

1. Motivation

This course will be 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 $G \times G \to G$ 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 $(-)^{-1} : G \to G$ 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 $\tilde{G} \to G$. For example, for $n > 2$ the universal cover of $SO(n)$ is given by the so-called spin group $\text{Spin}(n) \to SO(n)$.

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) Correspondence between Lie groups and Lie algebras: The tangent space of the identity $e \in G$ has a structure of a Lie algebra which completely determines the local structure of $G$ (and in fact determines it up to isomorphism if we assume that $G$ is simply-connected).

(2) Representation theory: A unitary representation of a compact Lie group on a Hilbert space splits as a direct sum of simple representations, as a consequence of Peter-Weyl theorem. Moreover, we have a relatively explicit construction of the irreducible representations using Borel-Weil theory.

(3) Group-theoretic properties: Closed subgroups of Lie groups are again Lie. Moreover, any Lie group 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.

Let’s go back to the $p$-adic analytic groups. Where do the $p$-adics come from? We begin with $\mathbb{Q}$ and look at different completions:

Completion with respect to the standard Archimedean metric gives the real field $\mathbb{R}$, but completions with respect to $p$-adic metrics instead yield $\mathbb{Q}_p$. The latter can be easily described using algebra, which we do first before moving to the metric description.

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

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

$$
\mathbb{Q}_p := \mathbb{Z}_p[p^{-1}] = \lim_{\leftarrow} \frac{\mathbb{Z}_p}{\mathbb{Z}_p p^n}
$$

which we endow with the colimit topology.

We now describe the metric on $\mathbb{Q}_p$ which induces the colimit-limit topology described before. 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 $| - |_p : \mathbb{Q}_p \to \mathbb{R}$ 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

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

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: 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 the 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

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

We will not delve too deeply into $p$-adic analysis, but let us give two instructive examples: one which shows that sometimes the non-Archimedean world is much more simple than the real one, and another one which shows that it also carries 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. $a_i \to 0 \in \mathbb{Q}_p$; equivalently, $|a_i|_p \to 0 \in \mathbb{R}$.

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

Using the limit description $\mathbb{Z}_p = \lim \mathbb{Z}_p/p^n$, 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 $a_i \in \{0, 1, \ldots, p - 1\}$. We now define $f$ by

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

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 the second example is that smooth $p$-adic functions can be very badly behaved. As a consequence, to define the $p$-adic analytic groups, we will 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 set. We say a function $f : U \to \mathbb{Q}_p$ is *locally analytic* if it is locally given by a convergent power series.

In more detail, $f : U \to \mathbb{Q}_p$ is locally analytic if for any $u \in U$ we can find

1. a real $\epsilon_u > 0$,
2. a power series $F_u \in \mathbb{Q}_p[[X_1, \ldots, X_n]]$

with the properties that

1. if we write $F_u = \sum_{I=(i_1, \ldots, i_n)} a_I X^I$
   
   
   
   then
   
   
   

   \[ \epsilon_u^{i_1 + \ldots + i_n} |a_I|_p \to 0 \]

   as $|i_1 + \ldots + i_n| \to \infty$,

2. if $u' = u + (x_1, \ldots, x_n) \in U$ 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

\[ F_u(u' - u) = \sum a_{(i_1, \ldots, i_n)} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n} \]

converges, so that the equation makes sense.

To define $p$-adic analytic groups we will mimic the definition of Lie groups. This means that we first need an appropriate notion of 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 $\varphi : U_\alpha \to \mathbb{Q}_p^n$ 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

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

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 (in the category of $p$-adic manifolds and locally analytic maps) to a disjoint union

$$X \cong \mathbb{Z}_p \sqcup \ldots \sqcup \mathbb{Z}_p$$

of copies of $\mathbb{Z}_p$. In particular, all non-empty compact $p$-adic manifolds of positive dimension are homeomorphic.

Note that 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 $m: G \times G \to G$ and inverse $(\cdot)^{-1}: G \to G$ maps are locally analytic.

Since these will be the central objects of study in this course, we give a few examples.

Example 1.13. The general linear group $\text{GL}_n(\mathbb{Q}_p)$, 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 $\text{GL}_n(\mathbb{Q}_p)$ has a compact open subgroup given by $\text{GL}_n(\mathbb{Z}_p)$, 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

$$\ldots \leq I + p^k \cdot M_n(\mathbb{Z}_p) \leq I + p \cdot M_n(\mathbb{Z}_p) \leq \text{GL}_n(\mathbb{Z}_p) \leq \text{GL}_n(\mathbb{Q}_p).$$

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 $K \supseteq \mathbb{Q}_p$. The ramified part of the maximal abelian extension $K^{ab} \subseteq K$ is known as the Lubin–Tate extension and is sometimes denoted $K_{LT}$. Local class field theory gives a canonical continuous isomorphism $\text{Gal}(K_{LT}/K) \cong \mathcal{O}_K^\times$ which shows that the Galois group has a natural structure of a $p$-adic analytic group.

Example 1.15. Let $G_0$ be the Honda formal group law over $F_p^n$, which is the unique $p$-typical formal group law whose $p$-series is given by $[p]_{G_0}(x) = x^{p^n}$. Then its automorphism group

$$\mathbb{G}_n := \text{Aut}(G_0)$$

can be shown to be the group of units in the integers of a certain central division algebra over $\mathbb{Q}_p$, and hence has a natural 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.

Recall Example 1.13 of the group $\text{GL}_n(\mathbb{Q}_p)$, which has a basis of open neighbourhoods of the identity given by compact open subgroups of the form $I + p^k \cdot M_n(\mathbb{Z}_p)$. The first large result we will prove in this course will be characterization of $p$-adic analytic groups in terms of their open subgroups, which is a celebrated theorem due to Lazard.

Theorem 1.1 (Lazard). 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 \( P \leq G \) which is a finitely generated pro-\( p \) group and which is powerful; that is, such that \( P/P^1 \) (the quotient by the closed subgroup generated by \( p \)-th powers) is abelian\(^1\).

(3) \( G \) has a compact open subgroup \( U \leq G \) which is finitely generated pro-\( p \) group and which is uniformly powerful; that is, powerful and torsion free.

The above result is truly remarkable, as it equates what is essentially an analytic condition (of admitting a compatible \( p \)-adic manifold structure) with very concrete, group-theoretic properties. Note that if \( G \) is compact, then any open subgroup is of finite index, so that any compact \( p \)-adic analytic group is an extension of a uniformly powerful subgroup by a finite group.

**Theorem 1.1** is very useful in practice, as uniformly powerful pro-\( p \)-groups are easy to understand. In this course, we will show that if \( U \) is (finitely generated) uniformly powerful, then

1. there is a homeomorphism \( U \cong \mathbb{Z}_p^n \) to a free module over the \( p \)-adics,
2. the group structure of \( U \) induces a \( \mathbb{Z}_p \)-Lie algebra on \( \mathbb{Z}_p^n \) which is abelian modulo \( p \); that is, such that

\[
[\mathbb{Z}_p^n, \mathbb{Z}_p^n] \subseteq p \mathbb{Z}_p^n.
\]

This correspondence between uniformly powerful groups and certain \( \mathbb{Z}_p \)-Lie algebras is in fact an equivalence of categories, so that uniformly powerful groups can be described up to isomorphism by essentially linear data. This can be thought of as the \( p \)-adic analogue of the classical Lie correspondence between Lie groups and Lie algebras.

Let us describe one more result which shows that uniformly powerful groups (and by extension, \( p \)-adic analytic groups), are quite special. Recall that if \( G \) is a group, then to give a \( G \)-representation is the same as to give a module over the group algebra \( \mathbb{Z}[G] \). For topological groups, we have a variant of the group algebra which takes the topology into account.

**Definition 1.16.** Let \( G = \lim \pi G_i \) be a profinite group; that is, a limit of finite groups equipped with its limit topology. The **completed group algebra** is given by

\[
\mathbb{Z}_p[[G]] = \varprojlim \mathbb{Z}_p[G_i].
\]

In favourable cases (such as for modules whose underlying \( \mathbb{Z}_p \)-module is finitely generated), a continuous action of \( G \) is the same datum as that of a \( \mathbb{Z}_p[[G]] \)-module, so that understanding \( G \)-representations is equivalent to understanding this ring. Often, it is quite a bit nicer than you would think, as the following example shows.

**Example 1.17.** There is a canonical isomorphism of topological rings

\[
\mathbb{Z}_p[[\mathbb{Z}_p]] \cong \mathbb{Z}_p[[x]]
\]
due to Iwasawa, where \( x = 1 - [1] \). This shows that to define a continuous action of the topological group \( \mathbb{Z}_p \) on a finitely generated \( \mathbb{Z}_p \)-module is the same as to give a single topologically nilpotent operator.

The following result which we will 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.** Let \( U \subseteq G \) be uniformly powerful of dimension \( d \). Then there exists a complete descending filtration

\[
\ldots \subseteq F_1\mathbb{Z}_p[[U]] \subseteq F_0\mathbb{Z}_p[[U]] = \mathbb{Z}_p[[U]]
\]
whose associated graded is isomorphic

\[
\bigoplus_{i \geq 0} \text{gr}_i \cong \bigoplus_{i \geq 0} F_i\mathbb{Z}_p[[U]]/F_{i+1}\mathbb{Z}_p[[U]] \cong \mathbb{F}_p[x_0, x_1, \ldots, x_d].
\]

\(^1\)When \( p = 2 \), this condition needs to be slightly modified. A pro-2-group is said to be **powerful** if \( P/P^2 \) is abelian. One intuition about this change is that \( P/P^2 \) is always abelian, which is not true at odd primes. We will discuss these differences in more detail later in the course.
to a polynomial $F_p$-algebra on $d + 1$ generators.

