so has an inverse which we write as

$$R \in \mathrm{CAlg}_{\mathbf{F}_p}^{\mathrm{perf}} \mapsto W(R) \in \mathrm{CAlg}^{\mathrm{Witt}}.$$

We call  $W(R)$  the *ring of Witt vectors of  $R$* ; it is the unique lift of  $R$  to a flat,  $p$ -complete  $\mathbb{Z}_p$ -algebra.

**Example 11.2.** We have

$$W(\mathbf{F}_p) \simeq \mathbb{Z}_p,$$

since the latter is flat over itself,  $p$ -complete and reduces to  $\mathbf{F}_p$ . More generally, if  $q = p^n$ , then we can write the finite field with  $q$  elements as  $\mathbf{F}_q = \mathbf{F}_p[\zeta_{q-1}]$ , where  $\zeta_{q-1}$  is a primitive  $(q-1)$ -th root of unity. Using this description one can check that

$$W(\mathbf{F}_q) = \mathbb{Z}_p[\zeta_{q-1}].$$

**Warning 11.3.** The ring of Witt vectors of [Recollection 11.1](#) should be more properly called the *ring of  $p$ -typical Witt vectors*, since there are other variants of this construction (including for algebras which are not perfect). For an exhaustive account, see [\[Hes05\]](#). In this course, we will not need other variants, in fact we will only work with Witt vectors of finite fields as in [Example 11.2](#).

**Definition 11.4.** Let  $R$  be a perfect  $\mathbf{F}_p$ -algebra. The *Witt vector Frobenius* is the unique ring automorphism

$$\sigma: W(R) \rightarrow W(R)$$

which reduces to the Frobenius modulo  $p$ ; that is, such that

$$\sigma(w) \equiv x^p \pmod{p}$$

for all  $w \in W(R)$ .

Note that the Witt vector Frobenius exists since the reduction mod  $p$  functor is an equivalence between rings of Witt vectors and perfect  $\mathbf{F}_p$ -algebras, so that any map of the latter (such as the Frobenius) lifts uniquely to rings of Witt vectors.

**Example 11.5.** In the case of the ring of Witt vectors of a finite field as in [Example 11.2](#), the Frobenius is given by the unique ring automorphisms such that

$$\sigma(\zeta_{q-1}) = \zeta_{q-1}^p;$$

that is, the Frobenius permutes the primitive  $(q-1)$ -th roots of unity.

To construct a formal group law of arbitrary finite height over  $\mathbf{F}_p$ , we will instead construct it first over the ring of Witt vectors. The following technical lemma of Lubin and Tate does all of the heavy lifting.

**Lemma 11.6** (Lubin-Tate). *Let  $R$  be a perfect  $\mathbf{F}_p$ -algebra such that  $r = r^q$  for all  $r \in R$  and let  $f(x) \in W(R)[[x]]$  be a power series such that*

- (1)  $f(x) \equiv px \pmod{x^2}$ ,
- (2)  $f(x) \equiv x^q \pmod{p}$

Then, for any linear form

$$\phi(x) = a_1x_1 + \dots + a_kx_k$$

linear form with coefficients in  $W(R)$  there exists a unique unique power series

$$\tilde{\phi}(x) \in W(R)[[x_1, \dots, x_k]]$$

such that

(1)  $\tilde{\phi}$  lifts  $\phi$ ; that is, we have

$$\tilde{\phi}(x_1, \dots, x_k) = \phi(x_1, \dots, x_k) + \text{terms of degree two and higher,}$$

(2)  $\tilde{\phi}$  commutes with  $f$ ; that is,

$$f(\tilde{\phi}(x_1, \dots, x_k)) = \tilde{\phi}(f(x_1), \dots, f(x_k))$$

*Proof.* For brevity, we write  $x$  to mean  $x_1, \dots, x_k$ . We will construct by induction a compatible sequence of degree  $n$  polynomials  $\phi_n(x)$  such that the second equations holds modulo terms of degree  $n + 1$  and higher, and that  $\phi_n(x)$  is unique subject to this property. The needed power series will be then given by

$$\tilde{\phi}(x) := \lim \phi_n(x),$$

the limit taken in the  $x$ -adic topology. The base case holds with  $\phi_1(x) := \phi(x)$ .

Now assume that  $\phi_n(x)$  is already constructed. By inductive assumption, the “error”

$$E(\phi_n) := f(\phi_n(x)) - \phi_n(f(x))$$

vanishes up to degree  $n$ . We define

$$\phi_{n+1} := \phi_n(x) + c(x)$$

where  $c(x)$  is a “correction term”, homogeneous of degree  $n + 1$ , such that

$$E(\phi_{n+1}) = f(\phi_{n+1}(x)) - \phi_{n+1}(f(x)).$$

vanishes modulo terms of degree  $n + 2$ . To see what equation  $c$  should satisfy, observe that by our assumption on  $f$ , we have that

$$f(\phi_{n+1}(x)) = f(\phi_n(x) + c(x)) \equiv f(\phi_n(x)) + pc(x) \pmod{x^{n+2}}$$

and similarly

$$\phi_{n+1}(f(x)) = \phi_n(f(x)) + c(f(x)) \equiv \phi_n(f(x)) + p^{n+1}c(x) \pmod{x^{n+2}}.$$

Thus  $E(\phi_{n+1}) \equiv 0 \pmod{x^{n+2}}$  is equivalent to

$$(11.2) \quad E(\phi_n) = (-p - p^{n+1})c(x) \pmod{x^{n+2}}.$$

The left hand side is of degree at least  $n + 1$ , and we claim that its homogeneous part  $E(\phi_n)_{n+1}$  of degree  $(n + 1)$  is divisible by  $p$ . We can thus define

$$c(x) := \frac{-E(\phi_n)_{n+1}}{p(1 - p^n)},$$

where we use that  $1 - p^n$  is a unit in any  $p$ -complete algebra, which gives the correction term with the needed properties. Note that since  $p$  is a non-zero divisor in  $W(R)$ , a  $c$  satisfying (11.2) is necessarily unique.

We are left with verifying the claim that  $E(\phi_n)_{n+1}$  is divisible by  $p$ ; equivalently, that its image vanishes in  $W(R)/p \simeq R$ . Since in the quotient  $f(x) = x^q$ , this amounts to checking that  $\phi_n(x^q) = \phi_n(x)^q$  as a power series over  $R$ . This holds for any power series  $\phi_n(x) = \sum_i a_i x^i$ , as

$$\sum_i a_i^q x^{qi} = \sum_i a_i x^{qi}$$

because  $a_i^q = a_i$  by our assumption on  $R$ . □

Note that the most important part of [Lemma 11.6](#) is that the resulting power series is unique. This uniqueness is not true for power series over  $R$ ; in fact, the proof proceeds by observing that over  $R$  itself *any* power series commutes with  $f(x) = x^q$ . The uniqueness is used in the proof of the following fundamental result:

**Theorem 11.7.** *Let  $R$  be a  $\mathbf{F}_p$ -algebra such that  $r = r^q$  for all  $r \in R$  and let  $f(x) \in W(R)[[x]]$  be a power series such that*

- (1)  $f(x) \equiv px \pmod{x^2}$ ,
- (2)  $f(x) \equiv x^q \pmod{p}$ .

*Then, there exists a unique formal group law  $F(x, y) \in W(R)[[x, y]]$  with  $f$  as an endomorphism. Moreover,  $[p]_F(x) = f(x)$ ; that is,  $f$  is precisely its  $p$ -series.*

*Proof.* Note that by unitality, if  $F$  is a formal group law, then we have

$$F(x, y) = x + y + \text{higher order terms.}$$

If  $f$  is its endomorphism, then we additionally have

$$F(f(x), f(y)) = f(F(x, y)).$$

By [Lemma 11.6](#), there exists a unique power series with these two properties, which we denote by

$$F(x, y) := \widetilde{(x + y)}.$$

We claim that  $F(x, y)$  is a formal group law; by construction, it is unital. To verify that it is associative, observe that  $F(F(x, y), z)$  and  $F(x, F(y, z))$  are both power series in three variables which are equal to  $x + y + z$  modulo terms of higher degree and which commute with  $f$ . By the uniqueness part of [Lemma 11.6](#), we deduce that

$$F(F(x, y), z) = F(x, F(y, z)).$$

Commutativity follows from the same argument applied to  $F(x, y)$  and  $F(y, z)$ , which both reduce to  $x + y$  and commute with  $f$ .

Finally, to see that we have  $[p]_F = f(x)$ , observe that both sides commute with  $f$  and are equal to  $px$  relative to terms of higher degree.  $\square$

**Definition 11.8.** The unique formal group law over  $F_f(x, y)$  with  $p$ -series  $[p]_F = f(x)$  is called the *Lubin-Tate formal group law* of  $R$ .

**Remark 11.9.** Using a variation of [Lemma 11.6](#), one can show that any two Lubin-Tate formal group laws (associated to possibly different power series  $f(x)$ , but such that  $f(x) \equiv x^q \pmod{p}$  for the same  $q = p^n$ ) are *canonically* isomorphic. For details, see the previous course [[Pst21](#), §14].

Note that arguably the most simple power series  $f(x)$  satisfying the conditions of [Lemma 11.6](#) is

$$f(x) = px + x^q.$$

The Lubin-Tate series associated to this  $f(x)$  has a special name.

**Definition 11.10.** The Lubin-Tate formal group law  $\Gamma_n$  over  $\mathbb{Z}_p$  with  $p$ -series  $[p]_{\Gamma_n} = px + x^q$  is called the *Honda formal group law of height  $n$* .

Note that the reduction of  $\Gamma_n$  to  $\mathbf{F}_p$  (which by abuse of terminology we also call the Honda formal group law) is of height  $n$ , since  $f(x) \equiv x^q = x^{p^n} \pmod{p}$ . In particular, we deduce the second part of [Theorem 10.17](#), which we state again in slightly different form:

**Corollary 11.11.** *Over any field  $k$  of characteristic  $p$ , there exist formal group laws of arbitrary height  $1 \leq n \leq \infty$ .*

*Proof.* Since any such field contains  $\mathbf{F}_p$ , it is enough to show this in this case. When  $n$  is finite, the needed formal group law is given by the one of Honda of [Definition 11.10](#). For  $n = \infty$ , we can take the additive formal group law of [Example 10.6](#).  $\square$

**Remark 11.12.** In this course, we will not prove the more interesting part of [Theorem 10.17](#), namely that over a separably closed field formal group laws are classified up to isomorphism by their height. For a detailed proof, see [[Pst21](#), §15].

The set of endomorphisms

$$\text{End}(F/R) := \{f(x) \in R[[x]] \mid f \text{ is an endomorphism of } F\}$$

of a formal group law  $F$  over a ring  $R$  can be made into a ring, with multiplication

$$f(x) \cdot_{\text{End}(F/R)} g(x) := f(g(x))$$

provided by composition and addition

$$f(x) +_{\text{End}(F/R)} g(x) := f(x) +_F g(x) = F(f(x), g(x))$$

provided by addition using  $F$  itself. This construction is functorial in the ring in the sense that if  $\phi: R \rightarrow R'$  is a ring homomorphism and  $F' := \phi^* F$ , then applying  $\phi$  to coefficients of a power series gives a ring homomorphism

$$\text{End}(F/R) \rightarrow \text{End}(F'/R').$$

A useful property of Lubin-Tate formal group laws which makes them convenient from our perspective is that they come equipped with a canonical family of endomorphisms in a way compatible with the structure of the endomorphism ring.

**Construction 11.13.** Let  $w \in W(R)$ . Then, by [Lemma 11.6](#) there exists a unique power series, which we denote by

$$[w](x) := \widetilde{w}x,$$

such that  $[w](x) = wx + \text{higher order terms}$  and such that  $[w]$  commutes with  $f$ .

**Proposition 11.14.** *The power series  $[w](x)$  of [Construction 11.13](#) is an endomorphism of the Lubin-Tate formal group law associated to  $f$ . Moreover, the construction*

$$w \mapsto [w](x)$$

*induces an isomorphism of rings*

$$W(R) \xrightarrow{\cong} \text{End}(F_f/W(R)).$$

*Proof.* To check that  $[w](x)$  is an endomorphism, we have to verify that

$$F_f([w](x), [w](y)) = [w](F_f(x, y)).$$

However, both sides agree on linear terms and commute with  $f$ , hence this follows from the uniqueness part of the Lubin-Tate lemma. To verify that  $w \mapsto [w](x)$  is a ring homomorphism, we have to check that

- (1)  $[w + w'](x) = [w](x) +_{F_f} [w'](x)$  (*addition*),
- (2)  $[ww'](x) = [w]([w'](x))$  (*multiplication*),
- (3)  $[1](x) = x$  (*unit*).

These three identities again follow from the fact that in each case both sides commute with  $f$  and agree on linear terms. To see that  $w \mapsto \widetilde{w}$  is an isomorphism, observe that any endomorphism commutes with the  $p$ -series, hence is uniquely determined by its leading term.  $\square$

12. THE MORAVA STABILIZER GROUP

In previous lecture, we introduced a construction of Lubin-Tate formal group laws, which are formal group laws over rings of Witt vectors with a prescribed  $p$ -series. In this lecture, we will calculate their endomorphism ring of their reduction modulo  $p$ .

As we observed in [Remark 11.9](#), up to isomorphism, a Lubin-Tate formal group law  $F$  over  $W(R)$  depends only on the integer  $q$  such that

$$[p]_F(x) = x^q \pmod{p}.$$

In other words, up to isomorphism they depend only on the height of their reduction mod  $p$ , which we recall is the integer  $n$  such that  $[p](x) = x^{p^n} +$  higher order terms. Thus, without loss of generality we can focus on the Honda formal group law of [Definition 11.10](#), which is the unique formal group law  $\Gamma_n$  over  $\mathbb{Z}_p$  with  $p$ -series

$$[p]_{\Gamma_n}(x) = px + x^q,$$

where  $q = p^n$ . Today, we calculate the automorphism group of  $\Gamma_n$  over the algebraic closure  $\overline{\mathbf{F}_p}$ , and show that it is a  $p$ -adic analytic group of dimension  $n^2$ .

**Notation 12.1.** We generally do not distinguish between  $\Gamma_n$  as a formal group law over  $\mathbb{Z}_p$  and its reduction mod  $p$ , which is a formal group law over  $\mathbf{F}_p$ . We will, however, be careful about distinguishing between endomorphisms defined over different rings, as these can be quite different from each other.

Note that by a result of Lazard, which we stated in [Theorem 10.17](#), all formal groups of height  $n$  over  $\overline{\mathbf{F}_p}$  are isomorphic, and thus so are their endomorphism rings. Thus, our calculation would give exactly the same result for any other formal group law of height  $n$ . One reason it is convenient to choose  $\Gamma_n$  specifically, besides its explicit construction, is the following:

**Proposition 12.2.** *Let  $k$  be a field of characteristic  $p$  which has a primitive  $(q - 1)$ -th root of unity. Then, any inclusion  $\mathbf{F}_q \hookrightarrow k$  induces an isomorphism of endomorphism rings*

$$\text{End}(\Gamma_n/\mathbf{F}_q) \simeq \text{End}(\Gamma_n/k).$$

In particular,

$$\text{End}(\Gamma_n/\mathbf{F}_q) \simeq \text{End}(\Gamma_n/\overline{\mathbf{F}_q}).$$

*Proof.* Let  $\phi: \Gamma_n \rightarrow \Gamma_n$  be an endomorphism with coefficients in  $k$  and write  $\phi(x) = \sum a_i x^i$ . Since it is an endomorphism,  $\phi$  commutes with the  $p$ -series  $[p]_{\Gamma_n}(x) = x^q$ , so that we have

$$\sum a_i^q x^{qi} = (\sum a_i x^i)^q = [p] \circ \phi = \phi \circ [p] = \sum a_i x^{qi}.$$

It follows that  $a_i^q = a_i$  for each  $i \geq 0$ , hence  $a_i \in \mathbf{F}_q$ , as needed. □

As a consequence of [Proposition 12.2](#), when working with the Honda formal group law, we can focus on endomorphisms over  $\mathbf{F}_q$ . In [Proposition 11.14](#), we saw that the Lubin-Tate construction provides a isomorphism of rings

$$W(\mathbf{F}_q) \xrightarrow{\simeq} \text{End}(\Gamma_n/W(\mathbf{F}_q)).$$

We can compose with reduction mod  $p$  to obtain a ring homomorphism

$$(12.1) \quad W(\mathbf{F}_q) \rightarrow \text{End}(\Gamma_n/\mathbf{F}_q).$$

However, the latter map is no longer surjective, as there are endomorphisms of  $\Gamma_n$  over  $\mathbf{F}_q$  which cannot be lifted to an endomorphism over the Witt vectors. A principal example of such a endomorphism is the Frobenius which we now define.

**Lemma 12.3.** *The power series  $S(x) = x^p$  is an endomorphism of  $\Gamma_n$  over  $\mathbf{F}_p$ .*

*Proof.* Since  $\Gamma_n$  is a reduction of a formal group law over the  $p$ -adics, we have  $\Gamma_n(x, y) = \sum a_{i,j} x^i y^j$  with  $a_{i,j} \in \mathbf{F}_p$ , so that  $a_{i,j}^p = a_{i,j}$ . Thus,

$$S(\Gamma_n(x, y)) = \left(\sum a_{i,j} x^i y^j\right)^p = \sum a_{i,j} x^{pi} y^{pj} = \Gamma_n(S(x), S(y)).$$

□

**Definition 12.4.** We call the endomorphism  $S \in \text{End}(\Gamma_n, \mathbf{F}_q)$  defined by  $S(x) = x^p$  the *Frobenius* of the Honda formal group law.

We now show that the endomorphism ring can be described explicitly in terms of the Lubin-Tate construction and Frobenius:

**Theorem 12.5.** *The ring homomorphism Equation (12.1) and the Frobenius induces an isomorphism of rings*

$$\text{End}(\Gamma_n/\mathbf{F}_q) \simeq W(\mathbf{F}_q)\langle S \rangle / (S^n = p, Sw = w^\sigma S),$$

where  $(-)\langle S \rangle$  denotes the ring obtained by attaching a new non-commuting variable and  $w \mapsto w^\sigma$  is the Witt vector Frobenius on  $W(\mathbf{F}_q)$ .

Note that the endomorphism ring inherits a canonical topology as a closed subspace

$$\text{End}(\Gamma_n) \subseteq \mathbf{F}_q[[x]],$$

where we equip the target with the limit topology coming from the identification

$$\mathbf{F}_q[[x]] \simeq \varprojlim \mathbf{F}_q[x]/x^n.$$

Concretely, a sequence of endomorphisms converges to zero if they eventually become divisible by  $x^n$  for all  $n$ . Observe that

- (1) as a closed subspace, the endomorphism ring is complete with respect to this topology,
- (2) since under the Lubin-Tate construction,  $p^k \mapsto [p]_{\Gamma_n}^k(x) = x^{kq}$ , which becomes highly divisible by  $x$  as  $k$  grows, the map

$$W(\mathbf{F}_q) \rightarrow \text{End}(\Gamma_n)$$

is continuous, where we equip the Witt vectors with the  $p$ -adic topology.

These two observations are useful, as they mean that one can evaluate certain infinite sums in both the Witt vectors and endomorphism ring, by taking limits of finite sums, in a compatible manner.

The proof of [Theorem 12.5](#) will proceed in steps. We first verify that the two relations involving the Frobenius and the endomorphisms coming from the Lubin-Tate construction do hold.

**Definition 12.6.** We say that an element  $a \in W(\mathbf{F}_q)$  is a *Teichmüller representative* if  $a^q = a$ .

**Lemma 12.7.** *We have that:*

- (1) any element  $\bar{a} \in \mathbf{F}_q$  has a unique lift to a Teichmüller representative,
- (2) any  $w \in W(\mathbf{F}_q)$  can be uniquely written as

$$w = \sum_{i \geq 0} a_i p^i$$

where  $a_i$  are Teichmüller representatives.

*Proof.* The first part is immediate from Hensel's lemma applied to the polynomial  $f(x) = x^q - x$ , whose derivative  $f'(x) = -1$  over  $\mathbf{F}_q$  is nowhere vanishing. For the second part, let  $a_0$  be the unique Teichmüller representative of the reduction of  $w \bmod p$ , so that

$$w = a_0 + pw'$$

for a uniquely defined  $w'$ . Inductively applying the construction to  $w'$  leads to the needed series expansion.  $\square$

**Lemma 12.8.** *Let  $a \in W(\mathbf{F}_q)$  be a Teichmüller representative. Then*

$$[a](x) = ax \in W(\mathbf{F}_q)\llbracket x \rrbracket,$$

where the left hand side is [Construction 11.13](#).

*Proof.* Observe that the left hand side commutes with the  $p$ -series

$$[p]_{\Gamma_n} = px + x^q$$

by construction. To see that so does the right hand side, we calculate

$$p(ax) + (ax)^q = pax + a^q x^q = a(px + x^q).$$

It follows from Lubin-Tate lemma that the two are equal, as they both have the same linear term.  $\square$

**Lemma 12.9.** *In  $\text{End}(\Gamma_n/\mathbf{F}_q)$ , the following equalities hold:*

- (1)  $S^n = p$ ,
- (2)  $Sw = w^\sigma S$  for each  $w \in W$ .

*Proof.* The first equality is saying that

$$S^n(x) = [p]_{\Gamma_n},$$

which is clear since both sides are equal to  $x^q = x^{p^n}$ .

We move to the second equality, where in terms of power series we have to show that

$$S([w](x)) = [w^\sigma](x^p),$$

where  $[-]$  denotes [Construction 11.13](#). We first show it in the special case when  $w = a$  is a Teichmüller representative. In this case, we have  $[a](x) = \bar{a}x$ , where  $\bar{a}$  is the image of  $a$  in  $\mathbf{F}_p$ , and we calculate

$$S([a](x)) = (\bar{a}x)^p = \bar{a}^p x^p = \bar{a}^p(x^p) = [a^p](S(x)),$$

where we use that  $(a^p)^q = a^p$ . Since by Hensel's lemma any element of  $\mathbf{F}_q$  has a *unique* lift to an element satisfying  $a^q = a$ , we deduce that  $a^\sigma = a^p$  on such elements, proving the claim.

By [Lemma 12.7](#), a general Witt vector can be uniquely written as

$$w = \sum a_i p^i,$$

where  $a_i$  are Teichmüller representatives. Since  $p$  is central in the endomorphism ring, we deduce that in  $\text{End}(\Gamma_n/\mathbf{F}_q)$  we have

$$Sw = S\left(\sum a_i p^i\right) = \sum a_i^\sigma p^i S = w^\sigma S,$$

since  $p^\sigma = p$  as  $\sigma$  is a ring automorphism. This ends the argument.  $\square$

Note that [Lemma 12.9](#) implies that the choice of the Frobenius and the Lubin-Tate construction yield a ring homomorphism

$$W(\mathbf{F}_q)\langle S \rangle / (S^n = p, Sw = w^\sigma S) \rightarrow \text{End}(\Gamma_n/\mathbf{F}_q)$$

We will complete the proof of [Theorem 12.5](#) by showing that this is an isomorphism of rings (in fact of topological rings).

We will need the following basic result of homomorphism of formal group laws in positive characteristic.

**Lemma 12.10.** *Let  $F_1, F_2$  be formal group laws over a field  $k$  of positive characteristic  $p$  and let  $\phi: F_1 \rightarrow F_2$  be a homomorphism. Then either*

- (1)  $\phi(x) = 0$ ,
- (2)  $\phi(x) = \psi(x^{p^n})$  for some  $n > 0$  and some power series  $\psi$  invertible under composition; that is, such that

$$\psi(x) = \lambda x + \text{higher order terms}$$

with  $\lambda \neq 0$ .

*Proof.* Let  $\phi$  be non-zero. If  $\phi(x) = \lambda_0 x + \text{higher order terms}$  with  $\lambda \neq 0$ , then there is nothing to be done, so suppose that  $\lambda_0 = 0$ . Since  $\phi$  is a homomorphism, we have

$$\phi(F_1(x, y)) = F_2(\phi(x), \phi(y)).$$

This is an equality of power series in two variables, and taking a partial derivative in the  $y$  direction we deduce that

$$(12.2) \quad (\partial_y F_1)(x, y) \cdot \phi'(F_1(x, y)) = \phi'(y) \cdot (\partial_y F_2)(\phi(x), \phi(y)).$$

Since for any formal group law  $F(x, y)$  unitality implies that

$$F(x, y) = x + y + \text{higher order terms},$$

we have

$$(\partial_y F)(x, y) = 1 + \text{higher order terms}.$$

Substituting  $y = 1$  into (12.2), we obtain an equality of power series in  $x$  of the form

$$(1 + \text{higher order terms}) \cdot \phi'(x) = \phi'(0) \cdot (\partial_y F_2)(\phi(x), 0).$$

Since  $\phi'(0) = \lambda_0$ , the right hand side vanishes. As  $(1 + \text{higher order terms})$  is invertible under multiplication, we deduce that  $\phi'(x)$  also vanishes. Since

$$\phi'(x) = \left(\sum a_i x^i\right)' = \sum i a_i x^{i-1},$$

we deduce that the only powers appearing in  $\phi(x)$  are  $p$ -th powers, so that  $\phi(x) = \psi(x^p)$ .

If  $\psi(x) = \lambda_1 x + \text{higher order terms}$  with  $\lambda_1 \neq 0$ , we are done. If not, the identity

$$F_2(\psi(x^p), \psi(y^p)) = \psi(F_1(x, y)^p)$$

shows that  $\psi$  defines a homomorphism  $\psi: \sigma^* F_1 \rightarrow F_2$ , where  $\sigma^* F_1$  is pullback of a formal group law along the Frobenius  $\sigma: k \rightarrow k$ , explicitly defined by

$$\sigma^*\left(\sum a_{i,j} x^i y^j\right) = \sum a_{i,j}^p x^i y^j.$$

We can thus apply the previous reasoning to  $\psi$ . Inductively, we obtain the needed statement.  $\square$

**Remark 12.11.** One can give a much more geometric proof of Lemma 12.10 using the theory of formal groups and invariant differentials, see [Pst21, Proposition 13.7].

**Remark 12.12.** If  $F$  is a formal group law with coefficients in  $\mathbf{F}_p$ , then  $\sigma^* F = F$ , where  $\sigma: k \rightarrow k$  is the Frobenius. In this case, the proof of Lemma 12.10 shows that if  $\phi$  is an endomorphism of  $F$  which can be written as  $\phi(x) = \psi(x^{p^n})$ , then  $\psi$  is also an endomorphism. Note that the relationship between the two can then be written as an equality

$$\phi = \psi \cdot S^n$$

in  $\text{End}(F/k)$ .

**Proposition 12.13.** Any endomorphism  $\phi \in \text{End}(\Gamma_n/\mathbf{F}_q)$  can be written uniquely as a convergent sum

$$\phi = a_0 + a_1 S + a_2 S^2 + \dots$$

with  $a_i$  Teichmüller representatives.

*Proof.* Write  $\phi(x) = \lambda x + \text{higher order terms}$ . Using Hensel's lemma, we can uniquely lift  $\lambda$  to an element  $\tilde{\lambda} \in W(\mathbf{F}_q)$  satisfying  $\tilde{\lambda}^q = \tilde{\lambda}$ . Since the leading term of  $[\tilde{\lambda}]$  is  $\lambda$  by construction, the leading term of  $\psi - \tilde{\lambda}$ , which in terms of power series is given by

$$\Gamma_n(\psi(x), [-\tilde{\lambda}](x)) = \lambda x + \text{higher order terms} + (-\lambda)x + \text{higher order terms},$$

vanishes. It follows from [Lemma 12.10](#) and [Remark 12.12](#) that in the endomorphism ring we have

$$\phi = \tilde{\lambda} + \psi S$$

for some endomorphism  $\psi$ . Applying the construction inductively to  $\psi$  we obtain the needed expression as an infinite sum.  $\square$

*Proof of Theorem 12.5:* By [Lemma 12.9](#) we have a ring homomorphism

$$(12.3) \quad W(\mathbf{F}_q)\langle S \rangle / (S^n = p, Sw = w^\sigma S) \rightarrow \text{End}(\Gamma_n / \mathbf{F}_q)$$

which we will show is an isomorphism. If  $\phi$  is an endomorphism, then by [Proposition 12.13](#) we can write it uniquely as

$$\phi = \sum a_i S^i,$$

where  $a_i \in W(\mathbf{F}_q)$  and  $a_i^q = a_i$ . We can divide this sum according to the value of  $i$  modulo  $n$ , which yields

$$\phi = \left( \sum_{i \equiv 0} a_i S^i \right) + \dots + \left( \sum_{i \equiv n-1} a_i S^i \right) = \sum_{0 \leq k \leq n-1} \left( \sum_{i \equiv k} a_i p^{\frac{i-k}{n}} S^k \right),$$

where we use that  $S^n = p$ . This means that

$$\phi = \sum_{0 \leq k \leq n-1} w_k S^k$$

for  $w_k \in W(\mathbf{F}_q)$  defined by

$$w_k = \sum_{i \equiv k} a_i p^{\frac{i-k}{n}}.$$

Any Witt vector can be uniquely written in this form for some  $a_i$  satisfying  $a_i^q = a_i$ , we deduce that the endomorphisms ring is free as a left module over  $W(\mathbf{F}_q)$  on the basis of  $\{1, S, \dots, S^{n-1}\}$ . As the same is true for the source ring of (12.3), the map is necessarily an isomorphism.  $\square$

**Remark 12.14.** Note that if  $a \in W(\mathbf{F}_q)$  is a Teichmüller representative, then we verified in [Lemma 12.8](#) that the element of  $\text{End}(\Gamma_n / \mathbf{F}_q)$  corresponding to it under [Theorem 12.5](#) is given by

$$[a](x) = bx,$$

where  $b := \bar{a}$  is the reduction mod  $p$ . Concretely, [Proposition 12.13](#) thus implies that any endomorphism  $\phi(x)$  of the Honda formal group law can be uniquely written as

$$\phi(x) = b_0 x +_{\Gamma_n} b_1 x^p +_{\Gamma_n} b_2 x^{p^2} + \dots$$

for a sequence  $b_i \in \mathbf{F}_q$ . Beware, however, that

$$bx +_{\Gamma_n} b'x \neq (b + b')x,$$

so that such expressions cannot be added naively! In terms of [Theorem 12.5](#), this corresponds to the fact that a sum of Teichmüller representatives is not in general a representative itself, so that the power series expressions of [Lemma 12.7](#) also cannot be naively added.

**Remark 12.15.** Note that under the identification of [Theorem 12.5](#), the Witt vectors  $W(\mathbf{F}_q)$  are *not* central in the endomorphism ring, since they do not commute with the Frobenius  $S$ . Thus, the endomorphism ring is not an algebra over the Witt vectors. It is, however, an algebra over the  $p$ -adic numbers

$$\mathbb{Z}_p \simeq W(\mathbf{F}_p) \subseteq W(\mathbf{F}_q).$$

As it is free of rank  $n$  over  $W(\mathbf{F}_q)$  (which itself are of rank  $n$  over  $\mathbb{Z}_p$ , as  $\dim_{\mathbf{F}_p}(\mathbf{F}_q) = n$ ), it is free of rank  $n^2$  over  $\mathbb{Z}_p$ .

It follows that

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \text{End}(\Gamma_n/\mathbf{F}_q),$$

which we can interpret as the ring of endomorphisms up to isogeny, is a  $\mathbb{Q}_p$ -algebra of dimension  $n^2$ . It is not difficult to see using our explicit description that it is a *central division algebra*; that is, it is a division algebra whose center is exactly  $\mathbb{Q}_p$ .

Local class field theory shows that over  $\mathbb{Q}_p$ , such algebras are classified by a so-called *Hasse invariant*, which is an element of  $\mathbb{Q}/\mathbb{Z}$ , see [[Ser13](#), Chapter XIII]. In the case of the endomorphism ring of the Honda formal group law, this Hasse invariant is equal to  $\frac{1}{n}$ .

We now move on to the group of automorphisms.

**Definition 12.16.** The (non-extended)<sup>8</sup> *Morava stabilizer group* at prime  $p$  and height  $n$  is the given by

$$\mathbb{G}_n := \text{Aut}(\Gamma_n/\mathbf{F}_q),$$

the group of automorphisms of the Honda formal group law.

Concretely,  $\mathbb{G}_n$  is the group of units of the endomorphism algebra

$$W(\mathbf{F}_q)\langle S \rangle / (S^n = p, Sw = w^\sigma S) \simeq \text{End}(\Gamma_n/\mathbf{F}_q)$$

and it follows from [Proposition 12.13](#) that it any of its elements can be uniquely written as a power series

$$a_0 + a_1S + a_2S^2 + \dots$$

where  $a_i$  are Teichmüller representatives and  $a_0 \neq 0$ .

Using our description of the endomorphism ring and our previous work on the general linear group, it is not difficult to see that  $\mathbb{G}_n$  is a virtually a pro- $p$  group of finite rank. To see this, note that  $\text{End}(\Gamma_n/\mathbf{F}_q)$  is free of rank  $n^2$  as a module over the  $p$ -adics, as we observed in [Remark 12.15](#). As the automorphism group acts on the endomorphism ring by multiplication on the left, a choice of a basis determines an injective group homomorphism

$$\mathbb{G}_n \rightarrow \text{GL}_{n^2}(\mathbb{Z}_p)$$

which identifies the Morava stabilizer group with a closed subgroup of the general linear group. As the latter is virtually pro- $p$  and of finite rank by [Theorem 8.8](#), we deduce the following:

**Proposition 12.17.** *The Morava stabilizer group  $\mathbb{G}_n$  is virtually a uniform pro- $p$ -group.*

However, the embedding into  $\text{GL}_{n^2}(\mathbb{Z}_p)$  is somewhat inefficient, as the target is much larger than the source. Due to the importance of  $\mathbb{G}_n$  in stable homotopy theory, we prove [Proposition 12.17](#) directly, by identifying an explicit uniform subgroup in [Proposition 12.25](#) below.

**Remark 12.18.** Our motivation for an identification of an explicit uniform subgroup is that the needed calculations give some basic insight into the structure of the Morava stabilizer group. For example, we will see that  $\dim(\mathbb{G}_n) = n^2$ , where dimension is that of [Definition 7.7](#).

---

<sup>8</sup>The *extended* Morava stabilizer group is the semi-direct product  $\mathbb{G}_n \rtimes \text{Gal}(\mathbf{F}_q/\mathbf{F}_p)$ . We will not consider it in this course, but it is this slightly larger group which appears most naturally in applications. Beware that many sources would use our notation  $\mathbb{G}_n$  to denote the extended group.

The endomorphism ring has a canonical topology induced by the identification

$$\text{End}(\Gamma_n/\mathbf{F}_q) \simeq \varprojlim \text{End}(\Gamma_n/\mathbf{F}_q)/S^k \text{End}(\Gamma_n/\mathbf{F}_q).$$

(note that  $S^k \text{End}(\Gamma_n/\mathbf{F}_q)$  is actually a two-sided ideal, so this is a limit of rings). This topology coincides with the topology inherited from the  $x$ -adic topology on  $\mathbf{F}_q[[x]]$ , as well as with the  $p$ -adic topology, since  $S^n = p$ . This suggests a canonical filtration on the Morava stabilizer group.

**Definition 12.19.** The canonical filtration on  $\mathbb{G}_n$  is given by the open subgroups

$$F_k \mathbb{G}_n := \mathbb{G}_n \cap \ker \left( \text{End}(\Gamma_n/\mathbf{F}_q) \rightarrow \text{End}(\Gamma_n/\mathbf{F}_q)/S^k \text{End}(\Gamma_n/\mathbf{F}_q) \right),$$

so that  $F_0 \mathbb{G}_n = \mathbb{G}_n$  and

$$F_k \mathbb{G}_n := \{1 + a_k S^k + a_{k+1} S^{k+1} + \dots\}.$$

Note that the canonical filtration is a filtration by normal subgroups. Using the description in terms of power series in  $S$  and a short calculation, we see that:

**Lemma 12.20.** *We have that*

(1) *the map*

$$(a_0 + a_1 S + \dots) \mapsto \overline{a_0} \in \mathbf{F}_q^\times$$

*induces an isomorphism*

$$\mathbb{G}_n/F_1 \mathbb{G}_n \simeq \mathbf{F}_q^\times$$

(2) *for each  $k \geq 1$ , the map*

$$(1 + a_k S^k + \dots) \mapsto \overline{a_k} \in \mathbf{F}_q$$

*induces an isomorphism*

$$F_k \mathbb{G}_n/F_{k+1} \mathbb{G}_n \simeq \mathbf{F}_q.$$

**Corollary 12.21.** *The groups  $F_k \mathbb{G}_n$  for  $k \geq 1$  are pro- $p$ .*

To prove that  $\mathbb{G}_n$  is virtually uniform, we have to study the structure of the  $p$ -th power map, which we do now.

**Proposition 12.22.** *Let  $k > n$ . Then the map  $x \rightarrow x^p$  restricts to a function*

$$F_k \mathbb{G}_n \rightarrow F_{k+n} \mathbb{G}_n$$

*and induces a bijection*

$$F_k \mathbb{G}_n/F_{k+1} \mathbb{G}_n \cong F_{k+n} \mathbb{G}_n/F_{k+n+1} \mathbb{G}_n$$

*Proof.* Let  $x = 1 + a_k S^k + a_{k+1} S^{k+1} + \dots \in F_k \mathbb{G}_n$ . Collecting the terms, we can write

$$x = 1 + \omega S^k,$$

where  $\omega = a_k + a_{k+1} S + \dots$ . Using the binomial formula, we obtain

$$x^p = 1 + p\omega S^k + \sum_{2 \leq i \leq p} \binom{p}{i} (\omega S^k)^i = x^p = 1 + \omega S^{k+n} + \sum_{2 \leq i \leq p} \binom{p}{i} (\omega S^k)^i.$$

All of the terms on the left are divisible by  $S^{2k}$ , and since  $k > n$  and thus  $k + n < 2k$ , we see that

$$x^p = 1 + a_k S^{k+n} + \text{terms with higher } S \text{ powers.}$$

It follows that under the identification of both quotients with  $\mathbf{F}_q$  of [Lemma 12.20](#),  $x \mapsto x^p$  corresponds to the identity, hence is a bijection as needed.  $\square$

**Remark 12.23.** Using the same argument as in the proof of [Proposition 12.22](#), one can analyze the way the  $p$ -th powers in  $\mathbb{G}_n$  interact with the canonical filtration for general  $k$ , without the simplifying assumption that  $k > n$ . The formulas get only slightly more involved, see [[Hen98](#), §3] for details.

**Corollary 12.24.** *If  $k > n$ , then*

$$\overline{(F_k \mathbb{G}_n)^p} = F_{k+n} \mathbb{G}_n,$$

where the left hand side is the closure of the subgroup generated by the  $p$ -th powers. In particular,  $F_k \mathbb{G}_n$  (and hence  $\mathbb{G}_n$  itself) is finitely generated.

*Proof.* Since both sides of the equality are closed subgroups, and since the canonical filtration forms a basis of neighbourhoods of the identity, it is enough to verify that

$$(F_k \mathbb{G}_n)^p F_{k+n+m} \mathbb{G}_n = F_{k+n} \mathbb{G}_n$$

for all  $m \geq 0$ . We prove this by induction. If  $m = 0$ , there is nothing to prove, so assume that  $m > 0$ . Applying [Proposition 12.22](#), we have

$$(F_{k+m} \mathbb{G}_n)^p F_{k+n+m} \mathbb{G}_n = F_{k+n+m-1} \mathbb{G}_n.$$

and thus

$$(F_k \mathbb{G}_n)^p F_{k+n+m} \mathbb{G}_n = (F_k \mathbb{G}_n)^p (F_{k+m} \mathbb{G}_n)^p F_{k+n+m} \mathbb{G}_n = (F_k \mathbb{G}_n)^p F_{k+n+m-1} \mathbb{G}_n = F_{k+n} \mathbb{G}_n,$$

where the last equality is the inductive assumption. This ends the argument.

To see that  $F_k \mathbb{G}_n$  is finitely generated, recall that by [Proposition 3.4](#) a pro- $p$  group is finitely generated if and only if the quotient by the Frattini subgroup is finite. Since

$$F_{k+n} \mathbb{G}_n = \overline{(F_k \mathbb{G}_n)^p} \leq \Phi(F_k \mathbb{G}_n),$$

the result follows since  $F_{k+n} \mathbb{G}_n \triangleleft F_k \mathbb{G}_n$  is of finite index. We deduce that the Morava stabilizer group is itself finitely generated, as  $F_k \mathbb{G}_n \triangleleft \mathbb{G}_n$  is also of finite index.  $\square$

**Proposition 12.25.** *Suppose that either*

- (1)  $k > n$  and  $p > 2$ ,
- (2)  $k > 2n$  and  $p = 2$ ,

Then  $F_k \mathbb{G}_n$  is a uniformly powerful  $p$ -group of dimension  $n^2$ .

*Proof.* To check that  $F_k \mathbb{G}_n$  is powerful, we have to verify that

$$F_k \mathbb{G}_n / \overline{(F_k \mathbb{G}_n)^p} \simeq F_k \mathbb{G}_n / F_{k+n} \mathbb{G}_n$$

(or  $F_k \mathbb{G}_n / F_{k+2n} \mathbb{G}_n$  when  $p = 2$ ) is abelian, where the identification is [Corollary 12.24](#).

Let  $x, y \in F_k \mathbb{G}_n$ , which we can write as  $x = 1 + wS^k$  and  $y = 1 + vS^k$ , where  $w, v$  are endomorphisms. We have to check that the images of  $x, y$  commute with each other in the quotient ring

$$\text{End}(\Gamma_n / \mathbf{F}_q) /_{S^{k+n}} \text{End}(\Gamma_n / \mathbf{F}_q),$$

that is; that the bracket  $[x, y] = xy - yx$  vanishes. Since the bracket is linear in each variable and 1 is central, we have

$$[x, y] = [vS^k, wS^k] = vS^k wS^k - wS^k vS^k.$$

Since the left ideal and right ideal generated by  $S^k$  coincide, this is a term divisible by  $S^{2k}$ , and hence  $S^{k+n}$  (or  $S^{k+2n}$  if  $p = 2$ ). We deduce that  $F_k \mathbb{G}_n$  is powerful, as needed.

As  $F_k \mathbb{G}_n$  is finitely generated by [Proposition 12.25](#), to check that it is uniform we have to verify that the subquotients arising in the lower  $p$ -series have the same size. However, we have

$$F_k \mathbb{G}_n / F_{k+n} \mathbb{G}_n \simeq |\mathbf{F}_q|^n = p^{n^2}$$

as a consequence of [Proposition 12.25](#), ending the argument.  $\square$

13. NORMED ALGEBRAS AND POWER SERIES

In this lecture, we begin our study of the analytic properties of  $p$ -adic groups.

**Definition 13.1.** A (non-archimedean) *norm* on a ring  $A$  is function  $\|-\| : A \rightarrow \mathbb{R}_{\geq 0}$  such that

- (1)  $\|a\| = 0$  if and only if  $a = 0$ .
- (2)  $\|ab\| \leq \|a\|\|b\|$ .
- (3)  $\|a + b\| \leq \max(\|a\|, \|b\|)$ .

A *normed algebra* is a ring equipped with a choice of a norm.

**Warning 13.2.** Beware that there is a more general notion of an archimedean norm, in which the last inequality is replaced by the weaker one  $\|a + b\| \leq \|a\| + \|b\|$ . A typical example would be the classical absolute value of a rational number. We will not consider archimedean norms in this course.

A norm on  $A$  induces a metric by the formula

$$d(a, b) := \|a - b\|.$$

In particular, a normed ring carries a canonical topology with respect to which the norm is continuous.

**Example 13.3.** Any ring  $A$  admits the trivial norm, in which

$$\|a\|_{\text{triv}} := 1$$

for all  $a \neq 0$ . The induced topology is discrete.

**Example 13.4.** If  $A = \mathbb{Q}$  and  $p$  is a prime. If  $q \in \mathbb{Q}$ , then its  *$p$ -adic valuation* is the unique

$$v(q) \in \mathbb{Z}$$

such that  $q = p^{v(q)}a/b$  with  $a, b$  coprime to  $p$ . The  *$p$ -adic norm* is defined by

$$\|q\|_p := p^{-v(q)}$$

By restriction, this determines a norm on the integers  $\mathbb{Z}$ .

**Remark 13.5.** Two norms are said to be equivalent if they induce the same topology. By a classical result of Ostrowski, all (non-archimedean) norms on  $\mathbb{Q}$  are equivalent to the  $p$ -adic norm for a uniquely determined prime  $p$  or the trivial norm.