Informally, the above result says that the completed group algebra of a uniformly powerful group behaves very much like a polynomial ring, despite not being commutative. Since any compact $p$-adic analytic group has a finite index uniformly powerful subgroup, we deduce the following:

**Corollary 1.18.** If $G$ is compact $p$-adic analytic, then $\mathbb{Z}_p[[G]]$ 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 $G = \varprojlim G_i$. If $M$ is a topological abelian group, then the cohomology groups

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

can be defined in several equivalent ways, for example:

1. as cohomology of the continuous cochain complex

   $$M \to \text{Fun}_{\text{cts}}(G, M) \to \text{Fun}_{\text{cts}}(G \times G, M) \to \cdots,$$

2. (when $M$ is a finitely generated $\mathbb{Z}_p$-module) as extension groups $\text{Ext}_{\mathbb{Z}_p[[G]]}^*(\mathbb{Z}_p, M)$,

3. (when $M$ is finite with trivial $G$-action) as the colimit $\varinjlim H^*(G_i; M)$ of ordinary cohomology groups of the finite groups $G_i$.

Here are some examples of how these groups arise in practice.

**Example 1.19.** Let $K$ be a field, $K^{\text{sep}}$ its separable closure and $\text{Gal} := \text{Gal}(K^{\text{sep}}/K)$ the absolute Galois group. Then the Brauer group of $K$ which describes central division $K$-algebras up to Morita equivalence, is canonically isomorphic to $H^2(K, (K^{\text{sep}})^*)$.

**Example 1.20.** Following up on Example 1.15, let $G_0$ be the Honda formal group law of height $n$ over the finite field $\mathbb{F}_{p^n}$ and let $G_n$ be its automorphism group, the Morava stabilizer group. Associated to $G_0$ 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

$$E = W(\mathbb{F}_{p^n})[[u_1, \ldots, u_{n-1}]]$$

to a power series algebra over the Witt vectors.

Since this construction is functorial in $G_0$, the Morava stabilizer group $G_n$ acts on both $E$ and $\omega$ in a compatible manner. One can show that there is a spectral sequence

$$H^*(G_n, \omega^{\otimes t}) \Rightarrow \pi_{2t-s}S^0_{K(n)},$$

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.

The following fundamental results of Lazard and Serre, respectively, show that $p$-adic analytic groups have excellent cohomological properties.

**Theorem 1.3** (Lazard, Serre). Let $G$ be a compact $p$-adic analytic group. Then

1. for any uniformly powerful subgroup $U \leq G$, the cohomology algebra $H^*(U; \mathbb{F}_p)$ is a finite-dimensional Poincaré duality algebra,

2. $H^*(G; \mathbb{F}_p)$ is a finite-dimensional Poincaré duality algebra if and only if $G$ is torsion-free.

Informally, this shows that as long as no torsion is present, cohomology of $p$-adic analytic groups behaves very much like cohomology algebra of a classical manifold.
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 will 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 very 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 will write \( H \leq G \). If it closed as a subset of \( G \), we will write \( H \leq_c G \). If it is open, we will write \( H \leq_o G \). We will denote normal subgroups by \( H \trianglelefteq G \), and closed and open ones, respectively, by \( H \trianglelefteq_c G \) and \( H \trianglelefteq_o G \).

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 \( \overline{H} \), and the latter is given as the intersection

\[
\overline{H} = \bigcap_{U \leq G \subseteq U} U
\]

of all open subgroups which contain \( H \).

**Proof.** We prove these one by one.

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

\[
U_{g_1}, \ldots, U_{g_n}
\]

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 \( U_{g_i} \cap U_{g_j} = \emptyset \) 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 \( U_{g_1} = U \). In this case the set-theoretic difference

\[
G \setminus U = \bigcup_{2 \leq i \leq n} U_{g_i}
\]

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 \( g_2, \ldots, g_n \) of \( G \) such that

\[
K, Kg_2, \ldots, Kg_n
\]

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 \((-) \cdot g : G \to G \) 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 \( U \trianglelefteq G \) such that \( H \subseteq U \) 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 \( K \trianglelefteq G \) 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 neighborhoods of the identity given by open normal subgroups \( K \cap U \), where \( U \trianglelefteq G \) is normal.

**Example 2.6.** If \( G \) is profinite and \( K \trianglelefteq G \) is a closed normal subgroup, then \( G/K \) is profinite with respect to the quotient topology induced by the projection \( G \to G/K \). 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 \( K \trianglelefteq G \) 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 \( p_1, \ldots, p_n \in P \) 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 \( I \text{disc} \) denote the subcategory with the same objects but only identity morphisms, so that the natural inclusion \( I \text{disc} \hookrightarrow I \) induces a canonical map

\[
\varprojlim G_i \to \prod_{i \in I} G_i.
\]

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

\[
\prod_{i \in I \setminus J} G_i \times \prod_{j \in J} \langle e_{G_j} \rangle \leq \prod_{i \in I \setminus J} G_i \times \prod_{j \in J} G_j = \prod_{i \in I} G_i
\]

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
\[ G \to \lim_{U \in P} G/U \]
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 \( G \to G/U \) 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 \( V \leq \lim_{U \in P} G/U \) 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
\[ \lim_{U \in P} G/U \to G/U_0. \]
Since the composite \( G \to \lim_{U \in P} G/U \to G/U_0 \) is surjective, we deduce the subgroup is the whole thing, as needed.

\[ \square \]

**Example 2.9.** If \( \Gamma \) is a group, the profinite group \( \hat{\Gamma} := \lim_{N \triangleleft G} \Gamma/N \) 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 \( \hat{\mathbb{Z}} \simeq \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \) of any finite field. The generator corresponding to \( 1 \in \hat{\mathbb{Z}} \) is given by the Frobenius \( x \mapsto x^q \).

**Warning 2.11.** Beware that the profinite completion map \( \Gamma \to \hat{\Gamma} \) is in general neither injective nor surjective.

Note that a profinite group is either finite or at least of cardinality of continuum. Despite this, we will show that 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 \( g_1, \ldots, g_d \) generate \( G \) if
\[ \langle g_1, \ldots, g_n \rangle = G; \]
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 \( \lim_{\alpha \in P} X_\alpha \) is also nonempty.

**Proof.** As in the proof of Theorem 2.8, forgetting the poset structure of \( P \) yields a natural map
\[ \lim_{\alpha \in P} X_\alpha \to \prod_{\alpha} X_\alpha \]
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 

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

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 $(\prod_{\alpha} X_{\alpha})^{P'}$. We deduce that the latter is non-empty.

As from the explicit description of the limit we have

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

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. \qed

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

$$G \cong \lim_{U \leq \text{open,} G} G/U$$

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

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

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

$$\lim_{U \leq \text{open,} G} \text{Gen}_d(G/U) \subseteq \lim_{U \leq \text{open,} G} (G/U)^d = G^d$$

is nonempty. A point of the limit can be identified with a tuple $(g_1, \ldots, g_d)$ 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 $g_1, \ldots, g_d$ is all of $G$, so $(g_1, \ldots, g_d) = G$ as needed. \qed

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

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

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 will show now, 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 group of the symmetric group $S_m$ along a continuous homomorphism $G \to S_m$. 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. □

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

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

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. □

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 will 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. □

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

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

the intersection of maximal proper open subgroups; that is, those $H \leq_o G$ 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 $K \triangleleft \Phi(G)$. 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. \qed

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 $g_1, \ldots, g_d \in G$, 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

$$\langle g_1, \ldots, g_n \rangle \neq G.$$  

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

$$\langle g_1, \ldots, g_n \rangle \leq U$$

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

$$\langle g_1, \ldots, g_n \rangle \Phi(G) \leq U \neq G,$$

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

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 $G$.

In the case of pro-$p$-groups, the Frattini subgroup can be identified very explicitly.
Lemma 3.8. If \( G \) is pro-\( p \), then every maximal proper open subgroup \( U \triangleleft G \) is normal and has index \( p \).

Proof. Since \( U \) is open, it contains an open normal subgroup \( V \subseteq U \). 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 3.9. If \( G \) is pro-\( p \), then
\[
\Phi(G) = \mathcal{G}p[G, G],
\]
the closed subgroup generated by \( p \)-th powers and commutators.

Proof. We begin with \( (\supseteq) \) containment, where we have to show that if \( U \triangleleft G \) is a maximal proper open subgroup, then \( \mathcal{G}p[G, G] \leq U \). By assumption, Lemma 3.8, \( U \) is normal and \( G/U \cong C_p \) 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 \( \mathcal{G}p[G, G] \), then \( \Phi(G) \leq U \). Observe that \( G/U \) is a finite elementary abelian \( p \)-group; in other words, we have \( G/U \cong F^\oplus n \) 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 3.10. If \( G \) is pro-\( p \) and \( K \triangleleft G \) 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 3.9, as needed. \( \square \)

Warning 3.11. Beware that Corollary 3.10 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 \( 3 : C_5 \to C_5 \) 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 3.12. 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 $U \trianglelefteq G$ be an open normal subgroup containing $\Phi(G) = \hat{G}/[G,G]$. Then $G/U$ is an abelian $p$-group of exponent $p$, so that $G/U \cong \mathbb{F}_p^n$ 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 3.13.** Beware that Theorem 3.12 fails spectacularly for general profinite groups. For example, if we consider the free profinite group on one generator $\hat{\mathbb{Z}}\cong \prod_p \mathbb{Z}_p$.

then its Frattini subgroup is given by

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

This is a closed subgroup which is not open.

As it happens, any pro-$p$-groups has a canonical filtration of which the Frattini subgroup is just the first step.