**Construction 13.6.** A filtered ring is a ring  $R$  equipped with a decreasing filtration

$$\dots \subseteq R_2 \subseteq R_1 \subseteq R_0 = R$$

by submodules with the property that

$$R_i R_j \subseteq R_{i+j}.$$

In particular, this implies that each  $R_i \leq R$  is a two-sided ideal. Suppose that we have a filtration which is *separated*; that is, such that

$$\bigcap_{i \geq 0} R_i = 0.$$

In this case, for each positive real  $c$  we can define a norm on  $R$  by

$$\begin{aligned} \|0\| &:= 0, \\ \|x\| &:= c^{-n} \text{ if } x \in R_n \setminus R_{n+1}. \end{aligned}$$

Note that all of these norms are equivalent in the sense that they induce the same topology, and that  $R_i$  form a basis of open neighbourhoods of zero.

**Example 13.7.** In the context of [Construction 13.6](#), if we take  $R = \mathbb{Z}$ ,  $R_i = p^i \mathbb{Z}$  and  $c = p$ , then we recover exactly the  $p$ -adic norm of [Example 13.4](#).

**Definition 13.8.** We say that a normed algebra is *complete* if it is complete with respect to the metric induced by the norm.

**Example 13.9.** Any ring  $A$  is complete with respect to the trivial norm of [Example 13.3](#).

**Construction 13.10.** The inclusion of the full subcategory of complete normed algebras admits a left adjoint. In other words, any normed algebra  $(A, \|\cdot\|)$  admits an initial map

$$(A, \|\cdot\|) \rightarrow (\hat{A}, \|\cdot\|)$$

into a complete one. We call  $\hat{A}$  the *completion* of  $A$ . Concretely,  $\hat{A}$  can be constructed as equivalence classes of Cauchy sequences, and  $A$  can be identified with the subring of sequences equivalent to a constant one.

**Example 13.11.** Let  $R$  be a filtered ring equipped with the norm of [Construction 13.6](#). In this case the completion in the sense of [Construction 13.10](#) can be identified with the completion with respect to the filtration; that is

$$\hat{R} \simeq \varprojlim R/R_n.$$

**Example 13.12.** The completion of the rationals with their  $p$ -adic norm is given by the  $p$ -adic numbers  $(\mathbb{Q}_p, \|\cdot\|_p)$  with the unique extension of the norm on the rationals. Concretely, any non-zero  $p$ -adic integers can be written as  $x = p^n u$  for unique  $n \in \mathbb{Z}$  and  $u \in \mathbb{Z}_p^\times$ , and

$$\|x\| = p^{-n}.$$

We now discuss convergence of series in a complete normed algebra. Since we only work with non-archimedean norms, this is much easier than the corresponding story in real analysis.

**Definition 13.13.** Let  $A$  be a complete normed algebra,  $T$  a countable index set and let  $(a_t)_{t \in T}$  be a family of elements in  $A$ . We say that a sum  $\sum_{t \in T} a_t$  *converges* to  $s \in A$  and write

$$\sum_{t \in T} a_t = s$$

if for all reals  $\epsilon > 0$  there exists a finite subset  $T' \subseteq T$  such that for all finite subsets  $T' \subseteq T'' \subseteq T$  we have

$$\left\| \sum_{t \in T''} a_t - s \right\| < \epsilon.$$

Note that if we replace  $A$  by the real numbers, then the notion of convergence given in [Definition 13.13](#) corresponds to *absolute convergence*. In the case of non-archimedean norms, this is equivalent to conditional convergence, as the following shows.

**Lemma 13.14.** *Let  $T$  be a countable set,  $(a_t)_{t \in T}$  a collection of elements of  $A$  and suppose that we have an ordering  $t_1, t_2, \dots$  of elements of  $T$ . Then*

$$\sum_{t \in T} a_t = s \text{ if and only if } \lim_{n \rightarrow \infty} \sum_{1 \leq k \leq n} a_{t_k} = s.$$

*Proof.* We first show forward implication. Let  $\epsilon > 0$ , by assumption there exists a finite subset  $T'$  such that for all  $T'' \supseteq T'$  we have  $\|\sum_{t \in T''} a_t - s\| < \epsilon$ . Let  $N \geq 0$  be such that  $T' \subseteq \{t_1, \dots, t_N\}$ . Then for all  $n \geq N$  we have

$$\left\| \sum_{1 \leq k \leq n} a_{t_k} - s \right\| \leq \epsilon.$$

It follows that the left hand side converges to zero as  $n \rightarrow \infty$ , so that  $(\sum_{1 \leq k \leq n} a_{t_k} - s) \rightarrow 0$  as needed.

We move to the backward implication. Let  $\epsilon > 0$ , and choose  $N \geq 0$  such that

$$\left\| \sum_{1 \leq k \leq n} a_{t_k} - s \right\| \leq \epsilon.$$

for all  $n \geq N$ . This implies that if  $m > n$ , then

$$\|a_{t_m}\| = \left\| \left( \sum_{1 \leq k \leq m} a_{t_k} - s \right) - \left( \sum_{1 \leq k \leq m-1} a_{t_k} - s \right) \right\| \leq \max(\epsilon, \epsilon) \leq \epsilon.$$

Take  $T' = \{1, \dots, N\}$  and suppose that  $T'' \supseteq T'$ . Then

$$\sum_{t \in T''} a_t - s = \left( \sum_{1 \leq k \leq N} a_{t_k} - s \right) + \left( \sum_{t \in T'' \setminus T'} a_t \right) \leq \max(\epsilon, \epsilon) \leq \epsilon,$$

where we use that the norm of the second sum is bounded by the norms of the summands, ending the argument.  $\square$

**Corollary 13.15.** *If  $A$  is a complete algebra, then  $\sum a_t$  converges if and only if there exists an (equivalently, for any) ordering of  $T$  such that  $\|a_{t_n}\| \rightarrow 0$ .*

*Proof.* If  $\|a_{t_n}\| \rightarrow 0$ , then since

$$\left\| \sum_{n \leq k \leq m} a_{t_k} \right\| \leq \max(\{ \|a_{t_k}\| \mid n \leq k \leq m \}),$$

the sequence  $\sum_{1 \leq k \leq n} a_{t_k}$  is Cauchy. Since  $A$  is assumed to be complete, it converges.  $\square$

**Proposition 13.16.** *Let  $T$  be a countable set and  $(a_t)_{t \in T}$  a collection of elements of  $A$ . Then*

(1) *if  $\sum_{t \in T} a_t = s$  then*

$$\|s\| \leq \sup_{t \in T} (\|a_t\|),$$

(2) *if  $\sum_{t \in T} a_t = s$  and there exists  $t_0 \in T$  such that  $\|a_{t_0}\| > \|a_t\|$  for any  $t \neq t_0$ , then*

$$\|s\| = \|a_{t_0}\|.$$

*Proof.* We start with the first part. By [Lemma 13.14](#), after choosing an ordering, we have

$$s = \lim_{n \rightarrow \infty} \sum_{1 \leq i \leq n} a_{t_i},$$

so that

$$\|s\| = \lim_{n \rightarrow \infty} \left\| \sum_{1 \leq i \leq n} a_{t_i} \right\| \leq \max_{1 \leq i \leq n} \|a_{t_i}\| \leq \sup_{t \in T} \|a_t\|.$$

For the second part, we have  $\sum_{t \in T} a_t = a_{t_0} + \sum_{t \neq t_0} a_t$ . Since the second term is norm-bounded by  $\|a_{t_0}\|$  by the assumption and the first part, the result follows.  $\square$

We will be interested in normed algebras which admit an action of the  $p$ -adics.

**Definition 13.17.** A *normed  $\mathbb{Q}_p$ -algebra* is a normed algebra  $A$  together with a  $\mathbb{Q}_p$ -algebra structure such that

$$\|\lambda a\| \leq \|\lambda\|_p \|a\|$$

for all  $\lambda \in \mathbb{Q}_p$  and  $a \in A$ .

**Lemma 13.18.** *If  $A$  is a normed  $\mathbb{Q}_p$ -algebra then*

$$\|\lambda a\| = \|\lambda\| \|a\|.$$

*Proof.* It's enough to show that  $\|\lambda a\| \geq \|\lambda\| \|a\|$  when  $\lambda \neq 0$ , as otherwise both sides are equal to zero. We have

$$\|a\| = \|\lambda^{-1} \lambda a\| \leq \|\lambda^{-1}\| \|\lambda a\|$$

and multiplying both sides by  $\|\lambda\|$  gives the desired inequality.  $\square$

Suppose that we have a formal power series  $f(x) \in A[[X]]$  with coefficients in a normed  $\mathbb{Q}_p$ -algebra. If we write  $f(x) = \sum a_i x^i$ , then by substituting  $x \mapsto \lambda \in \mathbb{Q}_p$  we obtain a sequence of elements of  $A$ . In good cases, this converges, and the fundamental identity property tells us that the sums of these sequences determine the coefficients.

**Proposition 13.19** (Identity). *Let  $\sum a_i x^i$  be a formal power series in a normed  $\mathbb{Q}_p$ -algebra. Suppose there is an open neighborhood  $V \subseteq \mathbb{Q}_p$  of zero such that for all  $\lambda \in V$ , we have*

$$\sum a_i \lambda^i = 0$$

Then  $a_n = 0$  for all  $n$ .

*Proof.* If  $a_n = 0$  for all  $n$ , there is nothing to show. Otherwise, choose  $m$  such that  $a_m \neq 0$  and that  $m$  is smallest with this property.

Pick  $\lambda_0 \in V$ ,  $\lambda_0 \neq 0$  and write  $r_0 = \|\lambda_0\|$ . Since  $\sum a_i \lambda_0^i$  is convergent, we deduce that

$$\lim \|a_i \lambda_0^i\| = \lim \|a_i\| r_0^i = 0.$$

In particular, these terms are bounded, so we can choose a real constant  $C$  such that  $\|a_i\| r_0^i < C$  for all  $i$ . Now choose  $\lambda_1 \in D$  such that  $r_1 = \|\lambda_1\|$  satisfies

$$r_1 < \min(r_0, \frac{r_0^{m+1} \|a_m\|}{C}).$$

Then for all  $n > m$  we have

$$\|a_n\| r_1^n = \|a_n\| r_1^{n-1} \cdot r_1 < \|a_n\| r_1^n = \|a_n\| r_1^{n-1} \cdot \frac{r_0^m \|a_m\|}{C}$$

and continuing

$$\|a_n\| r_1^{n-1} \cdot \frac{r_0^m \|a_m\|}{C} = (\|a_n\| r_0^n) \cdot (\frac{r_1}{r_0})^{n-1} \cdot \frac{r_0^m \|a_m\|}{C} \leq (\frac{r_1}{r_0})^{n-1} (r_0^m \|a_m\|)$$

and

$$(\|a_n\| r_0^n) \frac{r_1^{n-m-1}}{r_0^{n-m}} \frac{r_1^m \|a_m\|}{C} \leq \frac{r_1^{n-m-1}}{r_0^{n-m}} \frac{r_1^m \|a_m\|}{C}.$$

It follows that

$$\|a_n \lambda_1^n\| < \|a_m \lambda_1^m\|$$

for all  $n \neq m$ . As the left hand side converges to zero as  $n \rightarrow \infty$ , we deduce that

$$\sup(\{\|a_n \lambda_1^n\| \mid n \neq m\}) < \|a_m \lambda_1^m\|,$$

and from the second part we deduce that [Proposition 13.16](#)

$$\|\sum_i a_n \lambda_1^n\| = \|a_m \lambda_1^m\| \neq 0,$$

which is what we wanted to show. □

Similarly, a power series with coefficients in  $\mathbb{Q}_p$ , under suitable convergence hypothesis, can be used to define a self-map of a normed algebra. We will be interested in defining in this way functions in more than one variable, and here we have to be a little bit careful - since multiplication in a normed algebra is in general not commutative, formal power series in commuting variables are not suitable for our purposes.

**Definition 13.20.** Let  $X_1, \dots, X_m$  denote a set of variables. The monoid of *words* in  $X$  is given by the free monoid

$$W := W(X_1, \dots, X_m)$$

on  $\{X_1, \dots, X_m\}$ . The *degree* function on words is defined as the unique monoid homomorphism

$$\text{deg}: W \rightarrow (\mathbb{Z}_{\geq 0}, +)$$

with the property that  $\text{deg}(X_i) = 1$  for all  $1 \leq i \leq m$ .

Concretely, any word can be written as a (possibly empty) product of the variables and the degree is given by

$$\deg(X_{i_1}X_{i_2} \dots X_{i_k}) = k.$$

In other words, the degree is the number of the factors in the product expression.

**Definition 13.21.** The ring of *non-commutative polynomials* in variables  $X_1, \dots, X_m$  is the free ring

$$\mathbb{Q}_p\langle X_1, \dots, X_m \rangle := \mathbb{Q}_p[W]$$

on the monoid of words. The ring of *non-commutative power series* in variables  $X_1, \dots, X_m$  is the completion

$$\mathbb{Q}_p\langle\langle X_1, \dots, X_m \rangle\rangle := \varprojlim \mathbb{Q}_p[W]/(I)^n$$

at the double-sided ideal  $I$  generated by words of positive degree.

Concretely, non-commutative power series can be uniquely represented as (possibly infinite) expressions

$$\sum_{w \in W} a_w w$$

indexed by words, where  $a_w \in \mathbb{Q}_p$ . Multiplication and addition is performed using the usual formulas, which at any step always involve only finitely many terms and so are well-defined. The ring of non-commutative polynomials can be identified with the subring of those expressions such that  $a_w = 0$  for all but finitely many words.

**Definition 13.22.** Let  $A$  be a complete normed  $\mathbb{Q}_p$  algebra and let  $F(X) \in \mathbb{Q}_p\langle\langle X_1, \dots, X_m \rangle\rangle$  be a formal power series in non-commuting variables. Given  $x = (x_1, \dots, x_m) \in A^{\times m}$ , we say that  $F$  can be evaluated at  $x$  if

$$F(x) = \sum a_w w(x)$$

exists, where  $w(-): W \rightarrow (A, \cdot)$  is the unique homomorphism of monoids satisfying  $X_i \mapsto x_i$ .

In the context of [Definition 13.22](#), let  $\text{Ev}_x \subseteq \mathbb{Q}_p\langle\langle X \rangle\rangle$  be the subset of those power series which can be evaluated at  $x$ . Through some manipulation using double sums which we leave to the interested reader, one can show that

- (1)  $\text{Ev}_x$  is a  $\mathbb{Q}_p$ -subalgebra which contains the ring of non-commutative polynomials,
- (2) on this subalgebra, the association  $F(X) \mapsto F(x)$  defines a  $\mathbb{Q}_p$ -algebra homomorphism

$$\text{Ev}_x \rightarrow A.$$

We now define a particularly nice class of functions which arise from this construction.

**Definition 13.23.** Let  $r > 0$  be a real constant and consider the open subset

$$V_r = \{(x_1, \dots, x_m) \in A^{\times m} \mid \|x_i\| \leq r \text{ for all } 1 \leq i \leq m\}$$

We say that a function  $f: V_r \rightarrow A$  is *strictly analytic* if there exists a non-commuting power series

$$F(X) = \sum_{w \in W} a_w w$$

in  $m$  variables such that

- (1) we have

$$\lim \|a_w\| r^{\deg(w)} = 0$$

as  $\deg(w) \rightarrow \infty$ ,

- (2) for each  $x \in D$ , we have

$$F(x) = f(x).$$

**Remark 13.24.** The above definition only applies to functions defined in a neighbourhood of zero. We will slightly abuse the terminology, and more generally say that if  $x_0 \in A$ , then  $f: V_r + x_0 \rightarrow A$  is strictly analytic if its translate  $f(- + x_0): V_r \rightarrow A$  is strictly analytic in the sense of [Definition 13.23](#).

Note that the first condition of [Definition 13.23](#) does guarantee that  $F(x) = \sum a_w w(x)$  exists for all  $x \in V_r$ , since

$$(13.1) \quad \|a_w w(x)\| \leq \|a_w\| r^{\deg(w)}.$$

However, it is strictly stronger than just asking for all of  $F(x)$  to exist. Intuitively, it asks that  $\sum a_w w(x)$  converges “for a good reason”; that is, with a uniform bound depending only on  $\|x\|$ .

**Remark 13.25.** If a function  $f: V_r \rightarrow A$  is strictly analytic, then by a repeated application of [Proposition 13.19](#) one can show that a power series  $F$  representing it is unique.

**Proposition 13.26.** *Let  $f: V_r \rightarrow A$  be strictly analytic. Then  $f$  is continuous.*

*Proof.* Let  $\epsilon > 0$  be a real constant. Choose  $N$  such that  $\|a_w\| r^{\deg(w)} \leq \epsilon$  if  $\deg(w) \geq N$ . For any  $x \in V_r$ , we can write

$$F(x) = F_1(x) + F_2(x)$$

where

$$F_1(x) = \sum_{\deg(w) < N} a_w w(x)$$

and similarly

$$F_2(x) = \sum_{\deg(w) \geq N} w(x).$$

Using [\(13.1\)](#) and the first part of [Proposition 13.16](#) we see that  $F_2(x)$  has a norm bounded by  $\epsilon$ .

The function  $x \mapsto F_1(x)$  can be obtained in finitely many steps using the addition, multiplication, and scalar multiplication of  $A$ , all of which are continuous, so that it is continuous, too. It follows that there exists a  $\delta > 0$  such that if  $\|x' - x\| < \delta$ , then

$$\|F_1(x') - F_1(x)\| \leq \epsilon.$$

We then have

$$\|F(x') - F(x)\| = \|(F_1(x') - F_1(x)) + (F_2(x') - F_2(x))\| \leq \max(\epsilon, \epsilon) = \epsilon$$

so that  $F$  is continuous. □

We now define two classical functions, the exponential and logarithm, which are useful in relating pro- $p$ -groups of finite rank to Lie algebras.

**Definition 13.27.** The *exponential* is the power-series in one variable

$$\mathcal{E}(X) := \sum_{n \geq 0} \frac{1}{n!} X^n.$$

The *logarithm* is given by

$$\mathcal{L}(X) := \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} X^n.$$

**Warning 13.28.** Be careful to observe that the way we define the logarithm *power series* is the Taylor expansion of the classical logarithm *function* around  $1 \in \mathbb{R}$ , not around 0. The latter does not make sense.

To verify that the power series of [Definition 13.27](#) define functions, we need an upper bound on the norms of their coefficients.

**Lemma 13.29.** *Let  $n \geq 1$ . Then the  $p$ -adic valuation of the factorial satisfies*

$$v(n!) \leq \frac{n-1}{p-1}$$

so that

$$\|n!\|_p \leq p^{\frac{1-n}{p-1}}.$$

*Proof.* We have to count how many times  $n!$  is divisible by  $p$ . Choose  $k \geq 0$  such that  $p^k \leq n \leq p^{k+1}$ . Since there are  $\lfloor \frac{n}{p} \rfloor$  numbers  $k \leq n$  divisible by  $p$ ,  $\lfloor \frac{n}{p^2} \rfloor$  number divisible by  $p^2$  and so on, we see that  $n!$  is divisible by  $p$  at most

$$\frac{n}{p} + \frac{n}{p^2} + \dots + \frac{n}{p^k} = \frac{n(1-p^{-k})}{(1-p)} \leq \frac{n-1}{p-1}$$

times □

As a consequence, we deduce the following:

**Theorem 13.30.** *Let  $A$  be a complete normed  $\mathbb{Q}_p$ -algebra and write*

$$A_0 = \begin{cases} \{x \in A \mid \|x\| \leq \frac{1}{p}\} & p > 2 \\ \{x \in A \mid \|x\| \leq \frac{1}{4}\} & p = 2 \end{cases}$$

*Then the exponential and logarithm power series define strictly analytic functions which we denote by*

$$\exp: A_0 \rightarrow 1 + A_0$$

$$x \mapsto \sum_{n \geq 0} \frac{x^n}{n!}$$

and

$$\log: A_0 + 1 \rightarrow A_0$$

$$(x+1) \mapsto \sum_{n \geq 1} \frac{(-1)^{n+1} x^n}{n}$$

*Proof.* We only do the odd prime case; the even prime is analogous. For the exponential we have

$$\mathcal{E}(X) = 1 + \sum_{n \geq 1} \frac{X^n}{n!}$$

and the claim is that

- (1)  $\|\frac{1}{n!}\| p^{-n} \leq p^{-1}$  for all  $n \geq 1$ ,
- (2)  $\|\frac{1}{n!}\| p^{-n} \rightarrow 0$  as  $n \rightarrow \infty$ .

Here, the second property guarantees that  $\mathcal{E}$  defines a strictly analytic function on  $A_0$  and the first one that  $\exp(x) \in 1 + A_0$  if  $x \in A_0$ . By [Lemma 13.29](#), we have

$$\|\frac{1}{n!}\| p^{-n} \leq p^{\frac{n-1}{p-1}} p^{-n} = p^{\frac{n-1-np+n}{p-1}} = p^{\frac{-(p-2)n-2}{p-1}}$$

which satisfies both properties. For the logarithm, the analysis is analogous using power series  $\mathcal{L}$ , where we use that  $\|\frac{1}{n}\| \leq \|\frac{1}{n!}\|$ . □

Note that the power series  $\mathcal{E}$  and  $\mathcal{L}$  satisfy a number of classical properties, namely that

- (1)  $\mathcal{L}(\mathcal{E}(X) - 1) = X$ ,
- (2)  $\mathcal{E}(\mathcal{L}(X)) = X + 1$ ,
- (3)  $\mathcal{E}(nX) = \mathcal{E}(X)^n$
- (4)  $\mathcal{L}((1 + X)^n - 1) = n\mathcal{L}(X)$ .

Under reasonable convergence conditions (which are satisfied in this case), composition of formal power series (which is well-defined on power series with no constant term) corresponds to composition of strictly analytic functions. This yields the following:

**Proposition 13.31.** *Let  $A$  be a complete normed  $\mathbb{Q}_p$ -algebra and let  $A_0$  be as in [Theorem 13.30](#). Then for all  $x \in A_0$ , we have*

- (1)  $\log(\exp(x) - 1) = x$ ,
- (2)  $\exp(\log(1 + x)) = 1 + x$ ,
- (3)  $\exp(nx) = \exp(x)^n$ ,
- (4)  $\log((1 + x)^n) = n \log(1 + x)$ .

**Warning 13.32.** Beware that the series defining the logarithm and exponential might sometimes converge for  $x \notin A_0$ , but in this case, [Proposition 13.31](#) need not hold.

As an explicit example, consider

$$(13.2) \quad \log(-1) = \log(1 - 2) = \sum_{n \geq 1} \frac{(-2)^n (-1)^{n+1}}{n}.$$

In the field of 2-adic numbers, this is a convergent series. In formal power series, we have

$$\mathcal{L}((1 + X)^2 - 1) = \mathcal{L}(2X + X^2) = 2 \cdot \mathcal{L}(X)$$

(this is the multiplicativity of the logarithm), from which we deduce that

$$2 \cdot \log(-1) = 2 \cdot \sum_{n \geq 1} \frac{(-2)^n (-1)^{n+1}}{n} = \sum_{n \geq 1} \frac{(2 \cdot (-2) + (-2)^2)^n (-1)^{n+1}}{n} = 0.$$

It follows that

$$\exp(\log(-1)) = \exp(0) = 1 \neq -1.$$

The issue here is that the exponential converges on  $x = 0$ , but it does not converge on the individual terms of [\(13.2\)](#).

#### 14. THE COMPLETED GROUP ALGEBRA

If  $G$  is a finite group, the category of  $G$ -representations in abelian groups is equivalent to the category of left modules over the group algebra  $\mathbb{Z}[G]$ . In this lecture, we will study a variant of this construction for profinite groups acting continuously on  $\mathbb{Z}_p$ -modules, which requires one to take the topology of both the  $p$ -adics and the group itself into account.

We will show that the completed group algebra has very favourable properties when restricted to reasonable profinite groups. Today, we will show that

- (1) if  $G$  is finitely generated pro- $p$ , then the topology of the completed group algebra is induced by a canonical norm determined by the augmentation ideal, see [Definition 14.6](#),
- (2) if  $G$  is powerful, then the completed group algebra admits a set of topological generators given by monomials,
- (3) if  $G$  is moreover uniform, then the expression in terms of monomials is unique, see [Theorem 14.10](#).

The third property is one of the way in which the completed group algebra of a uniform group behaves like a power series ring, a theme we will explore further in the next lecture.

**Definition 14.1.** Let  $G$  be a profinite group. The ( $p$ -adic) *completed group algebra* is the limit

$$\mathbb{Z}_p[[G]] := \varprojlim_{N \triangleleft_o G} \mathbb{Z}_p[G/N]$$

taken over the poset of normal open subgroups of  $G$ .

Note that each of  $\mathbb{Z}_p[G/N]$  is a finite free  $\mathbb{Z}_p$ -algebra and so is  $p$ -complete; that is,

$$\mathbb{Z}_p[G/N] \simeq \varprojlim \mathbb{Z}/p^n[G/N].$$

This limit expression endows  $\mathbb{Z}_p[G/N]$  with a limit topology. The maps making the diagram in [Definition 14.1](#) are continuous so that  $\mathbb{Z}_p[[G]]$  is also naturally a topological ring.

We will be mainly interested in this construction when  $G$  is finitely generated and pro- $p$ . In this case, we recall from [Proposition 3.20](#) that we have a canonical basis of open neighbourhoods of the identity given by the lower  $p$ -series we denote by

$$G_k = P_k(G).$$

As a consequence,  $\mathbb{Z}_p[[G]]$  can be written as a *sequential* limit. To see this, notice that since  $G_k$  are open, we have canonical projection maps

$$\mathbb{Z}_p[[G]] \rightarrow \mathbb{Z}_p[G/G_k] \rightarrow \mathbb{Z}/p^k[G/G_k]$$

**Lemma 14.2.** *Let  $G$  be a finitely generated pro- $p$  group. Then*

$$\mathbb{Z}_p[[G]] \simeq \varprojlim \mathbb{Z}/p^k[G/G_k]$$

*as topological rings.*

*Proof.* By construction, the map from the left hand side to the right hand side is surjective. To see that it is injective, let  $x \in \mathbb{Z}_p[[G]]$  be non-zero, so that it has a non-zero image along

$$\mathbb{Z}_p[[G]] \rightarrow \mathbb{Z}_p[G/N]$$

for some open normal  $N$ . Since the target is  $p$ -complete,  $x$  also has non-zero image in  $\mathbb{Z}/p^a[G/N]$  for some  $a$ . Since  $G_k$  form a basis of neighbourhoods of the identity, we have  $G_b \leq N$ . Then we have a factorization

$$\mathbb{Z}_p[[G]] \rightarrow \mathbb{Z}/p^c[G/G_c] \rightarrow \mathbb{Z}/p^a[G/N]$$

for  $c = \max(a, b)$ , so that  $x$  has also non-zero image in the middle term.

As the comparison map is a continuous bijection between compact Hausdorff spaces, it is a homeomorphism.  $\square$

We would like to apply the theory of complete normed algebra developed in previous lectures to  $\mathbb{Z}_p[[G]]$ . To do so, we will equip the group algebra  $\mathbb{Z}_p[G]$  with a norm such that  $\mathbb{Z}_p[[G]]$  can be identified with the completion with respect to the norm. This is a non-trivial task, as the norm should encode at the same time the  $p$ -adic topology of  $\mathbb{Z}_p$  and the profinite topology of  $G$ .

To construct the needed norm, we will use an appropriately multiplicative family of ideals and [Construction 13.6](#). As motivation for our arguments, observe that one way to express [Lemma 14.2](#) is that

$$\mathbb{Z}_p[[G]] \simeq \varprojlim \mathbb{Z}_p[G]/I_k,$$

where

$$I_k := (G_k - 1) + p^k \mathbb{Z}_p[G]$$

and

$$(G_k - 1) := \ker(\mathbb{Z}_p[G] \rightarrow \mathbb{Z}_p[G/G_k]).$$

Instead of working with the family of ideals  $I_k$ , it is more convenient to work with powers of a single ideal, which we can do using the following calculation.

**Notation 14.3.** If  $G$  be a finitely generated, pro- $p$ , then we write  $J$  for the ideal

$$J = I_1 = (G - 1) + p \mathbb{Z}_p[G] \subseteq \mathbb{Z}_p[G].$$

It coincides with the kernel of the composite

$$\mathbb{Z}_p[G] \rightarrow \mathbb{Z}_p \rightarrow \mathbf{F}_p$$

and is often called the *augmentation ideal*.

**Proposition 14.4.** *For each  $k \geq 1$ , we have*

- (1)  $J^k \supseteq I_k$ ,
- (2)  $I_k \supseteq J^{k \cdot |G/G_k|}$ .

*In particular, taking either  $J^k$  or  $I_k$  as a basis of open neighbourhoods of  $\mathbb{Z}_p[G]$  defines the same topology.*

*Proof.* We prove the first statement by induction on  $k$ . Since it holds for  $k = 1$  by definition, we assume  $k > 1$ . As  $p \in J$ , we have  $p^k \in J^k$  and it is thus enough to show that  $(G_k - 1) \leq J^k$ . This is the equivalent to showing that the  $G$ -action on  $\mathbb{Z}_p[G]/J^k$  factors through  $G/G_k$ . As these are the generators of  $G_k = \Phi(G_{k-1})$ , we only have to check that elements of the form

- (1)  $x^p$  for  $x \in G_{k-1}$ ,
- (2)  $x^{-1}y^{-1}xy^9$  for  $x \in G_{k-1}, y \in G$ .

We analyse these cases separately. If we write  $u = x - 1$ , then the binomial theorem implies that inside  $\mathbb{Z}_p[G]$  we have

$$x^p - 1 = (u + 1)^p - 1 = u^p + puw$$

for some element  $w$ . If  $x \in G_{k-1}$ , then  $u \in J^{k-1}$  and so  $u^p \in J^{(k-1)p} \leq J^k$  and similarly  $pu \in J \cdot J^{k-1} = J^k$ . Thus,  $x^p - 1 \in J^k$  as needed.

For the case of group commutators, write  $u = x - 1 \in J^{k-1}$  and  $v = y - 1 \in J$ . Then

$$x^{-1}y^{-1}xy - 1 = x^{-1}y^{-1}(xy - yx)x^{-1}y^{-1}(uv - vu)$$

since 1 is central. As  $uv - vu \in J^k$ , the result follows.

We now move to the second part, namely that  $J^{k \cdot |G/G_k|} \subseteq I_k$ . Since  $G/G_k$  is a finite  $p$ -group, there exists a basis of the  $\mathbf{F}_p$ -vector space  $\mathbf{F}_p[G/G_k]$  such that the action factors through the upper unitriangular subgroup

$$U_{|G/G_k|}(\mathbf{F}_p) \subseteq GL_{|G/G_k|}(\mathbf{F}_p)$$

(studied previously in §6, see [Notation 6.13](#)), as it is a  $p$ -Sylow subgroup of the general linear group. It follows that for any  $g \in G$ , the action of

$$g - 1 \in J$$

is an action by a strictly upper triangular matrix of size  $|G/G_k| \times |G/G_k|$ . The product of any  $|G/G_k|$  such matrices is zero and we deduce that  $(G - 1)^{|G/G_k|} \subseteq (G_k - 1) + p\mathbb{Z}_p[G]$  and similarly  $J \subseteq (G_k - 1) + p\mathbb{Z}_p[G]$ . It follows that

$$J^{k|G/G_k|} \subseteq ((G_k - 1) + p\mathbb{Z}_p[G])^k \subseteq (G_k - 1) + p^k\mathbb{Z}_p[G] = I_k.$$

□

**Corollary 14.5.** *We have*

$$\bigcap_{k \geq 0} J^k = \{0\}$$

*as ideals of  $\mathbb{Z}_p[G]$ .*

*Proof.* Any non-zero element of  $\mathbb{Z}_p[G]$  can be expressed as a finite sum  $x = \sum_i \lambda_i g_i$  such that all  $g_i \in G$  are distinct and  $\lambda_i \in \mathbb{Z}_p$  are non-zero. We can find a  $k$  large enough such that all  $g_i$  are distinct in  $G/G_k$ . Choosing a  $k' > k$  such that  $\lambda_i \notin p^{k'}\mathbb{Z}_p$ , we see that the image of  $x$  is non-zero in

$$\mathbb{Z}_p[G]/((G_{k'} - 1) + p^{k'}\mathbb{Z}_p[G]) \simeq \mathbb{Z}/p^{k'}[G/G_{k'}].$$

It follows from [Proposition 14.4](#) that  $x$  is not contained in  $J^{k'|G/G_{k'}|}$ , ending the argument. □

---

<sup>9</sup>This is just the ordinary group commutator, but we don't use the bracket notation so that we don't confuse it with the Lie bracket of  $\mathbb{Z}_p[G]$ , which is different.

As a consequence of [Corollary 14.5](#), the  $J$ -adic filtration on the group algebra is separating, so can be used to define a norm as in [Construction 13.6](#).

**Definition 14.6.** Let  $G$  be a finitely generated pro- $p$  group. The *standard norm* on the group algebra is given by

$$\begin{aligned} \|0\| &:= 0, \\ \|x\| &:= p^{-n} \text{ if } x \in J^n \setminus J^{n+1}, \end{aligned}$$

**Proposition 14.7.** *The standard norm on  $\mathbb{Z}_p[G]$  has the following properties:*

- (1) *the completion with respect to the norm can be identified as a topological ring with the complete group algebra of [Definition 14.1](#),*
- (2) *the canonical map  $G \rightarrow \mathbb{Z}_p[G]$  is a homeomorphism onto its image.*

*Proof.* For the first part, observe that we have an identification

$$\widehat{\mathbb{Z}_p[G]} \simeq \varprojlim \mathbb{Z}_p[G]/J^k \simeq \varprojlim \mathbb{Z}_p[G]/I_k \simeq \mathbb{Z}_p[[G]],$$

where the left hand side is the completion with respect to the norm, the middle isomorphism is [Proposition 14.4](#) and the right isomorphism is [Lemma 14.2](#).

For the second part, as  $G$  is compact and the group algebra is Hausdorff (as the topology comes from a metric), it is enough to verify that the canonical map is continuous. The group of units of the group algebra has a basis of open neighbourhoods of the identity given by  $1 + J^k$ . Since  $(G_k - 1) \subseteq I_k \subseteq J_k$  by [Proposition 14.4](#), we deduce that the canonical map takes  $G_k$  to  $1 + J^k$  and hence is continuous.  $\square$

**Remark 14.8.** Since [Proposition 14.7](#) identifies  $\mathbb{Z}_p[[G]]$  with a completion with respect to a norm, it equips the completed group algebra with its own norm which we also refer to as the *standard norm*. This norm can be described explicitly analogously to that of  $\mathbb{Z}_p[G]$ : it is the norm associated through [Construction 13.6](#) to the filtration by powers of the ideal  $J\mathbb{Z}_p[[G]] = \ker(\mathbb{Z}_p[[G]] \rightarrow \mathbf{F}_p)$ .

We now describe how in the case where  $G$  is powerful, a choice of generators of  $G$  gives a convenient set of generators of the completed group algebra (as a topological  $\mathbb{Z}_p$ -module). This requires a little bit of notation, which we introduce first.

**Notation 14.9.** For the rest of the lecture,  $G$  denotes a powerful, finitely generated pro- $p$ -group. We fix a choice

$$g_1, \dots, g_m$$

of topological generators of  $G$  and write

$$b_i := g_i - 1 \in \mathbb{Z}_p[G].$$

Note that we have  $b_i \in J$ ; equivalently,  $\|b_i\| \leq p^{-1}$  with respect to the standard norm.

If  $(\alpha) = (\alpha_1, \dots, \alpha_m) \in \mathbb{N}^{\times m}$  is a multi-index, its degree is given by  $\deg(\alpha) = \alpha_1 + \dots + \alpha_m$ . Given generators as above, we write

$$g^{(\alpha)} = g_1^{\alpha_1} \cdots g_m^{\alpha_m}$$

and similarly

$$b^{(\alpha)} = b_1^{\alpha_1} \cdots b_m^{\alpha_m}.$$

Beware that since the group algebra is not commutative, these expressions do depend on the order of the  $g_i$ , so that we implicitly assume that our set of generators is ordered.

**Theorem 14.10.** *Let  $G$  be a powerful, finitely generated pro- $p$ -group with a choice of generators  $g_i$ . Then any  $x \in \mathbb{Z}_p[[G]]$  can be written as an infinite sum*

$$x = \sum_{(\alpha) \in \mathbb{N}^{\times m}} \lambda_\alpha b^{(\alpha)}$$

with  $\lambda_\alpha \in \mathbb{Z}_p$  and  $b^{(\alpha)}$  as in [Notation 14.9](#). If  $G$  is uniform and  $g_i$  is a minimal generating set, then such an expression is unique.

Observe that since  $\|b_i\| \leq p^{-1}$ , we have  $\|\lambda_\alpha b^{(\alpha)}\| \leq p^{-\deg(\alpha)}$ . It follows that any infinite sum as in [Theorem 14.10](#) is automatically convergent, for any finitely generated pro- $p$ -group. This is one of the ways in which monomials in the  $b_i$  are preferable to the “obvious” basis of monomials in  $g_i$ , which are units and hence of norm one.

The proof of [Theorem 14.10](#) will take the rest of this lecture.

**Lemma 14.11.** *For any multi-index  $(\beta)$  we have*

$$g^{(\beta)} = \sum_{(\alpha)} \binom{\beta_1}{\alpha_1} \cdots \binom{\beta_m}{\alpha_m} b^{(\alpha)},$$

where the sum is taken over all multi-indices  $(\alpha)$  and similarly

$$b^{(\beta)} = \sum_{(\alpha)} (-1)^{\deg(\beta) - \deg(\alpha)} \binom{\beta_1}{\alpha_1} \cdots \binom{\beta_m}{\alpha_m} g^{(\alpha)}$$

*Proof.* Observe that both of the sums are in fact finite, since the binomial coefficients vanish if  $\alpha_i > \beta_i$  for any  $1 \leq i \leq m$ . Since  $g_i = b_i + 1$ , we have

$$g^{(\beta)} = (b_1 + 1)^{\alpha_1} \cdots (b_m + 1)^{\alpha_m}.$$

Expanding the right hand side using the binomial theorem yields the first formula. The second one follows by similarly expanding the right hand side of

$$b^{(\beta)} = (g_1 - 1)^{\alpha_1} \cdots (g_m - 1)^{\alpha_m}.$$

□

**Notation 14.12.** If  $k \geq 1$ , we write

$$T_k = \{(\alpha) \in \mathbb{N}^{\times m} \mid \alpha_i \leq p^{k-1} \text{ for all } i\}$$

for the set of multi-indices which are term-wise less than  $p^{k-1}$ .

**Lemma 14.13.** *The images of elements  $b^{(\alpha)}$  with  $\alpha \in T_k$  span  $\mathbb{Z}_p[G/G_k]$ . If  $G$  is uniform and the chosen set of generators  $g_i$  is minimal, then these elements form a basis.*

*Proof.* By [Lemma 14.11](#), the span of images of  $b^{(\alpha)}$  with  $\alpha \in T_k$  is the same as that of  $g^{(\alpha)}$  with the same constraint. By [Lemma 7.11](#), any element of the powerful finite  $p$ -group  $G/G_k$  can be written as

$$g^{(\alpha)} = g^{\alpha_1} \cdots g^{\alpha_m}.$$

for some multi-index  $\alpha$ . As any element of  $G/G_k$  satisfies  $g^{p^{k-1}} = 1$ , we see that we can assume that  $\alpha \in T_k$ , showing the first part.

If  $G$  is uniform with a minimal generating set of cardinality  $m$ , then  $|G/G_k| = p^{(k-1)m}$ , which is the rank of  $\mathbb{Z}_p[G/G_k]$  as a  $\mathbb{Z}_p$ -module. Since this is also the cardinality of  $T_k$ , we deduce that these elements must also form a basis. □

*Proof of Theorem 14.10.* Consider the map of topological abelian groups

$$\prod_{\alpha \in \mathbb{N}^{\times m}} \mathbb{Z}_p \simeq \text{map}(\mathbb{N}^{\times m}, \mathbb{Z}_p) \rightarrow \mathbb{Z}_p[[G]]$$

given by

$$(\lambda_\alpha) \mapsto \sum_{(\alpha)} \lambda_\alpha b^{(\alpha)}.$$

Since  $\|b^{(\alpha)}\| \rightarrow 0$  when  $\text{deg}(\alpha) \rightarrow \infty$ , this is well-defined and continuous. As the source is compact Hausdorff, the image is closed, and it is dense by Lemma 14.13 since  $\mathbb{Z}_p[[G]] \simeq \varprojlim \mathbb{Z}_p[G/G_k]$  as topological rings. We deduce that the image is the whole completed group algebra, as needed.

Now suppose that  $G$  is uniform; we show that expressions in monomials are unique. Suppose by contradiction that we have

$$(14.1) \quad \sum \lambda_\alpha b^{(\alpha)} = 0$$

and that at least one  $\lambda_\alpha$  is non-zero. By dividing by  $p$  if necessary, we can assume that at least one of them is non-zero mod  $p$ .

Let  $k$  be an integer. Since (14.1) holds, there exists a finite subset  $S \subseteq \mathbb{N}^{\times m}$  such that  $T_k \subseteq S$  and

$$\left\| \sum_{\alpha \in S} \lambda_\alpha b^{(\alpha)} \right\| \leq p^{-|G/G_k|},$$

so that

$$\sum_{\alpha \in S} \lambda_\alpha b^{(\alpha)} \in J^{|G/G_k|}.$$

We then have

$$(14.2) \quad \sum_{T_k} \lambda_\alpha b^{(\alpha)} = \sum_S \lambda_\alpha b^{(\alpha)} - \sum_{S \setminus T_k} \lambda_\alpha b^{(\alpha)}.$$

Since any element of  $(G-1)^{|G/G_k|}$  acts trivially on  $\mathbf{F}_p[G/G_k]$ , as we observed in the proof of Proposition 14.4, we have  $J^{|G/G_k|} \subseteq (G_k-1) + p\mathbb{Z}_p[[G]]$ . Thus, as a consequence of (14.2) we have

$$\sum_{T_k} \lambda_\alpha b^{(\alpha)} \in (J^{|G/G_k|} + ((G_k-1) + p\mathbb{Z}_p[[G]]) = (G_k-1) + p\mathbb{Z}_p[[G]].$$

Since  $b^{(\alpha)}$  for  $\alpha \in T_k$  form a  $\mathbf{F}_p$ -basis of  $\mathbf{F}_p[G/G_k]$  by Lemma 14.13, this implies that  $\lambda_\alpha \equiv 0 \pmod p$  for  $\alpha \in T_k$ . As  $k$  was arbitrary, we deduce that  $\lambda_\alpha \equiv 0 \pmod p$  for all  $\alpha$ , which contradicts our assumption.  $\square$

## 15. THE GROUP ALGEBRA OF A UNIFORM GROUP

In Theorem 14.10, we had shown that in the completed group algebra of a uniform group  $G$ , any element can be uniquely written as a convergent sum

$$\sum \lambda_\alpha b^{(\alpha)}$$

of monomials in  $b_i = g_i - 1$ , where  $g_i$  is a minimal set of generators. Today, we will describe the standard norm of  $\mathbb{Z}_p[[G]]$  in terms of these coordinates. As applications, we will be able to show that

- (1) the standard norm of the complete group algebra extends uniquely to its rationalization, giving a complete  $\mathbb{Q}_p$ -algebra where we can apply the logarithm and exponential introduced in §13 to relate a uniform group to a suitable Lie algebra, see Theorem 15.5,
- (2) the completed group algebra has a canonical filtration whose associated graded is a polynomial ring, allowing us to deduce that it has excellent ring-theoretic properties, see Theorem 15.9.

The following is the main result of today's lecture:

**Theorem 15.1.** *Let  $G$  be a uniform group with a minimal set of generators  $g_1, \dots, g_m$ . Then for any element*

$$\sum_{\alpha} \lambda_{\alpha} b^{(\alpha)} \in \mathbb{Z}_p[[G]]$$

we have

$$\left\| \sum_{\alpha} \lambda_{\alpha} b^{(\alpha)} \right\| = \sup(\{\|p^{\deg(\alpha)} \lambda_{\alpha}\|\}) = \sup(\{p^{-\deg(\alpha)} \|\lambda_{\alpha}\|\}),$$

where the right hand side is the standard norm of [Definition 14.6](#) and the sum and suprema are taken over  $\alpha \in \mathbb{N}^{\times m}$ .