**Definition 3.14.** Let $G$ pro-$p$. The lower $p$-series of $G$ is the sequence of closed subgroups defined inductively by

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

**Example 3.15.** For any $G$, we have $P_2(G) = \Phi(G)$. More generally, $\Phi(P_i(G)) \leq P_{i+1}(G)$, although the inclusion can be strict. We will later show that for “nice” pro-$p$-groups, such as sufficiently small open neighbourhoods of pro-$p$ 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 $P_i(G)/P_{i+1}(G) \trianglelefteq G/P_{i+1}$

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

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

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

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

is zero. However, the elements of $P_{i-1}$ 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 3.17.** If $G$ is a finite $p$-group, then $P_i(G) = 0$ for all $i$ large enough.
**Proof.** By Proposition 3.16, it is enough to show that there exists some finite filtration
\[ 0 = G_{n+1} \leq G_n \leq G_{n-1} \leq \ldots \leq G_1 = G \]
where each group is central and of exponent \( p \) relative to the previous one. We will 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. \( \square \)

**Proposition 3.18.** Let \( G \) be pro-\( p \).

1. If \( K \leq G \), then \( P_1(G)K/K = P_1(G/K) \)
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 \( P_1(G)/P_{i+1}(G) \leq G/P_{i+1} \) 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 3.16 that \( P_1(G/K) \leq P_i(G/K) \) 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 3.17 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 3.12, we deduce that so is \( G_i \), as needed. \( \square \)

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

**Theorem 3.19.** 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 \( F_p \)-vector space. As a consequence of Theorem 3.19, the commutator of \( G \) induces a function
\[ [-,-]: \text{gr}_i(G) \times \text{gr}_j(G) \to \text{gr}_{i+j}(G). \]
One can show that this function is in fact a \( F_p \)-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 3.19, 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
\[ [a, b] := a^{-1}ab = a^{-1}b^{-1}ab \]
for the commutator. This can be extended to three elements by declaring that

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

**Recollection 3.20** (Hall-Witt identity). The celebrated Hall-Witt identity says that the expression

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

is equal to the identity in any group. With enough patience, this can be verified by expanding the left hand side out. As a consequence, we have the three subgroup lemma that 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 3.21** (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

\[ [ab, c] = [a, c][a, b]. \]

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

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

and similarly

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

**Proof of Theorem 3.19:** For brevity, we will write \( G_i := P_i(G) \). 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

\[ [G_m, G] \leq G_m^0 [G_m, G] = G_m^1. \]

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 3.18, we can replace \( G \) by \( G/N \) and thus assume that

1. \( G \) is 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 3.21, where we can ignore the conjugations since these commutators are central, we see that

\[ [x, y^p] = [g, x]^p = e. \]

Moreover, using the three subgroup lemma of Recollection 3.20 we have that

\[ [G_m, [G_{n-1}, G]] \leq [G_{n-1}, [G, G_m]] [G_m, G_{n-1}] = [G_{n+m-1}, G][G_m, G_{n-1}] = \{e\}. \]
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
\[ [G_m, G_n] = [G_m, G_n^p [G_{n-1}, G]] \leq \{e\} \]
which is what we wanted to show. \(\square\)

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 \(G \to G'\) is continuous.

**Proof.** We can write \(G' \simeq \varprojlim G'_\alpha\) as a limit of finite groups. To show that an abstract group homomorphism \(G \to G'\) is continuous, it is enough to verify that each of the composites \(G \to G' \to G'_\alpha\) 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 \(G \to G\) 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
\[ G^{(p^r)} \subseteq G^{(m)}, \]
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
\[ p^e = am + bp^e \]
and thus for any \(g \in G\) we have
\[ g^{p^e} = (g^a)^m (g^b)^{p^e} \in G^{(m)} N. \]
Since this holds for any \(N\) and \(G^{(m)}\) is closed, we deduce that \(g^{p^e} \in G^{(m)}\). This shows (4.1) and hence the needed statement. \(\square\)
The second result we will need is slightly more involved, and it will require us to use a little bit of theory of nilpotent groups.

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

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

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 3.17).

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

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

for some $g_i \in G$.

**Proof.** We will 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 will write $G_i = [G_{i-1}, G]$ for some $i \geq 1$. Since $G_c = [G_{c-1}, G]$ is in the center. Using the conjugate-linearity of the commutator of Recollection 3.21, which is simple linearity here as all of these commutators are in the center, we deduce that the map

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

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

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

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 $x_1 \otimes a_1 + \ldots + x_d \otimes a_d$ for some $x_i \in G_{c-1}$. Thus, any element $w \in G_c$ can be written in the form

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

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

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

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

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

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

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

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 $a_1, \ldots, a_d$ be generators of $G$, and consider the continuous map

$$[-, a_1] \cdots [-, a_d] : G^d \to G$$

whose image $X \subseteq G$ is closed and contained in $[G, G]$. We claim that $X = [G, G]$ which implies that $[G, G] = [G, G]$ 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 $N \trianglelefteq G$, which is an immediate consequence of Lemma 4.6 as $G/N$ is a nilpotent group generated by the images of the $a_i$. \qed

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 will 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 $G/H \cong C_p$, a cyclic group of order $p$. Since $G$ is finitely generated pro-$p$, we can rewrite the Frattini subgroup as


where the first equality is Proposition 3.9, 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 3.12, 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

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

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. \qed

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

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

\[ \text{If } G \text{ is abelian, then } x \to x^p \text{ is an endomorphism of } G, \text{ even before passing to quotients. In the powerful case, this is in general only true if we consider this as a map between the quotients } G^p/G^{p+1}. \]
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 $p = 2$.

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 will 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 $C_p \to \text{Aut}(C_p^2) \simeq (\mathbb{Z}/p^2)^*$. Then $G/C^p$ can be identified with
\[ (C_p^2/pC^2) \rtimes C_p \simeq C_p \times C_p \simeq C_p \times C_p, \]
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 $\mathbb{F}_p$.

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 powerful embedded in $G$, which we denote by $N \text{ p.e. } G$, if
\begin{enumerate}
\item $[N, G] \leq N^p$ and $p > 2$ or
\item $[N, G] \leq N^4$ and $p = 2$.
\end{enumerate}

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 $N \text{ p.e. } G$, 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 $K \trianglelefteq G$ are subgroups, the following hold:
\begin{enumerate}
\item if $N \text{ p.e. } G$, then $NK/K \text{ p.e. } G/K$,
\item if $K \leq N^p$, then the converse holds: if $NK/K \text{ p.e. } G/K$, then also $N \text{ p.e. } G$.
\end{enumerate}

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 $N \trianglelefteq G$ be a normal subgroup and suppose that $N$ is not powerfully embedded in $G$. If $p > 2$, then there exists a normal $J \trianglelefteq G$ such that
\[ N^p[N, G, G] \leq Y < N^p[N, G] \]

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 $p$. □

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


where the second inclusion is of index exactly 2. This turns out to be enough to also prove Proposition 5.13 at $p = 2$, in which 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 3.21, 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 $G \to Z(G)$. It follows that we have

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

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

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

which we can rewrite as

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

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 3.14. 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 will 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 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. \(G_1 = G^p = \Phi(G)\),
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 will 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 \([G_i, G] \leq G_1^p\), so that

\[\Phi(G_i) \leq P_{i+1}(G) = G_i^p[G_i, G] \leq G_1^p \leq \Phi(G)\]

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 \(p^i\)-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 \(G_2\) is central, since \(G\) is powerful and \(G_2\) p.e. \(G\). If \(x, y \in G\), then we have

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

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 \(H/[N, H]\) is has the image of \(N\) in its center, and is generated over its center 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 to 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 will 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. \( [G, G] \leq G^p \) and \( p > 2 \) or
2. \( [G, G] \leq G^4 \) and \( p = 2 \).

We say an open subgroup \( N \leq_o G \) is powerfully embedded, denoted by \( N \text{ p.e. } G \), if

1. \( [G, N] \leq N^p \) and \( p > 2 \) or
2. \( [G, N] \leq N^4 \) 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 \( N \text{ p.e. } G \) if and only if for each open normal \( O \leq_o G \), we have \( NO/O \text{ p.e. } G/O \).

Proof. This is immediate from the formula
\[ G^p = \bigcap G^p O, \]
where the intersection is taken over all open normal subgroups of \( G \), and similarly for \( G^4 \). \( \square \)

Corollary 6.3. A pro-$p$-groups \( G \) 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 \( G = \lim G/O \), where the limit is taken over the poset of open normal subgroups.

Conversely, suppose that \( G = \lim G_\alpha \) 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 \( G \to G_\alpha \) for some \( \alpha \), so that \( G/K \) is a quotient of \( G_\alpha \). It follows that \( G/K \) is also powerful. \( \square \)
Recall that in Definition 3.14 we introduced the lower $p$-series, which is a filtration of a pro-$p$-group $G$ by subgroups defined inductively by
\[(1) \ P_i(G) = G \]
\[(2) \ P_{i+1}(G) = P_i(G) / P_i(G, G). \]
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
\[(1) \ P_{i+1}(G) = \overline{G^{p^i}} = \{ g^{p^i} \mid g \in G \} \text{ and} \]
\[(2) \ P_{i+1}(G) \text{ is powerfully embedded in } G. \]

**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. \qed

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

**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
\[d(G) \leq rk(G). \]
If $G$ is abelian, these two quantities are in fact the same. This is not true in general, even for $p$-groups, as the following example shows.

**Example 6.8.** Let $F_3$ be a 3-dimensional vector space over $\mathbb{F}_3$, 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 $G := F_3 \rtimes C_3$ is generated by two elements $((1,0,0), 0)$ and $((0,0,0), 1)$. However, it has $F_3^3$ as a normal subgroup which cannot be generated by two elements. It follows that $rk(G) > d(G)$.

\[\text{For example, because any finite abelian group } A \text{ is (non-canonically) isomorphic to its Pontryagin dual } \text{Hom}(A, \mathbb{Q}/\mathbb{Z}). \text{ Since Pontryagin duality takes monomorphisms to epimorphisms, it follows that any subgroup of } A \text{ is isomorphic to some quotient of } A, \text{ and so can be generated by the same number of elements.} \]
The following beautiful result gives another piece of evidence that powerful $p$-groups are “morally abelian”.

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

**Proof.** For brevity, we write $G_2 := P_2(G) = G_p^p$ and $G_3 := P_3(G) = G_p^p$, 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

$$\pi G_2 \to G_2/G_3,$$

of $\mathbb{F}_p$-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 $h_1, \ldots, h_e \in H$ such that

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

We have that $\text{dim}_{\mathbb{F}_p}(\ker(\pi)) = r - m$, and thus

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

and therefore

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

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 $h_1^p, \ldots, h_e^p$ 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 $k_1, \ldots, k_{r-e}$ such that

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

We then have

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

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

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 $x_1, \ldots, x_n$ such that $G = \langle x_1, \ldots, x_n \rangle$ 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

$$\sup\{d(H) \mid H \leq G\} = \sup\{d(O) \mid O \leq G\} = \sup\{\text{rk}(G/O) \mid O \triangleleft G\}.$$

**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 $O \triangleleft G$. 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 $H \leq G$ 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. \qed
**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! 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 will need a partial converse to the latter; that is, we will 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 \( p \geq 0 \), we write \( \text{GL}_r(\mathbb{F}_p) := \text{Aut}(\mathbb{F}_p^r) \) for the general linear group over the field with \( p \) elements. We write \( U_r(\mathbb{F}_p) \leq \text{GL}_r(\mathbb{F}_p) \) for the subgroup of upper unitriangular matrices; that is, those which are upper triangular and have 1s on the diagonal.

Equivalently, \( U_r(\mathbb{F}_p) \) is the subgroup of those automorphisms of \( \mathbb{F}_p \) which preserve the standard complete flag

\[
0 \leq \mathbb{F}_p \leq \mathbb{F}_p^2 \leq \ldots \leq \mathbb{F}_p^r
\]

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

\[
|U_r(\mathbb{F}_p)| = p^{(r-1)r+(r-2)r+\ldots+1} = p^{r(r-1)/2}.
\]

As we have

\[
|\text{GL}_r(\mathbb{F}_p)| = (p^r - 1) \cdot (p^r - p) \cdot \ldots \cdot (p^r - p^{r-1})
\]

by a standard argument of choosing the images of basis elements, we see that \( U_r(\mathbb{F}_p) \leq \text{GL}_r(\mathbb{F}_p) \) 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

\[
V(G, r) := \bigcap_{\phi \in \text{GL}_r(\mathbb{F}_p)} \ker(\phi),
\]

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

\[
V(G, r) := \bigcap_{\phi \in U_r(\mathbb{F}_p)} \ker(\phi),
\]

of kernels of all homomorphisms \( G \to U_r(\mathbb{F}_p) \).

**Remark 6.15.** Note that the equivalence of the two variants of Definition 6.14 follows from the fact that \( U_r(\mathbb{F}_p) \leq \text{GL}_r(\mathbb{F}_p) \) 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.

\[^4\text{In the celebrated work of Lubotzky an Mann, see [LM87a] and [LM87b].}\]
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 $G/N \to \text{GL}_r(\mathbf{F}_p)$ can be identified with a subset of homomorphisms $G \to \text{GL}_r(\mathbf{F}_p)$. 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 will 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 $\phi : \mathbf{F}_p^s \to \mathbf{F}_p^{s'}$ 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

$$\begin{array}{ccc}
\mathbf{F}_p^s & \longrightarrow & \mathbf{F}_p^{s'} \\
\phi_1 \downarrow & & \phi \downarrow \\
\mathbf{F}_p^s & \longrightarrow & \mathbf{F}_p^{s'}
\end{array}$$

where we identify $\mathbf{F}_p^{s'} \cong \mathbf{F}_p^s/\mathbf{F}_p^{s'}$. 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 $\phi \mapsto \phi_1 \times \phi_2$ defines a map

$$U_r(\mathbf{F}_p) \to U_s(\mathbf{F}_p) \times U_{s'}(\mathbf{F}_p)$$

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 $v : \mathbf{F}_p^r \to \mathbf{F}_p^r$ 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

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

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. □

Corollary 6.20. Let $G$ be a $p$-group of rank $r$. Then $|G : V(G, r)| \leq p^{r^\lambda(r)}$. 
\textbf{Proof.} Since by construction \(G/V(G,r)\) embeds as a subgroup of a product of \(U_1(F_p)\), it follows from \textbf{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. \(\Box\)

\textbf{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. \(W\).

\textbf{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 \textbf{Lemma 5.10} outlined in \textbf{Remark 6.11}, 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 \textbf{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. \([N,W] = 0\),
2. \([N,W] = p\).

Note that in the quotient we will still have \(W \leq V(G,r)\) by \textbf{Remark 6.17}. We can find a normal subgroup \(M \triangleleft G\) such that

1. \([N,W] \leq M \leq G\)

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 central, 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. \(\Box\)

\textbf{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.

\textbf{Proof.} This is an application of \textbf{Proposition 6.21} to either \(N = V(G,r)\) or \(N = V(G,r)^2\). \(\Box\)

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

\textbf{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. \(p^\lambda(r)\) if \(p > 2\),
2. \(p^\lambda(r)^r\) if \(p = 2\).

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

\[2^{\lambda(r)^r} = 2^{\lambda(r)} \cdot 2^r,\]

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

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 $K \triangleleft G$, 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
\[ V(G, r) := \bigcap_{\phi : G \to \text{GL}_r(F_p)} \ker(\phi), \]
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
\[ \lim_{O \triangleleft G, O \triangleleft V(G, r)} G/O, \]
the limit of quotients indexed by the poset of open subgroups contained in $V(G, r)$. Since $V(G, r)$ is closed, we have
\[ V(G, r) \simeq \lim V(G, r)/O \simeq \lim V(G/O, r), \]
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 if $V(G, r)$ as their limit. If $p = 2$, we can take $V(G, r)^2$ instead. □

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 $N \triangleleft G$ 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 $G \to \text{GL}_r(F_p)$. We can then take

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

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 3.18, they are powerful for $i$ large enough as a consequence of Lemma 7.3. Since $x \mapsto x^p$ defines an epimorphism $G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ for all $i$ by Theorem 5.14, the sequence of numbers

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

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

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 will 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 $g^n = e$. 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

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

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. and both groups are of the same size by uniformity, this

(2 $\Rightarrow$ 1): We will show that if $G$ is not uniform, then $G$ is not torsion-free. By assumption, one of the maps $G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ 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 $G_1$, we can assume that $i = 1$.

We will inductively construct a sequence $x_2, x_3, \ldots$ 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 $G_n/G_{n+1} \to G_{n+1}/G_{n+2}$ 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 $x := \lim_{k \to \infty} x_k$; this limit exists as this sequence is Cauchy by the second condition above and $G$ is compact. Then

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

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

Corollary 7.5. Any pro-$p$ group $G$ of finite rank has an open characteristic subgroup $U \trianglelefteq G$ such that any open normal closed subgroup $N \trianglelefteq G$ 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 $V$. □

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. \qed

**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, as long as they’re compact, as 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 $N \trianglelefteq_o G$ 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 $\dim(G) = \dim_F(G/G^p)$ and similarly for $N$ and $G/N$. We have

$$\dim(G) = \dim_F(G/G^p) = \dim_F(NG^p/G^p) + \dim_F(G/NG^p).$$

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

$$\dim_F(N/(G^p \cap N)) + \dim_F(G/NG^p) = \dim_F(N/N^p) + \dim_F(G/NG^p) = \dim(N) + \dim(G/N),$$

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 $K \leq G$ 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

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

\qed

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

\[ a_1^{\lambda_1} \cdot a_2^{\lambda_2} \cdot \ldots \cdot a_d^{\lambda_d} \]

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

\[ g = a_1^{\lambda_1} \cdot a_2^{\lambda_2} \cdot \ldots \cdot a_d^{\lambda_d} x \]

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 will 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

\[ G \times \mathbb{Z}_p \to G \]

written as

\[ (g, \lambda) \mapsto g^\lambda \]

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

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

\[ G \times \mathbb{Z} \to G_\alpha. \]

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

\[
\begin{array}{ccc}
G \times \mathbb{Z}_p & \to & G \\
\uparrow & & \downarrow \\
G \times \mathbb{Z} & \to & G \times \mathbb{Z}/p^d \to G_\alpha
\end{array}
\]

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

\[ g^\lambda = \lim_{i \to \infty} g^{\lambda_i} \]

where on the right hand side we have the standard powers and \( \lambda_i \in \mathbb{Z} \) is a sequence of integers converging \( \lambda_i \to \lambda \) 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 \( a_1, \ldots, a_d \) be a minimal system of generators. Then the map

\[ \mathbb{Z}_p^d \to G \]

given by

\[ (\lambda_1, \ldots, \lambda_d) \mapsto a_1^{\lambda_1} \cdot \ldots \cdot a_d^{\lambda_d}, \]

the \( p \)-adic powers of Construction 7.12, is a homeomorphism.
Proof. Since $U/pU \cong U/U_2$ 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

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

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 $\mathbb{Z}_p^d \to G$ 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. \qed

8. The $p$-adic General Linear Group

In this lecture, we will verify that the archetypical example of a $p$-adic analytic group $GL_d(\mathbb{Z}_p)$, 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 $\Gamma_n \triangleleft GL_d(\mathbb{Z}_p)$ is the open subgroup given by the kernel

$$
\Gamma_n := \ker(GL_d(\mathbb{Z}_p) \to GL_d(\mathbb{Z}/p^n)).
$$

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, $GL_d(\mathbb{Z}_p)$ is profinite.