The proof of [Theorem 15.1](#) will require some preliminaries. Throughout this lecture,  $G$  denotes a powerful group and we write

$$J = \ker(\mathbb{Z}_p[[G]] \rightarrow \mathbf{F}_p) = (G - 1) + p\mathbb{Z}_p[[G]]$$

for the ideal defining the standard norm of the complete group algebra (note that this is really the completion of the ideal of  $\mathbb{Z}_p[[G]]$  introduced previously in [Notation 14.3](#), although we use the same notation), so that the norm is defined by

$$\begin{aligned} \|0\| &:= 0, \\ \|x\| &:= p^{-n} \text{ if } x \in J^n \setminus J^{n+1}, \end{aligned}$$

We will need to study this ideal, and the way it interacts with  $p$ , in more detail.

**Lemma 15.2.** *Let  $G$  be powerful and for each  $k \geq 0$ , write*

$$J_{k+1,1} := pJ^k + J^{k+2} \subseteq J^{k+1}.$$

Then for any  $x \in J^k$  and any  $g \in G$ , we have

$$[x, g] \in J_{k+1,1},$$

where the bracket  $[x, g] := xg - gx$  denotes the Lie bracket of the group algebra.

*Proof.* Note that since the bracket is bilinear in each variable, we have

$$[x, g] = [x, g - 1] = x(g - 1) - (g - 1)x$$

and since  $g - 1 \in J$ , the bracket defines a linear map

$$[-, g]: J^k/J^{k+1} \rightarrow J^{k+1}/J^{k+2}.$$

We have to show that the image of this map is contained in  $J^{k+1,1}$ .

If  $k = 0$ , then since  $J^0/J^1$  is additively spanned by 1, which is central, the bracket vanishes. If  $k = 1$ , then since  $J/J^2$  is spanned by  $b_i$  and  $p$  (which is central), we can assume that  $x = b_i$ . We have

$$[b_i, g] = [g_i, g] = gg_i(g_i^{-1}g^{-1}g_i g - 1) = gg_i(z^p - 1)$$

where we use that since  $G$  is powerful we can write  $g_i^{-1}g^{-1}g_i g = z^p$  for some  $z \in G$ . Since  $(z - 1)^p \equiv z^p - 1 \pmod{p}$  and  $(z - 1)^p \in J^p$ , we have  $z^p - 1 \in J^p + p\mathbb{Z}_p[[G]]$ . If  $p > 2$ , this is the desired statement. If  $p = 2$ , then  $g_i^{-1}g^{-1}g_i g \in G_3$  and hence  $g_i^{-1}g^{-1}g_i g - 1 \in J_3$  by [Proposition 14.4](#).

For  $k > 1$ , we argue by induction. Any element of  $J^k$  can be written as a linear combination  $x = uv$  with  $u \in J^k$  and  $v \in J$ . Then

$$[uv, g] = uvg - guv = uvg - ugv + ugv - guv = u[v, g] + [u, g]v$$

and the result follows from the inductive assumption applied to  $[v, g]$  and  $[u, g]$ . □

**Lemma 15.3.** *Let  $G$  be powerful with a set of generators  $g_i$  and associated elements  $b_i = g_i - 1$ . Then*

$$J^k = \sum_{\alpha} p^{k-\deg(\alpha)} \mathbb{Z}_p b^{(\alpha)} + J^{k+1}.$$

where the sum is taken over  $\alpha \in \mathbb{N}^{\times m}$  with  $\deg(\alpha) \leq k$ .

*Proof.* Let us write  $W_k = \text{span}(\{p^{k-\deg(\alpha)} b^{(\alpha)} \mid \deg(\alpha) \leq k\})$ . Since  $p, b_i \in J$ , we have  $W_k \subseteq J^k$ , so that

$$J^{k+1} + W_k \leq J^k.$$

We have to show that the converse holds as well.

The case of  $k = 0$  is clear, and we argue for  $k = 1$ . By [Lemma 14.13](#), we have

$$(15.1) \quad \mathbb{Z}_p \llbracket G \rrbracket = \sum_{\alpha \in T_2} b^{(\alpha)} + \ker(\mathbb{Z}_p \llbracket G \rrbracket \rightarrow \mathbb{Z}_p[G/G_2]),$$

where  $T_2 = \{\alpha \in \mathbb{N}^{\times m} \mid \alpha_i < p\}$ . Since

$$\ker(\mathbb{Z}_p \llbracket G \rrbracket \rightarrow \mathbb{Z}_p[G/G_2]) \subseteq J^2$$

by [Proposition 14.4](#) and similarly  $b^{(\alpha)} \in J^2$  when  $\deg(\alpha) > 1$ , we can rewrite (15.1) as

$$\mathbb{Z}_p \llbracket G \rrbracket = \mathbb{Z}_p \cdot 1 + \sum_{\deg(\alpha)=1} \mathbb{Z}_p b^{(\alpha)} + J^2.$$

Since the latter two summands are contained in  $J$ , intersecting this equality with  $J$  we obtain

$$J = (J \cap \mathbb{Z}_p \cdot 1) + \sum_{\deg(\alpha)=1} \mathbb{Z}_p b^{(\alpha)} + J^2 = W_1 + J^2,$$

since  $J \cap \mathbb{Z}_p \cdot 1 = \mathbb{Z}_p \cdot p$ , which is what we wanted to show.

For  $k > 1$  we argue by induction. By inductive assumption applied to  $k - 1$  and 1, we can write

$$J^k = J^{k-1} J = (W_{k-1} + J^k)(W_1 + J^2) \subseteq W_{k-1} W_1 + J^{k+1}.$$

Thus, to finish the proof it is enough to verify that  $W_{k-1} W_1 + J^{k+1} \subseteq W_k + J^{k+1}$ . As  $W_1$  is the linear span of  $p, b_i$  and  $pW_{k-1} \subseteq W_k$ , we only have to check that

$$p^{k-1-\deg(\alpha)} b^{(\alpha)} b_i \in W_k + J_{k+1}$$

for every  $1 \leq i \leq m$  and every word of degree  $\deg(\alpha) \leq k - 1$ . Note that if  $i = m$ , then  $b^{(\alpha)} b_m = b^{(\alpha')}$  where  $\alpha'_m = \alpha_m + 1$  and  $\alpha'_i = \alpha_i$  for  $i < m$ , in which case

$$p^{k-1-\deg(\alpha)} b^{(\alpha)} b_m = p^{k-\deg(\alpha')} b^{(\alpha')} \in W_k.$$

As usual, the difficulty lies in the group algebra not being commutative.

Let  $f = (\alpha_1, \dots, \alpha_i, 0, \dots)$  and  $b = (\dots, 0, \alpha_{i+1}, \dots, \alpha_m)$  be the division of  $(\alpha)$  into the “front” and “back” parts, so that  $b^{(\alpha)} = b^{(f)} b^{(b)}$ . Then

$$p^{k-1-\deg(\alpha)} b^{(\alpha)} b_i = p^{k-1-\deg(\alpha)} b^{(f)} b^{(b)} b_i = p^{k-1-\deg(\alpha)} b^{(f)} b_i b^{(b)} + p^{k-1-\deg(\alpha)} b^{(f)} [b^{(b)}, b_i].$$

The left summand is  $p^{k-1-\deg(\alpha)}$  times a monomial of degree  $\deg(\alpha) + 1$  and thus belongs to  $W_k$ . For the right summand, observe that by [Lemma 15.2](#) we have

$$[b^{(b)}, b_i] \in pJ^{\deg(b)} + J^{\deg(b)+2}$$

and thus

$$p^{k-1-\deg(\alpha)} b^{(f)} [b^{(b)}, b_i] \in p^{k-\deg(\alpha)} J^{\deg(\alpha)} + J^{k+1}.$$

Since  $J^{\deg(\alpha)} \subseteq W_{\deg(\alpha)} + J^{\deg(\alpha)+1}$ ,  $p^{k-\deg(\alpha)} W_{\deg(\alpha)} \subseteq W_k$  and  $p^{k-\deg(\alpha)} J^{\deg(\alpha)+1} \subseteq J^{k+1}$ , this ends the argument.  $\square$

We are now ready to prove an explicit formula for the norm of a completed group algebra in terms of the monomial basis.

*Proof of Theorem 15.1.* We have to show that given an element  $x = \sum_{\alpha} \lambda_{\alpha} b^{(\alpha)}$ , we have

$$(15.2) \quad \|x\| = \sup_{\alpha} (p^{-\deg(\alpha)} \|\lambda_{\alpha}\|_p)$$

Since  $p, b_i \in J$ , we have  $\|\lambda_{\alpha} b^{(\alpha)}\| \leq p^{-v(\lambda_{\alpha}) - \deg(\alpha)}$ , where  $v(-)$  is the  $p$ -adic valuation. Thus, the left hand side of 15.2 is bounded by the right hand side, and we only have to verify the inequality going to the other way.

If  $x = 0$ , then  $\lambda_{\alpha} = 0$  for all  $\alpha$  and there is nothing to show. Instead, suppose that  $\|x\| = p^{-c}$ , so that  $x \in J^c \setminus J^{c+1}$ . Using Lemma 15.3, we can write it as

$$(15.3) \quad x = \sum_{\deg(\alpha) \leq c} p^{c - \deg(\alpha)} u_{\alpha, c} b^{(\alpha)} + x'$$

with  $x' \in J^{c+1}$ . Expanding  $x'$  similarly and continuing inductively, we obtain that

$$x = \sum_{k \geq c} \left( \sum_{\deg(\alpha) \leq k} p^{k - \deg(\alpha)} u_{\alpha, k} b^{(\alpha)} \right)$$

which we can rewrite as

$$x = \sum_{\alpha} \left( \sum_{k \geq c} p^{k - \deg(\alpha)} u_{\alpha, k} \right) b^{(\alpha)}.$$

Since  $G$  is uniform, the uniqueness part of Theorem 14.10 applies, so that

$$(15.4) \quad \lambda_{\alpha} = \sum_{k \geq c} p^{k - \deg(\alpha)} u_{\alpha, k}.$$

Assume by contradiction that  $p^{-\deg(\alpha)} \|\lambda_{\alpha}\|_p < p^{-c}$  for each  $\alpha$ ; equivalently, that  $\|\lambda_{\alpha}\|_p < p^{\deg(\alpha) - c}$ . Since  $\|p^{k - \deg(\alpha)} u_{\alpha, k}\| < p^{-c}$  for  $k > c$ , by (15.4) this can only happen if also

$$\|p^{c - \deg(\alpha)} u_{\alpha, c}\| < p^{\deg(\alpha) - c};$$

equivalently, when each  $u_{\alpha, c}$  is divisible by  $p$ . Then

$$p^{c - \deg(\alpha)} u_{\alpha, c} b^{(\alpha)} \in pJ^c \subseteq J^{c+1}$$

and hence  $x \in J^{c+1}$  as a consequence of (15.3). This contradicts the assumption that  $\|x\| = p^{-c}$ , ending the argument.  $\square$

While Theorem 15.1 can seem somewhat opaque at first sight, it has many important consequences which we now outline.

**Notation 15.4.** The *rational* completed group algebra is given by

$$\mathbb{Q}_p[[G]] := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[G]].$$

Note that since  $\mathbb{Z}_p[[G]] \simeq \varprojlim \mathbb{Z}_p[G/G_k]$  is torsion-free, we have an *inclusion*

$$i: \mathbb{Z}_p[[G]] \hookrightarrow \mathbb{Q}_p[[G]].$$

Any element of the target can be written as  $p^{-n} \cdot i(x)$  for some  $x \in \mathbb{Z}_p[[G]]$  and  $n \geq 0$ .

**Theorem 15.5.** *If  $G$  is uniform, then the standard norm on  $\mathbb{Z}_p[[G]]$  uniquely extends to a norm on  $\mathbb{Q}_p[[G]]$  which makes the latter into a normed  $\mathbb{Q}_p$ -algebra.*

*Proof.* Any  $\mathbb{Q}_p$ -algebra norm has the property that  $\|p^{-n}x\| = p^n\|x\|$  by Lemma 13.18. As any element of the rational group algebra can be written as  $p^{-n}x$  for some  $x \in \mathbb{Z}_p[[G]]$ , it is clear that if an extension of the norm exists then it is unique. To see that the above formula gives a well-defined norm, suppose that

$$p^{-k}x = p^{-k'}x'$$

for some  $x, x' \in \mathbb{Z}_p[[G]]$  and  $k, k' \geq 0$ . We have to show that in this case

$$\|x\|p^k = \|x'\|p^{k'}.$$

By symmetry, we can assume that  $k \geq k'$ . The first centered equality can then be rewritten as

$$x = p^{k-k'}x'.$$

If we write  $x = \sum \lambda_\alpha b^{(\alpha)}$  and similarly for  $x'$ , then by the uniqueness of monomial expressions we have

$$\lambda_\alpha p^{k-k'} \lambda'_\alpha.$$

We deduce that  $\|x\| = \|p^{k-k'}\|_p \|x'\|$  as a consequence of the supremum formula for the norm of [Theorem 15.1](#). This shows the formula is well-defined.

Subadditivity and submultiplicativity of so-defined norm on  $\mathbb{Q}_p[[G]]$  can be verified by multiplying by a large enough power of  $p^n$  and using the corresponding property of the norm of  $\mathbb{Z}_p[[G]]$ .  $\square$

As another important consequence of [Theorem 15.1](#), observe that for any  $k \geq 0$ , we have

$$J^k = \{x \in \mathbb{Z}_p[[G]] \mid \|x\| \leq p^{-k}\} = \left\{ \sum_{\alpha \in \mathbb{N}^{\times m}} \lambda_\alpha b^{(\alpha)} \mid \|\lambda_\alpha\| \leq p^{\deg(\alpha)-k} \right\}$$

The second expression immediately implies the following:

**Corollary 15.6.** *Elements of the form*

$$p^{k-\deg(\alpha)} \cdot b^{(\alpha)}$$

*with  $\deg(\alpha) \leq k$  form a basis of the  $\mathbf{F}_p$ -vector space  $J^k/J^{k+1}$ .*

One can rephrase [Corollary 15.6](#) in the following way: the basis of  $J/J^2$  is given by

$$(15.5) \quad p, b_1, \dots, b_m$$

and for each  $k \geq 2$  the basis of  $J^k/J^{k+1}$  is given by ordered monomials in these elements of length  $k$ . In particular, we deduce that the dimensions of these vector spaces are given by the same formula as in the case of a polynomial ring:

**Corollary 15.7.** *Let  $G$  be a uniform group of dimension  $m$ . Then*

$$\dim_{\mathbf{F}_p}(J^k/J^{k+1}) = \binom{m+k}{k} = \dim_{\mathbf{F}_p}(\{p \in \mathbf{F}_p[x_0, \dots, x_m] \mid p \text{ homogenous of degree } k\})$$

The *associated graded*  $\text{gr}_J(\mathbb{Z}_p[[G]])$  of the completed group algebra is the graded ring given in degree  $k$  by

$$\text{gr}_J(\mathbb{Z}_p[[G]])_k := J^k/J^{k+1},$$

with product induced from that of the completed group algebra. It is an  $\mathbf{F}_p$ -algebra which by [Corollary 15.7](#) is in degree  $k$  of the same dimension as the graded polynomial ring  $\mathbf{F}_p[x_0, \dots, x_m]$ , where each  $x_i$  is of degree 1.

One might then guess that perhaps  $\text{gr}_*(\mathbb{Z}_p[[G]])$  itself is just a polynomial algebra. This is *almost* true. To see this, observe that the associated graded is generated in degree one, with generators given by images

$$\tilde{p}, \tilde{b}_1, \dots, \tilde{b}_m \in J/J^2$$

of elements of (15.5). If these elements commute with each other, then we have an induced homomorphism of graded rings

$$\mathbf{F}_p[x_0, \dots, x_m] \rightarrow \text{gr}_J(\mathbb{Z}_p[[G]])$$

defined by

$$x_0 \mapsto \tilde{p}$$

and

$$x_i \mapsto \tilde{b}_i$$

for  $1 \leq i \leq m$ . This is surjective in each degree since the images of  $x_i$  generate the target, and thus must be also injective by the dimension count of [Corollary 15.7](#). It is in this sense that the associated graded is almost a polynomial ring, with the obstruction being that the images of  $b_i$  need not commute (the image of  $p$  certainly does, as  $p$  is central).

However, observe that by [Lemma 15.2](#) we have

$$[b_i, b_j] \in pJ + J^3$$

for any  $1 \leq i, j \leq m$ . It follows that in the associated graded we have

$$(15.6) \quad [\tilde{b}_i, \tilde{b}_j] \in \tilde{p} \cdot \text{gr}_1(\mathbb{Z}_p[[G]]).$$

This essentially shows the following:

**Theorem 15.8.** *Let  $G$  be a uniform group and consider the  $\tilde{p}$ -adic filtration*

$$\dots \subseteq \tilde{p}^2 \cdot \text{gr}_J(\mathbb{Z}_p[[G]]) \subseteq \tilde{p} \cdot \text{gr}_J(\mathbb{Z}_p[[G]]) \subseteq \text{gr}_J(\mathbb{Z}_p[[G]])$$

*on the associated graded of the  $J$ -adic filtration on the completed group algebra, where  $\tilde{p} \in J/J^2$  is the image of  $p$ . Then the associated graded of the  $\tilde{p}$ -adic filtration is isomorphic as a bigraded ring to*

$$\mathbf{F}_p[x_0, x_1, \dots, x_m]$$

*where  $|x_0| = (1, 1)$  and  $|x_i| = (1, 0)$  for  $1 \leq i \leq m$ , where the first degree is  $J$ -adic and the second  $\tilde{p}$ -adic.*

*Proof.* The ring homomorphism is specified by

$$x_0 \mapsto \tilde{p},$$

which is in  $\tilde{p}$ -adic filtration one, and

$$x_i \mapsto \tilde{b}_i,$$

which is in  $\tilde{p}$ -adic filtration zero. By (15.6) the bracket between  $\tilde{b}_i$  is zero in the associated graded of the  $\tilde{p}$ -adic filtration, and so all of these elements commute and we have the needed ring homomorphism. Using the description of elements of  $\text{gr}_J(\mathbb{Z}_p[[G]])$  in terms of products of monomials in  $\tilde{p}$  and  $\tilde{b}_i$  we see that this map is surjective and injective by (a slight refinement of) the dimension count of [Corollary 15.7](#). Thus, the map is an isomorphism.  $\square$

As a consequence of the description of the associated graded, we deduce that the completed group algebra itself has excellent ring-theoretic properties.

**Theorem 15.9.** *Let  $G$  be a uniform group of dimension  $m$ . Then the completed group algebra  $\mathbb{Z}_p[[G]]$  has the following properties:*

- (1) *it is left and right noetherian,*
- (2) *has no zero-divisors,*
- (3) *it is of global dimension  $m + 1$ ; that is, for any left (or right) modules we have*

$$\text{Ext}_{\mathbb{Z}_p[[G]]}^s(M, N)$$

*for  $s > m + 1$ .*

*Proof.* One can show that if  $A$  is a ring complete with respect to a filtration whose associated graded has any of these three properties, then so does the algebra itself. This is not difficult, but would take us too far off course, so we instead refer the reader to the comprehensive account given in [\[HVOHvO96\]](#).

In the case at hand, the bigraded polynomial ring  $\mathbf{F}_p[x_0, \dots, x_m]$  has all three of these properties, and hence so does  $\text{gr}_J(\mathbb{Z}_p[[G]])$  by [Theorem 15.8](#) (note that the  $\tilde{p}$ -adic filtration is complete

by degree considerations). We deduce that the completed group algebra also has these three properties.  $\square$

**Corollary 15.10.** *Let  $G$  be a profinite group which is virtually uniform (for example, this is true if  $G$  is pro- $p$  of finite rank by [Corollary 7.5](#)). Then  $\mathbb{Z}_p[[G]]$  is both left and right noetherian.*

*Proof.* Let  $U \triangleleft G$  be an open uniform subgroup and let  $g_1, \dots, g_k \in G$  be a set of representatives for cosets  $G/U$ . Then  $\mathbb{Z}_p[[G]]$  is free on the images of  $g_i$  as a module over  $\mathbb{Z}_p[[U]]$ , in particular finitely generated. Since the latter ring is left and right noetherian by [Theorem 15.9](#), we deduce that so is  $\mathbb{Z}_p[[G]]$ .  $\square$

### 16. BAKER-CAMPBELL-HAUSDORFF FORMULA

The logarithm and exponential functions of [Proposition 13.31](#) allow one to relate the addition and multiplication of a complete normed  $\mathbb{Q}_p$ -algebra. Applied to a group algebra of a suitably nice profinite group, this allows one to identify the group itself with a linear subset of its group algebra (namely the image of the logarithm). This subset should rightfully be thought of as the Lie algebra, as we will explore in the next lecture.

Transporting the multiplication through the exponential, we obtain a group structure on the image of the logarithm, and it is natural to ask about a formula for this induced multiplication. This is the subject of the Baker-Campbell-Hausdorff formula which we discuss today.

Recall that in [Definition 13.27](#) we introduced the exponential

$$\mathcal{E}(X) = \sum_{n \geq 0} \frac{1}{n!} X^n$$

and logarithm

$$\mathcal{L}(X) = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} X^n$$

power series. If  $A$  is a complete normed  $\mathbb{Q}_p$ -algebra, then these two power series define the logarithm and exponential functions which are inverse bijections

$$\exp: A_0 \rightleftarrows 1 + A_0: \log$$

An elementary calculation shows that in the ring  $\mathbb{Q}_p[[X, Y]]$  of power series in two *commuting* variables, we have an equality

$$(16.1) \quad \mathcal{L}(\mathcal{E}(X)\mathcal{E}(Y) - 1) = \mathcal{L}(X) + \mathcal{L}(Y).$$

This means that for commutative normed algebras, the exponential and logarithm exchange multiplication and addition. In particular, in a group algebra of an *abelian group*, the only trace of the group multiplication is the module structure of the Lie algebra. This is not surprising, since we have seen in [§9](#) that abelian uniform groups are very easy to describe, all being isomorphic to a free  $\mathbb{Z}_p$ -module. Today, we will analyze the difference between the two sides of [\(16.1\)](#) in non-commuting variables, which is encoded by the following power series.

**Definition 16.1.** Let  $\mathbb{Q}_p\langle\langle X, Y \rangle\rangle$  be the power series ring in two non-commuting variables. The *Baker-Campbell-Hausdorff* power series  $\Phi(X, Y) \in \mathbb{Q}_p\langle\langle X, Y \rangle\rangle$  is given by

$$\Phi(X, Y) := \mathcal{L}(\mathcal{E}(X)\mathcal{E}(Y) - 1).$$

To get some practice in working with power series in non-commuting variables, let's calculate the low degree terms. Since

$$\mathcal{E}(X) = 1 + X + \frac{X^2}{2} + \text{terms of degree at least three}$$

and similarly for  $\mathcal{E}(Y)$ , we have

$$\mathcal{E}(X)\mathcal{E}(Y) - 1 = X + Y + XY + \frac{X^2}{2} + \frac{Y^2}{2} + \text{terms of degree at least three.}$$

Substituting this into the logarithm, we obtain

$$\Phi(X, Y) = X + Y + XY + \frac{X^2}{2} + \frac{Y^2}{2} - \frac{1}{2}(X + Y)^2 + \text{terms of degree at least three,}$$

which since  $(X + Y)^2 = X^2 + Y^2 + XY + YX$  we can rewrite as

$$\Phi(X, Y) = X + Y + \frac{1}{2}(X, Y) + \text{terms of degree at least three,}$$

where  $(X, Y) = XY - YX$  is the Lie bracket. The following celebrated theorem tells us that the appearance of the bracket is not an accident, and that the whole failure of (16.1) to hold in non-commuting variables is expressible in these terms.

**Notation 16.2.** If  $L$  is a Lie algebra (for example, an associative algebra with the induced Lie structure  $(a_1, a_2) := a_1a_2 - a_2a_1$ ), then the *iterated bracket of length  $n$*  is defined inductively as

$$(a_1, a_2, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n).$$

**Theorem 16.3** (Baker-Campbell-Hausdorff). *Write the homogeneous decomposition of  $\Phi(X, Y)$  as*

$$\Phi(X, Y) = \sum_{n \geq 1} u_n(X, Y),$$

so that each  $u_n(X, Y)$  is a linear combination of words of degree  $n$ . Then

- (1)  $u_1(X, Y) = X + Y$ ,
- (2) for each  $n \geq 2$ ,  $u_n(X, Y)$  is a linear combination with rational coefficients of brackets in  $X$  and  $Y$  of length  $n$ .

**Remark 16.4.** The algebra  $\mathbb{Q}\langle X, Y \rangle$  is the free associative  $\mathbb{Q}$ -algebra in two variables, and by inspecting universal properties thus be identified with the universal enveloping algebra of  $L(X, Y)$ , the free Lie algebra in two variables. By Poincaré-Birkhoff-Witt theorem, see [KK96, §3.1], the canonical map

$$(16.2) \quad L(X, Y) \rightarrow \langle X, Y \rangle$$

is injective. In this language, Theorem 16.3 is saying that each of the polynomials  $u_n(X, Y)$  is in the image of (16.2), and so defines an expression which can be evaluated in *any Lie algebra*, despite the fact that its definition uses associative algebras in an essential way.

This is important, as it allows one to define a multiplication on any Lie algebra in which  $\Phi(X, Y)$  can be shown to be convergent. We will use this in the next lecture to show that certain  $\mathbb{Z}_p$ -Lie algebras can be used to produce uniform groups.

Note that we have already calculated that Theorem 16.3 holds for  $n \leq 2$ . With enough patience, one can also calculate by hand that

$$u_3(X, Y) = \frac{1}{12}(X, Y, Y) - \frac{1}{12}(X, Y, X).$$

After that, the formulas become quite involved and our proof will proceed in a different way.

Since Theorem 16.3 is a purely algebraic statement about certain formal power series over the rationals, it admits purely algebraic proofs. Since in this class we're working with complete normed  $\mathbb{Q}_p$ -algebras, it will be convenient to give a proof using this technology, but we also outline the more usual argument.

**Remark 16.5** (The “standard” proof). To highlight a variety of approaches to this problem, we sketch the more standard algebraic argument leading to the Baker-Campbell-Hausdorff formula. After spelling out the necessary theory, it is not much shorter than the one given here, but it is arguably more conceptual, resting on a few fundamental properties of Lie algebras which are important in their own right. For details, see [Sch11, §16].

The algebra of non-commutative polynomials  $\mathbb{Q}\langle X, Y \rangle$  has a canonical Hopf-algebra structure with comultiplication determined by  $\Delta(X) = X \otimes 1 + 1 \otimes Y$  and  $\Delta(Y) = Y \otimes 1 + 1 \otimes Y$ . This comultiplication extends continuously to one on  $\mathbb{Q}\langle\langle X, Y \rangle\rangle$ , the ring of power series.

Given a Hopf algebra, one says that an element  $z$  is

- (1) *primitive* if  $\Delta(z) = z \otimes 1 + 1 \otimes Z$ ,
- (2) *grouplike* if  $\Delta(z) = z \otimes z$ .

An easy calculation shows that primitive elements form a Lie-subalgebra, and grouplike elements form a subgroup of multiplicative units.

As observed in Remark 16.4, the ring  $\mathbb{Q}\langle X, Y \rangle$  can be identified with the enveloping algebra of the free Lie algebra  $L(X, Y)$  generated by  $X, Y$ . As a consequence of Poincaré-Birkhoff-Witt theorem [KK96, §3.1],  $\mathbb{Q}\langle X, Y \rangle$  has a basis given by ordered monomial in basis elements of  $L(X, Y)$ . Calculating in this basis we see that the subspace of primitive elements of  $\mathbb{Q}\langle X, Y \rangle$  is exactly  $L(X, Y)$ , so that they are all linear combinations of brackets in  $X, Y$ . Passing to the completion  $\mathbb{Q}\langle\langle X, Y \rangle\rangle$ , we see that any primitive formal power series is a possibly infinite sum of the brackets.

Using basic properties of the exponential and logarithm, one calculates that if  $I \subseteq \mathbb{Q}\langle\langle X, Y \rangle\rangle$  is the maximal ideal of power series with no constant term, then  $\mathcal{E}(-)$  and  $\mathcal{L}(-)$  give a bijection

$$I \cong 1 + I$$

(there are no convergence issues here, since these are formal power series). An easy calculation shows that this restricts to a bijection between primitive and grouplike elements. Since  $X, Y$  are primitive,  $\mathcal{E}(X), \mathcal{E}(Y)$  are grouplike and thus is their product  $\mathcal{E}(X) \cdot \mathcal{E}(Y)$ . It follows that

$$\Phi(X, Y) = \mathcal{L}(\mathcal{E}(X)\mathcal{E}(Y) - 1)$$

is primitive and thus a sum of brackets by the discussion above.

Let  $A$  be a complete normed  $\mathbb{Q}_p$ -algebra. As previously, we write

$$A_0 = \begin{cases} \{x \in A \mid \|x\| \leq \frac{1}{p}\} & p > 2 \\ \{x \in A \mid \|x\| \leq \frac{1}{4}\} & p = 2 \end{cases}$$

so that the exponential and logarithm converge on, respectively,  $A_0$  and  $A_0 + 1$ . Given such an algebra, we can introduce another normed algebra by considering bounded operators.

**Definition 16.6.** We say that a  $\mathbb{Q}_p$ -linear map  $T: A \rightarrow A$  is *bounded* if its *operator norm*

$$\|T\| := \sup(\{\frac{\|Ta\|}{\|a\|} \mid a \in A, a \neq 0\})$$

is finite.

**Notation 16.7.** We write  $B(A)$  for the  $\mathbb{Q}_p$ -vector space of bounded operators on  $A$ . Using composition and the operator norm appearing in Definition 16.6, it becomes a complete normed  $\mathbb{Q}_p$ -algebra.

The space of bounded operators is related to the original algebra  $A$  by a variety of maps. The three particularly important maps  $A \rightarrow B(A)$  are the *left multiplication*, *right multiplication* and

the *adjoint representation* denoted by

$$\begin{aligned} a &\mapsto l_a, \\ a &\mapsto r_a, \\ a &\mapsto ad_a \end{aligned}$$

and defined by

$$\begin{aligned} l_a(b) &= ab, \\ r_a(b) &= ba, \\ ad_a(b) &= l_a(b) - r_a(b) = ab - ba = (a, b) \end{aligned}$$

Note that each of these is  $\mathbb{Q}_p$ -linear and norm-nonincreasing; in particular, they are continuous. Moreover, since

$$l_{ab}(c) = abc = l_a(l_b(c)),$$

$l_-$  is a map of algebras. By the same calculation,  $r_-$  is an anti-map of algebras; that is, it reverses the order of multiplication. On the other hand, the adjoint operator does not respect multiplication.

**Lemma 16.8.** *Let  $a \in A_0$ . Then*

$$\begin{aligned} l_{\exp(a)} &= \exp(l_a), \\ r_{\exp(a)} &= \exp(r_a) \end{aligned}$$

as bounded operators.

*Proof.* Notice that both sides make sense under given assumption, since  $l_a \in B(A)_0$ . The formula is clear for  $l$ , since it is a continuous map of algebras, and  $\exp$  is a limit of linear combinations of  $a^n$ . For  $r$ , we observe that  $a$  commutes with itself, so that similarly  $r_{a^n} = (r_a)^n$ .  $\square$

Recall that  $u_n(X, Y)$  denotes the degree  $n$  part of the Baker-Campbell-Hausdorff power series  $\Phi$ . The key step in the proof of [Theorem 16.3](#) is the observation that while the operator  $ad: A \rightarrow B(A)$  is not a map of algebras, it does respect these polynomials.

**Lemma 16.9.** *For any  $a, b \in A$ , we have an equality of bounded operators on  $A$*

$$ad_{u_n(a,b)} = u_n(ad_a, ad_b).$$

*Proof.* Suppose first that  $a, b \in A_0$ , so that the exponential converges on them. In this case, we have

$$\exp(l_a) \exp(l_b) = l_{\exp(a)} l_{\exp(b)} = l_{\exp(a) \exp(b)} = l_{\exp(\Phi(\exp(a), \exp(b)))} = \exp(l_{\Phi(a,b)}),$$

where we use the defining property of  $\Phi$ , namely that

$$(16.3) \quad \mathcal{E}(\Phi(X, Y)) = \mathcal{E}(X)\mathcal{E}(Y).$$

By the same argument, we have

$$\exp(r_b) \exp(r_a) = \exp_{r_{\Phi(a,b)}}$$

(notice the reversed order of  $a$  and  $b$ , since  $r$  reverses multiplication).

We have  $ad_a = l_a - r_a$ , and since the latter two operators commute with each other, we have

$$(16.4) \quad \exp(ad_a) = \exp(l_a) \exp(-r_a) = \exp(l_a) \exp(r_a^{-1}) = l_{\exp(a)} r_{\exp(b)}^{-1}.$$

We now calculate

$$\exp(\Phi(ad_a, ad_b)) = \exp(ad_a) \exp(ad_b) = l_{\exp(a)} r_{\exp(a)}^{-1} l_{\exp(b)} r_{\exp(b)}^{-1} = (l_{\exp(a)} l_{\exp(b)}) (r_{\exp(b)} r_{\exp(a)})^{-1},$$

where the first equality is (16.3), the second one is (16.4) and the third one again uses that left and right multiplication operators commute. We can further rewrite this as

$$l_{\exp(a)\exp(b)}(r_{\exp(a)\exp(b)})^{-1} = \exp(l_{\Phi(a,b)}\exp(r_{\Phi(a,b)}))^{-1} = \exp(ad_{\Phi(a,b)}).$$

Taking logarithms, we deduce that

$$\Phi(ad_a, ad_b) = ad_{\Phi(a,b)}$$

or, more concretely, that

$$\sum_{n \geq 1} u_n(ad_a, ad_b) = \sum_{n \geq 1} ad_{u_n(a,b)}$$

holds for all  $a, b \in A_0$ . If  $\lambda \in \mathbb{Z}_p$ , then since  $u_n$  is homogeneous of degree  $n$  and  $ad_{-}$  is linear, the above equality applied to  $\lambda a, \lambda b \in A_0$  becomes

$$\sum \lambda^n u_n(ad_a, ad_b) = \sum \lambda^n ad_{u_n(a,b)}.$$

As  $\mathbb{Z}_p \subseteq \mathbb{Q}_p$  is an open neighbourhood of zero, the identity property of Proposition 13.19 implies that

$$u_n(ad_a, ad_b) = ad_{u_n(a,b)}$$

for all  $n \geq 1$ , which is what we wanted to show. □

We are now ready to prove the Baker-Campbell-Hausdorff theorem.

*Proof of Theorem 16.3.* Let us write  $A$  for the quotient of the free algebra  $\mathbb{Q}_p\langle X, Y, t \rangle$  on three variables by the relations

$$\begin{aligned} tX &= Xt + X \\ tY &= Yt + Y. \end{aligned}$$

Explicitly, any element of  $A$  can be uniquely expressed as a finite sum

$$\sum_{n \geq 0, w \in W(X, Y)} a_{k,w} t^k w$$

indexed by the product of non-negative integers (specifying the power of  $t$ ) and the monoid of words in  $X, Y$ , where  $a_{k,w} \in \mathbb{Q}_p$ . Notice that  $A$  contains  $\mathbb{Q}_p\langle X, Y \rangle$  as a subalgebra. As a consequence of (16), we have

$$ad_t(X) = X$$

and analogously for  $Y$ , from which we deduce that if  $p(X, Y) \in \mathbb{Q}_p\langle X, Y \rangle$  is homogeneous of degree  $n$ , then

$$(16.5) \quad ad_t(p(X, Y)) = n \cdot p(X, Y).$$

This algebra  $A$  is specifically designed to be an enlargement of  $\mathbb{Q}_p\langle X, Y \rangle$  where the degree decomposition becomes an eigenspace decomposition for an operator  $ad_t$  attached to a new element  $t$ .

The formula

$$\|\sum a_{k,w} t^k w\| := \sup(\{\|a_{k,w}\| \mid k \geq 0, w \in W(X, Y)\})$$

defines a norm on  $A$  that makes it into a  $\mathbb{Q}_p$ -normed algebra and we write  $\hat{A}$  for its completion, which can be identified with the algebra of possibly infinite sums, but with the property that  $\sum a_{k,w}$  exists.

We now work in the algebra of bounded operators on  $\hat{A}$ . Using (16.5), we have

$$-n \cdot u_n(X, Y) = -ad_t(u_n(X, Y)) = ad_{u_n(X, Y)}(t) = u_n(ad_X, ad_Y)(t),$$

where the last equality is Lemma 16.9. If we write

$$u_n(X, Y) = \sum_{\deg(w)=n} c_w w(X, Y),$$

the above can be rewritten as

$$-n \cdot u_n(X, Y) = \sum c_w w(ad_X, ad_Y)(t),$$

where by  $w(ad_X, ad_Y)$  we mean the element of the algebra of operators obtained by substituting  $X \mapsto ad_X$  and  $Y \mapsto ad_Y$ . We claim that

$$w(ad_X, ad_Y)(t)$$

is a bracket of length  $n$  in  $X, Y$  when  $w$  is a word of length  $n \geq 2$ , which will finish the proof. To see this, write

$$w = Z_1 \cdot \dots \cdot Z_n,$$

where  $Z_i \in \{X, Y\}$ . Then

$$w(ad_X, ad_Y)(t) = ad_{Z_1} \dots ad_{Z_n}(t) = ad_{Z_1} \dots ad_{Z_{n-1}}(Z_n) = (Z_1, (Z_2, \dots, (Z_{n-1} Z_n) \dots))$$

which since the bracket is anti-symmetric gives

$$w(ad_X, ad_Y)(t) = (-1)^n (Z_n, Z_{n-1}, \dots, Z_1)$$

which is an iterated bracket in  $X, Y$  as claimed.  $\square$

The Baker-Campbell-Hausdorff formula is an algebraic statement, but to apply it to  $p$ -adic analytic groups, we will need some control over its coefficients to guarantee the convergence of  $\Phi(x, y)$  for suitable  $x, y$ .

**Notation 16.10.** The bounds are different at odd primes and at the even prime, so to state the result, we write

$$\epsilon = \begin{cases} 1 & p > 2, \\ 2 & p = 2, \end{cases}$$

so that  $A_0 = \{x \mid \|x\| \leq p^{-\epsilon}\}$ .

**Proposition 16.11.** Write the  $n$ -th Baker-Campbell-Hausdorff polynomial as

$$u_n(X, Y) = \sum_{\deg(w)=n} c_w w(X, Y).$$

Then the  $p$ -adic valuation  $v(-)$  of the coefficients satisfies

- (1)  $\epsilon(n-1) + v(c_w) \geq \epsilon$  if  $n \geq 3$ ,
- (2)  $\epsilon(n-1) + v(c_w) \rightarrow \infty$  as  $n \rightarrow \infty$ .

*Proof.* We only prove the second part. The reader interested in seeing also the first part (which is similar, but more tedious) should consult [DDSMS03, Lemma 6.41, §6.Exercise 10].

Observe that  $\mathcal{E}(X)\mathcal{E}(Y) - 1$  is given by

$$\sum_{i, j \geq 1} \frac{1}{i!j!} X^i Y^j.$$

Applying the logarithm to calculate  $\Phi(X, Y) = \mathcal{L}(\mathcal{E}(X)\mathcal{E}(Y) - 1)$ , we see that the terms of degree  $n$  are all sums of terms of the form

$$\frac{(-1)^{k+1}}{k} \frac{1}{i_1!j_1! \dots i_k!j_k!} X^{i_1} Y^{j_1} \dots X^{i_k} Y^{j_k},$$

where

- (1)  $1 \leq k \leq n$ ,
- (2)  $i_l + j_l \geq 1$  for all  $1 \leq l \leq k$ ,
- (3)  $i_1 + j_1 + \dots + i_k + j_k = n$ .

Using [Lemma 13.29](#), we see that the  $p$ -adic valuation of a coefficient of such a term is given by

$$v\left(\frac{(-1)^{k+1}}{k} \frac{1}{i_1!j_1! \dots i_k!j_k!}\right) \geq -\frac{k-1}{p-1} - \sum_{1 \leq l \leq k} \left(\frac{i_l-1}{p-1} + \frac{j_l-1}{p-1}\right) \geq -\frac{n-1}{p-1},$$

where the second bound uses that  $i_l, j_l$  sum to  $n$ . It follows that

$$v(c_w) \geq -\frac{n-1}{p-1}$$

for each word of length  $n$ , since the  $p$ -adic valuation of a sum is bounded below by the  $p$ -adic valuations of the summands. This ends the argument, since

$$\epsilon(n-1) + v(c_w) \geq \epsilon(n-1) - \frac{n-1}{p-1} \geq \frac{\epsilon}{2}(n-1)$$

and the last terms diverges to infinity when  $n \rightarrow \infty$ . □

### 17. THE LIE CORRESPONDENCE

Let  $G$  be a uniform group. Recall that in [§9](#) we introduced the *addition* of  $G$ , given by the explicit formula

$$g +_G h := \lim_{n \rightarrow \infty} (g^{p^n} h^{p^n})^{p^{-n}},$$

which we had shown in [Theorem 9.14](#) makes  $G$  into a free  $\mathbb{Z}_p$ -module of rank equal to its dimension.

In this lecture, we will enrich this construction to a  $\mathbb{Z}_p$ -Lie algebra, and show that this furnishes an equivalence of categories between uniform groups and certain Lie algebras, see [Theorem 17.10](#). This result, which can be thought as the  $p$ -adic analogue of the classical correspondence between real Lie algebras and simply-connected Lie groups, is a cornerstone of the theory of  $p$ -adic analytic groups.

**Definition 17.1.** Let  $G$  be a uniform group. Its *additive bracket* is defined by

$$(g, h)_G := \lim_{n \rightarrow \infty} (g^{-p^n} h^{p^{-n}} g^{p^n} h^{p^n})^{p^{-2n}} \text{ }^{10}.$$

**Remark 17.2.** Observe that since  $g^{p^n}, h^{p^n} \in G_{n+1}$ , we have

$$g^{-p^n} h^{p^{-n}} g^{p^n} h^{p^n} \in G_{2n+2}$$

by [Theorem 3.21](#), so that the  $p^{2n}$ -th roots in the definition above make sense. It also follows that we have

$$(g, h)_G \in G_2$$

for any  $g, h \in G$ . If  $p = 2$ , then we have

$$g^{-1} h^{-1} g h \in G_3$$

since  $G/G_3$  is abelian, and using arguments similar to the proof of [Lemma 9.7](#) one can show that

$$(g, h)_G \in G_3;$$

see [[DDSMS03](#), Lemma 4.28].

We now show the following:

**Theorem 17.3.** *If  $G$  is a uniform group, then the addition of [Definition 9.8](#) and the additive bracket of [Definition 17.1](#) make  $G$  into a  $\mathbb{Z}_p$ -Lie algebra.*

---

<sup>10</sup>In terms of group commutators, we can write  $(g, h)_G = \lim_{n \rightarrow \infty} [g^{p^n}, h^{p^n}]^{p^{-2n}}$ . As in some of the previous lectures, we will avoid using the group commutator notation to not confuse it with the other kinds of “brackets” we use, such as the additive bracket of a uniform group or a Lie bracket of a normed algebra.

To prove [Theorem 17.3](#), we will use the theory of normed algebras and the exponential and logarithm functions. We first set up the notation.

**Notation 17.4.** We write  $G$  for a fixed uniform group. We assume that we are given a completed normed  $\mathbb{Q}_p$ -algebra and a continuous monomorphism  $G \rightarrow A^\times$  into the group of units such that

$$G \leq 1 + A_0,$$

where

$$A_0 = \begin{cases} \{x \in A \mid \|x\| \leq \frac{1}{p}\} & p > 2 \\ \{x \in A \mid \|x\| \leq \frac{1}{4}\} & p = 2 \end{cases}.$$

In other words,  $A$  is a normed algebra containing  $G$  as a subgroup of units and such that

$$\|g - 1\| \leq p^{-1}$$

(or  $\|g - 1\| \leq 2^{-2}$  for  $p = 2$ ) for all  $g \in G$ .

**Example 17.5.** If  $p$  is odd, then an example of a algebra satisfying the conditions of [Notation 17.4](#) is the rational group algebra  $\mathbb{Q}_p[[G]]$ , which we verified admits a complete norm with the needed property in [Theorem 15.5](#).

If  $p = 2$ , this algebra might not work, as we are only guaranteed that the norms of  $g - 1$  are bounded by  $1/2$ , rather than  $1/4$ . If  $G = P_2(H)$  for some other uniform pro-2-group  $H$ , then we can take  $A = \mathbb{Q}_p[[H]]$ , which has the needed property by part (1) of [Proposition 14.4](#). In the general case, one can show that there is a different norm on  $\mathbb{Q}_p[[G]]$  which has the needed property, see [[DDSMS03](#), §7.Exercise 10], but we leave the details to an interested reader.