Lemma 8.2. We have

$$
|GL_d(\mathbb{Z}_p) : \Gamma_1| = (p^d - 1) \cdot (p^d - p) \cdot \ldots \cdot (p^d - p^{d-1})
$$

and

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

for each $n \geq 1$.

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

Corollary 8.3. The profinite group $GL_d(\mathbb{Z}_p)$ 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-$p$.

We now study the basic relationships between the congruence subgroups.

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

$$
a \equiv (a + p^n x) \mod \Gamma_n.
$$

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

Lemma 8.5. For any $n \geq 1$, we have $[\Gamma_n, \Gamma_n] \leq \Gamma_{2n}$.
Proof. Let $1 + p^na$ and $1 + p^nb$ be elements of $\Gamma_n$. Then

$$(1 + p^na)(1 + p^nb) \equiv (1 + p^na + p^nb + p^{2n}ab) \equiv (1 + p^n(a + p^n)b) \mod 2_n,$$

where the second equivalence is Lemma 8.4. The result follows since $p^n(a + p^n)b = p^n(b + p^n a)$. \hfill \Box

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

$$ (1 + p^n a)^p = 1 + \left( \begin{array}{c} p \\ 1 \end{array} \right) p^n a + \sum_{2 \leq k \leq p} \left( \begin{array}{c} p \\ k \end{array} \right) p^{nk} a^k $$

which we can rewrite as

$$ 1 + \left( \begin{array}{c} p \\ 1 \end{array} \right) p^n a + \sum_{2 \leq k \leq p} \left( \begin{array}{c} p \\ k \end{array} \right) p^{nk} a^k = 1 + p^{n+1}(a + \sum \left( \begin{array}{c} p \\ k \end{array} \right) p^{n(k-1)} a^k) $$

as needed. \hfill \Box

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

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

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 $x_1, x_2, \ldots$ of matrices in the subring generated by $a$ such that

$$ f(x_i) \equiv 0 \mod p^i $$

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

$$ f(x) = (x - a) + \sum_{2 \leq k \leq p} \left( \begin{array}{c} p \\ k \end{array} \right) p^{nk-1} x^k, $$

so that

$$ f(a) = \sum \left( \begin{array}{c} p \\ k \end{array} \right) p^{nk} a^k. $$

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 $\binom{p}{k}$ 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

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

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\footnote{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.}, we see that inductively defining

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

yields a Cauchy sequence which converges to the needed solution. \hfill \Box
**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

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

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

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

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 $GL_d(\mathbb{Z}_p)$ 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

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

$$T_eG \times T_eG \to T_eG.$$ 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 will become 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 will 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 $x \mapsto x^p$ induces a function of sets

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

\[ x \equiv y \mod G_{k+1} \]

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

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

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

\[ x^p \equiv y^p \mod G_{k+2}, \]

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 \( p^n(G)^k \), 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 \( G/G_{k+1} \to G_2/G_{k+2} \), 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 \( U \to U_{n+1} \).

Proof. This map can be identified with the limit of bijections between finite sets of Lemma 9.2 as \( k \to \infty \), 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 \( p^n : U_{n+1} \to U \) 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 \((U, +_n) \cong (U_{n+1}, \cdot)\), where \( \cdot \) is the standard multiplication of \( U_{n+1} \).

Lemma 9.7. If \( U \) is uniform and \( x, y \in U \), then

\[ x + n y \equiv x + n_1 y \mod U_n. \]

Moreover, for any \( u, v \in U_n \) we have

\[ u x + n_1 v y \equiv x + n y \mod U_n. \]

Proof. Since \([U_n, U_n] \leq U_{2n}\) by Theorem 3.19, we have

\[ (x^{p^{n-1}} y^{p^{n-1}})^p \equiv ((xy)^{p^{n-1}})^p \mod U_{2n}. \]

Taking \( p^n \)-th roots, this yields

\[ x + n y \equiv x + n \mod U_n. \]

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

\[ u x + n_1 v y \equiv ((ux)^{p^n} (vy)^{p^n})^{p^n} \equiv (x^{p^n} y^{p^n})^{p^n} \mod U_n. \]

Taking \( p^n \)-th powers shows that the above is equivalent to

\[ (ux)^{p^n} (vy)^{p^n} \equiv x^{p^n} y^{p^n} \mod U_{2n}, \]

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
\[
x +_1 y, x +_2 y, \ldots
\]
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
\[
(x, y) \mapsto x + y := \lim_{n \to \infty} x +_n y.
\]
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 \( -1 \).

**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
\[
(x + y) + z \equiv (x +_n y) + z \quad \text{mod } U_{n+1}
\]
\[
\equiv (x +_n y) +_n z \quad \text{mod } U_{n+1}
\]
\[
\equiv x +_n (y +_n z) \quad \text{mod } U_{n+1}
\]
\[
\equiv x + (y + z) \quad \text{mod } U_{n+1}.
\]
Since this is true for all \( n \), we get associativity.

We are left with showing that addition is commutative. 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
\[
(x + y) + z \equiv (x +_n y) + z \quad \text{mod } U_{n+1}
\]
\[
\equiv (x +_n y) +_n z \quad \text{mod } U_{n+1}
\]
\[
\equiv x +_n (y +_n z) \quad \text{mod } U_{n+1}
\]
\[
\equiv x + (y + z) \quad \text{mod } U_{n+1}.
\]
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 3.19, we have
\[
(x^{p^n} y^{p^n}) \equiv y^{p^n} x^{p^n} \quad \text{mod } U_{2n+2}.
\]
Taking \( p^n \)-th roots, we get that
\[
x +_n y \equiv y +_n x \quad \text{mod } U_{n+2}.
\]
Passing to the limit as \( n \to \infty \), 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 will 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
\[
(1) \text{ if } [x, y] = e, \text{ then } x + y = xy,
(2) x^m = mx,
(3) p^k U = U_{k+1}.
\]

**Proof.** For the first part, we have
\[
x +_n y = (x^{p^n} y^{p^n})^{p^{-n}}.
\]
Since \( x \) and \( y \) commute, this is equal to
\[
((xy)^{p^n})^{p^{-n}} = xy.
\]
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. □

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 \( U_n \leq U \) 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

\[
a + v \equiv a + (ve) \equiv a + e \equiv a \mod U_n.
\]

So \( a + v = au \) for some \( u \in U_n \) and \( a + U_n \subseteq aU_n \). Conversely,

\[
au - a \equiv a - a \equiv e \mod U_n.
\]

Thus \( au - a = v \) for some \( v \in U_n \), and therefore \( au = a + v \), showing that \( aU_n \subseteq a + U_n \). □

It follows from Lemma 9.11 that for any \( n \) and \( k \), the two quotients

\[
(U_n, +)/(U_n, \cdot) \simeq (U_n, \cdot)/(U_n, \cdot)
\]

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, \( x \mapsto x^p \) defines a group isomorphism \( U_n/U_{n+1} \to U_{nk}/U_{nk+1} \). It follows that \( +_k \) define the same group structure on \( U_n/U_{n+1} \) as standard multiplication and hence so does their limit \( + \). □

**Proposition 9.13.** The addition makes \( U \) into a uniform group of dimension \( \dim(U) \).

*Proof.* Since \( p^nU = U_{n+1} \) form a basis of neighborhoods of the identity and

\[
\left[(U, +) : p^nU\right] = \left[(U, \cdot) : U_{n+1}\right]
\]

by Lemma 9.11, we see that \( (U, +) \) is a pro-\( p \) group. Since \( U/pU \cong U/U_2 \) 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. □

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 \( a_1, \ldots, a_d \) of generators, \( (U, +) \) is a free \( \mathbb{Z}_p \)-module generated by \( a_1, \ldots, a_d \), so that we have a topological group isomorphism

\[
(U, +) \cong \mathbb{Z}_p^d.
\]

*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 \( \mathbb{Z}_p^d \to U \) defined by

\[
(\lambda_1, \ldots, \lambda_d) \mapsto \lambda_1a_1 + \ldots + \lambda_da_d
\]

is a homeomorphism. Since it is also a group homomorphism as \( (U, +) \) is abelian, the claim follows. □
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

\[ \text{Aut}(U) \leq \text{GL}_d(\mathbb{Z}_p) \]

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 \(\text{dim}(G) = d\). Then there exists an exact sequence of topological groups

\[ 0 \to \mathbb{Z}_p^e \to G \to \text{GL}_d(\mathbb{Z}_p) \times F, \]

where \(F\) is a finite \(p\)-group and \(e \leq d\).

**Proof.** By Proposition 7.4, \(G\) has a normal open uniform subgroup \(U \triangleleft G\). We look at the map

\[ G \to \text{Aut}(U) \times G/U \]

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 \(G \to \text{Aut}(\mathfrak{g})\) into the automorphims 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 group 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 only 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

$\hat{O}_{A, e} = k[x]$

at the identity $e \in A$ is non-canonically isomorphic to the ring of formal power series$^6$. The multiplication of $A$ induces a continuous map

$\phi : k[[x]] \to \hat{O}_{A, e} \to \hat{O}_{A, e} \hat{O}_{A, e} = k[[x_1, x_2]]$

$^6$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.
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* $\phi : F \to G$ is a power series $\phi \in R J x K$ 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 $\phi : R \to R'$ 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 $\phi^* : \{\text{Formal groups laws over } R\} \to \{\text{Formal groups laws over } R'\}$ 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

$$\{\text{Formal groups laws over } -\} : \text{CRing} \to \mathcal{S},$$

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.”

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 $\phi : F_a \to F_m$ 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

$$[p]F(x) := x + F + \ldots + F^p x.$$  

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 $\phi : F \to G$ 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.
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 lecture, 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 a 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 will be 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 will 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, $W = \lim\limits_{\rightarrow} W/p^n$,
(2) $W$ is flat over $\mathbb{Z}_p$,
(3) the $\mathbb{F}_p$-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

$$C\text{Alg}^{\text{Witt}} \to C\text{Alg}^{\text{perf}}_{F_p}$$

from the full subcategory of rings spanned by rings of Witt vectors to the full subcategory of rings spanned by perfect $F_p$-algebras. One can show using obstruction theory that (11.1) is an equivalence of categories, and so has an inverse which we write as

$$R \in C\text{Alg}^{\text{perf}}_{F_p} \mapsto W(R) \in C\text{Alg}^{\text{Witt}}.$$

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

$$W(F_p) \cong \mathbb{Z}_p,$$

since the latter is flat over itself, $p$-complete and reduces to $F_p$. More generally, if $q = p^n$, then we can write the finite field with $q$ elements as $F_q = F_p[\zeta_{q-1}]$, where $\zeta_{q-1}$ is a primitive $(q-1)$-th root of unity. Using this description one can check that

$$W(F_q) = \mathbb{Z}_p[\zeta_{q-1}].$$

**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 $F_p$-algebra. The Witt vector Frobenius is the unique ring automorphism

$$\sigma : W(R) \to W(R)$$

which reduces to the Frobenius modulo $p$; that is, such that

$$\sigma(w) \equiv x^p \mod p$$

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 $F_p$-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 $F_p$, 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 $F_p$-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. $f(x) \equiv px \mod x^2$,
2. $f(x) \equiv x^q \mod p$

The construction $W \mapsto W/pW$ provides a functor

$$C\text{Alg}^{\text{Witt}} \to C\text{Alg}^{\text{perf}}_{F_p}$$

from the full subcategory of rings spanned by rings of Witt vectors to the full subcategory of rings spanned by perfect $F_p$-algebras. One can show using obstruction theory that (11.1) is an equivalence of categories, and so has an inverse which we write as

$$R \in C\text{Alg}^{\text{perf}}_{F_p} \mapsto W(R) \in C\text{Alg}^{\text{Witt}}.$$
Then, for any linear form \( \phi(x) = a_1 x_1 + \ldots + a_k x_k \) linear form with coefficients in \( W(R) \) there exists a unique unique power series

\[
\tilde{\phi}(x) \in W(R)[x_1, \ldots, x_k]
\]
such that

1. \( \tilde{\phi} \) lifts \( \phi \); that is, we have

\[
\tilde{\phi}(x_1, \ldots, x_k) = \phi(x_1, \ldots, x_k) + \text{terms of degree two and higher},
\]
2. \( \tilde{\phi} \) commutes with \( f \); that is,

\[
f(\tilde{\phi}(x_1, \ldots, x_k)) = \tilde{\phi}(f(x_1), \ldots, f(x_k))
\]

Proof. For brevity, we will write \( x \) to mean \( x_1, \ldots, x_k \). We will construct by induction a compatible sequence of degree \( n \) polynomials \( \phi_n(x) \) such that the second equation 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 will 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

\[
f(\phi_{n+1}(x)) = f(\phi_n(x) + c(x)) \equiv f(\phi_n(x)) + pc(x) \mod x^{n+2}
\]
and similarly

\[
\phi_{n+1}(f(x)) = \phi_n(f(x)) + c(f(x)) \equiv \phi_n(f(x)) + p^{n+1}c(x) \mod x^{n+2}.
\]
Thus \( E(\phi_{n+1}) \equiv 0 \mod x^{n+2} \) is equivalent to

\[
(11.2) \quad E(\phi_n) = (-p - p^{n+1})c(x) \mod x^{n+2}.
\]
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 \( W(R)/p \cong R \). 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

\[
\sum_i a_i^q x^{q i} = \sum_i a_i x^{q i}
\]
because \( a_i^q = a_i \) by our assumption on \( R \). \(\square\)
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 \( \mathbb{F}_p \)-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. \( f(x) \equiv px \mod x^2 \),
2. \( f(x) \equiv x^q \mod p \).

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

\[ F(x, y) := \overline{x + y}. \]

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 \( F(x, y) \) 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 \( f(x) \equiv x^q \mod p \) 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 \( \mathbb{F}_p \) (which by abuse of terminology we will also call the Honda formal group law) is of height \( n \), since \( f(x) \equiv x^q = x^{p^n} \mod p \). 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 \( F_p \), 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. □

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 \( \phi : R \to R' \) is a ring homomorphism and \( F' := \phi^* F \), then applying \( \phi \) to coefficients of a power series gives a ring homomorphism

\[
 \text{End}(F/R) \to \text{End}(F'/R').
\]

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 \( w \in \mathcal{W}(R) \). Then, by Lemma 11.6 there exists a unique power series, which we denote by

\[
 [w](x) := \tilde{w} x,
\]

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

\[
 \mathcal{W}(R) \xrightarrow{\tilde{w}} \text{End}(F_f/W(R)).
\]

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 \( w \mapsto \tilde{w} \) is an isomorphism, observe that any endomorphism commutes with the \( p \)-series, hence is uniquely determined by its leading term. □
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 $[p]F(x) = x^q \mod p$.

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 $[p](x) = x^{p^n} + \text{higher order terms}$. 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 will calculate the automorphism group of $\Gamma_n$ over the algebraic closure $\overline{F}_p$, and show that it is a $p$-adic analytic group of dimension $n^2$.

**Notation 12.1.** We will generally 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 $\mathbb{F}_p$. 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 $\overline{F}_p$ are isomorphic, and thus so are their endomorphism rings. Thus, our calculation will 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 $\mathbb{F}_q \hookrightarrow k$ induces an isomorphism of endomorphism rings

$$\text{End}(\Gamma_n/\mathbb{F}_q) \cong \text{End}(\Gamma_n/k).$$

In particular,

$$\text{End}(\Gamma_n/\mathbb{F}_q) \cong \text{End}(\Gamma_n/\overline{\mathbb{F}}_p).$$

**Proof.** Let $\phi : \Gamma_n \to \Gamma_n$ 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

$$\sum a_i^q x^{qi} = \left(\sum a_i x^i\right)^q = [p] \circ \phi \circ [p] = \sum a_i x^{qi}.$$

It follows that $a_i^q = a_i$ for each $i \geq 0$, hence $a_i \in \mathbb{F}_q$, as needed. \hfill $\square$

As a consequence of Proposition 12.2, when working with the Honda formal group law, we can focus on endomorphisms over $\mathbb{F}_q$. In Proposition 11.14, we saw that the Lubin-Tate construction provides a isomorphism of rings

$$W(\mathbb{F}_q) \longrightarrow \text{End}(\Gamma_n/W(\mathbb{F}_q)).$$

We can compose with reduction mod $p$ to obtain a ring homomorphism

$$W(\mathbb{F}_q) \to \text{End}(\Gamma_n/\mathbb{F}_q).$$

(12.1)

However, the latter map is no longer surjective, as there are endomorphisms of $\Gamma_n$ over $\mathbb{F}_q$ 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 $\mathbb{F}_p$. 
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 $a_{i,j} \in \mathbb{F}_p$, so that $a^p_{i,j} = a_{i,j}$. 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 $S \in \text{End}(\Gamma_n, \mathbb{F}_q)$ defined by $S(x) = x^p$ the Frobenius of the Honda formal group law.

We will 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

$$\text{End}(\Gamma_n/\mathbb{F}_q) \cong W(\mathbb{F}_q)(S)/(S^m = p, S_w = w^\sigma S),$$

where $(-)(S)$ denotes the ring obtained by attaching a new non-commuting variable and $w \mapsto w^\sigma$ is the Witt vector Frobenius on $W(\mathbb{F}_q)$.

Note that the endomorphism ring inherits a canonical topology as a closed subspace

$$\text{End}(\Gamma_n) \subseteq \mathbb{F}_q[x],$$

where we equip the target with the limit topology coming from the identification

$$\mathbb{F}_q[x] = \lim_{\leftarrow} \mathbb{F}_q[x]/x^n.$$

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, $p^k \mapsto [p]_n^k(x) = x^{kq}$, which becomes highly divisible by $x$ as $k$ grows, the map

$$W(\mathbb{F}_q) \to \text{End}(\Gamma_n)$$

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 $a \in W(\mathbb{F}_q)$ is a Teichmüller representative if $a^q = a$.