Recall from [Proposition 13.31](#) that logarithm and exponential define mutually inverse functions

$$\exp: A_0 \rightleftarrows 1 + A_0: \log.$$

Since  $G \leq 1 + A_0$ , the logarithm is well-defined on elements of the group. We now relate the additive structure of the uniform group  $G$  to the algebra structure of  $A_0$  using the logarithm.

**Proposition 17.6.** *The logarithm  $\log: G \rightarrow A_0$  satisfies the following three identities for any  $g, h \in G, \lambda \in \mathbb{Z}_p$ :*

- (1)  $\log(g +_G h) = \log(g) + \log(h)$ ,
- (2)  $\log(g^\lambda) = \lambda \log(g)$ ,
- (3)  $\log((g, h)_G) = (\log(g), \log(h)) = \log(g) \log(h) - \log(h) \log(g)$ .

*Proof.* Throughout the proof, we use the shorthand  $\gamma := \log(g)$  and  $\eta := \log(h)$ . We write

$$\Phi(X, Y) = X + Y + \sum_{k \geq 2} u_k(X, Y)$$

for the degree decomposition of the Baker-Campbell-Hausdorff series of [Definition 16.1](#). As a consequence of [Proposition 16.11](#),  $\Phi(X, Y)$  defines a strictly analytic function

$$A_0 \times A_0 \rightarrow A_0.$$

Using the defining property  $\mathcal{E}(\Phi(X, Y)) = \mathcal{E}(X)\mathcal{E}(Y)$ , we see that

$$\log(gh) = \gamma + \eta + \sum_{k \geq 2} u_k(\gamma, \eta).$$

Since  $\log(x^n) = n \log(x)$  for  $x \in 1 + A_0$  by [Proposition 13.31](#) and since  $u_k$  is homogeneous of degree  $k$ , we have

$$\log(g^{p^n} h^{p^n}) = p^n \gamma + p^n \eta + \sum_{k \geq 2} p^{kn} u_k(\gamma, \eta).$$

We then have

$$\log((g^{p^n} h^{p^n})^{p^{-n}}) = \gamma + \eta + p^n \sum_{k \geq 2} p^{(k-1)n} u_k(\gamma, \eta).$$

Since the logarithm is continuous, we deduce that

$$\log(g +_G h) = \gamma + \eta + \lim_{n \rightarrow \infty} p^n \left( \sum_{k \geq 2} p^{(k-1)n} u_k(\gamma, \eta) \right) = \gamma + \eta,$$

since  $u_k(\gamma, \eta) \in A_0$  for all  $k$ . This proves part (1).

For part (2), observe that  $\log(g^\lambda) = \lambda \log(g)$  for all  $\lambda \in \mathbb{Z}$ . Since the integers are dense in  $\mathbb{Z}_p$  and both sides are continuous in  $\lambda$ , we deduce that this holds for all  $p$ -adic numbers.

For part (3), we argue in a way similar to (1), using instead of  $\Phi(X, Y)$  the formal power series

$$C(X, Y) := \mathcal{L}(\mathcal{E}(X)^{-1} \mathcal{E}(Y)^{-1} \mathcal{E}(X) \mathcal{E}(Y))$$

which has the property that

$$C(\gamma, \eta) = \log(g^{-1} h^{-1} g, h).$$

A direct calculation shows that

$$C(X, Y) = XY - YX + \sum_{k \geq 3} v_k(X, Y)$$

where  $v_k$  is homogeneous of degree  $k$ . We then have

$$\log((g, h)_G) = \lim_{n \rightarrow \infty} [\gamma, \eta] + p^n \left( \sum_{k \geq 3} p^{(k-3)n} v_k(\gamma, \eta) \right) = [\gamma, \eta]$$

which is what we wanted to show. □

*Proof of Theorem 17.3.* We have to show that the additive bracket of Definition 17.1 is  $\mathbb{Z}_p$ -linear in each variable and satisfies the Jacobi identity. By Proposition 17.6, parts (1) and (2), the logarithm defines a  $\mathbb{Z}_p$ -module isomorphism between  $G$  and a submodule of  $A$ . By part (3), this isomorphism takes the additive bracket to the Lie bracket of  $A$ , which is linear in each variable and satisfies the Jacobi identity. This ends the argument. □

Keeping Theorem 17.3 in mind, we make the following definition.

**Definition 17.7.** Let  $G$  be a uniform group. The *Lie algebra* of  $G$  is the  $\mathbb{Z}_p$ -Lie algebra

$$L(G) := (G, +_G, (-, -)_G)$$

given by the group itself together with its addition and the additive bracket.

**Remark 17.8.** Our definition of the Lie algebra of a uniform group is potentially confusing in that, as a set, the Lie algebra coincides with the group itself. Alternatively, one could define the Lie algebra as

$$L(G) := \log(G) \subseteq A_0,$$

the image of the logarithm. This has the advantage of being perhaps less confusing and the disadvantage of obscuring the fact that this structure does not depend on the choice of  $A$ : any normed group algebra as in Notation 17.4 would define the same  $L(G)$ , up to canonical isomorphism.

Observe that as a consequence of Theorem 9.14, addition makes a uniform group into a free  $\mathbb{Z}_p$ -module of finite rank equal to the dimension. Moreover, Remark 17.2 shows the additive bracket vanishes modulo  $p$  (or modulo 4 when  $p = 2$ ). Thus, the Lie algebra of Definition 17.7 is always of the following kind:

**Definition 17.9.** We say a  $\mathbb{Z}_p$ -Lie algebra  $L$  is *uniformly powerful* if it has the following two properties:

- (1) as a  $\mathbb{Z}_p$ -module, it is free of finite rank,
- (2)  $(L, L) \subseteq p \cdot L$  (resp.  $(L, L) \subseteq 4 \cdot L$  when  $p = 2$ ).

The notion of a uniformly powerful Lie algebra is precisely designed to state the following  $p$ -adic analogue of the correspondence between Lie groups and Lie algebras:

**Theorem 17.10** (The  $p$ -adic Lie correspondence). *The construction*

$$G \mapsto L(G)$$

of the Lie algebra of [Definition 17.7](#) gives an equivalence between

- (1) the category of uniformly powerful pro- $p$ -groups and continuous group homomorphism,
- (2) the category of uniformly powerful  $\mathbb{Z}_p$ -Lie algebras and Lie algebra homomorphisms.

To prove [Theorem 17.10](#), we will construct an explicit inverse to the functor  $G \mapsto L(G)$ . Let  $L$  be a uniformly powerful Lie algebra and write

$$\Phi(X, Y) = X + Y + \sum_{k \geq 2} u_k(X, Y)$$

for the Baker-Campbell-Hausdorff series. As a consequence of [Theorem 16.3](#), see [Remark 16.4](#), each of  $u_k(X, Y)$  can be (uniquely) identified with an element of a free  $\mathbb{Q}$ -Lie algebra in two variables, namely a linear combination of iterated brackets of length  $k$ . It follows that for any  $l_1, l_2 \in L$ , the expression  $u_k(l_1, l_2)$  can be evaluated to yield an element of the rationalization  $L_{\mathbb{Q}}$ .

Since  $(L, L) \subseteq p^\epsilon \cdot L$ , where  $\epsilon = 1$  when  $p > 2$  and  $\epsilon = 2$  when  $p = 2$ , we have that

- (1)  $u_2(l_1, l_2) = \frac{1}{2}(l_1, l_2) \in p \cdot L$ ,
- (2)  $u_k(l_1, l_2) \in p^\epsilon \cdot L$  for all  $k \geq 3$ ,
- (3)  $u_k(l_1, l_2) \rightarrow 0$  as  $k \rightarrow \infty$ , uniformly in  $l_1, l_2$ .

where the second and third parts are [Proposition 16.11](#). This furnishes the following definition.

**Definition 17.11.** Let  $L$  be a uniformly powerful Lie algebra. The *multiplication* of  $L$  is the binary operation

$$(17.1) \quad l_1 * l_2 := \Phi(l_1, l_2) = l_1 + l_2 + \sum_{k \geq 2} u_k(l_1, l_2)$$

**Remark 17.12.** Using properties (1) and (2) of  $u_k(l_1, l_2)$  outlined above, we see that

$$l_1 * l_2 \equiv l_1 + l_2 \pmod{p}$$

and additionally

$$l_1 * l_2 \equiv l_1 + l_2 + \frac{1}{2}(l_1, l_2) \pmod{4}$$

when  $p = 2$ .

**Lemma 17.13.** *The multiplication  $*$  makes  $L$  into a group.*

*Proof.* Applying the formal logarithm  $\mathcal{L}$  to

$$(\mathcal{E}(X)\mathcal{E}(Y))\mathcal{E}(Z) = \mathcal{E}(X)(\mathcal{E}(Y)\mathcal{E}(Z))$$

we see that the Baker-Campbell-Hausdorff series is associative in the sense that we have an equality

$$\Phi(\Phi(X, Y), Z) = \Phi(X, \Phi(Y, Z)).$$

It follows that the operation  $*$  of (17.1) is associative. To see that it makes  $L$  into a group, observe that immediately from the definition we see that

$$l * 0 = 0 * l = l$$

and

$$l * (-l) = 0$$

since the brackets defining  $u_k$  for  $k \geq 2$  vanish in this case. □

**Proposition 17.14.** *If  $L$  is uniformly powerful Lie algebra, then  $(L, *)$  with its  $p$ -adic topology is a uniformly powerful group.*

*Proof.* Since  $(l, l) = 0$  for any  $l \in L$ , we have

$$l^{*p} = p \cdot l.$$

From bilinearity of the bracket we see that

$$\{l^{*p} \mid l \in L\} = p \cdot L,$$

the subset of  $*p$ -th powers, is a  $*$ -subgroup. Since  $l_1 * l_2 \equiv l_1 + l_2 \pmod p$ ,

$$(L, *) / (p \cdot L, *)$$

is abelian so that  $(L, *)$  is powerful when  $p > 2$ . When  $p = 2$ , we instead observe that

$$l_1 * l_2 = l_1 + l_2 + \frac{1}{2}(l_1, l_2) \pmod 4,$$

so that

$$l_1 * l_2 * -(l_2 * l_1) \equiv l_1 + l_2 + \frac{1}{2}(l_1, l_2) - l_2 - l_1 - \frac{1}{2}(l_2, l_1) \equiv (l_1, l_2) \equiv 0 \pmod 4,$$

where we used the anti-symmetry of the bracket and the assumption that  $(L, L) \subseteq 4 \cdot L$ . We conclude that  $(L, *)$  is powerful also when  $p = 2$ .

Since  $l_1 * l_2 \equiv l_1 + l_2 \pmod p$ , the  $+$ - and  $*$ -cosets of  $L$  with respect to  $p \cdot L = L^{*p}$  coincide, and since  $L/p \cdot L$  is finite by assumption, we deduce that  $(L, *)$  is finitely generated. To see that  $(L, *)$  is uniform, observe that  $p^k \cdot L$  is a uniformly powerful Lie algebra for each  $k \geq 0$ , so that the arguments above apply to it equally well. Since

$$p^k L / p^{k+1} L \simeq L^{*p^k} / L^{*p^{k+1}}$$

and the order of the left hand side does not depend on  $k$  by the assumption that  $L$  is free over  $\mathbb{Z}_p$ , we deduce that  $(L, *)$  is uniform. □

*Proof of Theorem 17.10.* By construction, both of the functors  $G \mapsto L(G)$  and  $L \mapsto (L, *)$  are faithful (since they do not change the underlying set). In this situation, to show that they are inverse to each other, it is enough to verify that at least one of their composites is equal to the identity.

Let  $G$  be a uniformly powerful group with Lie algebra  $L(G)$ , which by Remark 17.8 we can identify with a Lie subalgebra

$$L(G) = \log(G) \subseteq A_0.$$

of a suitable a complete normed  $\mathbb{Q}_p$ -algebra as in Notation 17.4. Since

$$g \cdot h = \exp(\Phi(\log(g), \log(h))) = \exp(\log(g) * \log(h))$$

we see that the exponential defines an isomorphism

$$\exp: (L(G), *) \rightarrow (G, \cdot)$$

of groups. This ends the argument. □

18. ANALYTIC GROUPS

In this lecture, we begin our study of  $p$ -adic analytic groups, buildings towards the theorem of Lazard which characterizes them in terms of open uniform subgroups.

As expected from the name, we will need a little bit of analysis. We have previously studied functions defined by power series in the context of normed algebras in §13. Today, we will be only interested in functions from (the products of) the  $p$ -adics to themselves, which allows for some simplifications. For example, since  $\mathbb{Q}_p$  is commutative, it will be enough to work with the classical rings  $\mathbb{Q}_p[[X_1, \dots, X_n]]$  of power series in commutative variables, rather than their noncommutative variants.

We make a recollection of the relevant notions in this context.

**Notation 18.1.** If the number of variables  $n$  is understood from context, we often use the shorthand  $\mathbf{X}$  to denote the variables  $X_1, \dots, X_n$ . In particular, we write

$$\mathbb{Q}_p[[\mathbf{X}]] := \mathbb{Q}_p[[X_1, \dots, X_n]].$$

If  $I = (i_1, \dots, i_n) \in \mathbb{N}^{\times n}$  is a multi-index, we write

$$\mathbf{X}^I := X_1^{i_1} \dots X_n^{i_n}$$

so that a general power series can be uniquely expressed as

$$f(\mathbf{X}) = \sum_I a_I \mathbf{X}^I = \sum_{(i_1, \dots, i_n)} a_{(i_1, \dots, i_n)} X_1^{i_1} \dots X_n^{i_n}$$

with  $a_I \in \mathbb{Q}_p$ . We call the number  $i_1 + \dots + i_n$  the *degree* of a multi-index and denote it by  $\text{deg}(I)$ .

**Recollection 18.2.** If  $f(\mathbf{X})$  is a formal power series, we say that it can be *evaluated* at

$$x = (x_1, \dots, x_n) \in \mathbb{Q}_p^{\times n}$$

if the sum

$$f(x) := \sum_I a_I x^I = \sum_{(i_1, \dots, i_n)} a_i x_1^{i_1} \dots x_n^{i_n}$$

converges. In this case, we call  $f(x)$  the *value at  $x$* .

**Definition 18.3.** Let  $V \subseteq \mathbb{Q}_p^{\times n}$  be an open subset. We say a function  $f: V \rightarrow \mathbb{Q}_p$

- (1) is *analytic at  $v \in V$*  if there exists an open neighbourhood  $U \subseteq V$  and a formal power series  $F_v(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$  such that for each  $v' \in U$ ,  $F_v$  can be evaluated at  $v' - v$  and

$$F_v(v' - v) = f(v').$$

- (2) is *locally analytic* if it is analytic at  $v$  for all  $v \in V$ .

More generally, we say that function  $f: V \rightarrow \mathbb{Q}_p^{\times m}$  is *locally analytic* if each of its coordinate functions is analytic.

**Remark 18.4.** It is clear from the definition that a function  $f: V \rightarrow \mathbb{Q}_p$  is analytic at  $v \in V$  if and only if the function  $g: (V - v) \rightarrow \mathbb{Q}_p$  defined by  $g(x) := f(v + x)$  is analytic at 0. It follows that locally analytic functions are invariant under translation (in both source and target).

We now verify the basic properties of a power series locally defining an analytic function, namely that they coefficients enjoy bounded growth, and that they are unique.

**Lemma 18.5.** *Let  $f: V \rightarrow \mathbb{Q}_p$  be analytic at  $v \in V$  and let*

$$F(\mathbf{X}) = \sum_I a_I \mathbf{X}^I$$

be a power series locally defining it, so that

$$f(v') = F(v' - v)$$

in some neighbourhood of  $v$ . Then there exists an  $N \geq 0$  such that

$$|a_I|p^{-\deg(I) \cdot N} \rightarrow 0$$

as  $\deg(I) \rightarrow \infty$ .

*Proof.* Choose an  $N \geq 0$  such that

$$f(v + (p^N, \dots, p^N)) = F(p^N, \dots, p^N) = \sum_I a_I p^{\deg(I) \cdot N}.$$

Since the sum on the right is convergent by assumption, we deduce that the norms of the summands converge to zero, which gives the desired statement.  $\square$

**Corollary 18.6.** *If  $f: V \rightarrow \mathbb{Q}_p$  is locally analytic, then it is continuous.*

*Proof.* By Lemma 18.5, locally analytic functions in the sense of Definition 18.3 are locally given by a strictly analytic function in the sense of Definition 13.23 (which we defined more generally for complete normed algebras), so this is Proposition 13.26.  $\square$

**Lemma 18.7.** *Let  $f: V \rightarrow \mathbb{Q}_p$  be analytic at  $v$  and let  $F, G \in \mathbb{Q}_p[[\mathbf{X}]]$  be such that*

$$f(v') = F(v' - v) = G(v' - v)$$

for  $v'$  in some neighbourhood of  $v$ . Then  $F = G$ .

*Proof.* Considering the difference  $H := F - G$ , it's enough to show that if  $H \in \mathbb{Q}_p[[\mathbf{X}]]$  is a formal power series such that  $H(x) = 0$  for  $x$  in some neighbourhood of zero in  $\mathbb{Q}_p^{\times n}$ , then  $H = 0$ . This follows from the identity property Proposition 13.19 by induction on the number of variables, see [DDSMS03, Lemma 8.26] for details.  $\square$

One can show that locally analytic functions are closed under composition, and that the power series locally representing the composite corresponds to the algebraic composition of power series [DDSMS03, Lemma 8.5]. Moreover, they are differentiable, and the power series locally representing the derivative is given by the algebraic derivative of power series [Sch11, Proposition 6.1].

The class of locally analytic functions avoids many of the pathologies of smooth functions in the  $p$ -adic context; for example, a locally analytic function with vanishing derivative is locally constant [Sch11, Remark 6.2], so that in particular the ill-behaved function of Example 1.8 is smooth, but not locally analytic.

**Remark 18.8.** One might wonder why we call functions of Definition 18.3 *locally analytic*, while in either the real or complex setting the same definition would lead to the notion of an *analytic* function. The reason is that for many purposes, this class of functions is still too broad, due to the totally disconnected nature of the  $p$ -adics. For example, the locally constant function

$$b: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$$

given by

$$b(x) = \begin{cases} 1 & \|x\| = 1 \\ 0 & \|x\| < 1 \end{cases}$$

is locally analytic. Thus, from the point of view of locally analytic functions, the open unit disk is disconnected (and indeed it is disconnected in its  $p$ -adic topology).

In more serious approaches to adic geometry, such as Tate's theory of *rigid analytic* spaces, one works with more restricted class of functions (and a more restricted class of open coverings) which do not allow for such a decomposition and thus lead to a more interesting theory. Our

use of the term *locally analytic* is to distinguish our naive approach (which will be sufficient for our purposes) from these more involved ones.

Having define a good class of functions, we can now mimic a definition of a real or complex manifold.

**Definition 18.9.** We define a/an  $n$ -dimensional

- (1) *chart* on a topological space  $X$  to be a triple

$$(U, V, \phi),$$

where  $U \subseteq X$  is open,  $V \subseteq \mathbb{Q}_p^{\times n}$  is open, and  $\phi: U \rightarrow V$  is a homeomorphism,

- (2) *atlas* to be a collection of charts  $(U_\alpha, V_\alpha, \phi_\alpha)_{\alpha \in I}$  such that  $U_\alpha$  cover  $X$  and such that for any pair  $\alpha, \beta \in I$ , the transition function

$$\phi_\alpha^{-1}(U_\alpha \cap U_\beta) \xrightarrow{\varphi_\alpha^{-1}} U_\alpha \cap U_\beta \xrightarrow{\varphi_\beta} \phi_\beta(U_\alpha \cap U_\beta)$$

is locally analytic,

- (3)  *$p$ -adic manifold* to be a Hausdorff, second countable topological space together with a choice of a maximal atlas.

As with real or complex manifolds, given  $p$ -adic manifolds  $M$  and  $N$ , one can speak of *locally analytic* functions  $f: M \rightarrow N$ . These are functions which are locally analytic in the sense of [Definition 18.3](#) after composing with any chart of  $M$  and  $N$ .

Since locally analytic functions are differentiable,  $p$ -adic manifolds have at any point a tangent space, which is an  $n$ -dimensional  $\mathbb{Q}_p$ -vector space [[Sch11](#), §9]. These can be assembled into a tangent bundle, and locally analytic functions induces maps between tangent bundles through differentiation. Our encounter with  $p$ -adic manifolds in this course will be somewhat brief, so we will not expand on these matters.

**Example 18.10.** If  $X$  is a countable discrete topological space, then it can be made into a 0-dimensional  $p$ -adic manifold in a unique way.

**Example 18.11.** If  $V \subseteq \mathbb{Q}_p^{\times n}$  is an open subset, then it can be made into a  $p$ -adic manifold by declaring the identity  $\text{id}: V \rightarrow V$  to be a chart (and extending to a maximal atlas).

**Example 18.12.** Suppose that  $L$  is a free  $\mathbb{Z}_p$ -module of finite rank. Then  $L$  can be made into a  $p$ -adic manifold by declaring any linear isomorphism  $L \simeq \mathbb{Z}_p^{\times n} \subseteq \mathbb{Q}_p^{\times n}$  to be a chart. Any two such linear automorphisms differ by a linear transition functions, which is thus locally analytic.

The same strategy works for finite-dimensional  $\mathbb{Q}_p$ -vector spaces.

**Example 18.13.** Building on [Example 18.12](#), recall from [Theorem 9.14](#) that if  $G$  is a finitely generated uniform pro- $p$ -group, then the addition of [Definition 9.8](#) makes  $G$  into a free  $\mathbb{Z}_p$ -module of finite rank. It follows that a uniform group has a canonical structure of a  $p$ -adic manifold. Note that the dimension of  $G$  as a manifold is the same as its dimension as a group (that is, the minimal number of generators).

Our main interest is not so much in  $p$ -adic manifolds, but in the following  $p$ -adic analogue of the notion of a Lie group:

**Definition 18.14.** An  *$p$ -adic analytic group* is a topological group  $G$  together with a structure of a  $p$ -adic manifold such that

- (1) the multiplication map  $m: G \times G \rightarrow G$ ,  
 (2) the inverse map  $(-)^{-1}: G \rightarrow G$

are both locally analytic.

Using the  $p$ -adic analogue of the implicit function theorem, see [[DDSMS03](#), Theorem 6.17], one can show that the first condition implies the second one, but we will not need this fact.

**Example 18.15.** The group  $\mathrm{GL}_n(\mathbb{Q}_p)$  is a  $p$ -adic analytic Lie group of dimension  $n^2$  with respect to the manifold structure inherited as an open subset of  $M_n(\mathbb{Q}_p) \simeq \mathbb{Q}_p^{n^2}$ . Indeed, group structure is given by matrix multiplication which is defined by a polynomial formula and hence in particular a power series. This is the archetypical example of a  $p$ -adic analytic group.

**Example 18.16.** If  $G$  is  $p$ -adic analytic and  $U \leq G$  is an open subgroup, then  $U$  is also  $p$ -adic analytic (with respect to the open submanifold structure). In particular,

$$\mathrm{GL}_n(\mathbb{Z}_p) \leq \mathrm{GL}_n(\mathbb{Q}_p)$$

and its open subgroups are  $p$ -adic analytic.

**Example 18.17.** As a variation on [Example 18.15](#), the group of units in any  $\mathbb{Z}_p$ -algebra (or  $\mathbb{Q}_p$ -algebra) which is free of finite rank as a module is  $p$ -adic analytic. Looking at the endomorphism ring of the Honda formal group law, we see that the Morava stabilizer group of [Definition 12.16](#) is canonically  $p$ -adic analytic.

As we have seen in [Example 18.13](#), a uniform pro- $p$  group has a canonical structure of a  $p$ -adic manifold induced from its addition. It is natural to ask whether this structure is compatible with its multiplication, which we now verify using our hard work from previous lectures.

**Theorem 18.18.** *Let  $G$  be a uniform pro- $p$ -group. Then the manifold structure of [Example 18.13](#) makes  $G$  into a  $p$ -adic analytic group.*

*Proof.* By [Theorem 17.10](#),  $G$  can be identified with its Lie algebra  $L$  equipped with multiplication  $- * - := \Phi(-, -)$  defined by the Baker-Campbell-Hausdorff series. Since the manifold structure comes from the addition of  $G$ , which gets identified with the  $\mathbb{Z}_p$ -module structure of  $L$ , it is enough to verify that the multiplication  $*: L \times L \rightarrow L$  and the inverse  $-\mathrm{id}: L \rightarrow L$  are locally analytic.

Since  $\Phi$  can be written as power series in iterated brackets, which are polynomial (the bracket itself being bilinear and hence defined by a polynomial of degree 2), we see that  $\Phi$  gives a power series representing multiplication as needed. Similarly,  $-\mathrm{id}$  is linear and hence locally analytic.  $\square$

In the next lecture, we will prove Lazard’s beautiful characterization of  $p$ -adic analytic groups by providing a partial converse to [Theorem 18.18](#). Namely, we will show that a topological group admits a  $p$ -adic analytic structure if and only if it is *locally uniform* in the sense that it has an open uniform subgroup.

As a preparation for Lazard’s theorem in the next lecture, today we prove that admitting a  $p$ -adic analytic structure is indeed a local property in the following sense:

**Proposition 18.19.** *Let  $G$  be a topological group with open subgroup  $H \leq G$  and suppose that  $H$  has a  $p$ -adic analytic structure. Then there is at most one  $p$ -adic analytic structure on  $G$  such that the inclusion  $H \hookrightarrow G$  is locally analytic and it exists if and only if the following condition holds:*

- (1) for every  $g \in G$ , the conjugation

$$(-)^g: (gHg^{-1}) \cap H \rightarrow H$$

is locally analytic.

*Proof.* Let  $t_\alpha \in G$  be a set of representatives for cosets  $G/H$ . Then  $t_\alpha H$  forms an open cover of  $G$ . If  $G$  is  $p$ -adic analytic in a way compatible with the inclusion, then for any  $t_\alpha$  the map

$$(18.1) \quad t_\alpha \cdot -: H \rightarrow t_\alpha H$$

is a locally analytic isomorphism. This determines the  $p$ -adic manifold structure of an open cover of  $G$  and hence of  $G$  itself.

The needed condition is certainly necessary, as if  $G$  is  $p$ -adic analytic, then the conjugation map is locally analytic. We will show that it is sufficient under the simplifying assumption that  $H$  is normal. For the general case (which is almost identical, but with more involved notation) see [DDSMS03, Proposition 8.15].

The collection of products  $t_\alpha H \times t_\beta H$  form an open cover of  $G$  and hence to show that the multiplication of  $G$  is locally analytic, it is enough to verify that for each  $\alpha, \beta$ , the restricted multiplication

$$t_\alpha H \times t_\beta H \rightarrow t_\gamma H$$

is locally analytic, where  $t_\gamma$  is the representative for the coset of the product  $t_\alpha t_\beta$ . This map is given by

$$(t_\alpha h_1)(t_\beta h_2) = t_\alpha t_\beta h_1^{t_\beta} h_2 = t_\gamma (t_\gamma^{-1} t_\alpha t_\beta) h_1^{t_\beta} h_2.$$

If we declare the maps of 18.1 to be locally analytic isomorphisms, this function is analytic if and only if the map

$$H \times H \rightarrow H$$

defined by

$$(h_1, h_2) \mapsto (t_\gamma^{-1} t_\alpha t_\beta) h_1^{t_\beta} h_2$$

is locally analytic. This is a composite of multiplication, multiplication by a fixed element on the left, both of which are locally analytic, and conjugation by an element  $t_\beta \in G$ , which is locally analytic by assumption. We deduce that so is this map.  $\square$

**Remark 18.20.** We observe that a combination of Theorem 18.18 and Proposition 18.19 already gives one half of Lazard’s theorem: a topological group which has a uniform subgroup can be made  $p$ -adic analytic.

To see this, note that the  $p$ -adic manifold structure of a uniform group is uniquely determined by its addition, and hence by its multiplication and topology. It follows that the condition appearing in Proposition 18.19 is automatically satisfied: the conjugation is a continuous group automorphism and hence is linear with respect to addition and thus locally analytic.

### 19. LAZARD’S CHARACTERIZATION

In this lecture, we prove one of the main results of this course, namely Lazard’s characterization of  $p$ -adic analytic groups as those topological groups which admit an open uniform subgroup, see Theorem 19.11. As a consequence, we will be able to deduce that closed subgroups of  $p$ -adic analytic groups are themselves canonically  $p$ -adic analytic Corollary 19.14.

A key step in Lazard’s argument is an extraction of a suitable power series from an analytic group, which we describe now.

**Construction 19.1** (Local expansion of the product). Suppose that  $G$  is an  $n$ -dimensional  $p$ -adic analytic group. Translating as needed, we can find a neighbourhood  $U$  of  $e \in G$  which admits a chart

$$\phi: U \rightarrow p^k \cdot \mathbb{Z}_p^{\times n}$$

centered at the identity; that is, such that  $\phi(e) = 0$ . By assumption, the product  $m: G \times G \rightarrow G$  is locally analytic, so that the induced function

$$(\mathbb{Z}_p^{\times n})^2 \supseteq (\phi \times \phi)(m^{-1}(U) \cap U \times U) \rightarrow \phi(U) = \mathbb{Z}_p^{\times n}$$

can be expanded around zero into a collection of power series

$$F_i(\mathbf{X}, \mathbf{Y}) \in \mathbb{Q}_p[[\mathbf{X}, \mathbf{Y}]]$$

where  $1 \leq i \leq n$  in variables  $X_1, \dots, X_n$  and  $Y_1, \dots, Y_n$ .

Since the multiplication  $m$  is associative and unital with unit  $e$ ,  $F_i$  are also suitably associative and unital with unit 0. More precisely, they are an example of a formal group law, a notion which we have previously introduced in the case of dimension one in [Definition 10.1](#), and we now introduce in general.

**Definition 19.2.** Let  $R$  be a commutative ring. An  $n$ -dimensional formal group law over  $R$  is a collection of power series

$$F(\mathbf{X}, \mathbf{Y}) = (F_1(\mathbf{X}, \mathbf{Y}), \dots, F_n(\mathbf{X}, \mathbf{Y})) \in R[[\mathbf{X}, \mathbf{Y}]]^{\times n}$$

in variables  $\mathbf{X} = (X_1, \dots, X_n)$  and  $\mathbf{Y} = (Y_1, \dots, Y_n)$  such that

- (1)  $F(\mathbf{X}, 0) = \mathbf{X}$  (right unitality),
- (2)  $F(0, \mathbf{Y}) = \mathbf{Y}$  (left unitality)
- (3)  $F(F(\mathbf{X}, \mathbf{Y}), \mathbf{Z}) = F(\mathbf{X}, F(\mathbf{Y}, \mathbf{Z}))$  (associativity).

We invite the reader to make sure they are comfortable with our abusive notation above. Each of the three axioms in [Definition 19.2](#) is actually  $n$  different equations between power series in  $2n$ -variables; for example, the first one asks that

$$F_i(X_1, \dots, X_n, 0, \dots, 0) = X_i$$

and the last one that

$$F_i(F_1(\mathbf{X}, \mathbf{Y}), \dots, F_n(\mathbf{X}, \mathbf{Y}), Z_1, \dots, Z_n) = F_i(X_1, \dots, X_n, F_1(\mathbf{Y}, \mathbf{Z}), \dots, F_n(\mathbf{Y}, \mathbf{Z})).$$

for all  $1 \leq i \leq n$ .

**Example 19.3.** The local expansion of a product in an  $n$ -dimensional  $p$ -adic analytic group of [Construction 19.1](#) is an  $n$ -dimensional formal group law. This follows from the corresponding axioms of group multiplication and the fact that a local power series expansion of a function is unique.

Beware that this formal group law depends on the choice of an analytic chart around  $e \in G$  and so as a power series is not an invariant of  $G$ . One can introduce a notion of a morphism of  $n$ -dimensional formal group laws, similarly to what we have done in the case of  $n = 1$  in [Definition 10.7](#), and show that the formal group law of [Construction 19.1](#) is well-defined up to isomorphism, but we will not need it in this course.

**Lemma 19.4.** Let  $F(\mathbf{X}, \mathbf{Y})$  be an  $n$ -dimensional formal group law over a ring  $R$ . Then

$$F_i(\mathbf{X}, \mathbf{Y}) = X_i + Y_i + \text{terms of degree two and above}$$

for each  $1 \leq i \leq n$ .

*Proof.* By right unitality, we have

$$F_i(X_1, \dots, X_n, 0, \dots, 0) = X_i$$

so that

$$F_i(\mathbf{X}, \mathbf{Y}) = X_i + \text{terms divisible by } Y_k \text{ for some } 1 \leq k \leq n.$$

Similarly, by left unitality we have

$$F_i(\mathbf{X}, \mathbf{Y}) = Y_i + \text{terms divisible by } X_k \text{ for some } 1 \leq k \leq n.$$

Combining these two together yields the desired statement. □

What makes formal group laws very useful in the non-archimedean context is that the process of extracting it from an actual group can be partially reversed, as we now explain.

**Construction 19.5.** Suppose that we have an  $n$ -dimensional formal group law  $F(\mathbf{X}, \mathbf{Y})$  over the  $p$ -adic integers; ie.

$$F_i(\mathbf{X}, \mathbf{Y}) = \sum_{I, J} a_{i, I, J} \mathbf{X}^I \mathbf{Y}^J \in \mathbb{Z}_p[[\mathbf{X}, \mathbf{Y}]],$$

where  $I, J$  are multi-indices. In this case, given  $x_1, \dots, x_n, y_1, \dots, y_n \in p \cdot \mathbb{Z}_p$ , the series

$$F_i(\mathbf{x}, \mathbf{y}) = \sum_{I, J} a_{i, I, J} \mathbf{x}^I \mathbf{y}^J$$

is convergent for each  $1 \leq i \leq n$ . Since  $F$  is a formal group law, this produces an associative multiplication

$$S^{\times 2} \rightarrow S$$

with  $0 = (0, \dots, 0)$  as a two-sided unit, where  $S = p \cdot \mathbb{Z}_p^{\times n}$ .

We claim that this multiplication actually makes  $S$  into a group. To see this, observe that [Lemma 19.4](#), we have

$$(19.1) \quad F(\mathbf{x}, \mathbf{y}) \equiv \mathbf{x} + \mathbf{y} \pmod{p}.$$

It follows that

$$F(\mathbf{x}, -\mathbf{x}) \equiv 0 \pmod{p}$$

so that  $F(\mathbf{x}, -\mathbf{x}) \in p^2 \cdot \mathbb{Z}_p^{\times n}$ . We then have

$$F(\mathbf{x}, -\mathbf{x} - F(\mathbf{x}, -\mathbf{x})) = 0 \pmod{p^2}.$$

Proceeding inductively, we find an inverse of  $\mathbf{x}$  as a sum of a convergent power series.

**Remark 19.6.** Observe that as a consequence of the explicit description of the inverse as a convergent power series, if  $\mathbf{y}$  is the  $F$ -inverse of  $\mathbf{x} \in p \cdot \mathbb{Z}_p^{\times n}$  in the sense that  $F(\mathbf{x}, \mathbf{y}) = 0$ , then

$$\mathbf{y} \equiv -\mathbf{x} \pmod{p^2 \cdot \mathbb{Z}_p^{\times n}}.$$

More generally, if  $\mathbf{x} \in p^k \cdot \mathbb{Z}_p^{\times n}$ , then  $\mathbf{y} \equiv -\mathbf{x} \pmod{p^{k+1} \cdot \mathbb{Z}_p^{\times n}}$ .

The group structure on  $p \cdot \mathbb{Z}_p^{\times n}$  obtained from [Construction 19.5](#) is  $p$ -adic analytic by construction, since its multiplication is described by a convergent power series, namely the formal group law. Groups of this form are very convenient to work with and so deserve the following name:

**Definition 19.7.** Let  $F$  be an  $n$ -dimensional formal group law over  $\mathbb{Z}_p$ . The associated *standard group* is the  $p$ -adic analytic group given by

- (1)  $p \cdot \mathbb{Z}_p^{\times n}$  if  $p > 2$ ,
- (2)  $4 \cdot \mathbb{Z}_2^{\times n}$  if  $p = 2$

with the multiplication defined by  $F$  as in [Construction 19.5](#).

**Remark 19.8.** Note that even if  $p = 2$ , a formal group law over  $\mathbb{Z}_p$  defines a group structure on  $p \cdot \mathbb{Z}_p^{\times n}$ . In the context of [Definition 19.7](#), our convention of considering  $4 \cdot \mathbb{Z}_2^{\times n}$  rather than  $2 \cdot \mathbb{Z}_2^{\times n}$  has little to do with analysis and is instead made to ensure that standard groups are powerful, which has a different meaning depending on whether  $p > 2$  or  $p = 2$ . Our convention follows [\[DDSMS03\]](#), but is different from that of Bourbaki [\[Bou89, Chapter III §7.3\]](#).

**Proposition 19.9.** *As standard group of [Definition 19.7](#) is uniform of dimension  $n$ , and its analytic structure as an open subset of  $\mathbb{Z}_p^{\times n}$  coincides with the uniform  $p$ -adic analytic structure of [Theorem 18.18](#).*

*Proof.* We first show that a standard group is uniform as a topological group. It is clear from (19.1) that for each  $k \geq 2$ ,  $p^k \cdot \mathbb{Z}_p^{\times n}$  is a subgroup. These form a basis of open neighbourhoods of the identity.

We claim that these are of finite index, which is the same as their index as additive subgroups, which is  $p^{n \cdot (k-1)}$  (or  $p^{n \cdot (k-2)}$  when  $p = 2$ ). This in particular shows that a standard group is profinite. To see this, note that if  $\mathbf{x} \equiv \mathbf{y} \pmod{p^k \cdot \mathbb{Z}_p^{\times n}}$ , then

$$F(\mathbf{x}, -\mathbf{y}) \equiv 0 \pmod{p^{k+1} \cdot \mathbb{Z}_p^{\times n}}$$

which implies that  $\mathbf{x}, \mathbf{y}$  are in the same group coset. Arguing the other way, we see that multiplicative and additive cosets agree, giving the index formula.

By Lemma 19.4, we see that the series describing  $p$ -th powers in a standard group satisfies

$$(19.2) \quad F(\mathbf{X}, F(\mathbf{X}, F(\dots, \mathbf{X}) \dots)) = p \cdot \mathbf{X} + \text{terms of degree two and higher.}$$

Using an inductive argument as in the proof that a standard group admits inverses outlined in Construction 19.5 we see that the set of  $p$ -th powers of a standard group is exactly  $p^2 \cdot \mathbb{Z}_p^{\times n}$  when  $p > 2$  or  $p^3 \cdot \mathbb{Z}_p^{\times n}$  when  $p = 2$ . This shows that the standard group is finitely generated. To see that it is powerful, observe that by Lemma 19.4, if  $\mathbf{x}, \mathbf{y} \in p^k \cdot \mathbb{Z}_p^{\times n}$ , then

$$F(\mathbf{x}, \mathbf{y}) \equiv \mathbf{x} + \mathbf{y} \pmod{p^{2k} \cdot \mathbb{Z}_p^{\times n}},$$

so that the  $F$ -multiplication agrees with addition modulo  $p^2 \cdot \mathbb{Z}_p^{\times n}$  for  $p > 2$  and  $p^4 \cdot \mathbb{Z}_p^{\times n}$  for  $p = 2$ .

Uniformity and the given dimension are immediate consequences of the index formula for the subgroups  $p^k \cdot \mathbb{Z}_p^{\times n}$ .

We are left with comparing the analytic structures. Since the analytic structure of a uniform group appearing in Theorem 18.18 is induced from its additive structure, it is enough to check that the uniform addition of Definition 9.8 yields, when applied to a multiplication on  $p \cdot \mathbb{Z}_p^k$  (or  $p^2 \cdot \mathbb{Z}_p^{\times n}$  when  $p = 2$ ) induced by  $F$ , the standard addition of  $p$ -adic numbers. By inspection, this follows from (19.2) and Lemma 19.4.  $\square$

We will deduce from Proposition 19.9 by showing that, locally, any  $p$ -adic analytic group is standard.

**Proposition 19.10.** *Let  $G$  be a  $p$ -adic analytic group. Then there exists an open subgroup  $H \leq G$  which is isomorphic to a standard group in the sense of Definition 19.7.*

*Proof.* Using Construction 19.1, we can find an open neighbourhood of the identity  $U \subseteq G$  which admits a chart  $\phi: U \rightarrow p^k \cdot \mathbb{Z}_p^{\times n}$  in which the multiplication is expressed by a formal group law

$$F_i(\mathbf{X}, \mathbf{Y}) \in \mathbb{Q}_p = \sum_{I, J} a_{i, I, J} \mathbf{X}^I \mathbf{Y}^J \in \mathbb{Q}_p[[\mathbf{X}, \mathbf{Y}]]$$

By Lemma 18.5, there exists a  $k' \geq k$  such that  $F_i$  are convergent on  $p^{k'} \cdot \mathbb{Z}_p^{\times n}$ , so that

$$\|a_{i, I, J} p^{k' \cdot (\deg(I) + \deg(J))}\| \rightarrow 0$$

as  $\deg(I) + \deg(J) \rightarrow \infty$ , for each  $1 \leq i \leq n$ . By making the chart smaller if necessary, we can assume that  $k = k'$ , so that the formal power series converges on the whole chart.

Suppose that we change the chart  $\phi: U \rightarrow p^k \cdot \mathbb{Z}_p^{\times n}$  to  $\psi := \frac{1}{p^k} \cdot \phi$ , so that  $\psi: U \rightarrow \mathbb{Z}_p^{\times n}$ . This changes the coefficients of the formal group law by

$$a_{i, I, J} \mapsto a_{i, I, J} \cdot p^{k \cdot (\deg(I) + \deg(J) - 1)}.$$

Thus, by making this substitution, we can assume that  $k = 0$  and that

$$\|a_{i, I, J}\| \rightarrow 0.$$

In particular, all but finitely many coefficients are  $p$ -adic integers. We will now modify the chart again so that all of the coefficients are integral.

Note that since 0 is a unit, there are no constant terms, and the linear terms are already integers by [Lemma 19.4](#). Let  $w$  be the minimum of the  $p$ -adic valuations of  $a_{i,I,J}$  with  $\deg(I) + \deg(J) \geq 2$ . By first restricting the chart to  $p^w \cdot \mathbb{Z}_p^{\times n}$  and then replacing it by  $\psi' := \frac{1}{p^w} \psi$ , the above formula for the change of coefficients shows that they are all integral.

By construction, the preimage under the new chart  $\psi'$  of  $p \cdot \mathbb{Z}_p^{\times n}$  when  $p > 2$  or  $p^2 \cdot \mathbb{Z}_p^{\times n}$  is a standard group, since it has multiplication defined by an integral formal group law.  $\square$

The following is the main result of this lecture, and one of the main results of this course.

**Theorem 19.11** (Lazard). *For a topological group  $G$ , the following are equivalent:*

- (1)  $G$  admits a structure of a  $p$ -adic analytic group compatible with its topology,
- (2)  $G$  is locally uniform in the sense that it has an open subgroup  $H \leq G$  which is a uniform pro- $p$ -group of rank equal to the dimension of  $G$ ,
- (3)  $G$  is locally a pro- $p$  group of finite rank in the sense that it has an open subgroup which is a pro- $p$ -group of finite rank.

*Proof.* The implication (1)  $\Rightarrow$  (2) is a combination of [Proposition 19.9](#) and [Proposition 19.10](#). That (2)  $\Rightarrow$  (1) holds is a consequence of [Theorem 18.18](#) and [Proposition 18.19](#), as explained in [Remark 18.20](#).

The equivalence of (2) and (3) is [Theorem 6.12](#) and [Proposition 7.4](#).  $\square$

**Remark 19.12** (Groups with  $p$ -valuations). While we attribute [Theorem 19.11](#) to Lazard, who started the serious study of  $p$ -adic analytic groups and was first to prove a variant of it. However, we note that Lazard worked in slightly different terms than the one presented in this course.

In more detail, Lazard worked with groups equipped with  $p$ -valuations, which are maps

$$v: G \setminus \{e\} \rightarrow \mathbb{R}_{>0}$$

satisfying a variety of conditions (some of which relate to  $p$ -th powers, hence “ $p$ ” in the name), see [[Sch11](#), §23]. He then showed that a group is  $p$ -adic analytic if and only if it has an open subgroup admitting a certain kind of  $p$ -valuation, see [[Sch11](#), Theorem 27.1] (or better yet, the original works of Lazard [[Laz65](#)], who wrote in French).