Lemma 12.7. We have that:

1. any element $a \in \mathbb{F}_q$ has a unique lift to a Teichmüller representative,
2. any $w \in W(\mathbb{F}_q)$ 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 $\mathbb{F}_q$ is nowhere vanishing. For the second part, let $a_0$ be the unique Teichmüller representative of the reduction of $w \mod p$, so that

$$w = a_0 + pw'$$

for a uniquely defined $w'$. Inductively applying the construction to $w'$ leads to the needed series expansion. □
Lemma 12.8. Let \( a \in W(F_q) \) be a Teichmüller representative. Then
\[
[a](x) = ax \in W(F_q)[[x]],
\]
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 \( \text{End}(\Gamma_n/F_q) \), 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 \([\cdot]\) denotes Construction 11.13. We first show it in the special case when \( w = a \) is a Teichmüller representative. In this case, we have \([a](x) = \overline{a}x\), where \( \overline{a} \) is the image of \( a \) in \( F_p \), and we calculate
\[
S([a](x)) = (\overline{a}x)^p = \overline{a}^p x^p = \overline{a^p}(x^p) = [a^p](S(x)),
\]
where we use that \((a^p)^q = a^q\). Since Hensel’s lemma any element of \( F_q \) has a unique lift to an element satisfying \( a^q = a \), we deduce that \( a^q = a^p \) 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 \( \text{End}(\Gamma_n/F_q) \) we have
\[
Sw = S(\sum a_i p^i) = \sum a_i^\sigma p^i S = w^\sigma S,
\]
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
\[
W(F_q)(S)/ (S^n = p, Sw = w^\sigma S) \rightarrow \text{End}(\Gamma_n/F_q)
\]
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) \( \phi(x) = \psi(x^p) \) 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
\[
(\partial_y F_1)(x, y) \cdot \phi'(F_1(x, y)) = \phi'(y) \cdot (\partial_y F_2)(\phi(x), \phi(y)).
\]
Since for any formal group law \( F(x, y) \) unitarity 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
\[
\phi'(x) = (\sum a_i x^i)' = \sum i a_i x^{i-1},
\]
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 \( \psi: \sigma^* F_1 \to F_2 \), where \( \sigma^* F_1 \) is pullback of a formal group law along the Frobenius \( \sigma: k \to k \), 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 \( \sigma: k \to k \) 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 \( \phi(x) = \psi(x^p) \), 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 \( \phi \in \text{End}(\Gamma_n/F_q) \) can be written uniquely as a convergent sum
\[
\phi = a_0 + a_1 S + a_2 S^2 + \ldots
\]
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 \( \lambda \in W(\mathbb{F}_q) \) satisfying \( \lambda^n = \lambda \). Since the leading term of \([\lambda]\) is \( \lambda \) by construction, the leading term of \( \psi - \lambda \), which in terms of power series is given by

\[
\Gamma_n(\psi(x), [-\lambda](x)) = \lambda x + \text{higher order terms} + (-\lambda)x + \text{higher order terms},
\]

vanishes. It follows from Lemma 12.10 and Remark 12.12 that in the endomorphism ring we have

\[ \phi = \lambda + \psi S \]

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

\[
W(\mathbb{F}_q)(S) \to (S^n = p, Sw = w^a S) \to \text{End}(\Gamma_n/\mathbb{F}_q)
\]

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 \( a_i \in W(\mathbb{F}_q) \) and \( a_i^q = a_i \). We can divide this sum according to the value of \( i \) modulo \( n \), which yields

\[ \phi = \left( \sum_{i \equiv 0} a_i S^i \right) + \ldots + \left( \sum_{i \equiv n-1} a_i S^i \right) = \sum_{0 \leq k \leq n-1} \left( \sum_{i \equiv k} a_i p^{\frac{i-k}{n}} S^i \right), \]

where we use that \( S^n = p \). This means that

\[ \phi = \sum_{0 \leq k \leq n-1} w_k S^k \]

for \( w_k \in W(\mathbb{F}_q) \) defined by

\[ w_k = \sum_{i \equiv k} a_i p^{\frac{i-k}{n}}. \]

Any 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 \( W(\mathbb{F}_q) \) on the basis of \( \{ 1, S, \ldots , S^{n-1} \} \). 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 \( a \in W(\mathbb{F}_q) \) is a Teichmüller representative, then we verified in Lemma 12.8 that the element of \( \text{End}(\Gamma_n/\mathbb{F}_q) \) corresponding to it under Theorem 12.5 is given by

\[ [a](x) = bx, \]

where \( b \equiv \overline{a} \) 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

\[ \phi(x) = b_0 x + \Gamma_n b_1 x^p + \Gamma_n b_2 x^{p^2} + \ldots \]

for a sequence \( b_i \in \mathbb{F}_q \). 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 a 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 \( W(\mathbb{F}_q) \) 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

\[ \mathbb{Z}_p \cong W(\mathbb{F}_p) \subseteq W(\mathbb{F}_q). \]
As it is free of rank $n$ over $W(F_q)$ (which itself are of rank $n$ over $\mathbb{Z}_p$, as $\dim_{\mathbb{F}_p}(F_q) = n$), it is free of rank $n^2$ over $\mathbb{Z}_p$.

It follows that
\[\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \text{End}(\Gamma_n/F_q),\]
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)\(^7\) Morava stabilizer group at prime $p$ and height $n$ is the given by
\[
\mathcal{G}_n := \text{Aut}(\Gamma_n/F_q),
\]
the group of automorphisms of the Honda formal group law.

Concretely, $\mathcal{G}_n$ is the group of units of the endomorphism algebra
\[
W(F_q)/S^n = p, \quad S^w = w^n S \simeq \text{End}(\Gamma_n/F_q)
\]
and it follows from Proposition 12.13 that it any of its elements can be uniquely written as a power series
\[
a_0 + a_1 S + a_2 S^2 + \ldots
\]
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 $\mathcal{G}_n$ is virtually a pro-$p$ group of finite rank. To see this, note that $\text{End}(\Gamma_n/F_q)$ 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
\[
\mathcal{G}_n \rightarrow \text{GL}_{n^2}(\mathbb{Z}_p)
\]
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 $\mathcal{G}_n$ 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 $\mathcal{G}_n$ in stable homotopy theory, we will 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 $\dim(\mathcal{G}_n) = n^2$, where dimension is that of Definition 7.7.

The endomorphism ring has a canonical topology induced by the identification
\[
\text{End}(\Gamma_n/F_q) = \lim_{\leftarrow \text{End}(\Gamma_n/F_q)/S^k \text{End}(\Gamma_n/F_q)}.
\]
(note that $S^k \text{End}(\Gamma_n/F_q)$ 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 $F_q[x]$, as well as with the $p$-adic topology, since $S^n = p$. This suggests a canonical filtration on the Morava stabilizer group.

---

\(^7\)The extended Morava stabilizer group is the semi-direct product $\mathcal{G}_n \rtimes \text{Gal}(F_q/F_p)$. 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 $\mathcal{G}_n$ to denote the extended group.
Definition 12.19. The canonical filtration on $G_n$ is given by the open subgroups

$$F_k G_n := G_n \cap \ker \left( \text{End}(\Gamma_n/F_q) \to \text{End}(\Gamma_n/F_q) / S^k \text{End}(\Gamma_n/F_q) \right),$$

so that $F_0 G_n = G_n$ and

$$F_k G_n := \{ 1 + a_k S^k + a_{k+1} S^{k+1} + \ldots \}.$$

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 $(a_0 + a_1 S + \ldots) \mapsto \bar{a_0} \in F_q^*$

   induces an isomorphism $G_n/F_1 G_n \cong F_q^*$

2. for each $k \geq 1$, the map $(1 + a_k S^k + \ldots) \mapsto \bar{a_k} \in F_q$

   induces an isomorphism $F_k G_n/F_{k+1} G_n \cong F_q$.

Corollary 12.21. The groups $F_k G_n$ for $k \geq 1$ are pro-$p$.

To prove that $G_n$ 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 $x \mapsto x^p$ restricts to a function

$$F_k G_n \to F_{k+n} G_n$$

and induces a bijection

$$F_k G_n/F_{k+1} G_n \cong F_{k+n} G_n/F_{k+n+1} G_n.$$

Proof. Let $x = 1 + a_k S^k + a_{k+1} S^{k+1} + \ldots \in F_k G_n$. Collecting the terms, we can write

$$x = 1 + \omega S^k,$$

where $\omega = a_k + a_{k+1} S + \ldots$. Using the binomial formula, we obtain

$$x^p = 1 + p \omega S^k + \sum_{2 \leq i \leq p} \binom{p}{i} (\omega S^k)^i = x^p = 1 + \omega S^k + \sum_{2 \leq i \leq p} \binom{p}{i} (\omega S^k)^i.$$

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 $F_q$ of Lemma 12.20, $x \mapsto x^p$ corresponds to the identity, hence is a bijection as needed.

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 $G_n$ interact with the canonical filtration for general $k$, without simplifying assumption that $k > n$. The formulas get only slightly more involved, see [Hen98, §3].

Corollary 12.24. If $k > n$, then

$$(F_k G_n)^p = F_{k+n} G_n,$$

where the left hand side is the closure of the subgroup generated by the $p$-th powers. In particular, $F_k G_n$ (and hence $G_n$ 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

\[(F_k G_n)^p F_{k+n+m} G_n = F_{k+n} G_n\]

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

\[(F_{k+m} G_n)^p F_{k+n+m} G_n = F_{k+n+m-1} G_n.\]

and thus

\[(F_k G_n)^p F_{k+n+m} G_n = (F_k G_n)^p (F_{k+n} G_n)^p F_{k+n+m} G_n = (F_k G_n)^p F_{k+n+m-1} G_n = F_{k+n} G_n,\]

where the last equality is the inductive assumption. This ends the argument.

To see that \(F_k G_n\) 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

\[F_{k+n} G_n = (F_k G_n)^p \leq \Phi(F_k G_n),\]

the result follows since \(F_{k+n} G_n \triangleright F_k G_n\) is of finite index. We deduce that the Morava stabilizer group is itself finitely generated, as \(F_k G_n \triangleright G_n\) 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 \(F_k G_n\) is a uniformly powerful \(p\)-group of dimension \(n^2\).

**Proof.** To check that \(F_k G_n\) is powerful, we have to verify that

\[F_k G_n/(F_k G_n)^p \cong F_k G_n/F_{k+n} G_n\]

(or \(F_k G_n/F_{k+2n} G_n\) when \(p = 2\)) is abelian, where the identification is Corollary 12.24.