In our account, the technical notion of valuations is replaced by the theory of powerful and uniformly powerful groups and their lower  $p$ -series. This approach, while equivalent in some respects, is much more recent, as powerful groups were introduced by Lubotzky and Mann in [[LM87a](#)] and uniformly powerful groups by Dixon, Du Sautoy, Mann and Segal in [[DDSMS03](#)].

While [Theorem 19.11](#) gives a characterization of groups which can be made  $p$ -adic analytic in concrete, group-theoretic terms, it is also natural to ask about the uniqueness of the resulting analytic structure. Here, we have the following striking result:

**Theorem 19.13** (Lazard). *The forgetful functor from  $p$ -adic analytic groups and locally analytic homomorphisms into topological groups is fully faithful. In particular:*

- (1) if a topological group admits a  $p$ -adic analytic structure, then it admits a unique one,
- (2) all continuous maps between  $p$ -adic analytic groups are locally analytic.

*Proof.* It is enough to prove the second assertion, so let  $G_1$  and  $G_2$  be  $p$ -adic analytic and let  $f: G_1 \rightarrow G_2$  be a continuous map. Since being locally analytic is a local property and  $f$  is a group homomorphism, it is enough to verify that  $f$  is locally analytic on some open subgroup. By a combination of [Proposition 19.9](#) and [Proposition 19.10](#), we can thus assume that  $G_1$  and  $G_2$  are uniform groups equipped with their analytic structures of [Theorem 18.18](#).

Since  $f$  is a continuous group homomorphism, it preserves the uniform addition of [Definition 9.8](#) in the sense that

$$f(g +_{G_1} h) = f(g) +_{G_2} f(h).$$

It follows that it is linear in additive coordinates of [Example 18.13](#) and hence locally analytic.  $\square$

**Corollary 19.14** (Closed subgroup theorem). *If  $G$  is  $p$ -adic analytic, then any closed subgroup  $K \leq G$  admits a unique  $p$ -adic analytic structure such that the inclusion  $K \hookrightarrow G$  is locally analytic.*

*Proof.* The third characterization in [Theorem 19.11](#) is clearly closed under passing to closed subgroups, so that  $K$  admits a  $p$ -adic analytic structure. This structure is unique and the inclusion is locally analytic by [Theorem 19.13](#).  $\square$

**Remark 19.15.** The analogues of [Theorem 19.13](#) and [Corollary 19.14](#) are also true in the classical setting of real Lie groups, see [[Lee](#), [Theorem 20.12](#)].

Note that all group homomorphisms between uniform groups are continuous, as a consequence of Serre’s [Theorem 4.1](#) and [Corollary 4.2](#). Thus, for compact  $p$ -adic analytic groups, [Theorem 19.13](#) has the following striking variant:

**Theorem 19.16.** *The forgetful functor from the category of compact  $p$ -adic analytic groups and locally analytic homomorphisms into the category of groups is fully faithful.*

## 20. COHOMOLOGY OF PROFINITE GROUPS

One of the reasons why it is often important to establish that a given group is  $p$ -adic analytic is that they have excellent cohomological properties, which in many ways mirror the behaviour of cohomology of finite-dimensional manifolds. In this lecture, we begin our study with a recollection on cohomology of profinite groups in general.

If  $G$  is a topological group, then a *topological  $G$ -module* is a topological abelian group  $M$  together with a continuous action of  $G$ , ie. with the property that the action map  $G \times M \rightarrow M$  is continuous. To a topological  $G$ -module, one can associate a sequence of groups

$$M \mapsto H^*(G, M)$$

given by (continuous) *cohomology of  $G$  with coefficients in  $M$* .

These cohomology groups can be defined in a variety of different ways, perhaps the most flexible of which is the use of condensed mathematics of [[Sch19](#)] (in which case  $M$  can be more generally a condensed  $G$ -module). However, most important properties of group cohomology are arguably already visible when  $M$  has discrete topology, and so to avoid complexity, today we will only work with cohomology in this special case.

**Definition 20.1.** Let  $G$  be a profinite group. A *discrete  $G$ -module* is an abelian group  $M$  together with a left action of  $G$  such that the action map  $G \times M \rightarrow M$  is continuous if we equip  $M$  with the discrete topology.

We denote the category of discrete  $G$ -modules and equivariant maps by  $\text{Mod}_G(\text{Ab})$ .

**Remark 20.2.** The condition of being a discrete  $G$ -module can be phrased purely algebraically. Namely, it asks that for any  $m \in M$ , the map  $G \rightarrow M$  given by

$$g \rightarrow g \cdot m$$

is locally constant and hence factors through a finite quotient of  $G$ . This is equivalent to the stabilizer subgroup  $\text{Stab}(m) \leq G$  being open. Thus, an abelian group with a  $G$ -action is a discrete  $G$ -module if and only if

$$M = \bigcup_{U \leq G} M^U,$$

where the union is taken over all open subgroups of  $G$ .

Observe that a diagram  $X: I \rightarrow \text{Mod}_G(\text{Ab})$  of discrete  $G$ -modules can be identified with an action of  $G$  on  $X$  considered as a functor valued in the category of abelian groups. It follows that the limit  $\varprojlim X$  and colimit  $\varinjlim X$  calculated in the category of abelian groups have an induced action of  $\hat{G}$ . Moreover, one verifies using [Remark 20.2](#) that

- (1) the colimit  $\varinjlim X$  is again a discrete  $G$ -module,
- (2) the limit  $\varprojlim X$  is again a discrete  $G$ -module if the diagram  $I$  is finite.

This implies the following:

**Lemma 20.3.** *The category  $\text{Mod}_G(\text{Ab})$  of discrete  $G$ -modules is abelian. Moreover, the forgetful functor into abelian groups is exact and preserves filtered colimits.*

Recall that an abelian category is said to be *Grothendieck* if it has exact filtered colimits and is generated under colimits by a set of objects. We now verify that  $\text{Mod}_G(\text{Ab})$  is Grothendieck.

**Lemma 20.4.** *Objects of the form  $\mathbb{Z}[G/U]$ , where  $U \triangleleft G$  is a normal open subgroup of  $G$ , generate  $\text{Mod}_G(\text{Ab})$  under colimits.*

*Proof.* If  $M$  is a discrete  $G$ -module and  $m \in M$  is an element, then by [Remark 20.2](#) there exists an open normal  $U \triangleleft G$  such that  $m \in M^U$ . It follows  $m$  is in the image of a map  $\mathbb{Z}[G/U] \rightarrow M$ . Finding such a map for every  $m \in M$ , we deduce that  $M$  is a quotient of a suitably large direct sum of modules of the needed form, which implies the claim.  $\square$

**Proposition 20.5.** *The category  $\text{Mod}_G(\text{Ab})$  of discrete  $G$ -modules is Grothendieck abelian and the forgetful functor  $\text{Mod}_G(\text{Ab}) \rightarrow \text{Ab}$  is an exact left adjoint.*

*Proof.* The first part is a combination of [Lemma 20.3](#) and [Lemma 20.4](#). The second follows from [Lemma 20.3](#) since any cocontinuous functor between Grothendieck categories is a left adjoint.  $\square$

**Warning 20.6.** Beware that a limit of discrete  $G$ -modules, calculated in abelian groups, need not be discrete. In terms of [Proposition 20.5](#), this is saying that the forgetful functor need not preserve infinite limits.

For a specific example, recall from [Definition 14.1](#) that the ( $p$ -adic) completed group algebra of a profinite group  $G$  is defined as

$$\mathbb{Z}_p[[G]] := \varprojlim \mathbb{Z}_p[G/U],$$

where the limit is taken over the poset of open subgroups  $U \leq G$ . Each of  $\mathbb{Z}_p[G/U]$  is a discrete  $G$ -module, but the completed group algebra itself is not unless  $G$  is finite: the stabilizer of  $1 \in \mathbb{Z}_p[[G]]$  is the trivial group.

The forgetful functor appearing in [Proposition 20.5](#) can be identified with *restriction* of representations along the unique map  $1 \rightarrow G$  from the trivial group. More generally, given a closed subgroup  $H \leq G$ , we have a restriction (ie. forgetful) functor

$$\text{res}_H^G: \text{Mod}_G(\text{Ab}) \rightarrow \text{Mod}_H(\text{Ab})$$

and this is also an exact left adjoint, as a consequence of [Proposition 20.5](#). It will be useful to have an explicit description of the right adjoint, which we give now.

**Definition 20.7.** Let  $G$  be a profinite group,  $H \leq G$  a closed subgroup and let  $M$  be a discrete  $H$ -module. The *coinduced  $G$ -module* is given by

$$\text{coind}_H^G(M) := \text{map}_{cts}^H(G, M) = \{ f: G \rightarrow M \mid f \text{ is continuous, } \forall h \in H, g \in G f(h \cdot g) = h \cdot f(g) \}$$

the module of continuous,  $H$ -equivariant maps, with  $G$ -action defined by

$$(g \cdot f)(g_0) := f(g_0g).$$

The following is a fundamental property of coinduction.

**Lemma 20.8.** *The coinduction functor  $\text{coind}_H^G: \text{Mod}_H(\text{Ab}) \rightarrow \text{Mod}_G(\text{Ab})$  is exact and preserves filtered colimits.*

*Proof.* One can show that the quotient map  $G \rightarrow G/H$  (of topological spaces) admits a continuous section  $s: G/H \rightarrow G$ , see [Ser97, §1.2, Proposition 1], which we can think of as a continuous choice of representatives for each coset.

Since an  $H$ -equivariant map  $G \rightarrow M$  is uniquely determined by its values at the set of representatives, any choice of a section  $s$  determines an isomorphism of abelian groups

$$\text{coind}_H^G(M) \simeq \text{map}_{cts}(G/H, M).$$

As  $M$  is equipped with the discrete topology, the right hand side is the module of locally constant functions. This can be written as a filtered colimit of functions constant with respect to a chosen open cover, with the colimit taken over the poset of all open covers. Since filtered colimits and finite products are exact and commute with filtered colimits in the category of abelian groups, we deduce that  $M \mapsto \text{map}_{cts}(G/H, M)$  has these properties as well.  $\square$

We recall the classical fact that restriction and coinduction functors form an adjunction of signature

$$\text{res}_H^G: \text{Mod}_G(\mathcal{A}b) \rightleftarrows \text{Mod}_H(\mathcal{A}b): \text{coind}_H^G.$$

**Construction 20.9.** Suppose that  $M$  is a  $G$ -module,  $N$  is an  $H$ -module and that we have an  $H$ -equivariant map  $\phi: M \rightarrow N$ , which we can identify with a morphism  $\text{res}_H^G(M) \rightarrow N$  in  $\text{Mod}_H(\mathcal{A}b)$ . We can then define a map  $\psi: M \rightarrow \text{coind}_H^G(N)$  by

$$\psi(m)(g) = \phi(gm).$$

One then verifies that the construction  $\phi \mapsto \psi$  define a natural isomorphism

$$\text{Hom}_{\text{Mod}_H(\mathcal{A}b)}(\text{res}_H^G(M), N) \simeq \text{Hom}_{\text{Mod}_G(\mathcal{A}b)}(M, \text{coind}_H^G(N)).$$

**Remark 20.10.** The restriction functor between categories of discrete modules does not have a left adjoint in general, as it may fail to preserve limits. However, it does have a left adjoint when  $H \leq G$  is open, given by the classical *induced representation* construction. Concretely, if we identify abelian groups with a  $G$ -action with  $\mathbb{Z}[G]$ -modules, the left adjoint is given by

$$\text{ind}_H^G(M) := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M.$$

One can verify directly that this is a discrete  $G$ -module if  $M$  is a discrete  $H$ -module.

**Remark 20.11** (Induction and coinduction are isomorphic). If  $H \leq G$  is of finite index, then as we observed in Remark 20.10, the restriction functor has both left and right adjoints, given by induction and coinduction. These two are naturally isomorphic; that is, for any  $M \in \text{Mod}_H(\mathcal{A}b)$ , there is a canonical isomorphism

$$\text{ind}_H^G(M) \simeq \text{coind}_H^G(M).$$

After unwrapping the definition, we see that we have to produce a canonical map

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \rightarrow \text{map}_{cts}^H(G, M).$$

By adjunction, such a map is determined by a map  $\psi: M \rightarrow \text{map}_{cts}^H(G, M)$  of discrete  $H$ -modules, which we define by

$$\psi(m)(g) = \begin{cases} gm, & g \in H \\ 0 & \text{otherwise} \end{cases}$$

A direct calculation shows the induced morphism of  $G$ -modules is an isomorphism.

We want to define the cohomology groups of a profinite group as derived functors of the *invariants* functor

$$M \in \text{Mod}_G(\mathcal{A}b) \mapsto M^G \in \mathcal{A}b.$$

A convenient way to do this is to observe that if we equip  $\mathbb{Z}$  with the trivial  $G$ -action, then we have a canonical isomorphism

$$\mathrm{Hom}_{\mathrm{Mod}_G(\mathcal{A}b)}(\mathbb{Z}, M) \simeq M^G.$$

This motivates the following definition.

**Definition 20.12.** Let  $G$  be a profinite group and  $M$  a discrete  $G$ -module. The *continuous cohomology groups with coefficients in  $M$*  are given by extension groups

$$H^s(G, M) := \mathrm{Ext}_{\mathrm{Mod}_G(\mathcal{A}b)}^s(\mathbb{Z}, M)$$

in the category of discrete  $G$ -modules.

Continuous cohomology groups are often denoted with subscript “cts”, ie. one writes

$$H_{cts}^s(G, M) = H^s(G, M)$$

to emphasize that this depends on the topology of  $G$ . To avoid clutter, we omit the subscript, since there is no other kind of group cohomology we will consider in this course.

**Remark 20.13.** If  $G$  is finite, then  $\mathrm{Mod}_G(\mathcal{A}b)$  is just the category of all  $G$ -representations in abelian groups and [Definition 20.12](#) reduces to cohomology of finite groups in the usual sense.

**Construction 20.14.** The cohomology groups are covariantly functorial in continuous maps. To see this, suppose that  $f: G_1 \rightarrow G_2$  is a continuous map of profinite groups. Then, via restriction, any discrete  $G_2$ -module yields a discrete  $G_1$ -module, providing an exact, cocontinuous functor

$$\mathrm{res}(f): \mathrm{Mod}_{G_1}(\mathcal{A}b) \rightarrow \mathrm{Mod}_{G_2}(\mathcal{A}b).$$

Since  $\mathrm{res}(f)(\mathbb{Z}) \simeq \mathbb{Z}$ , where both sides have the trivial action, the morphism on Ext-groups induced by  $\mathrm{res}(f)$  provides a natural transformation

$$\mathrm{res}_M: H^*(G_1, M) \rightarrow H^*(G_2, \mathrm{res}(f)(M)).$$

called the *restriction*.

We now show that [Definition 20.12](#) is equivalent to a construction of cohomology groups in terms of group cochains.

**Lemma 20.15** (Shapiro’s lemma). *Let  $H \leq G$  be a closed subgroup and let  $M$  be a discrete  $H$ -module. Then there is a natural isomorphism*

$$H^s(G, \mathrm{coind}_H^G(M)) \simeq H^s(H, M).$$

*Proof.* Since  $\mathrm{coind}_H^G(-)$  is exact by [Lemma 20.8](#), the left hand side can be identified with derived functors of

$$M \mapsto H^0(G, \mathrm{coind}_H^G(M)).$$

Thus, it is enough to construct the needed natural isomorphism when  $s = 0$ . We have an identification

$$H^0(G, \mathrm{coind}_H^G(M)) \simeq (\mathrm{map}_{cts}^H(G, M))^G$$

and we observe that a function  $G \rightarrow M$  is a fixed point for the  $G$  action on the source if and only if it is constant. However, a constant function is  $H$ -equivariant if and only if its value is fixed by  $H$ , so that

$$\mathrm{map}_{cts}^H(G, M)^G \simeq M^H.$$

□

**Construction 20.16** (Coinduction complex). The adjunction  $\text{res}_1^G \dashv \text{coind}_1^G$  induced by the inclusion of the trivial subgroup determines a monad  $S := \text{coind}_H^G \circ \text{res}_H^G$  on  $\text{Mod}_G(\mathcal{A}b)$  and thus for any discrete  $G$ -module  $M$  we obtain an augmented cosimplicial object

$$(20.1) \quad M \rightarrow S(M) \rightrightarrows S^2(M) \rightrightarrows \dots$$

This in turn determines a cochain complex of discrete  $G$ -modules of the form

$$S(M) \rightarrow S^2(M) \rightarrow S^3(M) \rightarrow \dots$$

where the differentials are given by alternating sums of coboundary maps of (20.1), together with an augmentation map  $M \rightarrow S(M)$ .

**Definition 20.17.** The *group cochain complex* associated to  $M$  is the complex of abelian groups

$$C^s(G, M) := (S^{s+1}(M))^G$$

obtained by taking invariants in the complex of [Construction 20.16](#).

**Remark 20.18** (Explicit form of group cochains). By unwrapping the definition of coinduction, the complex of discrete  $G$ -modules of [Construction 20.16](#) can be rewritten as

$$\text{map}_{cts}(G, M) \rightarrow \text{map}_{cts}(G \times G, M) \rightarrow \text{map}_{cts}(G \times G \times G, M) \rightarrow \dots$$

Applying invariants, we see that the group cochain complex is of the form

$$(20.2) \quad M \rightarrow \text{map}_{cts}(G, M) \rightarrow \text{map}_{cts}(G \times G, M) \rightarrow \dots$$

With enough patience, one can calculate that in these terms the differential

$$d: C^s(G, M) \rightarrow C^{s+1}(G, M)$$

is given by the formula

$$(df)(g_1, \dots, g_{s+1}) = g_1 f(g_2, \dots, g_{s+1}) + \sum_{1 \leq i \leq s} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{s+1}) + (-1)^{s+1} f(g_1, \dots, g_s).$$

**Proposition 20.19.** *Let  $M$  be a discrete  $G$ -module. Then the groups  $H^*(G, M)$  of [Definition 20.12](#) can be calculated as cohomology of the group cochain complex of (20.2).*

*Proof.* By construction, the cosimplicial object used to define the coinduction complex of [Construction 20.16](#) is split after applying  $\text{res}_1^G: \text{Mod}_G(\mathcal{A}b) \rightarrow \mathcal{A}b$ , and hence the resulting augmented complex is exact as a complex of abelian groups. It follows that it is exact and hence can be thought of as a resolution of  $M$ .

To check that the Ext-group defining group cohomology can be calculated using this resolution it is enough to verify that

$$H^s(G, \text{coind}_1^G(M)) \simeq \text{Ext}_{\text{Mod}_G(\mathcal{A}b)}^s(\mathbb{Z}, \text{coind}_1^G(M))$$

vanishes for  $s > 0$ . By Shapiro’s [Lemma 20.15](#), this can be identified with

$$H^s(1, M) \simeq \text{Ext}_{\mathcal{A}b}^s(\mathbb{Z}, M)$$

which vanishes in positive degrees since  $\mathbb{Z}$  is projective as an abelian group. □

**Remark 20.20.** If  $f: G_1 \rightarrow G_2$  is a continuous homomorphism of profinite groups, then composing with products of  $f$  yields a map of chain complexes

$$C^*(G_1, M) \rightarrow C^*(G_2, M),$$

where on the right hand side we consider  $M$  with the restricted  $G_2$ -action. The induced map on cohomology coincides with the one obtained through abstract considerations of [Construction 20.14](#).

**Example 20.21** (Zero-th cohomology). After retracing the definitions, we see that the first differential

$$d: M \rightarrow \text{map}_{cts}(G, M)$$

in the group cochain complex is given by the formula

$$d(m)(g) = g \cdot m - m.$$

Thus, the kernel of the first differential is exactly the subgroup of invariants.

**Example 20.22** (First cohomology). The second differential  $d: \text{map}_{cts}(G, M) \rightarrow \text{map}_{cts}(G^2, M)$  in the group cochain complex is given by

$$d(f)(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1)$$

It follows that the 1-cocycles are given by those continuous maps  $f: G \rightarrow M$  such that

$$f(g_1 g_2) = g_1 f(g_2) + f(g_1).$$

Such maps are called *crossed homomorphisms*. In the special case when the action of  $G$  on  $M$  is trivial, these are precisely the group homomorphisms  $G \rightarrow M$ .

A *principal* crossed homomorphism is one of the form  $f(g) = g \cdot m - m$  for some  $m \in M$ . These are precisely the 1-boundaries, so by [Proposition 20.19](#) the first cohomology group  $H^1(G, M)$  is the quotient group of crossed homomorphism modulo the principal ones. If the action of  $G$  on  $M$  is trivial, then only the zero crossed homomorphism is principal, so that

$$H^1(G, M) \simeq \text{Hom}_{grp}(G, M).$$

Another consequence of [Proposition 20.19](#) is that formation of continuous group cohomology is compatible with filtered colimits. Using this, we will be able to show that it can be calculated in terms of cohomology of finite groups.

**Corollary 20.23.** *For any  $s \geq 0$ , the functor  $M \mapsto H^s(G, M)$  preserves filtered colimits.*

*Proof.* This is immediate from [Proposition 20.19](#), since taking cohomology of cochain complex, the invariants functor and coinduction all preserve filtered colimits, the last one by [Lemma 20.8](#).  $\square$

Note that if  $M$  is a discrete  $G$ -module and  $H \leq G$  is a closed normal subgroup, then the  $H$ -invariants  $M^H$  are again a discrete  $G$ -module. In fact, since  $H$  acts trivially, they are a discrete  $G/H$ -module. We thus obtain a canonical map

$$H^s(G/H, M^U) \rightarrow H^s(G, M^U) \rightarrow H^s(G, M)$$

where the first arrow is functoriality in the group and the second one is induced by the inclusion  $M^H \hookrightarrow M$ .

**Proposition 20.24.** *For any discrete  $G$ -module  $M$  and any  $s \geq 0$ , we have*

$$H^s(G, M) \simeq \varinjlim H^s(G/U, M^U).$$

where the colimit is taken over the (opposite of) the poset of open normal subgroups  $U \triangleleft G$ .

*Proof.* Since both sides commute with filtered colimits in  $M$  by [Corollary 20.23](#) and  $M$  is a filtered colimit of its finitely generated submodules, we can assume that  $M$  is finitely generated as a discrete  $G$ -module.

Since each of the finitely many generators of  $M$  is stabilizer by an open subgroup by [Remark 20.2](#), we deduce that if  $U$  is sufficiently small, then  $M = M^U$ . Restricting to the subposet of such open subgroups  $V$ , we only have to show that

$$H^s(G, M) \simeq \varinjlim H^s(G/V, M).$$

By [Proposition 20.19](#), we can calculate both sides by the group cochain complex, and the needed claim follows from the fact that

$$\text{map}_{cts}(G^s, M) \simeq \varinjlim \text{map}((G/V)^s, M)$$

since any locally constant function  $G^s \rightarrow M$  factors through  $(G/V)^s$  for small enough  $V$ .  $\square$

### 21. COHOMOLOGICAL DIMENSION AND MOD $p$ COHOMOLOGY

In this lecture, we will introduce the notion of cohomological dimension of a profinite group. We will show that the dimension depends only on the  $p$ -Sylow subgroups, and relate it in the case of pro- $p$ -groups to their mod  $p$  cohomology ring. Finally, we will relate the low dimensional cohomology groups to generators and relations of the group itself.

Today, we will be only interested in cohomology with coefficients in *torsion*  $G$ -modules, which admit a canonical decomposition along primes as we now describe.

**Remark 21.1.** Suppose that  $M$  is a discrete  $G$ -module which is torsion as an abelian group. We then have a direct sum decomposition

$$M \simeq \bigoplus_p M[p^\infty],$$

into  $p$ -torsion parts for different primes  $p$ , which yields a cohomology decomposition

$$H^*(G, M) \simeq \bigoplus_p H^*(G, M[p^\infty]),$$

where we use that cohomology of a profinite group commutes with arbitrary direct sums as it commutes with finite products and filtered colimits, the latter by [Corollary 20.23](#).

It follows from [Remark 21.1](#) that when studying cohomology with coefficients in torsion modules, we can fix a prime and consider only  $p$ -torsion modules. This makes the following definition very natural:

**Definition 21.2.** Let  $G$  be a profinite group. We say that  $G$  is of  $(p)$ -cohomological dimension

- (1) *at most*  $n$ , denoted by  $\text{cd}_p(G) \leq n$ , if

$$H^s(G, A) = 0$$

for any  $p$ -torsion discrete  $G$ -module  $A$  and any  $s > n$ ,

- (2) *exactly*  $n$ , denoted by  $\text{cd}_p(G) = n$ , if  $\text{cd}_p(G) \leq n$  but  $\text{cd}_p(G) \not\leq n - 1$ ,
- (3) *infinity* if  $\text{cd}_p(G) \not\leq n$  for any finite  $n$ .

**Notation 21.3.** Throughout the rest of the lecture, we consider the prime  $p$  to be fixed and call  $p$ -cohomological dimension simply *cohomological dimension*.

We will be interested in how cohomological dimension of a group interacts with dimensions of its subgroups. We first observe that we have an easy inequality going in one direction.

**Lemma 21.4.** *Let  $G$  be a profinite group and  $H \leq G$  a closed subgroup. Then*

$$\text{cd}_p(H) \leq \text{cd}_p(G).$$

*Proof.* If  $A$  is a  $p$ -torsion discrete  $H$ -module, then  $\text{coind}_H^G(A)$  is a  $p$ -torsion discrete  $G$ -module. Then

$$H^s(H, A) \simeq H^s(G, \text{coind}_H^G(A))$$

by Shapiro's [Lemma 20.15](#) and the claim follows.  $\square$

Similarly, one can bound the cohomological dimension of an extension using the dimensions of the factors. This requires the use of an important spectral sequence which we recall now.

**Construction 21.5** (Lyndon-Hochschild-Serre spectral sequence). Let  $G$  be a profinite group with closed normal subgroup  $N \triangleleft G$ , so that  $G/N$  is again a profinite group. If  $M$  is a discrete  $G$ -module, then  $M^N$  has an induced action of the quotient group  $G/N$ . Moreover, there is a canonical isomorphism

$$M^G \simeq (M^N)^{G/N};$$

in other words, the diagram

$$(21.1) \quad \begin{array}{ccc} \text{Mod}_G(\mathcal{A}b) & \xrightarrow{(-)^G} & \mathcal{A}b \\ & \searrow^{(-)^N} & \nearrow^{(-)^{G/N}} \\ & & \text{Mod}_{G/N}(\mathcal{A}b) \end{array}$$

commutes. If  $A$  is an abelian group, then

$$(\text{coind}_1^G(A))^N \simeq \text{map}_{cts}(G, A)^N \simeq \text{map}_{cts}(G/N, A),$$

so that the left vertical arrow in (21.1) takes  $H^0(G, -)$ -acyclics to  $H^0(G/N, -)$ -acyclics. We thus have a Grothendieck spectral sequence of a composite of derived functors which is of signature

$$H^s(G/N, H^t(N, M)) \Rightarrow H^{s+t}(G, M).$$

This is known as the *Lyndon-Hochschild-Serre spectral sequence*.

**Lemma 21.6.** *Let  $G$  be a profinite group and  $N \triangleleft G$  a closed normal subgroup. Then*

$$\text{cd}_p(G) \leq \text{cd}_p(N) + \text{cd}_p(G/N).$$

*Proof.* If  $A$  is a  $p$ -torsion discrete  $G$ -module, then  $H^t(N, M)$  is a discrete  $p$ -torsion  $G$ -module for any  $t$ . Thus, all of the terms on the second page of the Lyndon-Hochschild-Serre spectral sequence

$$H^s(G/N, H^t(N, M)) \Rightarrow H^{s+t}(G, M).$$

vanish when  $s > \text{cd}_p(G/N)$  or  $t > \text{cd}_p(N)$ . In particular, they vanish when  $s + t > \text{cd}_p(G/N) + \text{cd}_p(N)$ , which implies the desired statement.  $\square$

**Warning 21.7.** Beware that while being of finite cohomological dimension is stable under subgroups and extensions, as we observed above, it is most decidedly not stable under taking quotients! For example,  $\mathbb{Z}_p$  is of finite cohomological dimension but  $\mathbb{Z}/p\mathbb{Z}$  is not, see [Example 21.15](#) and [Example 21.18](#) below.

Recall from [Lemma 3.8](#) that any profinite group  $G$  has a Sylow  $p$ -subgroups  $S \leq G$ , which is a closed subgroup such that

- (1)  $S$  is pro- $p$ ,
- (2)  $G/S$  is a limit of finite groups of order coprime to  $p$ .

Moreover, any two such subgroups are conjugate. We will now show that the notion of  $p$ -cohomological dimension depends only on the  $p$ -Sylow subgroup. This requires us to introduce the *covariant* functoriality of group cohomology.

**Construction 21.8.** Let  $G$  be a profinite group,  $U \leq G$  an open subgroup and  $M$  a discrete  $G$ -module. Recall that associated to (the restriction of)  $M$  we have a coinduced modules

$$\text{coind}_U^G(M) := \text{map}_{cts}^U(G, M)$$

of  $U$ -equivariant continuous maps, with  $G$ -acting on the source by right multiplication. We define a map of discrete  $G$ -modules

$$(21.2) \quad \pi: \text{coind}_U^G(M) \rightarrow M$$

by

$$\pi(f) = \sum_i x_i^{-1} f(x_i)$$

where  $x_i$  is any set of representatives for left cosets  $U \backslash G$ . This does not depend on the choice of representatives, since if  $x_i = ux'_i$ , then

$$x_i^{-1} f(x_i) = (x'_i)^{-1} u^{-1} f(ux'_i) = (x'_i)^{-1} u^{-1} u f(x'_i) = (x'_i)^{-1} f(x'_i),$$

where we've used that  $f$  is  $U$ -equivariant. Applying  $G$ -cohomology functor to (21.2) and using Shapiro's Lemma 20.15 we obtain a map

$$(21.3) \quad \text{cores} : H^*(U, M) \rightarrow H^*(G, M).$$

**Remark 21.9.** As we observed in Remark 20.11, if  $U \leq G$  is open, then there is a canonical isomorphism

$$\text{coind}_U^G(M) \simeq \text{ind}_U^G(M)$$

between induced and coinduced modules. In terms of this explicit isomorphism, the map  $\text{coind}_U^G(M) \rightarrow M$  of Construction 21.8 is the counit map  $\text{ind}_U^G(M) \rightarrow M$  of the adjunction  $\text{ind}_U^G \dashv \text{res}_U^G$ .

**Definition 21.10.** We call the map on cohomology groups of (21.3) the *corestriction map*.

An important property of the corestriction map is its behaviour when composed with the contravariant functoriality of group cohomology; that is, the restriction of Construction 20.14.

**Lemma 21.11.** *Let  $G$  be a profinite group,  $U \leq G$  an open subgroup and  $M$  a discrete  $G$ -module. Then the composite*

$$H^*(G, M) \rightarrow H^*(U, M) \rightarrow H^*(G, M)$$

*of the restriction and corestriction maps coincides with multiplication by the index  $|U : G|$ .*

*Proof.* Both restriction and corestriction are obtained by applying cohomology to suitable maps of discrete  $G$ -modules. We show something stronger, namely that the composite of these two maps

$$M \rightarrow \text{coind}_U^G(M) \rightarrow M$$

coincides with multiplication by the index. To see this, we calculate that the composite is given by

$$m \mapsto \sum_i x_i^{-1}(x_i m) = |U : G| \cdot m$$

where  $x_i$  is a set of representatives of left cosets. This gives the claim. □

**Proposition 21.12.** *Let  $G$  be a profinite group and let  $S \leq G$  be a Sylow subgroup. Then for any  $p$ -torsion discrete  $G$ -module  $A$ , the restriction map*

$$(21.4) \quad H^*(G, A) \rightarrow H^*(S, A)$$

*is injective. In particular,*

$$\text{cd}_p(G) = \text{cd}_p(S).$$

*Proof.* Since both sides commute with filtered colimits in  $A$  by Corollary 20.23, we can assume that  $A$  is finitely generated and hence stabilized by an open subgroup  $U \leq G$ . Since the open normal subgroups  $V \triangleleft G$  contained in  $U$  form a basis of open neighbourhoods of the identity of  $G$ , and similarly with  $V \cap S$  for  $S$ , using Proposition 20.24 we can identify (21.4) with the filtered colimit of maps

$$H^*(G/V, A) \rightarrow H^*(S/(S \cap V), A).$$

Since  $S/(S \cap V)$  is a Sylow subgroup of  $G/V$ , the composite

$$H^*(G/V, A) \rightarrow H^*(S/(S \cap V), A) \rightarrow H^*(G/V, A)$$

of restriction and corestriction is equal to multiplication by an integer coprime to  $p$  by [Lemma 21.11](#). As these groups are  $p$ -torsion, since  $A$  is, we deduce that the composite is an isomorphism and hence the first map is injective. We deduce that so is the filtered colimit, as needed.

The injectivity of the restriction maps shows that  $\text{cd}_p(G) \leq \text{cd}_p(S)$ . The inequality going the other way is [Lemma 21.4](#).  $\square$

As a consequence of [Proposition 21.12](#), when discussing  $p$ -cohomological dimension it is enough to consider the case of pro- $p$ -groups. In this case, cohomological dimension is characterized by cohomology with respect to a single module.

**Lemma 21.13** (Complete reducibility of  $p$ -torsion modules). *Let  $G$  be a pro- $p$ -group and let  $A$  be a finitely generated  $p$ -torsion discrete  $G$ -module. Then  $A$  can be built from  $\mathbf{F}_p$  using iterated extensions, where we consider  $\mathbf{F}_p$  with the trivial  $G$ -action.*

*Proof.* If  $A$  is both  $p$ -torsion and finitely generated, then  $p^k \cdot A = 0$  for some  $k \geq 0$ . We thus have a finite filtration

$$0 = p^k \cdot A \subseteq p^{k-1} \cdot A \subseteq \dots \subseteq A$$

whose subquotients are simple  $p$ -torsion. This reduces us to the case when  $A$  is a finite-dimensional  $\mathbf{F}_p$ -vector space.

Choosing a basis, the action of  $G$  is specified by a continuous homomorphism  $G \rightarrow \text{GL}_r(\mathbf{F}_p)$ , where  $r = \dim_{\mathbf{F}_p}(A)$ . As  $G$  is pro- $p$ , this homomorphism factors through a Sylow subgroup of the general linear group, which by changing the basis if necessary we can assume is given by the subgroup  $U_r(\mathbf{F}_p) \leq \text{GL}_r(\mathbf{F}_p)$  of unitriangular matrices of [Notation 6.13](#). It follows that with respect to this basis, the action of  $G$  preserves the standard flag of subspaces

$$0 \leq \mathbf{F}_p \subseteq \mathbf{F}_p^{\oplus 2} \subseteq \dots \subseteq \mathbf{F}_p^{\oplus r} \simeq A.$$

This gives a filtration of  $A$  by  $G$ -submodules with subquotients isomorphic to  $\mathbf{F}_p$ , necessarily with a trivial action since  $|\text{Aut}(\mathbf{F}_p)| = p - 1$ , ending the argument.  $\square$

**Proposition 21.14.** *Let  $G$  be a pro- $p$ -group. The following are equivalent:*

- (1)  $\text{cd}_p(G) \leq n$ ,
- (2)  $H^s(G, \mathbf{F}_p) = 0$  for  $s > n$ ,
- (3)  $H^{n+1}(G, \mathbf{F}_p) = 0$ .

*Proof.* The forward implications are clear, so we only argue (3)  $\Rightarrow$  (1). Observe that if

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is a short exact sequence of discrete  $G$ -modules, then

$$H^{n+1}(G, A) \rightarrow H^{n+1}(G, B) \rightarrow H^{n+1}(G, C)$$

is exact in the middle. It follows that the class of discrete  $G$ -modules  $A$  such that  $H^{n+1}(G, A) = 0$  is closed under extensions. By [Corollary 20.23](#), it is also closed under filtered colimits. Since  $H^{n+1}(G, \mathbf{F}_p) = 0$  by assumption, to show that  $H^{n+1}(G, A) = 0$  for any  $p$ -torsion  $G$ , it is enough to verify that  $p$ -torsion discrete  $G$ -modules are generated under filtered colimits and extensions by  $\mathbf{F}_p$ . This is immediate from [Lemma 21.13](#) and the fact that any discrete  $G$ -module is a filtered colimit of its finitely generated submodules.

Now suppose by induction that we showed that  $H^{n+k}(G, A) = 0$  for all  $p$ -torsion  $A$  and some  $k \geq 1$ . We have a short exact sequence of  $p$ -torsion discrete  $G$ -modules

$$0 \rightarrow A \rightarrow \text{coind}_1^G(A) \rightarrow C \rightarrow 0$$

where  $C$  is the cokernel of the unit map. Since coinduced modules have no positive degree cohomology, the long exact sequence of cohomology associated to the above extension shows that

$$H^{n+k}(G, C) \simeq H^{n+k+1}(G, A).$$

The left hand side vanishes by the inductive assumption and hence so does the right hand side. This shows that  $H^s(G, A) = 0$  for all  $s > n$ , as needed.  $\square$

First, we observe that cohomological dimension is only interesting in the profinite case: no finite groups, and no groups which contain torsion, can be finite-dimensional.

**Example 21.15.** Let  $C_p$  be the cyclic group with  $p$  elements. For finite groups, cohomology in the sense of [Definition 20.12](#) can be identified with cohomology of the classifying space.

We have  $BC_2 \simeq \mathbf{RP}^\infty$  and  $BC_p \simeq L_p$  (the infinite lens space) for  $p > 2$ . Standard calculations in algebraic topology then show that

$$H^*(C_2, \mathbf{F}_2) \simeq \mathbf{F}_2[x],$$

a polynomial algebra on a class of degree  $|x| = 1$ <sup>11</sup>. Here, the element  $x$  can be any generator of the first cohomology group, which we can identify through [Example 20.22](#) with an isomorphism of groups  $C_p \simeq \mathbf{F}_p$ .

At  $p > 2$ , we instead have

$$H^*(C_p, \mathbf{F}_p) \simeq \Lambda(x) \otimes \mathbf{F}_p[y],$$

a tensor product of an exterior algebra on a class of degree  $|x| = 1$  and a polynomial algebra on a class of degree  $|y| = 2$ . Here,  $x$  is again a chosen isomorphism  $C_p \simeq \mathbf{F}_p$  and  $y = \beta(x)$  is given by its Bockstein.

**Remark 21.16.** Note that at any prime  $p$ , cup product with the Bockstein  $\beta(x)$  of a generator (which is equal to  $x^2$  when  $p = 2$ ) induces an isomorphism

$$H^k(C_p, \mathbf{F}_p) \simeq H^{k+2}(C_p, \mathbf{F}_p)$$

for all  $k \geq 0$ . This 2-fold periodicity in cohomology of a cyclic group will come up again as an essential argument in [§23](#), where we prove a partial converse to [Proposition 21.17](#) below.

One consequence of the calculation of [Example 21.15](#) is that torsion obstructs finiteness of cohomological dimension:

**Proposition 21.17.** *Let  $G$  be a profinite group of finite  $p$ -cohomological dimension. Then  $G$  is  $p$ -torsion free; that is, if  $g^p = e$  for some  $g \in G$ , then  $g = e$ .*

*Proof.* We observed in [Example 21.15](#) that  $C_p$  is of infinite cohomological dimension. If  $g^p = e$  and  $g \neq 0$ , then  $C_p \leq G$  as a subgroup generated by  $g$ , and it follows from [Lemma 21.4](#) that  $\text{cd}_p(G) = \infty$ .  $\square$

Note that in particular, [Proposition 21.17](#) shows that all non-zero finite  $p$ -groups are of infinite cohomological dimension. Thus, the latter notion is really only interesting for infinite groups. The following gives an example of such a group.

**Example 21.18.** Using the fact that  $\mathbb{Z}_p$  is a free pro- $p$ -group on a single generator, one can show that the cohomology groups of a  $p$ -torsion  $\mathbb{Z}_p$ -module  $M$  can be calculated as the cohomology of the cochain complex

$$M \xrightarrow{1-\sigma} M,$$

where  $\sigma \in \mathbb{Z}_p$  is the topological generator. It follows that  $\mathbb{Z}_p$  is of  $p$ -cohomological dimension 1.

One reason why [Proposition 21.14](#) is particularly useful is that mod  $p$  cohomology of a group has a canonical structure of a ring. One way to see this is the isomorphism

$$H^*(G, \mathbf{F}_p) \simeq \varinjlim H^*(G/U, \mathbf{F}_p),$$

---

<sup>11</sup>The ring structure on cohomology is that of a cup product. In case of group cohomology, it can be produced purely algebraically, as we will do in the next lecture.

where on the right hand side we have a filtered colimit of rings since cohomology groups of a finite group have a ring structure coming from the cup product using the identification with cohomology of the classifying space. This also endows the cohomology groups with the action of Steenrod operations.

**Remark 21.19.** In the next lecture, we will construct the product structure on cohomology purely algebraically (in greater generality, allowing non-trivial coefficients). One can similarly construct the Steenrod operations in a purely algebraic fashion, but any construction of the Steenrod squares and powers is necessarily involved - too involved for us to do so in this course.

Another reason while considering mod  $p$ -cohomology is convenient is that low-dimensional cohomology groups admit straightforward interpretation.

**Lemma 21.20.** *Let  $G$  be a pro- $p$ -group with Frattini subgroup  $G_2 \leq G$ . Then*

$$H^1(G, \mathbf{F}_p) \simeq (G/G_2)^* := \text{Hom}_{\mathbf{F}_p}^{cts}(G/G_2, \mathbf{F}_p);$$

*that is,  $H^1(G, \mathbf{F}_p)$  is the continuous linear dual of the profinite  $\mathbf{F}_p$ -vector space  $G/G_2$ .*

*Proof.* Since the action of  $G$  on  $\mathbf{F}_p$  is trivial, by [Example 20.22](#) we have

$$H^1(G, \mathbf{F}_p) \simeq \text{Hom}^{cts}(G, \mathbf{F}_p),$$

the group of continuous group homomorphisms. Since  $\mathbf{F}_p$  is abelian of exponent  $p$ , any such homomorphism factors uniquely through  $G/G_2$ .  $\square$

**Corollary 21.21.** *A pro- $p$ -group is finitely generated if and only if  $H^1(G, \mathbf{F}_p)$  is finite-dimensional as an  $\mathbf{F}_p$ -vector space.*

*Proof.* This is a combination of [Lemma 21.20](#) and [Proposition 3.4](#), since a profinite  $\mathbf{F}_p$ -vector space is finitely generated if and only if it is finite-dimensional, if and only if its continuous dual is finite-dimensional.  $\square$

By [Lemma 21.20](#), elements of  $H^1(G, \mathbf{F}_p)$  can be thought of as “cogenerators” of  $G$  in the sense that its elements can detect generators. More precisely, identifying first cohomology with homomorphisms we have a pairing

$$H^1(G, \mathbf{F}_p) \times G \rightarrow \mathbf{F}_p$$

and a set of elements of  $G$  generates it if and only if no element of first cohomology vanishes on the whole set.

Similar, one can think of  $H^2(G, \mathbf{F}_p)$  as encoding “relations” in the group. For example, we have the following result, which relates the second cohomology to finite presentation:

**Proposition 21.22.** *Let  $G$  be a pro- $p$ -group generated by  $g_1, \dots, g_n$  and let  $R := \ker(F(n) \rightarrow G)$  be the kernel of the induced homomorphism from the free pro- $p$ -group generated by  $n$  elements. Then the following are equivalent:*

- (1)  $R$  is finitely generated,
- (2)  $H^2(G, \mathbf{F}_p)$  is a finite-dimensional  $\mathbf{F}_p$ -vector space.

We do not prove [Proposition 21.22](#) in this course; an interested reader should consult [[Ser97](#), §4.3, Proposition 27]. Instead, we will prove a related result which will be useful in the next lecture.

As motivation for the statement, observe that by [Lemma 21.20](#) the group  $C_p^{\times n}$  is the smallest pro- $p$ -group whose first cohomology is  $n$ -dimensional. As the smallest such group, one can think that it has the most “relations”. The following result relates this to the second cohomology being sufficiently large.

**Theorem 21.23** (Serre). *Let  $G$  be a pro- $p$ -group and let  $(y_i)_{i \in I}$  be a well-ordered basis of  $H^1(G, \mathbf{F}_p)$ . Then the following are equivalent:*

- (1) the induced group homomorphism  $G \rightarrow \prod_{i \in I} C_p$  is an isomorphism,
- (2) the cohomology classes  $y_i y_j$  for  $i < j$  and  $\beta(y_i)$  are linearly independent as elements of  $H^2(G, \mathbf{F}_p)$ .

*Proof.* Using the calculation of cohomology of  $H^*(C_p, \mathbf{F}_p)$  of [Example 21.15](#) (where at  $p = 2$  we have  $\beta(x) = x^2$ ) and the Künneth theorem for cohomology of products, we see that the given elements form a basis of  $H^2(-, \mathbf{F}_p)$  for any finite product of  $C_p$ . Since an infinite product is a limit of finite products, this is also a basis for infinite products by [Proposition 20.24](#). This shows that (1)  $\Rightarrow$  (2).

We now argue that (2)  $\Rightarrow$  (1). Since  $y_i \in H^1(G, \mathbf{F}_p)$  are linearly independent, the induced map into any finite product of  $C_p$  is surjective. It follows that the map into the whole product has dense image and thus is surjective as  $G$  is compact. Using the description of cohomology of the product from the previous paragraph, we see that condition (2) is equivalent to the induced map

$$H^2\left(\prod_{i \in I} C_p, \mathbf{F}_p\right) \rightarrow H^2(G, \mathbf{F}_p)$$

being injective.

Let  $K = \ker(G \rightarrow \prod C_p)$  be the kernel; we have to show that  $K$  is trivial. We have the Lyndon-Hochschild-Serre spectral sequence of [Construction 21.5o](#) of signature

$$H^s\left(\prod C_p, H^t(K, \mathbf{F}_p)\right) \Rightarrow H^{s+t}(G, \mathbf{F}_p)$$

whose second page (in low degrees) is given by

$$\begin{array}{ccccc} H^0(\prod C_p, H^1(K, \mathbf{F}_p)) & & \dots & & \\ & \searrow^{d_2} & & & \\ H^0(\prod C_p, \mathbf{F}_p) & & H^1(\prod C_p, \mathbf{F}_p) & \rightarrow & H^2(\prod C_p, \mathbf{F}_p) \end{array}$$

Since  $H^1(\prod C_p, \mathbf{F}_p) \rightarrow H^1(G, \mathbf{F}_p)$  is an isomorphism by construction, on the  $E_\infty$ -page the  $(0, 1)$ -term must vanish. The only way this can happen is if all of the non-zero elements support the pictured  $d_2$  differential. However, as  $H^2(\prod C_p, \mathbf{F}_p) \rightarrow H^2(G, \mathbf{F}_p)$  is injective, none of the elements in the  $(2, 0)$ -term can be hit by a differential. It follows that the pictured differential vanishes so that

$$H^0\left(\prod C_p, H^1(K, \mathbf{F}_p)\right) = 0.$$

Since any non-zero representation of a pro- $p$ -group on a  $\mathbf{F}_p$ -vector space has a non-zero vector as a consequence of [Lemma 21.13](#), this implies that

$$H^1(K, \mathbf{F}_p) = 0.$$

By [Lemma 21.20](#), this implies that  $K = 0$ , as needed. □

## 22. THE DERIVED $\infty$ -CATEGORY AND CUP PRODUCTS

In the previous lecture, we observed that the mod  $p$  cohomology ring of a profinite group acquires a ring structure with respect to the cup product using the isomorphism

$$H^*(G, \mathbf{F}_p) \simeq \varinjlim H^*(G/U, \mathbf{F}_p) \simeq \varinjlim H^*(B(G/U), \mathbf{F}_p),$$

where the right hand side is given by the cohomology of the classifying space. Today, we will give a general construction of cup product in group cohomology of a profinite group, allowing non-trivial modules as coefficients.

**Warning 22.1.** There is a low-technology construction of the cup product in group cohomology, given by writing down an explicit formula in terms of the group cochain complex of [Definition 20.17](#). However, we will proceed differently, instead endowing the derived  $\infty$ -category of discrete  $G$ -modules with a suitable symmetric monoidal structure, which is often useful in its own right.

As a first step towards the construction of cup products, we observe that we have a suitable symmetric monoidal structure on the category of coefficients.

**Construction 22.2** (Tensor product of discrete  $G$ -modules). If  $M, N$  are discrete  $G$ -modules, then their tensor product  $M \otimes_{\mathbb{Z}} N$  acquires a canonical discrete  $G$ -module structure defined uniquely by

$$g \cdot (a \otimes b) := (g \cdot a) \otimes (g \cdot b).$$

This makes  $\text{Mod}_G(\mathcal{A}b)$  into a presentably symmetric monoidal category with unit  $\mathbb{Z}$  (equipped with the trivial  $G$ -action). If  $m \in M, n \in N$  are  $G$ -invariants, then so is  $m \otimes n \in M \otimes N$ , and this defines a bilinear pairing

$$(22.1) \quad H^0(G, M) \otimes H^0(G, N) \rightarrow H^0(G, M \otimes N).$$

The cup product on cohomology should be obtained by a suitably extending (22.1) to a pairing of derived functors. To more easily manipulate derived functors, it will be convenient to work with a variant of the derived  $\infty$ -category of discrete  $G$ -modules.

**Recollection 22.3** (Unseparated derived  $\infty$ -category). If  $\mathcal{C}$  is a presentable, stable  $\infty$ -category equipped with a t-structure compatible with filtered colimits, then the heart  $\mathcal{C}^\heartsuit$  is a Grothendieck abelian category. One can show that in this context, the construction

$$\mathcal{C} \mapsto \mathcal{C}^\heartsuit,$$

has a left adjoint<sup>12</sup> which we denote by

$$\mathcal{A} \mapsto \check{\mathcal{D}}(\mathcal{A}),$$

see [[Lur](#), Corollary C.5.8.9]. We call  $\check{\mathcal{D}}(\mathcal{A})$  the *unseparated derived  $\infty$ -category*.

**Remark 22.4.** Concretely, the unseparated derived  $\infty$ -category  $\check{\mathcal{D}}(\mathcal{A})$  can be described as the homotopy coherent nerve of the dg-category of chain complexes of injectives of  $\mathcal{A}$ .

**Remark 22.5** (Extension groups in terms of the derived  $\infty$ -category). The unseparated derived  $\infty$ -category encodes the homological algebra of  $\mathcal{A}$  in the sense that

- (1) the unit map  $\mathcal{A} \rightarrow \check{\mathcal{D}}(\mathcal{A})^\heartsuit$  of the adjunction of [Recollection 22.3](#) is an equivalence of categories,
- (2) there are isomorphisms

$$\text{Ext}_{\mathcal{A}}^n(a, b) \simeq \pi_{-n} \text{map}_{\check{\mathcal{D}}(\mathcal{A})}(a, b)$$

between the extension groups of  $\mathcal{A}$  (in a classical sense, defined as derived functors) and homotopy groups of the mapping spectra between  $a, b \in \mathcal{A}$ , considered as objects of the heart.

These are really the only two properties of the unseparated derived  $\infty$ -category which we will use and we encourage a reader unfamiliar with this construction to take them on faith.

---

<sup>12</sup>For this to be true, one should really consider  $\mathcal{C} \rightarrow \mathcal{C}^\heartsuit$  as a functor from presentable, stable  $\infty$ -categories equipped with a right complete t-structure compatible with filtered colimits and t-exact left adjoints, into Grothendieck abelian categories and exact left adjoints. This is more pleasantly expressed (although it would mean the same thing) in the language of Grothendieck prestable  $\infty$ -categories. We recommend [[Lur](#), Appendix C] for details.

**Warning 22.6.** The reader might be familiar with the *separated* derived  $\infty$ -category  $\mathcal{D}(\mathcal{A})$ , which is the localization

$$\check{\mathcal{D}}(\mathcal{A}) \rightarrow \mathcal{D}(\mathcal{A})$$

obtained by inverting all quasi-isomorphisms. This functor is sometimes an equivalence; for example, when  $\mathcal{A}$  is the category of modules over a regular ring. Moreover, it always induces an equivalence between subcategories of objects bounded with respect to the t-structure.

In particular,  $\mathcal{D}(\mathcal{A})$  also satisfies the two properties outlined in [Remark 22.5](#), and so for the purpose of this course, either of these two  $\infty$ -categories would do. However, in our context, the unseparated variant is both slightly easier to describe and better-behaved, so this is the one we will work with.

To construct the cup product, we will endow the unseparated derived  $\infty$ -category of discrete  $G$ -modules with a symmetric monoidal structure. To motivate our construction, we first describe the category of discrete  $G$ -modules as an Ind-completion.

**Lemma 22.7.** *If  $G$  is profinite and  $U \triangleleft G$  is open normal, then  $\mathbb{Z}[G/U]$  is compact as an object of the category of discrete  $G$ -modules. Moreover, objects of this form generate  $\text{Mod}_G(\text{Ab})$  under colimits.*

*Proof.* We have

$$\text{Hom}_{\text{Mod}_G(\text{Ab})}(\mathbb{Z}[G/U], M) \simeq M^U \simeq H^0(U, M)$$

so that compactness follows from [Corollary 20.23](#). Since any element of a discrete  $G$ -module is stabilized by some open subgroup, any element is in the image of a map from  $\mathbb{Z}[G/U]$  for some  $U$ , and we deduce that these objects generate.  $\square$

**Corollary 22.8.** *If  $M$  is discrete  $G$ -module which is finitely generated as an abelian group, then  $M$  is compact. Conversely, any compact object is finitely generated as an abelian group.*

*Proof.* By [Lemma 22.7](#),  $M$  can be written as a quotient of a direct sum of objects of the form  $\mathbb{Z}[G/U]$  which are compact. Since  $M$  is finitely generated, the direct sum can be chosen to be finite, so that the kernel is again finitely generated as an abelian group. We deduce that  $M$  belongs to the smallest subcategory of  $\text{Mod}_G(\text{Ab})$  containing  $\mathbb{Z}[G/U]$  and closed under finite colimits, which is exactly the subcategory of compact objects.  $\square$

**Theorem 22.9.** *Let  $\text{Mod}_G(\text{Ab}^{fg}) \subseteq \text{Mod}_G(\text{Ab})$  be the subcategory of modules which are finitely generated as an abelian group. Then*

- (1)  $\text{Mod}_G(\text{Ab}^{fg}) \simeq \varinjlim \text{Mod}_{G/U}(\text{Ab}^{fg})$ , where the filtered colimit of categories is taken using restriction functors and is indexed by the opposite of the poset of normal open subgroups,
- (2) the inclusion induces an equivalence

$$\text{Mod}_G(\text{Ab}) \simeq \text{Ind}(\text{Mod}_G(\text{Ab}^{fg})),$$

where the right hand side is the free cocompletion under filtered colimits.

*Proof.* Let  $M$  be a discrete  $G$ -module generated as an abelian group by elements  $m_1, \dots, m_n \in M$ . Each of  $m_i$  is stabilized by an open normal subgroup  $U_i$ , hence all of  $M$  is stabilized by  $U := U_1 \cap \dots \cap U_n$ . It follows that  $M$  is obtained by restriction from  $G/U$  and thus the comparison functor

$$\varinjlim \text{Mod}_{G/U}(\text{Ab}^{fg}) \rightarrow \text{Mod}_G(\text{Ab}^{fg})$$

is essentially surjective. Since each of  $\text{Mod}_{G/U}(\text{Ab}^{fg}) \rightarrow \text{Mod}_G(\text{Ab}^{fg})$  is fully faithful, so is the comparison functor. This ends the first part.

The second part is a formal consequence of [Lemma 22.7](#) and [Corollary 22.8](#), since for any cocomplete  $\infty$ -category  $\mathcal{C}$  generated by its subcategory  $\mathcal{C}^\omega \subseteq \mathcal{C}$  of compact objects we have  $\text{Ind}(\mathcal{C}^\omega) \simeq \mathcal{C}$ , see [[Lur09](#), Proposition 5.3.5.11].  $\square$

To endow the derived  $\infty$ -category with a symmetric monoidal structure, we will describe  $\check{\mathcal{D}}(\mathrm{Mod}_G(\mathcal{A}b))$  in terms similar to the abelian case covered in [Theorem 22.9](#).

**Recollection 22.10.** Recall that an object  $X \in \mathcal{D}(\mathbb{Z})$  of the derived  $\infty$ -category of the integers is called perfect if it satisfies one of the following equivalent conditions:

- (1) it is compact,
- (2) it is dualizable with respect to the derived tensor product,
- (3) it has finitely many non-zero homology groups, each of which is finitely generated as an abelian group.

**Notation 22.11.** We write  $\mathrm{Perf}(\mathbb{Z}) \subseteq \mathcal{D}(\mathbb{Z})$  for the full subcategory spanned by perfects.

**Definition 22.12.** The  $\infty$ -category of *discrete perfect  $G$ -modules* is given by the filtered colimit

$$\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z})) := \varinjlim \mathrm{Fun}(\mathrm{B}(G/U), \mathrm{Perf}(\mathbb{Z}))$$

of  $\infty$ -categories of perfect complexes equipped with an action of  $G/U$ . Here, the colimit is taken over the poset of open normal subgroups and the functors are given by restriction.

Note that for each normal open  $U \triangleleft G$

$$\mathrm{Mod}_{G/U}(\mathrm{Perf}(\mathbb{Z})) \simeq \mathrm{Fun}(\mathrm{B}(G/U), \mathrm{Perf}(\mathbb{Z}))$$

inherits a pointwise  $t$ -structure from perfect complexes with heart

$$\mathrm{Mod}_{G/U}(\mathrm{Perf}(\mathbb{Z}))^\heartsuit \simeq \mathrm{Mod}_{G/U}(\mathrm{Perf}(\mathbb{Z})^\heartsuit) \simeq \mathrm{Mod}_{G/U}(\mathcal{A}b^{fg})$$

Restriction of representation functors are  $t$ -exact with respect to these  $t$ -structures and it follows that  $\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z}))$  inherits a  $t$ -structure as a filtered colimit.

This  $t$ -structure then formally extends to one on Ind-completion, namely the unique one compatible with filtered colimits, whose heart is given by

$$(22.2) \quad \mathrm{Ind}(\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z})))^\heartsuit \simeq \mathrm{Ind}(\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z})^\heartsuit)^\heartsuit) \simeq \mathrm{Mod}_G(\mathcal{A}b),$$

where the second identification is [Theorem 22.9](#). Through the universal property of the unseparated derived  $\infty$ -category of [Recollection 22.3](#), this equivalence induces a cocontinuous,  $t$ -exact functor

$$(22.3) \quad \check{\mathcal{D}}(\mathrm{Mod}_G(\mathcal{A}b)) \rightarrow \mathrm{Mod}_G(\mathcal{D}(\mathbb{Z})).$$

**Theorem 22.13.** *The comparison functor of (22.3) is an equivalence of  $\infty$ -categories.*

*Proof.* This is completely formal, but the argument requires some theory of Grothendieck prestable  $\infty$ -categories. We advise the reader not familiar with the latter to take the result on faith.

For an interested reader, we observe that by [[Lur](#), Theorem C.6.7.1], the subcategory

$$(\mathrm{Ind}(\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z})))_{\geq 0}) \simeq \mathrm{Ind}(\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z})_{\geq 0}))$$

of connective objects is anticomplete. As it is also 0-complicial, generated under colimits by  $\mathbb{Z}[G/U]$  for open normal subgroups  $U \triangleleft G$ , we deduce that it is an unseparated derived  $\infty$ -category of its heart by [[Lur](#), Corollary C.5.8.11].  $\square$

As a consequence, we obtain the desired symmetric monoidal structure.

**Construction 22.14.** The  $\infty$ -category  $\mathcal{D}(\mathbb{Z})$  has a canonical symmetric monoidal structure given by the derived tensor product over the integers. Considering pointwise tensor product we obtain an induced symmetric monoidal structure on each of the functor  $\infty$ -categories and hence on the filtered colimit

$$\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z})) \simeq \varinjlim \mathrm{Fun}(\mathrm{B}(G/U), \mathrm{Perf}(\mathbb{Z})).$$

This is exact in each variable and hence uniquely extends to a symmetric monoidal structure on

$$\check{\mathcal{D}}(\mathrm{Mod}_G(\mathcal{A}b)) \simeq \mathrm{Ind}(\mathrm{Mod}_G(\mathrm{Perf}(\mathbb{Z})))$$

which preserves colimits in each variable.

**Remark 22.15.** The symmetric monoidal structure of [Construction 22.14](#) is uniquely determined by the following two properties:

- (1) for each open normal  $U \triangleleft G$ , the composite

$$\text{Fun}(\mathbf{B}(G/U), \text{Perf}(\mathbb{Z})) \rightarrow \text{Mod}_G(\text{Perf}(\mathbb{Z})) \rightarrow \text{Ind}(\text{Mod}_G(\text{Perf}(\mathbb{Z}))) \simeq \check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b))$$

is symmetric monoidal,

- (2) the tensor product preserves colimits in each variable.

More precisely, given a presentably symmetric monoidal stable  $\infty$ -category  $\mathcal{C}$ , a collection of compatible exact symmetric monoidal functors

$$\text{Fun}(\mathbf{B}(G/U), \text{Perf}(\mathbb{Z})) \rightarrow \mathcal{C}$$

uniquely extends to a symmetric monoidal left adjoint  $\check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b))$ .

**Remark 22.16.** One can similarly ask about a symmetric monoidal structure on the separated (ie. classical) derived  $\infty$ -category  $\mathcal{D}(\text{Mod}_G(\mathcal{A}b))$ . Since the forgetful functor

$$\text{Mod}_G(\mathcal{A}b) \rightarrow \mathcal{A}b$$

is a conservative exact left adjoint, we deduce that the same is true for

$$\mathcal{D}(\text{Mod}_G(\mathcal{A}b)) \rightarrow \mathcal{D}(\mathbb{Z}).$$

It follows that the quasi-isomorphisms in the unseparated derived  $\infty$ -category  $\check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b))$  can be identified with those maps which are inverted by the functor

$$(22.4) \quad \check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b)) \rightarrow \check{\mathcal{D}}(\mathcal{A}b) \simeq \mathcal{D}(\mathbb{Z}),$$

where we use that for the category of abelian groups, the two variants of the derived  $\infty$ -category coincide by [\[Lur, C.5.8.12\]](#).

Using the universal property of [Remark 22.15](#), the functor of (22.4) can be made symmetric monoidal, so that the class of arrows it inverts is closed under the tensor product on both sides. We deduce formally that there is a unique symmetric monoidal structure on  $\mathcal{D}(\text{Mod}_G(\mathcal{A}b))$  such that the canonical localization

$$\check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b)) \rightarrow \mathcal{D}(\text{Mod}_G(\mathcal{A}b))$$

is symmetric monoidal.

**Construction 22.17** (Cup products). Let  $\mathbb{Z} \in \check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b))$  be the integers with the trivial  $G$ -action, considered as an object of the heart. Since the derived  $\infty$ -category is stable, we have an internal mapping spectrum functor

$$\text{map}(\mathbb{Z}, -): \check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b)) \rightarrow \mathcal{S}p$$

and since  $\mathbb{Z}$  is the monoidal unit, this has a canonical lax symmetric monoidal structure. As passing to homotopy groups is also lax symmetric monoidal, the same is true for the composite

$$\pi_* \text{map}(\mathbb{Z}, -): \check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b)) \rightarrow \text{gr}\mathcal{A}b.$$

If  $M, N$  are discrete  $G$ -modules, considered as objects of the heart, then

$$\pi_{-s} \text{map}(\mathbb{Z}, M) \simeq \text{Ext}_{\text{Mod}_G(\mathcal{A}b)}^s(\mathbb{Z}, M) \simeq H^s(G, M)$$

by [Remark 22.5](#) and similarly for  $N$ . We have a canonical comparison map  $M \otimes_{\mathbb{Z}}^L N \rightarrow M \otimes_{\mathbb{Z}} N$  between the derived and ordinary tensor products, and the composite

$$\pi_{-s} \text{map}(\mathbb{Z}, M) \otimes_{\mathbb{Z}} \pi_{-t} \text{map}(\mathbb{Z}, N) \rightarrow \pi_{-s-t} \text{map}(\mathbb{Z}, M \otimes_{\mathbb{Z}}^L N) \rightarrow \pi_{-s-t} \text{map}(\mathbb{Z}, M \otimes_{\mathbb{Z}} N)$$

can be identified with a map

$$(22.5) \quad H^s(G, M) \otimes_{\mathbb{Z}} H^t(G, N) \rightarrow H^{s+t}(G, M \otimes_{\mathbb{Z}} N).$$

Concretely, the map of (22.5) can be described as follows. A pair of classes  $x \in H^s(G, M)$  and  $y \in H^t(G, N)$  can be identified with a homotopy class of maps  $x: \mathbb{Z} \rightarrow \Sigma^s M$  and  $y: \mathbb{Z} \rightarrow \Sigma^t N$  in the derived  $\infty$ -category. The cup product is then represented by the homotopy class of the composite

$$\mathbb{Z} \simeq \mathbb{Z} \otimes \mathbb{Z} \xrightarrow{x \otimes y} \Sigma^{s+t}(M \otimes_{\mathbb{Z}}^L N) \longrightarrow \Sigma^{s+t}(M \otimes_{\mathbb{Z}} N)$$

**Definition 22.18.** We call the map of

$$\cup: H^s(G, M) \otimes_{\mathbb{Z}} H^t(G, N) \rightarrow H^{s+t}(G, M \otimes_{\mathbb{Z}} N)$$

of Construction 22.17 the exterior *cup product* in cohomology.

The cup product endows the functor  $H^*(G, -): \text{Mod}_G(\mathcal{A}b) \rightarrow \text{grAb}$  with a lax symmetric monoidal structure. In other words, the pairing of Definition 22.18 is suitably commutative, associative and unital. Moreover, by unwrapping the arguments we see that in cohomological degree zero it coincides with the pairing of invariants described in Construction 22.2.

**Remark 22.19.** Suppose that  $R$  is a monoid in  $\text{Mod}_G(\mathcal{A}b)$ , which we can identify with a ring  $R$  together with a continuous action of  $G$  through ring automorphisms. The composite

$$H^s(G, R) \otimes_{\mathbb{Z}} H^t(G, R) \rightarrow H^{s+t}(G, R \otimes_{\mathbb{Z}} R) \rightarrow H^{s+t}(G, R)$$

of the cup product and the ring multiplication is called the *internal cup product*. It endows  $H^*(G, R)$  with a structure of a graded ring, and it is graded-commutative if  $R$  is a commutative. In the particular case of trivial action, this recovers the ring structure coming from the isomorphism

$$H^*(G, R) \simeq \varinjlim H^*(G/U, R) \simeq \varinjlim H^*(B(G/U), R),$$

where the right hand side is endowed with the topological cup product.

We have previously constructed contravariant and covariant functoriality in group cohomology, given respectively by restriction and corestriction. We now describe how these two operations interact with the cup product. This will require us to consider restriction and coinduction at the level of derived  $\infty$ -categories and the way they interact with the derived symmetric monoidal structure.

**Construction 22.20.** If  $K \leq G$  is a closed subgroup, we have an adjunction

$$\text{res}_K^G \dashv \text{coind}_K^G: \text{Mod}_G(\mathcal{A}b) \rightleftarrows \text{Mod}_K(\mathcal{A}b).$$

Both of these functors are exact left adjoints, in the case of coinduction by Lemma 20.8. Since the association  $\mathcal{A} \rightarrow \check{\mathcal{D}}(\mathcal{A})$  is functorial in exact left adjoints, we obtain an induced adjunction between derived  $\infty$ -categories, which we also denote by

$$\text{res}_K^G \dashv \text{coind}_K^G: \check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b)) \rightleftarrows \check{\mathcal{D}}(\text{Mod}_K(\mathcal{A}b)).$$

In terms of the description of the derived  $\infty$ -category of Theorem 22.13, the restriction is induced by the functors

$$\text{Fun}(B(G/U), \text{Perf}(\mathbb{Z})) \rightarrow \text{Fun}(B(K/(U \cap K)), \text{Perf}(\mathbb{Z})) \rightarrow \check{\mathcal{D}}(\text{Mod}_K(\mathcal{A}b)).$$

This is canonically symmetric monoidal, and this produces a symmetric monoidal structure on the restriction functor.

**Lemma 22.21.** *Let  $K \leq G$  be a closed subgroup. Then the restriction*

$$\text{res}: H^*(G, -) \rightarrow H^*(K, -)$$

*has a canonical structure of a monoidal transformation of functors  $\text{Mod}_G(\mathcal{A}b) \rightarrow \text{grAb}$ . In particular, for any monoid  $R$  in discrete  $G$ -modules, the map*

$$H^*(G, R) \rightarrow H^*(K, R).$$

*is a homomorphism of rings.*

*Proof.* We recall from [Construction 20.14](#) that restriction on cohomology is defined as the morphism on Ext-groups induced by  $\text{res}_K^G: \text{Mod}_G(\mathcal{A}b) \rightarrow \text{Mod}_K(\mathcal{A}b)$ . The latter can be identified with the morphism induced on homotopy groups by the derived functor

$$\text{res}_K^G: \check{\mathcal{D}}(\text{Mod}_G(\mathcal{A}b)) \rightarrow \check{\mathcal{D}}(\text{Mod}_K(\mathcal{A}b)).$$

This functor is symmetric monoidal by [Construction 22.20](#) which yields the needed result.  $\square$

To describe the interaction of the cup product with corestriction, we will make use of the projection formula.

**Recollection 22.22.** Suppose that we have an adjunction  $L \dashv R: \mathcal{C} \rightleftarrows \mathcal{D}$  between monoidal categories such that  $L$  is monoidal. In this case, for any  $X \in \mathcal{D}$ ,  $Y \in \mathcal{C}$ , we have a canonical *projection formula* map

$$(22.6) \quad R(X) \otimes Y \rightarrow R(X \otimes L(Y))$$

defined as the adjoint of

$$L(R(X) \otimes Y) \simeq L(R(X)) \otimes L(Y) \rightarrow X \otimes L(Y)$$

obtained by applying the counit to the left factor.

**Remark 22.23.** In the context of the restriction and coinduction adjunction, the projection formula map of [Recollection 22.22](#) for  $M \in \text{Mod}_K(\mathcal{A}b)$  and  $N \in \text{Mod}_G(\mathcal{A}b)$  takes the form

$$p: \text{coind}_K^G(M) \otimes N \rightarrow \text{coind}_K^G(M \otimes \text{res}_K^G(N)).$$

Identifying coinduced modules with the set of  $K$ -equivariant functions in  $G$ , unwrapping the definition we see that if  $f \in \text{map}_{cts}^K(G, M)$  and  $n \in N$ , then the projection formula map is determined by

$$p(f \otimes n) := (g \mapsto f(g) \otimes gn).$$

From there, it is not difficult to verify that  $p$  is a natural isomorphism, although we will not need this fact.

**Lemma 22.24.** *Let  $U \leq G$  be an open subgroup and let  $M, N$  be discrete  $G$ -modules. Then*

$$\text{cores}(x) \cup y = \text{cores}(x \cup \text{res}(y)) \in H^{s+t}(G, M \otimes_{\mathbb{Z}} N)$$

for any  $x \in H^s(U, M)$ ,  $y \in H^t(G, N)$ .

*Proof.* We first claim that the diagram

$$\begin{array}{ccc} \text{coind}_K^G(M) \otimes N & \xrightarrow{p} & \text{coind}_K^G(M \otimes \text{res}_K^G(N)) \\ & \searrow \pi_1 & \swarrow \pi_2 \\ & M \otimes N & \end{array}$$

where the horizontal map is the projection formula map of [Recollection 22.22](#) and the vertical maps are induced by [Construction 21.8](#), commutes. Calculating using the formula of [Remark 22.23](#), this amounts to observing that if  $x_i$  are representatives for left cosets  $U \backslash G$ , then

$$\pi_1(f \otimes n) = \left( \sum_i x_i^{-1} f(x_i) \right) \otimes n = \sum_i x_i^{-1} (f(x_i) \otimes x_i n) = \pi_2(p(f \otimes n)).$$

We now prove the needed statement. We can identify the two cohomology classes of maps with homotopy classes of maps  $x: \mathbb{Z} \rightarrow \text{coind}_K^G(M)$  and  $y: \mathbb{Z} \rightarrow N$  in the derived  $\infty$ -category of discrete  $G$ -modules, where we suppress the suspensions from the notation. A diagram chase shows that the class  $\text{cores}(x) \cup y$  is then represented by the composite  $\pi_1 \circ (x \otimes y)$ , and the class  $\text{cores}(x \cup \text{res}(y))$  by the composite  $\pi_2 \circ (p \circ (x \otimes y))$ . Since the above diagram commutes, these two are the same.  $\square$

23. TORSION-FREE GROUPS AND LOCALITY OF COHOMOLOGICAL DIMENSION

In general, cohomological dimension is not a local property of profinite groups; that is, it cannot be detected on open subgroups. For example, the cyclic group  $C_p$  contains the trivial group as an open subgroup, but it is not itself of finite cohomological dimension by the calculation of [Example 21.15](#).

More generally, any profinite group which contains  $p$ -torsion cannot be of finite cohomological dimension since it contains a copy of  $C_p$ . The main result of this lecture is the following beautiful result of Serre which shows that  $p$ -torsion is essentially the only obstruction to locality of cohomological dimension:

**Theorem 23.1** (Serre). *Let  $G$  be a profinite group with  $U \leq G$  an open subgroup of finite  $p$ -cohomological dimension. Then the following are equivalent:*

- (1)  $G$  is of finite  $p$ -cohomological dimension,
- (2)  $\text{cd}_p(G) = \text{cd}_p(U)$ ,
- (3)  $G$  is  $p$ -torsion-free.

To prove [Theorem 23.1](#), we will closely follow the original paper of Serre [[Ser65](#)]. The proof is somewhat involved and will take the remainder of the lecture.

**Recollection 23.2.** Recall that a subset

$$V \subseteq \overline{\mathbf{F}}_p^{\times n}$$

is called *algebraic* if it is cut out by polynomial equations; that is, if there exists a subset

$$S \subseteq \overline{\mathbf{F}}_p[x_1, \dots, x_n]$$

of a polynomial ring such that

$$V = \{ (a_1, \dots, a_n) \in \overline{\mathbf{F}}_p^{\times n} \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in S \}.$$

Declaring algebraic subsets as closed defines the *Zariski topology* on  $\overline{\mathbf{F}}_p^{\times n}$ . As a consequence of the Nullstellensatz, the subset  $V$  determines the radical of  $S$  as

$$\text{Rad}(S) = \{ f \in \overline{\mathbf{F}}_p[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in V \}.$$

**Recollection 23.3.** An  $\overline{\mathbf{F}}_p$ -vector subspace  $V \subseteq \overline{\mathbf{F}}_p^{\times n}$  is called  $\mathbf{F}_p$ -rational if there exists a  $\mathbf{F}_p$ -vector subspace  $V' \subseteq \mathbf{F}_p^{\times n}$  such that

$$V = \overline{\mathbf{F}}_p \otimes_{\mathbf{F}_p} V'$$

as subspaces of  $\overline{\mathbf{F}}_p^{\times n} \simeq \overline{\mathbf{F}}_p \otimes_{\mathbf{F}_p} \mathbf{F}_p^{\times n}$ .

Since  $\mathbf{F}_p \subseteq \overline{\mathbf{F}}_p$  has Galois group generated by the Frobenius  $x \mapsto x^p$ , if  $F: \overline{\mathbf{F}}_p^{\times n} \rightarrow \overline{\mathbf{F}}_p^{\times n}$  denotes Frobenius morphism defined by

$$F(x_1, \dots, x_n) := (x_1^p, \dots, x_n^p),$$

one can show that  $V$  is  $\mathbf{F}_p$ -rational if and only if  $F(V) \subseteq V$ .

**Proposition 23.4.** *Let  $V \subseteq \overline{\mathbf{F}}_p^{\times n}$  be an algebraic subset such that*

- (1)  $\lambda \cdot V \subseteq V$  for all  $\lambda \in \overline{\mathbf{F}}_p$  (that is,  $V$  is a cone),
- (2)  $\theta(V) \subseteq V$ , where  $\theta := F + \text{id}_{\overline{\mathbf{F}}_p^{\times n}}$ .

*Then  $V$  is a union of  $\mathbf{F}_p$ -rational linear subspaces.*

*Proof.* If  $x \in V$  and  $r \geq 1$ , we write  $W_r(x)$  to be the  $\overline{\mathbf{F}}_p$ -linear subspace of  $\overline{\mathbf{F}}_p^{\times n}$  generated by  $x, Fx, \dots, F^{r-1}x$ . We first argue by induction that  $W_r(x) \subseteq V$ . The case of  $r = 1$  follows from the first condition on  $V$ .

Now suppose that  $r > 1$  and that  $W_{r-1}(x) \subseteq V$ . Any element of  $W_r(x)$  can be written as

$$y_1 \cdot x + \dots + y_r F^{r-1}x$$

for some  $y_i \in \overline{\mathbf{F}}_p$ . By inductive assumption and the two conditions on  $V$ , all elements of the form

$$z_0(z + Fz)$$

with  $z_0 \in \overline{\mathbf{F}}_p$  and

$$z = z_1 \cdot x + \dots + z_{r-1} F^{r-2}x \in W_{r-1}(x),$$

belong to  $V$ . Thus, it is enough to show that any element of  $W_r(x)$  can be written in this form.

Since  $Fz = z_1^p Fx + \dots + z_{r-1}^p F^{r-1}x$ , by comparing the coefficients of  $F^k x$  for  $0 \leq k \leq r-1$ , this amounts to solving a system of polynomial equations

$$\begin{aligned} y_1 &= z_0 z_1 \\ y_2 &= z_0(z_2 + z_1^p) \\ y_3 &= z_0(z_3 + z_2^p) \\ &\dots \\ y_r &= z_0 z_{r-1}^p \end{aligned}$$

An elementary calculation shows that this system of equations has a solution whenever  $y_1$  and at least one of  $y_2, \dots, y_r$  is non-zero. Combinations of  $y_i$  with this property form a Zariski-dense subset of the space of all combinations and since  $V$  is Zariski closed, we deduce that  $W_r(x) \subseteq V$ .

We now prove the Proposition. If  $x \in V$ , then by what we shown above we have

$$W(x) := \cup_{r \geq 1} W_r(x) \subseteq V.$$

Since  $W(x)$  is an  $F$ -stable linear subspace of  $V$ , it is  $\mathbf{F}_p$ -rational by [Recollection 23.3](#). As any point of  $V$  is contained in a rational linear subspace, we deduce that  $V$  is a union of such subspaces, as needed.  $\square$

**Corollary 23.5.** *Let  $S \subseteq \mathbf{F}_p[x_1, \dots, x_n]$  be a non-zero ideal defining an algebraic subset  $V \subseteq \overline{\mathbf{F}}_p^{\times n}$  satisfying the conditions of [Proposition 23.4](#). Then  $S$  contains a product*

$$\prod_{1 \leq i \leq k} u_i$$

for some  $k$  and  $u_i \in \mathbf{F}_p[x_1, \dots, x_n]$  non-zero homogeneous polynomials of degree one.

*Proof.* Note that since  $\mathbf{F}_p$  is finite, there are only finitely many  $\mathbf{F}_p$ -rational subspaces of  $\overline{\mathbf{F}}_p^{\times n}$ , hence  $V$  is in fact a finite union of such subspaces. Since the ideal is non-zero,  $V$  is not the whole affine space, so each such such subspace is proper. In particular, there exists a homogeneous degree one polynomial vanishing on it.

The product of such polynomials for each subspace then vanishes on all of  $V$  and thus belongs to the radical of  $S$ . It follows that some power of the product, which is also a product of polynomial of degree one, is in  $S$ .  $\square$

To relate the above analysis to group cohomology, we will need to use Steenrod operations, whose existence follows from the isomorphism

$$H^*(G, \mathbf{F}_p) \simeq H^*(B(G/U), \mathbf{F}_p)$$

of [Proposition 20.24](#) between cohomology of a profinite group and the colimit of cohomologies of the classifying spaces of finite quotients. We will only need very formal properties of the Steenrod operations; see [[Hat78](#), §4.L] for an introduction.

**Proposition 23.6.** *Let  $G$  be a profinite group and let  $x_1, \dots, x_n \in H^2(G, \mathbf{F}_p)$ . If  $p = 2$ , assume moreover that  $Sq^1 x_i = 0$  for all  $1 \leq i \leq n$ . Let  $S$  be the kernel of the induced homomorphism*

$$\pi: \mathbf{F}_p[x_1, \dots, x_n] \rightarrow H^2(G, \mathbf{F}_p).$$

*Then  $S$  contains a product of homogeneous polynomials of degree one.*

*Proof.* By [Corollary 23.5](#), it is enough to verify that the algebraic subset corresponding to  $S$  satisfies the conditions of [Proposition 23.4](#). It satisfies the first one since  $S$  is a kernel of a homomorphism of graded rings if we make each  $x_i$  of degree two. We move on to the second condition, where we will need to use Steenrod powers.

First assume that  $p > 2$ . By the Cartan formula, the total Steenrod power

$$P := \sum_{i \geq 0} P^i$$

induces a ring endomorphism of the cohomology algebra  $\bigoplus_{q \geq 0} H^q(G, \mathbf{F}_p)$ . If  $x \in H^2(G, \mathbf{F}_p)$ , we have  $P^0 x = x$ ,  $P^1 x = x^p$  and  $P^i x = 0$  for  $i > 0$ , so that

$$P(x) = x + x^p.$$

Thus, if  $\theta$  denotes the endomorphism of  $\mathbf{F}_p[x_1, \dots, x_n]$  uniquely determined by  $\theta(x_i) = x_i + x_i^p$ , then  $P \circ \pi = \pi \circ \theta$ . Thus,  $S \subseteq \theta^{-1}(S)$ , which implies that the algebraic subset cut out by  $S$  satisfies the needed second condition.

If  $p = 2$ , we have a ring endomorphism of the cohomology algebra given by the total Steenrod square

$$Sq := \sum_{i \geq 0} Sq^i.$$

On  $x \in H^2(G, \mathbf{F}_p)$ , it is given by

$$Sq(x) = x + Sq^1 x + x^2.$$

Thus, by the additional assumption on  $x_i$ , we have

$$Sq(x_i) = x_i + x_i^2.$$

The rest of the argument proceeds as in the previous paragraph. □

**Proposition 23.7.** *Let  $G$  be a profinite group with a well-ordered basis  $(y_i)_{i \in I}$  of  $H^1(G, \mathbf{F}_p)$ . Suppose that there exists a non-trivial relation*

$$(23.1) \quad \sum_{i < j} a_{i,j} y_i y_j + \sum_i b_i \beta(y_i) = 0 \in H^2(G, \mathbf{F}_p)$$

*with  $a_{i,j}, b_i \in \mathbf{F}_p$ . Then, there exists a sequence  $z_1, \dots, z_m$  of non-zero elements of  $H^1(G, \mathbf{F}_p)$  such that*

$$\prod_{1 \leq i \leq m} \beta(z_i) = 0 \in H^{2m}(G, \mathbf{F}_p).$$

*Proof.* Suppose first that all of  $a_{i,j}$  are zero. In this case, we can take  $m = 1$  and

$$z_1 = \sum_i b_i y_i$$

since  $\beta(z_1) = 0$ , as needed.

Now suppose that one of  $a_{i,j}$  is non-zero. If we write  $x_i = \beta(y_i)$ , then

$$P^1(x_i) = x_i^p, P^1(y_i) = 0, \beta(x_i) = 0$$

when  $p > 2$  and

$$Sq^2(x_i) = x_i^2, Sq^2(y_i) = 0, \beta(x_i) = 0$$

when  $p = 2$ . It follows that if we apply the operation  $\beta \circ P^1 \circ \beta$  when  $p > 2$  or  $\beta \circ \text{Sq}^2 \circ \beta$  when  $p = 2$ , (23.1) becomes

$$(23.2) \quad \sum_{i < j} a_{i,j} x_i^p x_j - x_i x_j^p = 0,$$

where we use the Cartan formula to calculate the Steenrod powers evaluated on a cup product. Since we assumed one of  $a_{i,j}$  is non-zero, (23.2) is also non-trivial. If we choose the finitely many indices such that  $x_1, \dots, x_m$  appear in the non-zero relation, we deduce that the ideal of relations between these elements is non-zero, so that by Proposition 23.6 there exists a relation

$$\prod_{1 \leq i \leq k} u_i$$

where each  $u_i$  is a non-zero linear combination of  $x_i$ . If we write

$$u_i = \sum_{1 \leq j \leq m} c_{i,j} x_j,$$

then we can set

$$z_i := \sum_{1 \leq j \leq m} c_{i,j} y_j$$

and we see that  $\prod \beta(z_i) = \prod u_i = 0$  as needed. □

We now move to the study of  $p$ -cohomological dimension. The main idea is to reduce to the case of pro- $p$  groups and prove the needed result by induction on the index. The most interesting case is that when

$$U \leq G$$

is a normal subgroup of index  $p$ , so that  $G/U \simeq C_p$ , the cyclic group of order  $p$ .

As we observed in Remark 21.16, if  $x \in H^1(C_p, \mathbf{F}_p)$  denotes a generator, then cup product with  $\beta(x) \in H^2(C_p, \mathbf{F}_p)$  induces a 2-fold periodicity in the cohomology algebra of the cyclic group. We now observe that this periodicity is visible in cohomology with any coefficients, and leaves a slightly weaker periodicity in cohomology of  $G$  itself under the assumption that  $U$  is of finite cohomological dimension.

**Lemma 23.8.** *Let  $A$  be a  $C_p$ -module in  $\mathbf{F}_p$ -vector spaces. Then*

$$\beta(x) \cdot - : H^k(C_p, A) \rightarrow H^{k+2}(C_p, A)$$

induced by the cup product is

- (1) an epimorphism when  $k = 0$ ,
- (2) an isomorphism when  $k > 0$ .

*Proof.* We can identify the cohomology groups appearing in the statement with homotopy groups

$$H^k(C_p, A) \simeq \pi_{-k} \text{map}_{C_p}(\mathbf{F}_p, A)$$

of the mapping spectrum in the derived  $\infty$ -category of  $C_p$ -modules in  $\mathbf{F}_p$ -vector spaces. In these terms, the claim is equivalent to the cofibre of the map

$$\text{map}_{C_p}(\mathbf{F}_p, A) \rightarrow \Sigma^2 \text{map}_{C_p}(\mathbf{F}_p, A)$$

induced by the cup product with  $\beta(x)$  being connective. This condition is stable under extensions and filtered colimits, and since any  $A$ -module in  $\mathbf{F}_p$ -vector spaces is built out of filtered colimits and extensions out of  $\mathbf{F}_p$  by Lemma 21.13, the result follows. □

**Proposition 23.9.** *Suppose we have an extension of profinite groups*

$$0 \rightarrow U \rightarrow G \rightarrow C_p \rightarrow 0$$

*and that  $U$  is of finite  $p$ -cohomological dimension  $q$ . If  $x \in H^1(G, \mathbf{F}_p)$  denotes the image of a generator of  $H^1(C_p, \mathbf{F}_p)$ , then for any discrete  $G$ -module  $A$  in  $\mathbf{F}_p$ -vector spaces the map*

$$\beta(x) \cdot - : H^k(G, A) \rightarrow H^{k+2}(G, A)$$

*induced by the cup product is*

- (1) *an epimorphism when  $k = q$ ,*
- (2) *an isomorphism when  $k > q$ .*

*In particular, either  $\text{cd}_p(G) = \text{cd}_p(U)$  or the cohomological dimension of  $G$  is infinite.*

*Proof.* As in the proof of [Lemma 23.8](#) above, the relevant cohomology groups can be identified with homotopy groups of a mapping spectrum in the derived  $\infty$ -category of continuous  $G$ -modules in  $\mathbf{F}_p$ -vector spaces. The claim is equivalent to showing that the cup product map

$$\text{map}_G(\mathbf{F}_p, A) \rightarrow \Sigma^2 \text{map}_G(\mathbf{F}_p, A)$$

has a  $-q$ -connective cofibre. We have an identification

$$\text{map}_G(\mathbf{F}_p, A) \simeq \text{map}_{C_p}(\text{map}_U(\mathbf{F}_p, A))$$

(this is the identification inducing the Lyndon-Hochschild-Serre spectral sequence of [Construction 21.5](#)). Since  $U$  is of finite cohomological dimension, the homotopy groups of  $\text{map}_U(\mathbf{F}_p, A)$  are concentrated in degrees between  $-q$  and  $0$ . It follows that by using the Postnikov tower,  $\text{map}_U(\mathbf{F}_p, A)$  can be obtained by iterated extensions from  $k$ -th shift of objects in the heart for  $-q \leq k \leq 0$ . Each of those has a cofibre of  $\beta(x) \cdot -$  which is  $-q$ -connective by [Lemma 23.8](#) and hence so does their extension, as needed.  $\square$

**Corollary 23.10.** *In the context of [Proposition 23.9](#), for  $G$  to be of finite cohomological dimension, it is sufficient and necessary for some power of  $\beta(x)$  to be zero.*

**Lemma 23.11.** *Let  $G$  be a pro- $p$  group such that all of its open normal subgroups  $U \triangleleft G$  of index  $p$  are of finite cohomological dimension. Then either  $G$  is itself of finite cohomological dimension or it is isomorphic to  $C_p$ .*

*Proof.* By the given condition on normal subgroups, if  $G$  is isomorphic to a (possibly infinite) product of  $C_p$ , then it is isomorphic to  $C_p$  itself. We thus have to show that if  $G$  is not isomorphic to such a product, then it is of finite cohomological dimension.

By [Theorem 21.23](#), if  $(y_i)_{i \in I} \in H^1(G, \mathbf{F}_p)$  is a well-ordered basis, then the elements  $y_i y_j$  for  $i < j$  and  $\beta(y_i)$  are not linearly independent. By [Proposition 23.7](#), it follows that there exists a sequence  $z_1, \dots, z_m \in H^1(G, \mathbf{F}_p)$  of non-zero elements such that the product

$$\beta(z_1) \cdot \dots \cdot \beta(z_m)$$

is zero. Each of  $z_i$  can be identified with a surjective homomorphism  $G \rightarrow C_p$  whose kernel is of finite cohomological dimension by assumption, so that

$$\beta(z_i) \cdot - : H^k(G, \mathbf{F}_p) \rightarrow H^{k+2}(G, \mathbf{F}_p)$$

is an isomorphism for large enough  $k$  by [Proposition 23.9](#). It follows that the multiplication by the product of  $\beta(z_i)$  induces an isomorphism

$$H^k(G, \mathbf{F}_p) \simeq H^{k+2m}(G, \mathbf{F}_p)$$

for  $k$  large enough. Since this product is zero, it follows that these groups vanish in large enough degrees. Since  $G$  is pro- $p$  by assumption, it follows that it is of finite cohomological dimension by [Proposition 21.14](#).  $\square$

**Lemma 23.12.** *Let  $G$  be a profinite group and let  $H_\alpha$  be a cofiltered family of closed subgroups of  $G$  with intersection  $H := \bigcap_\alpha H_\alpha$ . Then*

$$H^*(H, \mathbf{F}_p) \simeq \varinjlim H^*(H_\alpha, \mathbf{F}_p).$$

*Proof.* If  $V_i$  is a basis of open normal subgroups of  $G$ , then

$$H^*(H, \mathbf{F}_p) \simeq \varinjlim_i H^*(H/(H \cap V_i), \mathbf{F}_p) \simeq \varinjlim_i \varinjlim_\alpha H^*(H_\alpha/(H_\alpha \cap V))$$

where the first isomorphism is that of [Corollary 20.23](#) and the second is the observation that  $H_\alpha/(H_\alpha \cap V) \simeq H/(H \cap V)$  for small enough  $H_\alpha$ . As colimits commute with colimits, we can rewrite this as

$$H^*(H, \mathbf{F}_p) \simeq \varinjlim_\alpha \varinjlim_i H^*(H_\alpha/(H_\alpha \cap V)) \simeq \varinjlim_\alpha H^*(H_\alpha, \mathbf{F}_p).$$

□

**Lemma 23.13.** *Let  $G$  be a profinite group which contains an open normal subgroup of index  $p$  which is of finite cohomological dimension. Let  $S$  be the poset of closed subgroups  $H$  of infinite cohomological dimension. If  $S$  is not empty, then it has a minimal element.*

*Proof.* By Zorn’s lemma, it is enough to show that if  $H_\alpha$  is a descending chain of closed normal subgroups of  $G$  which are of infinite cohomological dimension, then  $H := \bigcap_\alpha H_\alpha$  is also of infinite cohomological dimension. Since the  $p$ -cohomological dimension of a profinite group is the same as that of its Sylow subgroup by [Proposition 21.12](#), by intersecting  $H_\alpha$  with a Sylow subgroup of  $G$  we can assume that  $G$  itself is pro- $p$  and hence so are its subgroups.

By assumption, there exists an element  $z \in H^1(G, \mathbf{F}_p)$ , which we can identify with a group homomorphism  $G \rightarrow \mathbf{F}_p$  whose kernel  $U$  is of finite cohomological dimension. Since  $H_\alpha$  are of infinite cohomological dimension by assumption, they cannot be contained in  $U$ , hence the image of the class  $z$  in  $H^1(H_\alpha, \mathbf{F}_p)$  is non-zero for all  $\alpha$ . It follows from [Corollary 23.10](#) that all of the powers of  $\beta(z)$  are also non-zero in  $H^*(H_\alpha, \mathbf{F}_p)$ . By [Lemma 23.12](#), we have

$$H^*(H, \mathbf{F}_p) \simeq \varinjlim H^*(H_\alpha, \mathbf{F}_p)$$

and thus the powers of  $\beta(z)$  are also non-zero in  $H^*(H, \mathbf{F}_p)$ , so that  $H$  is also of infinite cohomological dimension by another application of [Corollary 23.10](#). □

*Proof of Theorem 23.1:* We observed that  $(1 \Rightarrow 3)$  holds in [Proposition 21.17](#). We will prove  $(3 \Rightarrow 2)$ . Since  $(2 \Rightarrow 1)$  is immediate, this will end the proof of the result.

Let  $G$  be a torsion-free profinite group with an open subgroup  $U \leq G$  of finite cohomological dimension; we have to show that  $\text{cd}_p(G) = \text{cd}_p(U)$ . By [Proposition 21.12](#), a profinite group has the same  $p$ -cohomological dimension as its Sylow subgroup, so we can assume that  $G$  is pro- $p$ . By intersecting  $U$  with its conjugates, we can assume that it is normal. Since  $G/U$  is a finite  $p$ -group, by repeatedly choosing a central subgroup of index  $p$ , we construct a finite filtration

$$U = U_0 \leq U_1 \leq \dots \leq U_k = G$$

where each subgroup is normal and of index  $p$  in the next one. By induction, we can thus assume that  $U \leq G$  is of index  $p$ . Let  $S$  be the poset of closed subgroups of  $G$  which are of infinite cohomological dimension. We want to show that  $S$  is empty.

Assume by contradiction that  $S$  is not empty, in which case it has a minimal element  $H \leq G$  by [Lemma 23.13](#). It follows that all proper subgroups of  $H$ , in particular all open subgroup of index  $p$ , are of finite cohomological dimension. Since  $H$  is not by assumption, we deduce that it is finite cyclic by [Lemma 23.11](#), which is a contradiction since  $G$  is torsion-free.

This shows that  $G$  is also of finite dimension, and so we must have  $\text{cd}_p(G) = \text{cd}_p(U)$  by [Proposition 23.9](#), ending the argument. □

24. POINCARÉ DUALITY

If  $X$  is a topological space and  $k$  is a ring, then the cohomology groups  $H^*(X, k)$  acquire a canonical structure of a ring with respect to the *cup product*. The celebrated Poincaré duality theorem tells us that if  $X$  is an orientable, compact manifold of dimension  $n$  and  $k$  is a field, then

- (1)  $H^n(X, k)$  is one-dimensional,
- (2) the cup product  $H^k(X, k) \otimes_k H^{n-k}(X, k) \rightarrow H^n(X, k)$  is a perfect pairing for all  $k \in \mathbb{Z}$ ; that is, it induces an isomorphism

$$\text{Hom}_k(H^k(X, k), H^n(X, k)) \simeq H^{n-k}(X, k).$$

This motivates the following definition:

**Definition 24.1.** We say that a pro- $p$  group  $G$  is *Poincaré of dimension  $n$*  (at a prime  $p$ ) if:

- (1)  $H^n(G, \mathbf{F}_p)$  is a 1-dimensional  $\mathbf{F}_p$ -vector space,
- (2) for all  $k \in \mathbb{Z}$ , the cup product pairing

$$H^k(G, \mathbf{F}_p) \times H^{n-k}(G, \mathbf{F}_p) \rightarrow H^n(G, \mathbf{F}_p)$$

is perfect; that is, it induces an isomorphism

$$H^k(G, \mathbf{F}_p) \simeq \text{Hom}_{\mathbf{F}_p}(H^{n-k}(G, \mathbf{F}_p), H^n(G, \mathbf{F}_p)).$$

**Example 24.2.** Using the description of cohomology of the  $p$ -adics  $\mathbb{Z}_p$  of [Example 24.14](#) one can show that  $H^0(\mathbb{Z}_p, \mathbf{F}_p) \simeq \mathbf{F}_p$ ,  $H^1(\mathbb{Z}_p, \mathbf{F}_p) \simeq \mathbf{F}_p$  and that the other cohomology groups vanish. It follows that

$$H^*(\mathbb{Z}_p, \mathbf{F}_p) \simeq \Lambda_{\mathbf{F}_p}(x),$$

an exterior algebra on a single class of degree  $|x| = 1$ . It follows that  $\mathbb{Z}_p$  is Poincaré of dimension one.

The main result of this lecture is that for pro- $p$  groups, being Poincaré in the sense [Definition 24.1](#) is equivalent to having a duality in cohomology with coefficients in any finite  $p$ -local  $G$ -module, namely that:

- (1) there is a  $G$ -equivariant analogue of Pontryagin duality  $A \mapsto A^{*G}$  which yields a self-duality of the category of  $\text{Mod}_G(\mathcal{A}b_{(p)}^\omega)$  of  $G$ -modules in finite abelian  $p$ -groups,
- (2) there are natural isomorphisms

$$H^k(G, A^{*G}) \simeq H^{n-k}(G, A)^*,$$

where  $(-)^* = \text{Hom}_{\mathcal{A}b}(-, \mathbb{Z}/p^\infty)$  denotes the classical Pontryagin duality.

The conditions (1) and (2) combined give a reasonable definition of being Poincaré in the setting of a general profinite group, not necessarily pro- $p$ . A pleasant property of this notion is that for profinite groups of cohomological dimension  $n$ , being Poincaré is a local property; that is, it can be detected on open subgroups. We will later use this to show that all torsion-free compact  $p$ -adic analytic groups are Poincaré.

**Warning 24.3.** Beware that [Definition 24.1](#) is really only appropriate in the context of pro- $p$  groups. In the case of a general profinite group, one needs to use the more elaborate [Definition 24.24](#). The two are equivalent for pro- $p$  groups.

**Warning 24.4.** If  $X$  is an orientable compact manifold, then a choice of an isomorphism  $H^n(X, k) \simeq k$  combined with Poincaré duality gives a degree-shifting isomorphism

$$H^k(X, k) \simeq \text{Hom}_k(H^{n-k}(X, k), H^n(X, k)) \simeq \text{Hom}_k(H^{n-k}(X, k), k) \simeq H_{n-k}(X, k)$$

between homology and cohomology.

Beware that in general, there is no naive notion of *homology* of profinite groups that would be a dual to cohomology, which is why our discussion of Poincaré duality will be only in terms of cohomology and the cup product. For a specific example, if  $I$  is a countable indexing set, then

$$H^1\left(\prod_{i \in I} \mathbf{F}_p, \mathbf{F}_p\right) \simeq \text{Hom}_{\text{Grp}}^{cts}\left(\prod_{i \in I} \mathbf{F}_p, \mathbf{F}_p\right) \simeq \bigoplus_{i \in I} \mathbf{F}_p.$$

This is a countably dimensional  $\mathbf{F}_p$ -vector space, hence it is not a linear dual of any other  $\mathbf{F}_p$ -vector space. However, for certain special classes of profinite groups, it is possible to have well-behaved homology, see [SW00, §3.7].

We first show that Poincaré pro- $p$  groups have a duality in cohomology with coefficients in  $G$ -modules in  $\mathbf{F}_p$ -vector spaces.

**Lemma 24.5.** *Let  $G$  be a pro- $p$  groups which is Poincaré of dimension  $n$ . Then*

- (1)  $H^k(G, \mathbf{F}_p)$  is finite-dimensional for every  $k \in \mathbb{Z}$ .
- (2)  $G$  is finitely generated and of  $p$ -cohomological dimension  $n$ .

*Proof.* Applying the second property of Definition 24.1 to  $k$  and  $n - k$  we see that  $H^k(G, \mathbf{F}_p)$  is isomorphic to the linear dual of  $H^{n-k}(G, \mathbf{F}_p)$  and vice versa. This can only happen if both are finite-dimensional, as otherwise the linear dual has a basis of strictly larger cardinality.

The finiteness of cohomological dimension in the pro- $p$  case follows immediately from Proposition 21.14 and the fact that  $H^k(G, -)$  vanishes for  $k < 0$ . Finite generation is Corollary 21.21.  $\square$

**Proposition 24.6.** *Let  $G$  be Poincaré of dimension  $n$  which is a pro- $p$ -group. Then for discrete  $G$ -module  $V$  which is a finite-dimensional  $\mathbf{F}_p$ -vector space and any  $k \in \mathbb{Z}$  the cup product pairing*

$$H^k(G, V) \times H^{n-k}(G, V^*) \rightarrow H^n(G, V \otimes_{\mathbf{F}_p} V^*) \rightarrow H^n(G, \mathbf{F}_p)$$

*induces an isomorphism*

$$H^k(G, V) \simeq \text{Hom}_{\mathbf{F}_p}(H^{n-k}(G, V^*), H^n(G, \mathbf{F}_p))$$

*Proof.* We work in the  $\infty$ -category of  $\mathbf{F}_p$ -modules in the derived  $\infty$ -category  $\check{\mathcal{D}}(\text{Mod}_G(\text{Ab}))$ , which one can identify with the derived  $\infty$ -category  $\check{\mathcal{D}}(\text{Mod}_G(\text{Vect}_{\mathbf{F}_p}))$  of discrete  $\mathbf{F}_p$ -vector spaces. If  $V$  is a  $\mathbf{F}_p$ -vector space in discrete  $G$ -modules, then its cohomology groups can be identified with homotopy of

$$\text{map}_G(\mathbf{F}_p, V) := \text{map}_{\check{\mathcal{D}}(\text{Mod}_G(\text{Vect}_{\mathbf{F}_p}))}(\mathbf{F}_p, V).$$

This is canonically an object of the derived  $\infty$ -category  $\mathcal{D}(\mathbf{F}_p)$  of vector spaces, and since the latter is semisimple, we have a canonical direct sum decomposition

$$\text{map}_G(\mathbf{F}_p, V) \simeq \bigoplus_{k \in \mathbb{Z}} \Sigma^{-k}(H^k(G, V)),$$

where we identify each cohomology group with an object of the heart.

In these terms, the cup product pairing in question is induced by the composite

$$\text{map}_G(\mathbf{F}_p, V) \otimes_{\mathbf{F}_p} \text{map}_G(\mathbf{F}_p, V^*) \rightarrow \text{map}_G(\mathbf{F}_p, \mathbf{F}_p) \rightarrow \Sigma^{-n}(H^n(G, \mathbf{F}_p))$$

which is adjoint to a map in  $\mathcal{D}(\mathbf{F}_p)$  of the form

$$(24.1) \quad \text{map}_G(\mathbf{F}_p, V) \rightarrow \text{map}_{\mathbf{F}_p}(\text{map}_G(\mathbf{F}_p, V^*), \Sigma^{-n}(H^n(G, \mathbf{F}_p))).$$

The desired statement is equivalent to the assertion that this map is an equivalence.

By assumption, (24.1) is an equivalence when  $V = \mathbf{F}_p$ . Since short exact sequences of discrete  $G$ -modules become cofibre sequences in the derived  $\infty$ -category, both sides of (24.1) take short exact sequences to cofibre sequences in  $\mathcal{D}(\mathbf{F}_p)$ . As  $G$  is pro- $p$ , any finite-dimensional  $\mathbf{F}_p$ -vector space in discrete  $G$ -modules can be built using iterated extensions from  $\mathbf{F}_p$  by Lemma 21.13 and the claim follows.  $\square$

**Corollary 24.7.** *Let  $G$  be a pro- $p$ -group which is Poincaré of dimension  $n$  and let  $U \leq G$  be an open subgroup. Then*

- (1) *corestriction induces an isomorphism  $H^n(U, \mathbf{F}_p) \simeq H^n(G, \mathbf{F}_p)$ ,*
- (2)  *$U$  is also Poincaré of dimension  $n$ .*

*Proof.* For the first property we recall that

$$H^n(U, \mathbf{F}_p) \simeq H^n(G, \text{coind}_U^G(\mathbf{F}_p))$$

and that the corestriction map is induced by the surjection  $\text{coind}_U^G(\mathbf{F}_p) \rightarrow \mathbf{F}_p$  of [Construction 21.8](#). Using [Proposition 24.6](#), the corestriction map on top cohomology can be identified (by choosing an isomorphism  $H^n(G, \mathbf{F}_p) \simeq \mathbf{F}_p$ ) with the linear dual of

$$H^0(G, \mathbf{F}_p) \rightarrow H^0(G, \text{coind}_U^G(\mathbf{F}_p)^*) \simeq H^0(G, \mathbf{F}_p[G/U])$$

induced by the map  $\mathbf{F}_p \hookrightarrow \mathbf{F}_p[G/U]$  defined by  $1 \mapsto \sum_{g \in G/U} g$ . This map is an isomorphism on invariants, as needed.

We move on to the second property. By the first part, we know that  $H^n(U, \mathbf{F}_p)$  is one-dimensional and we are left with verifying the non-degeneracy of the cup product. By [Remark 20.11](#), there's a canonical self-duality isomorphism

$$\text{coind}_U^G(\mathbf{F}_p)^* \simeq \text{ind}_U^G(\mathbf{F}_p)^* \simeq \text{coind}_U^G(\mathbf{F}_p)$$

under which the cup product pairing

$$H^k(U, \mathbf{F}_p) \times H^{n-k}(U, \mathbf{F}_p) \rightarrow H^n(U, \mathbf{F}_p)$$

gets identified with the pairing

$$H^k(G, \text{coind}_U^G(\mathbf{F}_p)) \times H^{n-k}(G, \text{coind}_U^G(\mathbf{F}_p)) \rightarrow H^n(G, \mathbf{F}_p)$$

This is a perfect pairing by [Proposition 24.6](#), giving the needed claim. □

**Remark 24.8** (Poincaré duality interchanges restriction and corestriction). Suppose that  $G$  is a Poincaré pro- $p$  group of dimension  $n$  and that we fix an isomorphism  $H^n(G, \mathbf{F}_p) \simeq \mathbf{F}_p$ . In this case, by [Proposition 24.6](#), for any discrete  $G$ -module  $V$  in finite-dimensional  $\mathbf{F}_p$ -vector spaces, the cup product induces a duality isomorphism

$$H^k(G, V) \simeq H^{n-k}(G, V^*)^*.$$

If  $U \leq G$  is an open subgroup, then by [Lemma 22.24](#) corestriction induces an isomorphism  $\mathbf{F}_p \simeq H^*(G, \mathbf{F}_p) \simeq H^n(U, \mathbf{F}_p)$ , and we similarly have duality in cohomology of  $U$ . Thus, applying linear duals to the restriction homomorphism we obtain for each  $k \in \mathbb{Z}$  a canonical map

$$H^k(U, V) \simeq H^{n-k}(U, V^*)^* \xrightarrow{\text{res}^*} H^{n-k}(G, V^*)^* \simeq H^k(G, V)$$

As a consequence of [Lemma 22.24](#), this map can be identified with the corestriction homomorphism in cohomology.

To extend the duality in cohomology of [Proposition 24.6](#) from  $\mathbf{F}_p$ -vector spaces to arbitrary  $p$ -torsion coefficients, we will need a more refined notion of duality in coefficients than just the linear duality of vector space. This duality is given by a  $G$ -equivariant version of Pontryagin duality.

The construction of the needed self-duality of the category of coefficients rests on the notion of a dualizing module, which exists more generally for profinite group of  $p$ -cohomological dimension  $n$ . This is a discrete  $G$ -module  $I$  which, informally, represents the functor

$$M \mapsto H^n(G, M)$$

on the category of  $p$ -torsion  $G$ -modules. As stated, this does not quite make sense, since the cohomology functor is covariant in the module, but any functor represented by an object is

necessarily contravariant. To fix this discrepancy, we will make use of Pontryagin duality in  $p$ -torsion abelian groups, which we now recall.

**Recollection 24.9** ( $p$ -torsion Pontryagin duality). In the category of  $p$ -local abelian groups, the group

$$\mathbb{Z}/p^\infty \simeq \varinjlim \mathbb{Z}/p^k \simeq \mathbb{Q}_p/\mathbb{Z}_p$$

is an injective cogenerator; that is, it is injective and any object embeds into a sufficiently large product of  $\mathbb{Z}/p^\infty$ . The classical Pontryagin duality theorem shows that the functor

$$\mathrm{Hom}_{\mathcal{A}b}(-, \mathbb{Z}/p^\infty): (\mathcal{A}b_{(p)}^\omega)^{op} \rightarrow \mathcal{A}b_{(p)}^\omega$$

is a self-duality (that is, a contravariant autoequivalence) of the category of finite abelian  $p$ -groups. If  $A$  is a  $p$ -torsion abelian group, we write

$$A^* := \mathrm{Hom}_{\mathcal{A}b}(A, \mathbb{Z}/p^\infty)$$

for its Pontryagin dual.

**Example 24.10.** Since the simple  $p$ -torsion subgroup of  $\mathbb{Z}/p^\infty$  is given by  $\mathbb{Z}/p \simeq \mathbb{F}_p$ , if  $A$  is an  $\mathbb{F}_p$ -vector space, then its Pontryagin dual as an abelian group can be identified with its linear dual; that is

$$A^* \simeq \mathrm{Hom}_{\mathbb{F}_p}(A, \mathbb{F}_p).$$

**Remark 24.11.** Using the simple calculation that

$$\mathrm{Hom}_{\mathcal{A}b}(\mathbb{Z}/p^k, \mathbb{Z}/p^\infty) \simeq \mathbb{Z}/p^k$$

and classification of finite abelian groups, one can show that for any finite  $p$ -local abelian group there exists a *non-canonical* isomorphism

$$A \simeq A^*.$$

Taking into account [Example 24.10](#), this extends the familiar fact that any finite-dimensional vector space is non-canonically isomorphic to its linear dual.

**Definition 24.12.** Let  $G$  be a profinite group of  $p$ -cohomological dimension  $n$ . A ( $p$ -typical) *dualizing module* is a discrete  $G$ -module  $I$  representing the functor

$$M \mapsto H^n(G, M)^* \simeq \mathrm{Hom}_{\mathcal{A}b}(H^n(G, M), \mathbb{Z}/p^\infty)$$

on the category of  $p$ -torsion discrete  $G$ -modules.

Note that to represent a functor is an additional structure rather than a property. In more detail, a dualizing module is a discrete  $G$ -module  $I$  together with a map

$$\alpha: H^n(G, I) \rightarrow \mathbb{Z}/p^\infty$$

such that for any  $p$ -torsion  $M$ , composition with  $\alpha$  yields a bijection

$$\mathrm{Hom}_{\mathrm{Mod}_G(\mathcal{A}b)}(M, I) \simeq H^n(G, M)^*$$

**Proposition 24.13.** *Let  $G$  be a profinite group of  $p$ -cohomological dimension at most  $n$ . Then a dualizing module  $I$  for  $G$  exists.*

*Proof.* Let us denote by

$$\mathrm{Mod}_G^{p\text{-tors}}(\mathcal{A}b) \subseteq \mathrm{Mod}_G(\mathcal{A}b)$$

the full subcategory spanned by  $p$ -torsion discrete  $G$ -modules. This subcategory is closed under extensions, quotients, kernels and direct sums, so that it is a localizing subcategory. In particular, it is itself Grothendieck abelian and hence presentable.

In any presentable category, a functor is representable if and only if it takes colimits to limits. Thus, we have to verify that

$$M \mapsto \mathrm{Hom}_{\mathcal{A}b}(H^n(G, M), \mathbb{Z}/p^\infty).$$

takes colimits to limits. Since  $\text{Hom}_{\mathcal{A}b}(-, \mathbb{Z}/p^\infty)$  has this property, it's enough to check that

$$H^n(G, -): \text{Mod}_G^{p\text{-tors}}(\mathcal{A}b) \rightarrow \mathcal{A}b$$

preserves colimits. By [Corollary 20.23](#), it preserves filtered colimits, so it's enough to verify that it is right exact. If

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is a short exact sequence of  $p$ -torsion discrete  $G$ -modules, then the long exact sequence of cohomology ends in

$$\dots \rightarrow H^n(G, A) \rightarrow H^n(G, B) \rightarrow H^n(G, C) \rightarrow 0$$

by the assumption that  $G$  is of cohomological dimension  $n$ . This shows that  $H^n(G, -)$  is right exact, as needed.  $\square$

**Example 24.14.** We recall the fact previously used in [Example 21.18](#) that for  $p$ -torsion discrete  $\mathbb{Z}_p$ -modules, their group cohomology can be calculated as the cohomology of the cochain complex

$$M \xrightarrow{1-\sigma} M ,$$

where  $\sigma \in \mathbb{Z}_p$  is the topological generator. Since  $(-)^*$  is exact, we deduce that

$$\text{Hom}_{\text{Mod}_{\mathbb{Z}_p}(\mathcal{A}b)}(M, I) \simeq H^1(\mathbb{Z}_p, M)^*$$

can be calculated as the kernel of

$$M^* \xrightarrow{1-\sigma} M^* .$$

If  $M$  is a finite discrete  $G$ -module, then so is  $M^*$ , and we can rewrite this as

$$\text{Hom}_{\text{Mod}_{\mathbb{Z}_p}(\mathcal{A}b)}(M, I) \simeq H^0(\mathbb{Z}_p, M^*) \simeq \text{Hom}_{\mathcal{A}b}(M, \mathbb{Z}/p^\infty)^{\mathbb{Z}_p} \simeq \text{Hom}_{\text{Mod}_{\mathbb{Z}_p}(\mathcal{A}b)}(M, \mathbb{Z}/p^\infty).$$

It follows that for  $G = \mathbb{Z}_p$ , the dualizing module is given by  $\mathbb{Z}/p^\infty$ , equipped with the trivial  $G$ -action.

We now show that [Example 24.14](#) is somewhat typical; namely, that a dualizing module of a Poincaré pro- $p$  group  $G$  is isomorphic as an abelian group  $\mathbb{Z}/p^\infty$  (possibly with a non-trivial  $G$ -action). The first step is to verify that formation of dualizing modules is compatible with passing to open subgroups.

**Lemma 24.15.** *Let  $G$  be a cohomological group of  $p$ -cohomological dimension at most  $n$ . Then for any open subgroup  $U \leq G$ , the restriction  $\text{res}_U^G(I)$  of the dualizing module for  $G$  is the dualizing module for  $U$ .*

*Proof.* Let  $A$  be a finite  $p$ -local discrete  $U$ -module. Then

$$H^n(U, A)^* \simeq H^n(G, \text{coind}_U^G(A))^* \simeq \text{Hom}_{\text{Mod}_G(\mathcal{A}b)}(\text{coind}_U^G(A), I) \simeq \text{Hom}_{\text{Mod}_U(\mathcal{A}b)}(U, \text{res}_U^G(I)),$$

where we use that for open subgroups, the coinduction functor is also left adjoint to restriction, as observed in [Remark 20.11](#).  $\square$

**Lemma 24.16.** *Let  $G$  be an Poincaré pro- $p$ -group. Then for any finite  $p$ -local discrete  $G$ -module  $A$ , the groups  $H^k(G, A)$  are finite.*

*Proof.* This is immediate from [Lemma 24.5](#), [Lemma 21.13](#) and the long exact sequence of cohomology.  $\square$

**Lemma 24.17.** *Let  $G$  be a pro- $p$  Poincaré group of dimension  $n$  and for each  $k \in \mathbb{Z}$  consider the functor*

$$A \mapsto T_k(A) := \varprojlim H^k(U, A),$$

where the limit is taken over the poset of open normal subgroups  $U \triangleleft G$  along corestriction maps. Then

- (1)  $T_k(A)$  vanishes for  $k \neq n$  and all  $A$ ,

(2)  $A \mapsto T_n(A)$  is exact.

*Proof.* As a consequence of [Lemma 24.16](#) and [Corollary 24.7](#), the groups  $H^k(U, A)$  are finite for each  $k \in \mathbb{Z}$  and each open normal subgroup  $U$ . It follows that for each  $k$  and each  $A$ , the diagram  $H^k(-, A)$  satisfies the Mittag-Leffler condition and thus the derived functors of the limit vanish. We deduce that a short exact sequence of modules induces a long exact sequences of functors  $T_k$ . This implies that the second part of the claim will follow from the first.

Using the long exact sequence and [Lemma 21.13](#), it is enough to verify the vanishing of  $T_k(\mathbf{F}_p)$  for  $k \neq n$ . We have

$$T_k(\mathbf{F}_p) \simeq \varinjlim H^k(U, \mathbf{F}_p) \simeq \varinjlim H^{n-k}(U, \mathbf{F}_p)^* \simeq (\varinjlim H^{n-k}(U, \mathbf{F}_p))^*,$$

where the colimit on the right is taken over restriction homomorphism, where we use that Poincaré duality interchanges restriction and corestriction as observed in [Remark 24.8](#). We have

$$\varinjlim H^{n-k}(U, \mathbf{F}_p) \simeq \varinjlim H^{n-k}(G, \text{coind}_U^G(\mathbf{F}_p)) \simeq H^{n-k}(G, \text{coind}_1^G(\mathbf{F}_p)) \simeq H^{n-k}(1, \mathbf{F}_p)$$

which vanishes unless  $k = n$ , ending the argument.  $\square$

**Theorem 24.18.** *Let  $G$  be a profinite group of cohomological dimension  $n$  which has an open subgroup which is a Poincaré pro- $p$ -group. Then the dualizing module  $I$  of  $G$  is isomorphic, as an abelian group, to  $\mathbb{Z}/p^\infty$ .*

*Proof.* By [Lemma 24.15](#), formation of the dualizing module is compatible with passing to open subgroups, so that we can assume that  $G$  itself is pro- $p$ . By another application of this result, if  $A$  is a finite  $p$ -local discrete  $G$ -module, then

$$H^n(U, A) \simeq \text{Hom}_{\text{Mod}_U(\mathcal{A}b)}(A, I)^*.$$

Passing to the limit over the poset of open subgroups along the corestriction maps, we see that

$$T_n(A) \simeq (\varinjlim \text{Hom}_{\text{Mod}_U(\mathcal{A}b)}(A, I))^* \simeq \text{Hom}_{\mathcal{A}b}(\text{Hom}_{\mathcal{A}b}(A, I), \mathbb{Z}/p^\infty),$$

where the left hand side is the functor appearing in [Lemma 24.17](#). This is exact, and since  $\mathbb{Z}/p^\infty$  is an injective cogenerator of  $p$ -local abelian groups, we deduce that

$$A \mapsto \text{Hom}_{\mathcal{A}b}(A, I)$$

is exact. It follows that  $I$  is injective.

As  $I$  is injective, the map  $p: I \rightarrow I$  is surjective, and as it is  $p$ -torsion by construction, to verify that  $I \simeq \mathbb{Z}/p^\infty$  as abelian groups it is enough to verify that

$$\text{Hom}_{\mathcal{A}b}(\mathbf{F}_p, I) \simeq \mathbf{F}_p.$$

Since  $G$  is Poincaré, we have  $H^n(U, \mathbf{F}_p) \simeq \mathbf{F}_p$  for all open subgroups by [Corollary 24.7](#), and thus

$$\mathbf{F}_p \simeq T_n(\mathbf{F}_p) \simeq \text{Hom}_{\mathcal{A}b}(\text{Hom}_{\mathcal{A}b}(\mathbf{F}_p, I), \mathbb{Z}/p^\infty)$$

which gives the needed result.  $\square$

For groups whose dualizing module is isomorphic to  $\mathbb{Z}/p^\infty$ , such as Poincaré pro- $p$  groups, Pontryagin duality has the following  $G$ -equivariant variation:

**Definition 24.19.** Let  $G$  be a group whose dualizing module  $I$  is isomorphic as an abelian group to  $\mathbb{Z}/p^\infty$ . If  $A$  is a finite  $p$ -local discrete  $G$ -module, its  $G$ -Pontryagin dual is given by

$$A^{*G} := \text{Hom}_{\mathcal{A}b}(A, I),$$

with action defined by

$$(g \cdot f)(a) = g \cdot f(g^{-1}a).$$

**Remark 24.20.** The Pontryagin dual of [Definition 24.19](#) can be identified with the internal Hom in discrete  $G$ -modules; that is, the right adjoint to the tensor product. It has the property that

$$(A^{*G})^U \simeq \text{Hom}_{\text{Mod}_U(Ab)}(A, I)$$

for any open subgroup  $U$ . More generally, the same formula defines the internal Hom whenever  $A$  is finitely generated.<sup>13</sup>

It follows from the corresponding properties of Pontryagin duality that the functor  $*_G$  defines an exact contravariant equivalence from the category of finite  $p$ -local discrete  $G$ -modules to itself. Moreover, there is a canonical isomorphism

$$A \simeq (A^{*G})^{*G}.$$

**Remark 24.21.** If  $G$  is pro- $p$  group satisfying the conditions of [Definition 24.19](#), then the simple  $p$ -torsion subgroup

$$I[p] \simeq (\mathbb{Z}/p^\infty)[p] \simeq \mathbb{Z}/p$$

is necessarily acted on trivially by  $G$ . It follows that a choice of an isomorphism  $I[p] \simeq \mathbb{F}_p$  yields for any discrete  $G$ - $\mathbb{F}_p$ -vector space  $V$  an isomorphism

$$V^{*G} \simeq V^* \simeq \text{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p)$$

In other words, for pro- $p$  groups,  $G$ -Pontryagin duality is essentially equivalent to the usual linear duality of vector spaces.

The notion of a  $G$ -equivariant Pontryagin dual is important, as cohomology of  $A$  and its dual are naturally related by a bilinear pairing:

**Construction 24.22.** Let  $G$  be a profinite group whose dualizing module  $I$  is isomorphic to  $\mathbb{Z}/p^\infty$  as an abelian group. If  $A$  is a discrete  $G$ -module in finite abelian  $p$ -groups, then the map  $A \times A^{*G} \rightarrow I$  defined by

$$a \times f \mapsto f(a)$$

induces a map of  $G$ -modules

$$A \otimes_{\mathbb{Z}} A^{*G} \rightarrow I.$$

For any  $k$  we obtain a bilinear pairing as a composite

$$H^k(G, A) \times H^{n-k}(G, A^{*G}) \rightarrow H^n(G, A \otimes_{\mathbb{Z}} A^{*G}) \rightarrow H^n(G, I) \rightarrow \mathbb{Z}/p^\infty.$$

This yields a map

$$H^{n-k}(G, A^{*G}) \rightarrow H^k(G, A)^*,$$

where the right hand side is the classical Pontryagin dual of the cohomology group.

If  $G$  is pro- $p$ , by [Proposition 24.6](#) linear duality of  $\mathbb{F}_p$ -vector spaces gives a duality in cohomology. Since the latter is a special case of  $G$ -Pontryagin duality by [Remark 24.21](#), it is not unreasonable to expect that the latter yields a duality in cohomology with more general coefficients. This is indeed the case, and it characterizes Poincaré pro- $p$  groups as we now show:

**Theorem 24.23.** *Let  $G$  be a pro- $p$  group of cohomological dimension  $n$  whose dualizing module is isomorphic as an abelian group to  $\mathbb{Z}/p^\infty$ . Then the following are equivalent:*

- (1)  $G$  is Poincaré of dimension  $n$  in the sense of [Definition 24.1](#),

---

<sup>13</sup>Beware that  $\text{Hom}_{Ab}(A, I)$  is not necessarily the internal Hom in discrete  $G$ -modules if  $A$  is not finitely generated. For example

$$\text{Hom}_{Ab}(\text{map}_{cts}(G, \mathbb{F}_p), \mathbb{F}_p) \simeq \mathbb{F}_p[[G]],$$

which is not discrete as a  $G$ -module. In general, the internal Hom is given by the submodule of  $\text{Hom}_{Ab}$  consisting of those vectors which are stabilized by some open subgroup.

(2) the map of [Construction 24.22](#) induces an isomorphism

$$H^{n-k}(G, A^{*G}) \rightarrow H^k(G, A)^*,$$

for any discrete  $G$ -module  $A$  in finite abelian  $p$ -groups.

*Proof.* The argument for  $(1 \Rightarrow 2)$  is essentially the same as in [Proposition 24.6](#), using that  $A \mapsto A^{*G}$  is exact since  $I$  is injective as an abelian group and that any finite  $p$ -local discrete  $G$ -module can be obtained by iterated extensions from  $\mathbf{F}_p$ .

We now argue that  $(2 \Rightarrow 1)$  by verifying the two conditions of [Definition 24.1](#). Observe that we have isomorphisms

$$\mathbf{F}_p^{*G} \simeq \text{Hom}_{Ab}(\mathbf{F}_p, I) \simeq I[p]$$

and that all three have trivial  $G$ -actions since they're one-dimensional and  $G$  is pro- $p$ . By assumption, we have

$$I[p] \simeq H^0(G, I[p]) \simeq H^0(G, \mathbf{F}_p^{*G}) \simeq H^n(G, \mathbf{F}_p)$$

so the latter is one-dimensional as needed, verifying the first condition.

For the second condition, observe that

$$H^n(G, I[p]) \rightarrow H^n(G, I) \rightarrow \mathbb{Z}/p^\infty$$

the composite is non-zero, or else the pairing of [Construction 24.22](#) would be zero for all  $\mathbf{F}_p$ -vector spaces. Since the source is one-dimensional by the previous paragraph, the composite induces an isomorphism

$$H^n(G, I[p]) \simeq (\mathbb{Z}/p^\infty)[p].$$

Since the pairing of [Construction 24.22](#) is perfect by assumption, it follows that the pairing of  $\mathbf{F}_p$ -vector spaces

$$H^k(G, \mathbf{F}_p) \times H^{n-k}(G, I[p]) \rightarrow H^n(G, I[p])$$

is also perfect. Since  $I[p] \simeq \mathbf{F}_p$  as  $G$ -modules, this implies the same for the cup product pairing

$$H^k(G, \mathbf{F}_p) \times H^{n-k}(G, \mathbf{F}_p) \rightarrow H^n(G, \mathbf{F}_p),$$

which is what we wanted to show. □

Using the above result, we can extend the notion of being Poincaré to general profinite groups:

**Definition 24.24.** We say a profinite group  $G$  is *Poincaré of dimension  $n$*  (at a prime  $p$ ) if:

- (1) it is of cohomological dimension  $n$ ,
- (2) the dualizing module  $I$  is isomorphic to  $\mathbb{Z}/p^\infty$  as an abelian group,
- (3) the pairing of [Construction 24.22](#) induces an isomorphism

$$H^{n-k}(G, A^{*G}) \rightarrow H^k(G, A)^*,$$

for any discrete  $G$ -module  $A$  in finite abelian  $p$ -groups.

**Warning 24.25.** If  $G$  is pro- $p$ , then the above definition of Poincaré group is equivalent to the one we gave in [Definition 24.24](#) as a consequence of [Definition 24.24](#). In other words, for pro- $p$  groups, Poincaré duality is detected by the non-degeneracy of the cup product in mod  $p$  cohomology.

Beware that this is not true for general profinite groups. For a concrete example, let us identify the cyclic group  $C_{p-1} \leq \mathbb{Z}_p^\times$  with the subgroup of  $(p-1)$ -th roots of unity. This acts on  $\mathbb{Z}_p$  by multiplication and we can consider the semi-direct product

$$G := \mathbb{Z}_p \rtimes C_{p-1}.$$

Since  $C_{p-1}$  is of order coprime to  $p$ , the Lyndon-Hochschild-Serre spectral sequence of [Construction 21.5](#) collapses and we see that

$$H^*(G, \mathbf{F}_p) \simeq H^*(\mathbb{Z}_p, \mathbf{F}_p)^{C_{p-1}}.$$

Since  $H^1(\mathbb{Z}_p, \mathbf{F}_p)$  is generated by the quotient map  $\mathbb{Z}_p \rightarrow \mathbf{F}_p$  (under the description of [Example 20.22](#)), it is acted on non-trivially by the roots of unity, so that  $H^*(G, \mathbf{F}_p)$  vanishes in positive degrees. Despite this,  $G$  is not a Poincaré group of dimension zero.

As the last part of today’s class, we describe how the property of being Poincaré interacts with passing to open subgroups:

**Lemma 24.26.** *Let  $G$  be profinite group of cohomological dimension  $n$  and let  $U \leq G$  be an open subgroup. Then the following are equivalent:*

- (1)  $G$  is Poincaré of dimension  $n$ ,
- (2)  $U$  is Poincaré of dimension  $n$ .

**Warning 24.27.** In the context of [Lemma 24.26](#), beware that it is important to assume that  $G$  is of finite cohomological dimension. For example, the cyclic group  $C_p$  has the trivial group as an open subgroup, which is necessarily Poincaré of dimension zero. However,  $C_p$  is not of finite cohomological dimension by the calculation of [Example 21.15](#), so in particular it is not Poincaré.

*Proof of Lemma 24.26:* By [Lemma 21.4](#),  $U$  is also of cohomological dimension at most  $n$ . By [Lemma 24.15](#),  $G$  has a dualizing module isomorphic as an abelian group to  $\mathbb{Z}/p^\infty$  if and only if  $U$  does. Thus, we only need to verify that the third condition of [Definition 24.24](#) holds for  $G$  if and only if it holds for  $U$ .

First assume that it holds for  $G$ . If  $A$  is a discrete  $U$ -module in finite abelian  $p$ -groups, then  $H^*(U, A) \simeq H^*(G, \text{coind}_U^G(A))$  by Shapiro’s [Lemma 20.15](#). Moreover, the map

$$H^{n-k}(U, A^{*U}) \rightarrow H^k(U, A)^*$$

can be identified with

$$H^{n-k}(G, (\text{coind}_U^G(A))^{*G}) \rightarrow H^k(G, \text{coind}_U^G(A))^*$$

and so it is an isomorphism.

Now suppose that  $U$  is Poincaré and let  $A$  be a discrete  $G$ -module in finite abelian  $p$ -groups. Since they are given by Ext-groups, in terms of the derived  $\infty$ -category of [§22](#), the cohomology groups can be identified

$$H^*(G, A) \simeq \pi_{-*}(\text{map}_{\mathcal{D}(\text{Mod}_G(Ab))}(\mathbb{Z}, A)).$$

In these terms, the map of [Construction 24.22](#) is obtained by applying  $\pi_{-*}(-)$  to a map of spectra

$$(24.2) \quad \text{map}_{\mathcal{D}(\text{Mod}_G(Ab))}(\mathbb{Z}, A^{*G}) \rightarrow \text{map}_{\mathcal{D}(\mathbb{Z})}(\text{map}_{\mathcal{D}(\text{Mod}_G(Ab))}(\mathbb{Z}, A), \mathbb{Z}/p^\infty).$$

We denote the cofibre of this map by  $C(A)$ ; we want to show that it is zero. By construction, it has homotopy concentrated in degrees  $-n \leq k \leq 1$ .

Since both the source and target of [\(24.2\)](#) do, the construction  $A \mapsto C(A)$  takes short exact sequences of modules to cofibre sequences of spectra. Consider the short exact sequence

$$0 \rightarrow A \rightarrow \text{coind}_U^G(A) \rightarrow \underline{\text{coind}}_U^G(A) \rightarrow 0,$$

where the underline denotes the cokernel of the first map. Since the pairing on  $G$ -cohomology of  $\text{coind}_U^G(A)$  can be identified with the pairing on  $U$ -cohomology of  $A$  which is an isomorphism by assumption, we deduce that  $C(\text{coind}_U^G(A)) = 0$  and thus

$$C(\underline{\text{coind}}_U^G(A)) \simeq \Sigma C(A).$$

Iterating this we see that

$$C((\underline{\text{coind}}_U^G)^{n+2}(A)) \simeq \Sigma^{n+2} C(A).$$

Since the left hand side has homotopy in degrees  $-n \leq k \leq 1$  and the right hand side (as an  $(n + 2)$ -fold suspension) in degrees  $2 \leq k \leq n + 3$ , we deduce that they are both zero, ending the argument.  $\square$

25. COHOMOLOGY OF  $p$ -ADIC ANALYTIC GROUPS

In this lecture, we will prove a theorem of Lazard that uniform groups have very simple mod  $p$  cohomology; in particular, they are Poincaré groups. Since any compact  $p$ -adic analytic group has a normal open uniform subgroup, this gives an efficient way of calculating their cohomology in general, by first calculating the cohomology of a uniform subgroup and then using the Lyndon-Hochschild-Serre spectral sequence.

**Theorem 25.1** (Lazard). *Let  $G$  be a uniform pro- $p$ -group. Then the inclusion of elements of cohomological degree one induces an isomorphism*

$$H^*(G, \mathbf{F}_p) \simeq \Lambda_{\mathbf{F}_p} H^1(G, \mathbf{F}_p)$$

between the cohomology algebra and the exterior algebra on the first cohomology group.

Using the work of Serre on cohomology of profinite groups, we deduce the following:

**Corollary 25.2.** *Let  $G$  be a compact  $p$ -torsion-free  $p$ -adic analytic group. Then  $G$  is a Poincaré group of cohomological dimension equal to its dimension as a  $p$ -adic manifold.*

*Proof.* First assume that  $G$  is uniform, so that its dimension is equal to its rank. As a consequence of [Theorem 6.9](#), a rank of a powerful pro- $p$ -group is equal to the cardinality of a minimal generating set, which by [Lemma 21.20](#) is equal to the dimension of  $H^1(G, \mathbf{F}_p)$ . It follows that  $H^{\text{rk}(G)}(G, \mathbf{F}_p)$  is one-dimensional. Since in an exterior algebra the products are non-degenerate, the statement follows from [Theorem 25.1](#) and [Theorem 24.23](#).

If  $G$  a general compact  $p$ -adic analytic group, then it has a finite index open uniform subgroup  $U \leq G$  of rank equal to the dimension of  $G$  by [Theorem 19.11](#). It follows from the previous paragraph that  $U$  is Poincaré. Since  $G$  is  $p$ -torsion-free, it is of the same cohomological dimension as  $U$  by Serre’s [Theorem 23.1](#). It follows that it is also Poincaré by [Lemma 24.26](#).  $\square$

We first describe the general idea leading to the proof of [Theorem 25.1](#). If  $G$  is a finite group, then  $G$ -modules in  $\mathbf{F}_p$ -vector spaces can be identified with left modules over the group algebra  $\mathbf{F}_p[G]$ . Similarly, if  $G$  is profinite, then a discrete  $G$ -module determines a module over the completed group algebra  $\mathbf{F}_p[[G]] \simeq \varprojlim \mathbf{F}_p[G/U]$ , and this functor is fully faithful<sup>14</sup>. Using this correspondence, discrete  $G$ -modules can be studied by applying ring-theoretic techniques to the completed group algebra.

In [§15](#), we described a canonical filtration on the completed group algebra of a uniform group, and we had shown that the associated graded ring has a very regular structure. Any multiplicative filtration on a ring determines a spectral sequence relating the Ext-groups of the ring itself with the associated graded. In this lecture, we apply a variation on this spectral sequence to calculate the cohomology of uniform groups.

The bulk of this lecture is devoted to the construction of a convergent spectral sequence. The methods we employ work in vast generality, but for concreteness we focus on the case of finitely generated pro- $p$ -groups and the augmentation ideal filtration, making the following convention:

**Notation 25.3.** Throughout this lecture,  $G$  denotes a finitely generated pro- $p$ -group,

$$\mathbf{F}_p[[G]] := \varprojlim \mathbf{F}_p[G/G_k]$$

denotes the completed group algebra, and

$$I := \ker(\mathbf{F}_p[[G]] \rightarrow \mathbf{F}_p)$$

denotes the augmentation ideal.

<sup>14</sup>The inclusion of discrete  $G$ -modules into left  $\mathbf{F}_p[[G]]$ -modules is fully faithful, but not an equivalence of categories unless  $G$  is finite. For example, if  $G$  is infinite then  $\mathbf{F}_p[[G]]$  itself is not induced from any discrete  $G$ -module.

The most natural method of constructing and manipulating spectral sequences is to use the language of filtered objects in stable  $\infty$ -categories, which we now recall.

**Notation 25.4.** If  $X \in \mathcal{D}(\mathbf{F}_p)$  is an object of the derived  $\infty$ -category of  $\mathbf{F}_p$ , we use the homotopical notation and write

$$\pi_k(X) := (X_{\geq 0})_{\leq 0} \in \mathcal{D}(\mathbf{F}_p)^\heartsuit \simeq \mathbf{Vect}_{\mathbf{F}_p}$$

for its homotopy groups with respect to the standard t-structure. This notation is justified by the fact that  $\mathcal{D}(\mathbf{F}_p)$  can be identified with  $\mathbf{F}_p$ -modules in spectra, and in these terms  $\pi_k(X)$  is really the  $k$ -th homotopy group of the underlying spectrum.

Note that in terms of the classical description of  $\mathcal{D}(\mathbf{F}_p)$  using chain complexes,  $\pi_k(-)$  corresponds to the  $k$ -th *homology* group.

**Definition 25.5.** A *filtered complex* is a functor of  $\infty$ -categories  $X: \mathbb{Z}^{op} \rightarrow \mathcal{D}(\mathbf{F}_p)$ , where we consider  $\mathbb{Z}$  as a poset. The *filtered derived  $\infty$ -category*

$$\mathcal{D}^{fil}(\mathbf{F}_p) := \mathbf{Fun}(\mathbb{Z}^{op}, \mathcal{D}(\mathbf{F}_p))$$

is the  $\infty$ -category of filtered complexes and natural transformations.

Concretely, a filtered complex can be identified with a diagram

$$\dots \rightarrow X_1 \rightarrow X_0 \rightarrow X_{-1} \rightarrow \dots$$

where  $X_i \in \mathcal{D}(\mathbf{F}_p)$  and the arrows are in the derived  $\infty$ -category.

**Recollection 25.6** (Local grading). The filtered derived  $\infty$ -category has a canonical self-equivalence  $(-)(1) := \mathcal{D}^{fil}(\mathbf{F}_p) \rightarrow \mathcal{D}^{fil}(\mathbf{F}_p)$  induced from the function  $- + 1 \cdot \mathbb{Z} \rightarrow \mathbb{Z}$ , concretely given by

$$X(1)_n := X_{n-1}$$

We refer to  $X(i)$  as *shifts* of  $X$ .

**Recollection 25.7.** There are two important objects one can associate to a filtered complex:

- (1) the *associated graded object*

$$\mathrm{gr}_p(X) := \mathrm{cofib}(X_{p+1} \rightarrow X_p),$$

which we can identify with a functor  $\mathbb{Z}^{ds} \rightarrow \mathcal{D}(\mathbf{F}_p)$ , where  $\mathbb{Z}^{ds}$  denotes the category of integers with only identity morphisms,

- (2) the *colimit*

$$\varinjlim X := \varinjlim (\dots \rightarrow X_1 \rightarrow X_0 \rightarrow X_{-1} \rightarrow \dots)$$

which is an object of  $\mathcal{D}(\mathbf{F}_p)$ .

Both of these constructions are exact and preserve colimits. Moreover, they are jointly conservative; that is, if  $\mathrm{gr}_*(X) = 0$  and  $\varinjlim X = 0$ , then  $X = 0$ .

**Recollection 25.8** (The spectral sequence). Associated to a filtered complex  $X$  we have a spectral sequence of  $\mathbf{F}_p$ -vector spaces with first page

$$E_1^{p,q} = \pi_{p+q}(\mathrm{gr}_p(X))$$

and differentials of degree

$$d_r: E_r^{p,q} \rightarrow E_r^{p+r, q-r-1}.$$

If we assume that there exists a  $N \in \mathbb{Z}$  such that  $X_n = 0$  for  $n \geq N$ , this is a convergent spectral sequence of signature

$$E_1^{p,q} \Rightarrow \pi_{p+q}(\varinjlim X).$$

For details on this construction, see [Lur17, §1.2.2].

In our case, the relevant filtered object will arise from a resolution of a module over a filtered ring. To discuss the latter, we recall the symmetric monoidal structure on the filtered derived  $\infty$ -category.

**Recollection 25.9** (Tensor product of filtered complexes). The filtered derived  $\infty$ -category  $\mathcal{D}^{\text{fil}}(\mathbb{Z})$  has a canonical symmetric monoidal structure induced by left Kan extension from that the (derived) tensor product of complexes and the abelian group structure of  $\mathbb{Z}$ . Concretely, the filtered tensor product is given by the formula

$$(X \otimes Y)_n := \varinjlim X_k \otimes_{\mathbb{Z}} Y_l$$

where the colimit is taken over the poset

$$(\mathbb{Z}^{op} \times \mathbb{Z}^{op})_{-/n} = \{(a, b) \in \mathbb{Z}^{op} \times \mathbb{Z}^{op} \mid a + b \geq n\}.$$

**Recollection 25.10.** With respect to the tensor product of filtered complexes, both the colimit functor

$$\varinjlim: \mathcal{D}^{\text{fil}}(\mathbf{F}_p) \rightarrow \mathcal{D}(\mathbf{F}_p)$$

and the associated graded object

$$\text{gr}: \mathcal{D}^{\text{fil}}(\mathbb{Z}) \rightarrow \text{Fun}(\mathbb{Z}^{ds}, \mathcal{D}(\mathbf{F}_p))$$

are symmetric monoidal, where we equip the  $\infty$ -category  $\text{Fun}(\mathbb{Z}^{ds}, \mathcal{D}(\mathbf{F}_p))$  of graded objects with the graded tensor product given by

$$(X \otimes Y)_n := \bigoplus_{k \in \mathbb{Z}} X_k \otimes Y_{n-k}.$$

**Example 25.11.** Suppose that  $R$  is an  $\mathbf{F}_p$ -algebra and that  $I \leq R$  is a two-sided ideal. Then, the filtered complex defined by the formula

$$F_I R_n := \begin{cases} I^n & n \geq 0 \\ R & \text{otherwise,} \end{cases}$$

where we think of each  $I^n \subseteq R$  as an element of the heart  $\mathcal{D}(\mathbf{F}_p) \simeq \text{Vect}_{\mathbf{F}_p}$ , admits a unique structure of an associative algebra such that the obvious isomorphism

$$\varinjlim F_I R_n \simeq R$$

is an isomorphism of algebras. The associated graded object is given by the associated graded algebra

$$\text{gr}_n(F_I R) \simeq \begin{cases} I^n / I^{n+1} & k \geq 0 \\ 0 & \text{otherwise,} \end{cases}$$

Moreover, if  $M$  is a left  $R$ -module, then the formula

$$F_I M := \begin{cases} I^n M & n \geq 0 \\ M & \text{otherwise,} \end{cases}$$

with  $I^n \subseteq M$  the submodule generated by  $I^n \cdot M$ , defines a left module over  $F_I R$  in the filtered derived  $\infty$ -category.

In our case, we will work with the filtered ring defined by the completed group algebra.

**Construction 25.12.** Let  $\mathbf{F}_p[[G]]$  be the completed group algebra, considered as a filtered ring using the  $I$ -adic filtration, where  $I$  is the augmentation ideal. As in [Example 25.11](#),  $\mathbf{F}_p[[G]]$  defines an associative algebra object of the filtered derived  $\infty$ -category, so that we have the associated  $\infty$ -category of left modules. The forgetful functor

$$\text{Mod}_{F_I(\mathbf{F}_p[[G]])}(\mathcal{D}^{\text{fil}}(\mathbf{F}_p)) \rightarrow \mathcal{D}^{\text{fil}}(\mathbf{F}_p)$$

admits a right adjoint given by the cofree module construction

$$X \in \mathcal{D}^{\text{fil}}(\mathbf{F}_p) \mapsto \underline{\text{map}}(F_I(\mathbf{F}_p[[G]]), X)$$

where  $\underline{\text{map}}$  is the internal mapping object of the filtered derived  $\infty$ -category, concretely given by

$$\underline{\text{map}}(F_I(\mathbf{F}_p[[G]]), X)_n \simeq \text{map}_{\mathcal{D}^{\text{fil}}(\mathbf{F}_p)}(F_I(\mathbf{F}_p[[G]])(n), X),$$

the mapping spectrum from a shift by the local grading as in [Recollection 25.6](#).

We now show that on the class of filtered modules which are bounded from above in the Beilinson t-structure, [Construction 25.12](#) can be identified with a filtered refinement of the coinduced discrete  $G$ -module construction

$$M \mapsto \text{coind}_1^G(M) \simeq \text{map}_{\text{cts}}(G, M),$$

relating it to continuous group cohomology. This is not obvious, since a naive guess might be that since we work with the completed group algebra, we would instead obtain a filtered refinement of

$$M \mapsto \text{Hom}_{\mathbf{F}_p}(\mathbf{F}_p[[G]], M),$$

which is a different functor if  $G$  is infinite.

This automatic continuity essentially follows from the following consideration. Suppose that  $M$  is non-positively filtered vector space together with a module structure over  $\mathbf{F}_p[[G]]$  compatible with the  $I$ -adic filtration. Then, since

$$I^{k+1} \cdot M_k \subseteq M_{-1} = 0$$

we see that in any given degree, the action factors through that of  $\mathbf{F}_p[[G]]/I^{k+1}$ . It follows that the induced action of  $G$  is continuous if we equip  $M$  with the discrete topology.

In practice, even though we are essentially only interested in filtered vector spaces, the category of the latter has somewhat pathological properties (for example, it is not abelian), so that it is easier to work with filtered complexes in the sense of [Definition 25.5](#). Our argument will essentially be a derived version of the one sketched in the previous paragraph.

**Recollection 25.13.** A filtered complex  $X$  is *Beilinson connective* if  $\text{gr}_n(X) \in \mathcal{D}(\mathbf{F}_p)_{\geq -n}$  for all  $n$ . It is *Beilinson coconnective* if  $X_n \in \mathcal{D}(\mathbf{F}_p)_{\leq -n}$  for all  $n \in \mathbb{Z}$ . The pair of subcategories

$$(\mathcal{D}^{\text{fil}}(\mathbf{F}_p)_{\geq 0}, \mathcal{D}^{\text{fil}}(\mathbf{F}_p)_{\leq 0})$$

of Beilinson (co)connective objects defines a pair t-structure on the filtered derived  $\infty$ -category, see [\[BMS19, §5.1\]](#).

**Example 25.14.** Let  $V_*$  be a non-positively filtered vector space, which we can identify with a filtered complex

$$V_0 \hookrightarrow V_{-1} \hookrightarrow \dots$$

which is levelwise contained in the heart and which vanishes in positive degrees. Then  $V_*$  is Beilinson coconnective.

**Lemma 25.15.** For each  $k \geq 0$ , let  $F_I(\mathbf{F}_p[[G]]/I^k)$  denote the  $I$ -adic filtration on  $\mathbf{F}_p[[G]]/I^k$ . Then for any filtered complex  $X$  which is bounded above with respect to the Beilinson t-structure:

(1) the quotient maps induce an equivalence

$$\varinjlim_k \underline{\text{map}}(F_I(\mathbf{F}_p[[G]]/I^k), X) \simeq \underline{\text{map}}(F_I(\mathbf{F}_p[[G]]), X)$$

of filtered complexes

(2) for any  $k \geq 0$ , the canonical map

$$\varinjlim_k \underline{\text{map}}(F_I(\mathbf{F}_p[[G]]/I^k), X) \rightarrow \text{map}_{\mathbf{F}_p}(\mathbf{F}_p[[G]]/I^k, \varinjlim_k X)$$

is an equivalence in  $\mathcal{D}(\mathbf{F}_p)$ .

*Proof.* Since  $\underline{\mathrm{map}}(-, X)_n \simeq \underline{\mathrm{map}}(, X(-n))$ , and a shift of a Beilinson bounded above filtered complex is again bounded above, it's enough to verify the claim on ordinary mapping spectra; that is, to check that

$$\varinjlim_k \mathrm{map}(F_I(\mathbf{F}_p[[G]]/I^k), X) \simeq \mathrm{map}(F_I(\mathbf{F}_p[[G]]), X).$$

By shifting  $X$  if necessary, we can assume that it is 0-coconnective. We claim that in this case for each  $k \geq 0$ , the map

$$(25.1) \quad \mathrm{map}(F_I(\mathbf{F}_p[[G]]/I^k), X) \rightarrow \mathrm{map}(F_I(\mathbf{F}_p[[G]]), X)$$

has a  $-k$ -coconnective cofibre. Thus, as  $k$  goes to  $\infty$ , it becomes an equivalence, as needed. We have a cofibre sequence of filtered complexes

$$(\dots \rightarrow I^{k+2} \rightarrow I^{k+1} \rightarrow I^k \rightarrow I^k \dots) \rightarrow F_I(\mathbf{F}_p[[G]]) \rightarrow F_I(\mathbf{F}_p[[G]]/I^k)$$

The left hand term is  $(-k)$ -Beilinson connective. It follows from t-structure axioms that

$$\mathrm{map}(\dots \rightarrow I^{k+2} \rightarrow I^{k+1} \rightarrow I^k \rightarrow I^k \dots, X)$$

is  $(-k)$ -coconnective as a spectrum. Since this mapping spectrum can be identified with the cofibre of (25.1), this ends the proof of the first part.

For the second part, we observe that since  $F_I(\mathbf{F}_p[[G]]/I^k)$  vanishes in sufficiently high degrees and has finite-dimensional associated graded concentrated in degrees  $k \geq i \geq 0$ , it can be obtained in finitely many extensions from positive shifts of the free filtered complex generated in degree zero, which is of the form

$$\dots \rightarrow 0 \rightarrow 0 \rightarrow \mathbf{F}_p \rightarrow \mathbf{F}_p \rightarrow \dots$$

It follows that  $F_I(\mathbf{F}_p[[G]]/I^k)$  is compact as an object of  $\mathcal{D}^{\mathrm{fil}}(\mathbf{F}_p)$  which implies the claim.  $\square$

Using Lemma 25.15, we now relate the category of filtered  $F_I(\mathbf{F}_p[[G]])$ -modules to the derived  $\infty$ -category of discrete  $G$ -modules.

**Construction 25.16.** The forgetful functor from discrete  $G$ -modules in  $\mathbf{F}_p$ -vector spaces gives rise an adjunction

$$\mathcal{D}(\mathrm{Mod}_G(\mathrm{Vect}_{\mathbf{F}_p})) \rightleftarrows \mathcal{D}(\mathbf{F}_p).$$

The left adjoint is conservative<sup>15</sup>, so that we can identify the source with the  $\infty$ -category of algebras for the associated comonad, which we can identify with the derived functor of the comonad

$$\mathrm{map}_{cts}(G, -) \simeq \mathrm{Hom}_{\mathbf{F}_p}^{cts}(\mathbf{F}_p[[G]], -) \simeq \varinjlim \mathrm{Hom}_{\mathbf{F}_p}(\mathbf{F}_p[[G]]/I^k, -)$$

on vector spaces. Using the last description, we see that  $\mathcal{D}(\mathrm{Mod}_G(\mathrm{Vect}_{\mathbf{F}_p}))$  can be identified with coalgebras for the comonad on  $\mathcal{D}(\mathbf{F}_p)$  defined by

$$\varinjlim \mathrm{map}_{\mathcal{D}(\mathbf{F}_p)}(\mathbf{F}_p[[G]]/I^k, -)$$

By Lemma 25.15, if  $X$  is a  $F_I(\mathbf{F}_p[[G]])$ -module which is bounded above in the Beilinson t-structure, then its colimit has a canonical structure of a coalgebra for this comonad. It follows that the colimit functor can be refined to a functor  $U$  which makes the diagram

$$\begin{array}{ccc} \mathrm{Mod}_{F_I(\mathbf{F}_p[[G]])}(\mathcal{D}^{\mathrm{fil}}(\mathbf{F}_p)_{<\infty}) & \xrightarrow{U} & \mathcal{D}(\mathrm{Mod}_G(\mathbf{F}_p)) \\ \downarrow & & \downarrow \\ \mathcal{D}^{\mathrm{fil}}(\mathbf{F}_p) & \xrightarrow{\varinjlim} & \mathcal{D}(\mathbf{F}_p) \end{array}$$

<sup>15</sup>The conservativity of the left adjoint follows since it is a derived functor of  $\mathrm{Mod}_G(\mathrm{Vect}_{\mathbf{F}_p}) \rightarrow \mathrm{Vect}_{\mathbf{F}_p}$ , which is conservative. This would not be true if we work with the unseparated variant of the derived  $\infty$ -category of discrete  $G$ -modules as in §22; that is, the functor  $\hat{\mathcal{D}}(\mathrm{Mod}_G(\mathrm{Vect}_{\mathbf{F}_p})) \rightarrow \hat{\mathcal{D}}(\mathbf{F}_p) \simeq \mathcal{D}(\mathbf{F}_p)$  is not conservative.

commute, where both of the vertical arrows are forgetful functors and

$$\mathcal{D}^{\text{fil}}(\mathbf{F}_p)_{<\infty} := \bigcup_{n \in \mathbb{Z}} \mathcal{D}^{\text{fil}}(\mathbf{F}_p)_{\leq n}$$

is the Beilinson bounded above filtered derived  $\infty$ -category.

**Remark 25.17.** More informally,  $\text{Mod}_{F_I(\mathbf{F}_p[[G]])}(\mathcal{D}^{\text{fil}}(\mathbf{F}_p)_{<\infty})$  can be thought of as a filtered variant of the derived  $\infty$ -category of discrete  $G$ -modules, where the behaviour of stabilizers is controlled by the filtration. In this picture, the functor  $U$  of [Construction 25.16](#) is akin to forgetting the filtration.

If  $M$  is a discrete  $G$ -module in vector spaces, we can consider it as an object of the heart of  $\mathcal{D}(\text{Mod}_G(\text{Vect}_{\mathbf{F}_p}))$ , in which case the homotopy groups of the mapping spectrum out of  $\mathbf{F}_p$  encode cohomology in the sense that

$$H^k(G, M) \simeq \text{Ext}_{\text{Mod}_G(\text{Vect}_{\mathbf{F}_p})}^k(M, N) \simeq \pi_{-k} \text{map}_{\mathcal{D}(\text{Mod}_G(\text{Vect}_{\mathbf{F}_p}))}(M, N).$$

We now show that if  $M$  is equipped with a filtration which makes it into a  $F_I(\mathbf{F}_p[[G]])$ -module, we can use the comparison functor  $U$  to provide a filtered refinement of this mapping spectrum and hence a spectral sequence.

**Definition 25.18.** A *filtered discrete  $G$ -module*  $M$  is a diagram

$$M_0 \hookrightarrow M_{-1} \hookrightarrow M_{-2} \hookrightarrow \dots$$

of discrete  $G$ -modules such that the induced  $\mathbf{F}_p[[G]]$ -action makes it into  $F_I(\mathbf{F}_p[[G]])$ -module; that is, such that

$$I^k \cdot M_n \subseteq M_{n+k}$$

for all  $n, k$

**Example 25.19.** The trivial  $G$ -module  $\mathbf{F}_p$  can be promoted to a filtered discrete  $G$ -module by equipping with the constant filtration

$$\mathbf{F}_p \hookrightarrow \mathbf{F}_p \hookrightarrow \mathbf{F}_p \hookrightarrow \dots$$

The underlying filtered complex is the free one generated in degree zero.

If  $M$  is a filtered discrete  $G$ -module, then it gives rise to a filtered complex contained levelwise in the heart and vanishing in positive degrees. The condition on the action of  $G$  guarantees that the  $\mathbf{F}_p[[G]]$ -action makes it into a  $F_I(\mathbf{F}_p[[G]])$ -module. This determines a fully faithful functor of  $\infty$ -categories so that we abusively identify filtered discrete  $G$ -modules with a subcategory of modules in filtered complexes. In these terms, we can give one more natural example.

**Example 25.20.** Let  $V$  be a non-positively filtered vectored spaces thought of as a filtered complex as in [Example 25.14](#). Then the internal mapping object

$$\text{map}_{\mathcal{D}^{\text{fil}}(\mathbf{F}_p)}(F_I(\mathbf{F}_p[[G]]), V)$$

is a filtered discrete  $G$ -module. Unwrapping the proof of [Lemma 25.15](#), we see that it can be identified with the coinduced  $G$ -module  $\text{map}_{\text{cts}}(G, V)$  with filtration which is in degree  $n$  given by the subvector space spanned by the images of the maps

$$\text{Hom}_{\mathbf{F}_p}(\mathbf{F}_p[[G]]/I^{k+n}, V_k) \rightarrow \text{map}_{\text{cts}}(G, V)$$

for all  $k \in \mathbb{Z}$ . This is the filtered analogue of the coinduced module construction.

Associated to a filtered discrete  $G$ -module we have an internal mapping object defined by

$$\underline{\text{map}}_{\text{Mod}_{F_I(\mathbf{F}_p[[G]])}}(\mathbf{F}_p, X)_n \simeq \text{map}_{\text{Mod}_{F_I(\mathbf{F}_p[[G]])}}(\mathbf{F}_p(n), X),$$

where the right hand side is the mapping spectrum in modules and  $\mathbf{F}_p$  denotes the constant filtered module of [Example 25.19](#). Since both the source and target are bounded above in the

Beilinson t-structure, [Construction 25.16](#) induces a map from the colimit of this filtered spectrum into the mapping spectrum in the derived  $\infty$ -category.

**Proposition 25.21.** *For any filtered discrete  $G$ -module  $X$  the canonical map*

$$\varinjlim \underline{\mathrm{map}}_{\mathrm{Mod}_{F_I}(\mathbf{F}_p[[G]])}(\mathbf{F}_p, X) \rightarrow \mathrm{map}_{\mathcal{D}(\mathrm{Mod}_G(\mathrm{Vect}_{\mathbf{F}_p}))}(\mathbf{F}_p, X)$$

*is an equivalence of spectra.*

*Proof.* Since the underlying filtered complex of  $\mathbf{F}_p$  is free in degree zero, the internal filtered mapping spectrum in  $F_I(\mathbf{F}_p[[G]])$ -modules appearing on the left hand side can be identified with limit in filtered spectra of the cobar cosimplicial diagram

$$X \rightrightarrows C(X) \rightrightarrows C^2(X) \rightrightarrows \dots$$

where

$$C(-) = \underline{\mathrm{map}}_{\mathcal{D}^{\mathrm{fil}}(\mathbf{F}_p)}(F_I(\mathbf{F}_p[[G]]), -)$$

Here, each of  $C^k(X)$  is a non-negatively filtered vector space with underlying vector space  $\varinjlim C^k(X)_n \simeq \mathrm{map}_{\mathrm{cts}}(G^{\times k}, X)$  as in [Example 25.20](#).

Since the homotopy groups of the totalization of a cosimplicial vector space, considered as a cosimplicial spectrum levelwise contained in the heart, corresponds to the cohomology of the corresponding cochain complex, we have

$$\pi_{-k} \underline{\mathrm{map}}_{\mathrm{Mod}_{F_I}(\mathbf{F}_p[[G]])}(\mathbf{F}_p, X)_n \simeq \mathrm{H}^k(X_n \rightarrow C(X)_n \rightarrow C^2(X)_n \rightarrow \dots).$$

Since cohomology commutes with filtered colimits, we deduce that the homotopy groups of the left hand side in the statement can be calculated as the cohomology of the cochain complex

$$X \rightarrow \mathrm{map}_{\mathrm{cts}}(G, X) \rightarrow \mathrm{map}_{\mathrm{cts}}(G^{\times 2}, X) \rightarrow \dots$$

This is the group cochain complex which also calculates the homotopy of the right hand side by [Proposition 20.19](#).  $\square$

More informally, [Proposition 25.21](#) guarantees that if  $X$  is a discrete  $G$ -module, then a filtration on  $X$  satisfying the conditions of [Definition 25.18](#) induces a filtration on its group cochain complex and hence a spectral sequence calculating its cohomology through [Recollection 25.8](#).

This filtration can be presented very explicitly in terms of group cochains using [Example 25.20](#). The advantage of our categorical approach is that the filtration comes out of very abstract considerations. This makes it quite easy to describe the first page of the associated spectral sequence; equivalently, the homotopy groups of the associated graded of the filtration.

**Proposition 25.22.** *Let  $X$  be a filtered discrete  $G$ -module. Then, there is a canonical isomorphism*

$$E_1^{p,q} = \pi_{p+q} \mathrm{gr}_p(\underline{\mathrm{map}}_{\mathrm{Mod}_{F_I}(\mathbf{F}_p[[G]])}(\mathbf{F}_p, X)) \simeq \mathrm{Ext}_{\mathrm{gr}_*(\mathbf{F}_p[[G]])}(\mathbf{F}_p, \mathrm{gr}_*(X))$$

*between the first page of the spectral sequence associated to the filtration of [Proposition 25.21](#) and the Ext-groups in the category of graded modules over  $\mathrm{gr}_*(\mathbf{F}_p[[G]]) \simeq I^*/I^{*+1}$ .*

*Proof.* For any pair  $X, Y$  of filtered complexes, there's a canonical equivalence

$$\mathrm{gr}_*(\underline{\mathrm{map}}_{\mathcal{D}^{\mathrm{fil}}(\mathbf{F}_p)}(X, Y)) \simeq \underline{\mathrm{map}}_{\mathrm{Fun}(\mathbb{Z}^{ds}, \mathcal{D}(\mathbf{F}_p))}(\mathrm{gr}_*(X), \mathrm{gr}_*(Y))$$

between the associated graded of the filtered mapping spectrum and maps between associated graded objects. If  $X, Y$  are  $F_I(\mathbf{F}_p[[G]])$ -modules, this becomes

$$\mathrm{gr}_*(\underline{\mathrm{map}}_{\mathrm{Mod}_{F_I}(\mathbf{F}_p[[G]])}(\mathcal{D}^{\mathrm{fil}}(\mathbf{F}_p)))(X, Y) \simeq \underline{\mathrm{map}}_{\mathrm{Mod}_{\mathrm{gr}_*(\mathbf{F}_p[[G]])}(\mathrm{Fun}(\mathbb{Z}^{ds}, \mathcal{D}(\mathbf{F}_p)))}(\mathrm{gr}_*(X), \mathrm{gr}_*(Y)).$$

Since the inclusion of objects contained in the heart induces an equivalence

$$\mathrm{Fun}(\mathbb{Z}^{ds}, \mathcal{D}(\mathbf{F}_p)) \simeq \mathcal{D}(\mathrm{grVect}_{\mathbf{F}_p})$$

and  $\text{gr}_*(\mathbf{F}_p[[G]])$  is levelwise contained in the heart, we have

$$\text{Mod}_{\text{gr}_*(\mathbf{F}_p[[G])}(\text{Fun}(\mathbb{Z}^{ds}, \mathcal{D}(\mathbf{F}_p))) \simeq \mathcal{D}(\text{Mod}_{\text{gr}_*(\mathbf{F}_p[[G])}(\text{grVect}_{\mathbf{F}_p})).$$

It follows that the first page of the spectral sequence can be identified with homotopy classes of maps  $\mathbf{F}_p \rightarrow \text{gr}_*(X)$  in the derived  $\infty$ -category of modules over  $\text{gr}_*(\mathbf{F}_p[[G]]) \simeq I^*/I^{*+1}$ . The latter can be identified with the relevant Ext-groups, as needed.  $\square$

We can summarize the discussion up to this point as follows:

**Theorem 25.23.** *Let  $X$  be a discrete  $G$ -module in  $\mathbf{F}_p$ -vector spaces. Then any exhaustive filtration*

$$X_0 \hookrightarrow X_{-1} \hookrightarrow X_{-2} \hookrightarrow \dots$$

*satisfying the conditions of Definition 25.18 induces a convergent spectral sequence of signature*

$$E_1^{p,q} = \text{Ext}_{I^*/I^{*+1}}^{-p-q,p}(\mathbf{F}_p, \text{gr}_*(X)) \Rightarrow H^{-p-q}(G, X).$$

*Proof.* This spectral sequence is induced by the identification of Proposition 25.21. The description of the first page of the spectral sequence follows from Proposition 25.22.  $\square$

The rest of this lecture is devoted to the proof of Lazard’s Theorem 25.1. To recall the latter, we want to show that if  $G$  is uniform, then the inclusion of elements of cohomological degree one induces an isomorphism of algebras

$$H^*(G, \mathbf{F}_p) \simeq \Lambda_{\mathbf{F}_p} H^1(G, \mathbf{F}_p)$$

Our main tool will be the spectral sequence of Theorem 25.23. The needed algebraic input is the description of the associated graded of the completed group algebra of a uniform group.

Previously in §14, we gave a description of the  $p$ -adic completed group algebra. This can be used to easily deduce the structure of the  $\mathbf{F}_p$ -group algebra, which we now describe.

**Proposition 25.24.** *If  $G$  is uniform, then the associated graded ring  $\text{gr}_I^*(\mathbf{F}_p[[G]]) := I^*/I^{*+1}$  is commutative. Moreover, for any minimal generating set  $g_1, \dots, g_n \in G$ , the inclusion of classes of the elements  $b_i := g_i - 1 \in I$  induces an isomorphism*

$$\mathbf{F}_p[b_1, \dots, b_n] \simeq \text{gr}_I^*(\mathbf{F}_p[[G]])$$

*between the associated graded ring and a graded polynomial algebra on classes in degree  $|b_i| = 1$ .*

*Proof.* Let  $\mathbb{Z}_p[[G]] := \mathbb{Z}_p[G/G_k]$  denote the  $p$ -adic completed group algebra and let

$$J := \ker(\mathbb{Z}_p[[G]] \rightarrow \mathbf{F}_p).$$

denote the  $p$ -adic augmentation ideal. The quotient map of rings  $\mathbb{Z}_p[[G]] \rightarrow \mathbf{F}_p[[G]]$  induces an epimorphism  $J \twoheadrightarrow I$  and hence an epimorphism of the associated graded rings.

We claim that for each  $k \geq 1$ , multiplication by the class  $\tilde{p} \in J/J^2$  of  $p \in J$  induces a short exact sequence

$$I^{k-1}/I^k \xrightarrow{\tilde{p}} I^k/I^{k+1} \longrightarrow J^k/J^{k+1} \longrightarrow 0.$$

This is clearly exact on the right. We have to check that it is also exact on the middle.

Suppose that the image of  $x \in J^k$  vanishes in  $I^k/I^{k+1}$ . We have to show that the class of  $x$  in  $J^k/J^{k+1}$  is in the image of multiplication by  $\tilde{p}$ . If  $x \in J^{k+1}$ , there is nothing to be done, so let’s assume that’s not the case. Then  $\|x\| = p^{-k}$ , where  $\|\cdot\|$  denotes the  $J$ -adic filtration norm.

If the image of  $x$  is zero in  $I^k/I^{k+1}$ , then since  $J^{k+1} \rightarrow I^{k+1}$  is an epimorphism, we can write

$$(25.2) \quad x = j + p \cdot y$$

for some  $j \in J^{k+1}$  and  $y \in \mathbb{Z}_p[[G]]$ , so that

$$x \equiv p \cdot y \pmod{J^{k+1}}.$$

By [Theorem 15.5](#), the norm on  $\mathbb{Z}_p[[G]]$  extends to a norm on rationalization and since  $\|x\| = p^{-k}$ , we deduce from [\(25.2\)](#) that

$$\|y\| = p^{k-1},$$

hence  $y \in J^{k-1}$ . Thus,  $x = \tilde{p} \cdot y$  in  $J^k/J^{k+1}$ , as needed.

We deduce that we have an isomorphism

$$\mathrm{gr}_I^*(\mathbf{F}_p[[G]]) \simeq \mathrm{gr}_J^*(\mathbb{Z}_p[[G]])/\tilde{p}.$$

The right hand side is the degree zero-part of the associated graded of the  $\tilde{p}$ -adic filtration which we described explicitly in [Theorem 15.8](#) as a polynomial ring in the specified variables. This ends the argument.  $\square$

*Proof of Lazard's [Theorem 25.1](#):* We first show that the inclusion of elements of cohomological degree one extends to a map of graded algebras

$$\Lambda_{\mathbf{F}_p} H^1(G, \mathbf{F}_p) \rightarrow H^*(G, \mathbf{F}_p).$$

As the target is graded-commutative, we only have to show that the elements of  $H^1(G, \mathbf{F}_p)$  square to zero. If  $p > 2$ , this already follows from graded commutativity of the target, since

$$x \cdot x = (-1) \cdot x \cdot x.$$

If  $p = 2$ , we have to work a little harder. We can identify the square operator on elements of cohomological degree one with the Bockstein

$$x \mapsto x^2 = \beta(x)$$

associated to the short exact sequence of trivial  $G$ -modules

$$0 \rightarrow \mathbf{F}_2 \rightarrow \mathbb{Z}/4 \rightarrow \mathbf{F}_2 \rightarrow 0.$$

Thus, we have to show that any class  $x \in H^1(G, \mathbf{F}_2)$  lifts to a class in  $H^1(G, \mathbb{Z}/4)$ . Using [Example 20.22](#), we can identify such an  $x$  with a homomorphism of groups  $G \rightarrow \mathbf{F}_2$ , and the claim is that any such homomorphism lifts to  $\mathbb{Z}/4$ . Since  $G$  is powerful and  $p = 2$ ,  $G/G^4$  is abelian. As  $G/G^2 \simeq \mathbf{F}_2^{\oplus r}$  where  $r = H^1(G, \mathbf{F}_2)$  is the rank, cardinality considerations and uniformity imply that

$$G/G^2 \simeq (\mathbb{Z}/4)^{\oplus r}$$

which gives the desired claim.

By [Theorem 25.23](#), we have a spectral sequence

$$\mathrm{Ext}_{I^*/I^{*+1}}^{*,*}(\mathbf{F}_p, \mathbf{F}_p) \Rightarrow H^*(G, \mathbf{F}_p).$$

Since  $G$  is uniform, by [Proposition 25.24](#) the graded ring  $I^*/I^{*+1}$  is a polynomial algebra in  $r$  variables of degree one, so that

$$\mathrm{Ext}_{I^*/I^{*+1}}^{*,*}(\mathbf{F}_p, \mathbf{F}_p) \simeq \Lambda_{\mathbf{F}_p}(y_1, \dots, y_r);$$

an exterior algebra on classes of degree  $|y_i| = (1, 1)$ . We claim that this is really a spectral sequence of algebras; that is, that

- (1) the differentials satisfy the Leibniz rule,
- (2) the multiplication on the first page corresponds to the Yoneda product on  $\mathrm{Ext}$ ,
- (3) the  $E_\infty$ -page is an associated graded with respect to a multiplicative filtration on  $H^*(G, \mathbf{F}_p)$  considered as a ring under the cup product.

To see this, note that the spectral sequence comes from the filtered spectrum

$$\underline{\mathrm{map}}_{\mathrm{Mod}_{F_I}(\mathbf{F}_p[[G]])}(\mathbf{F}_p, \mathbf{F}_p)$$

This is an associative algebra in filtered spectra with respect to composition and this makes the associated spectral sequence multiplicative. Properties two and three follow from the fact that the identifications

$$\varinjlim \underline{\text{map}}_{\mathcal{M}\text{od}_{F_I}(\mathbf{F}_p[[G]])}(\mathbf{F}_p, \mathbf{F}_p) \simeq \text{map}_{\mathcal{D}(\text{Mod}_G(\text{Vect}_{\mathbf{F}_p}))}(\mathbf{F}_p, \mathbf{F}_p)$$

and

$$\text{gr}_*(\underline{\text{map}}_{\mathcal{M}\text{od}_{F_I}(\mathbf{F}_p[[G]])}(\mathbf{F}_p, \mathbf{F}_p)) \simeq \underline{\text{map}}_{\mathcal{D}(I^*/I^{*+1})}(\mathbf{F}_p, \mathbf{F}_p)$$

are induced by a functor and so are similarly identifications of associative algebras under composition<sup>16</sup>.

Observe that the generating classes  $y_i \in \text{Ext}_{I^*/I^{*+1}}(\mathbf{F}_p, \mathbf{F}_p)$  are the only elements on the first page of cohomological degree 1. Since  $\dim_{\mathbf{F}_p}(\text{H}^1(G, \mathbf{F}_p)) = \text{rank}(G) = r$  by Lemma 21.20, we deduce that all linear combinations of  $y_i$  are permanent cycles as otherwise the  $E_\infty$  page would be too small. Since they multiplicatively generate the whole first page, we deduce that all elements are permanent cycles so that the spectral sequence collapses.

The elements  $y_i$  lift to  $\text{H}^1(G, \mathbf{F}_p)$  and since their images generate  $E_\infty$  page, which is an associated graded of  $\text{H}^*(G, \mathbf{F}_p)$ , we deduce that they generate the whole cohomology ring. It follows that the map

$$\Lambda_{\mathbf{F}_p} \text{H}^1(G, \mathbf{F}_p) \rightarrow \text{H}^*(G, \mathbf{F}_p).$$

is surjective and hence an isomorphism by a dimension count.  $\square$

#### REFERENCES

- [BMS19] Bhargav Bhatt, Matthew Morrow, and Peter Scholze, *Topological hochschild homology and integral p-adic hodge theory*, Publications mathématiques de l’IHÉS **129** (2019), no. 1, 199–310.
- [Bou89] Nicolas Bourbaki, *Lie groups and lie algebras: Chapters 1-3*, vol. 1, Springer Science & Business Media, 1989.
- [DDSMS03] John D Dixon, Marcus PF Du Sautoy, Avinoam Mann, and Dan Segal, *Analytic pro-p groups*, no. 61, Cambridge University Press, 2003.
- [Hat78] A. E. Hatcher, *Concordance spaces, higher simple-homotopy theory, and applications*, Algebraic and geometric topology (Stanford Univ., Stanford, CA, 1976), Proc. Symp. Pure Math., vol. 32, Amer. Math. Soc., Providence, R.I., 1978, pp. 3–21.
- [Hen98] Hans-Werner Henn, *Centralizers of elementary abelian p-subgroups and mod-p cohomology of profinite groups*.
- [Hes05] Lars Hesselholt, *Lecture notes on witt vectors*, Survey article, unpublished (2005), <https://www.math.nagoya-u.ac.jp/~larsh/papers/s03/wittsurvey.pdf>.
- [HVOHvO96] Li Huishi, Freddy Van Oystaeyen, Li Huishi, and Freddy van Oystaeyen, *Zariskian filtrations*, Springer, 1996.
- [KK96] Anthony W Knapp and Anthony William Knapp, *Lie groups beyond an introduction*, vol. 140, Springer, 1996.
- [Laz65] Michel Lazard, *Groupes analytiques p-adiques*, Publications Mathématiques de l’IHÉS **26** (1965), 5–219.
- [Lee] John M Lee, *Smooth manifolds*, Introduction to Smooth Manifolds.
- [LM87a] Alexander Lubotzky and Avinoam Mann, *Powerful p-groups. i. finite groups*, Journal of Algebra **105** (1987), no. 2, 484–505.
- [LM87b] ———, *Powerful p-groups. ii. p-adic analytic groups*, Journal of Algebra **105** (1987), no. 2, 506–515.
- [Lur] Jacob Lurie, *Spectral algebraic geometry*, <https://www.math.ias.edu/~lurie/papers/SAG-rootfile.pdf>.
- [Lur09] Jacob Lurie, *Higher topos theory*, Annals of Mathematics Studies, vol. 170, Princeton University Press, Princeton, NJ, 2009. MR 2522659
- [Lur17] ———, *Higher algebra*, [math.ias.edu/~lurie/papers/HA.pdf](https://www.math.ias.edu/~lurie/papers/HA.pdf), September 2017.

<sup>16</sup>Note that the cup product on  $\text{H}^*(G, \mathbf{F}_p) \simeq \pi_{-*} \text{map}_{\mathcal{D}(\text{Mod}_G(\text{Vect}_{\mathbf{F}_p}))}(\mathbf{F}_p, \mathbf{F}_p)$  can be induced either using the algebra structure on  $\mathbf{F}_p$  or using composition of maps in the derived  $\infty$ -category. These two coincide by the Eckmann-Hilton argument.

- [Pst21] Piotr Pstragowski, *Finite height chromatic homotopy theory, harvard math 252y*, [https://people.math.harvard.edu/~piotr/252y\\_notes.pdf](https://people.math.harvard.edu/~piotr/252y_notes.pdf).
- [Rav03] Douglas C Ravenel, *Complex cobordism and stable homotopy groups of spheres*, American Mathematical Soc., 2003.
- [Sch11] Peter Schneider, *p-adic lie groups*, vol. 344, Springer Science & Business Media, 2011.
- [Sch19] Peter Scholze, *Condensed mathematics*, Lecture notes based on joint work with D. Clausen. Available at Scholze's webpage (2019).
- [Ser65] Jean-Pierre Serre, *Sur la dimension cohomologique des groupes profinis*, *Topology* **3** (1965), no. 4, 413–420.
- [Ser97] J.-P. Serre, *Galois cohomology*, Springer-Verlag, New York, 1997.
- [Ser13] Jean-Pierre Serre, *Local fields*, vol. 67, Springer Science & Business Media, 2013.
- [Sta18] The Stacks Project Authors, *Stacks Project*, <https://stacks.math.columbia.edu>, 2018.
- [SW00] Peter Symonds and Thomas Weigel, *Cohomology of p-adic analytic groups*, *New horizons in pro-p groups*, Springer, 2000, pp. 349–410.