Let \(x, y \in F_k G_n\), which we can write as \(x = 1 + w S^k\) and \(y = 1 + v S^k\), where \(w, v\) are endomorphisms. We have to check that the images of \(x, y\) commute with each other in the quotient ring

\[\operatorname{End}(\Gamma_n/F_q) / S^{k+n} \operatorname{End}(\Gamma_n/F_q),\]

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] = [v S^k, w S^k] = v S^k w S^k - w S^k v S^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 \(F_k G_n\) is powerful, as needed.

As \(F_k G_n\) 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

\[F_k G_n/F_{k+n} G_n \cong |F_q|^{n^2} = p^{n^2}\]

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 \(\|\cdot\| : A \to \mathbb{R}_{\geq 0}\) 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 $a \neq 0$.

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 $q = p^{v(q)}a$, 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

$$\ldots \subseteq R_2 \subseteq R_1 \subseteq R_0 = R$$

by submodules with the property that

$$R_i R_j \subseteq R_{i+j}.$$

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

$$\|0\| := 0,$$

$$\|x\| := c^{-n} \text{ if } x \in R_n \setminus R_{n+1}.$$ 

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
\[
\hat{R} \simeq \lim_{\rightarrow} R/R_n.
\]

**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
\[
\|\sum_{t \in T'} a_t - s\| < \epsilon.
\]

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 \(t_1, t_2, \ldots\) of elements of \(T\). Then
\[
\sum_{t \in T} a_t = s \text{ if and only if } \lim_{n \to \infty} \sum_{1 \leq k \leq n} a_{t_k} = s.
\]

**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 \(T' \subseteq \{t_1, \ldots, t_N\}\). Then for all \(n \geq N\) we have
\[
\|\sum_{1 \leq k \leq n} a_{t_k} - s\| \leq \epsilon.
\]

It follows that the left hand side converges to zero as \(n \to \infty\), so that \((\sum_{1 \leq k \leq n} a_{t_k} - s) \to 0\) as needed.

We move to the backward implication. Let \(\epsilon > 0\), and choose \(N \geq 0\) such that
\[
\|\sum_{1 \leq k \leq n} a_{t_k} - s\| \leq \epsilon.
\]
for all \(n \geq N\). This implies that if \(m > n\), then
\[
\|a_{t_m}\| = \|\left(\sum_{1 \leq k \leq m} a_{t_k} - s\right) - (\sum_{1 \leq k \leq m-1} a_{t_k} - s)\| \leq \max(\epsilon, \epsilon) \leq \epsilon.
\]
Take $T' = \{1, \ldots, N\}$ and suppose that $T'' \supseteq T'$. Then
\[
\sum_{t \in T''} a_t - s = (\sum_{1 \leq k \leq N} a_t - s) + (\sum_{t \in T'' \setminus T'} a_t) \leq \max(\epsilon, \epsilon), \leq \epsilon,
\]
where we use that the norm of the second sum is bounded by the norms of the summands, ending the argument.

**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 $\|a_{t_n}\| \to 0$.

**Proof.** If $\|a_{t_n}\| \to 0$, then since
\[
\| \sum_{n \leq k \leq m} a_t \| \leq \max(\{\|a_t\| \mid n \leq k \leq m\}),
\]
the sequence $\sum_{1 \leq k \leq n} a_t$ is Cauchy. Since $A$ is assumed to be complete, it converges. □

**Proposition 13.16.** Let $T$ be a countable set and $(a_t)_{t \in T}$ a collection of elements of $A$. Then
\begin{enumerate}
\item if $\sum_{t \in T} a_t = s$ then
\[
\|s\| \leq \sup_{t \in T} \|a_t\|,
\]
\item 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
\[
\|s\| = \|a_t\|.
\]
\end{enumerate}

**Proof.** We start with the first part. By Lemma 13.14, after choosing an ordering, we have
\[
s = \lim_{n \to \infty} \sum_{1 \leq i \leq n} a_{t_i},
\]
so that
\[
\|s\| = \lim_{n \to \infty} \| \sum_{1 \leq i \leq n} a_{t_i} \| \leq \max_{1 \leq i \leq n} \|a_{t_i}\| \leq \sup_{t \in T} \|a_t\|.
\]
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. □

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. □

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 $x \rightarrow \lambda \in \mathbb{Q}_p$ 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 \(\lambda_0 \in V\), \(\lambda \neq 0\) and write \(r_0 = \|\lambda_0\|\). Since \(\sum a_i \lambda_i^1\) is convergent, we deduce that
\[
\lim \|a_i \lambda_i^1\| = \lim \|a_i\| r_0^1 = 0.
\]
In particular, these terms are bounded, so we can choose a real constant \(C\) such that \(\|a_i\| r_0^1 < C\) 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
\[
\|a_n\| r_1^{n-1} \cdot \frac{r_0^{m} \|a_m\|}{C} = (\|a_n\| r_0^n) \cdot \left(\frac{r_1}{r_0}\right)^{n-1} \cdot \frac{r_0^{m} \|a_m\|}{C} \leq (\frac{r_1}{r_0})^{n-1} (\frac{r_0^{m} \|a_m\|}{C}),
\]
and
\[
(\|a_n\| r_0^n) \frac{r_1^{n-m-1} r_0^{m} \|a_m\|}{C} \leq \frac{r_1^{n-m-1} r_0^{m} \|a_m\|}{C}.
\]
It follows that
\[
\|a_n \lambda_1^n\| < \|a_m \lambda_1^m\|
\]
for all \(n \neq 0\). As the left hand side converges to zero as \(n \to \infty\), 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
\[
\|a_{\lambda_1^n} \| = \|a_{m \lambda_1^m}\| \neq 0,
\]
which is what we wanted to show. \(\square\)

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 \(X_1, \ldots, X_m\) denote a set of variables. The monoid of *words* in \(X\) is given by the free monoid
\[
W := W(X_1, \ldots, X_m)
\]
on \(\{X_1, \ldots, X_m\}\). The *degree* function on words is defined as the unique monoid homomorphism
\[
\deg : W \to (\mathbb{Z}_{\geq 0},+)
\]
with the property that \(\deg(X_i) = 1\) 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
\[
\deg(X_{i_1} X_{i_2} \ldots X_{i_k}) = k.
\]
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 $X_1, \ldots, X_m$ is the free ring
\[
\mathbb{Q}_p \langle X_1, \ldots, X_m \rangle := \mathbb{Q}_p \langle W \rangle
\]
on the monoid of words. The ring of *non-commutative power series* in variables $X_1, \ldots, X_m$ is the completion
\[
\mathbb{Q}_p \langle X_1, \ldots, X_m \rangle := \lim_{\leftarrow/\left( I \right)} \mathbb{Q}_p \langle W \rangle/(I)^n
\]
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 $F(X) \in \mathbb{Q}_p \langle X_1, \ldots, X_m \rangle$ be a formal power series in non-commuting variables. Given $x = (x_1, \ldots, x_m) \in A^m$, we say that $F$ can be evaluated at $x$ if
\[
F(x) = \sum_{w \in W} a_w w(x)
\]
extists, where $w(-) : W \to (A, \cdot)$ is the unique homomorphism of monoids satisfying $X_i \mapsto x_i$.

In the context of Definition 13.22, let $\text{Ev}_x \subseteq \mathbb{Q}_p \langle X \rangle$ 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 $\text{Ev}_x : A$.

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
\[
V_r = \{(x_1, \ldots, x_m) \in A^m \mid \|x_i\| \leq r \text{ for all } 1 \leq i \leq m\}
\]
We say that a function $f : V_r \to A$ 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 $\deg(w) \to \infty$,
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 $f : V_r + x_0 \to A$ is strictly analytic if its translate $f(- + x_0) : V_r \to A$ 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 $x \in V$, since
\begin{equation}
\|a_w w(x)\| \leq \|a_w\| r^{d(w)}.
\end{equation}
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 $f : V \to A$ 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 $f : V \to A$ be strictly analytic. Then $f$ is continuous.

Proof. Let $\epsilon > 0$ be a real constant. Choose $N$ such that $\|a_w\| r^{d(w)} \leq \epsilon$ if $d(w) \geq N$. For any $x \in V$, we can write
\[F(x) = F_1(x) + F_2(x)\]
where
\[F_1(x) = \sum_{d(w) < N} a_w w(x)\]
and similarly
\[F_2(x) = \sum_{d(w) \geq N} w(x)\]
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. \qed

We will define two classical functions, the exponential and logarithm, which will be useful in relating pro-$p$-groups of finite rank to Lie algebras.

Definition 13.27. The exponential is the power-series in one variable
\[E(X) := \sum_{n \geq 0} \frac{1}{n!} X^n.\]
The logarithm is given by
\[L(X) := \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} X^n.\]

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
\[\|n!\|_p \leq p^{\frac{v(n!)}{p - 1}}.\]
Proof. We have to count how many times $n!$ is divisible by $p$. Choose $k \geq 0$ such that $p^k \leq n < p^{k+1}$. 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

$$\frac{n}{p} + \frac{n}{p^2} + \ldots + \frac{n}{p^k} = \frac{n(1-p^{-k})}{(1-p)} \leq \frac{n-1}{p-1}$$

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

$$\exp : A_0 \to 1 + A_0$$

$$x \mapsto \sum_{n \geq 0} \frac{x^n}{n!}$$

and

$$\log : A_0 + 1 \to A_0$$

$$(x + 1) \mapsto \sum_{n \geq 1} \frac{(-1)^{n+1} x^n}{n}$$

Proof. We only do the odd prime case; the even prime is analogous. For the exponential we have

$$\exp(x) = 1 + \sum_{n \geq 0} \frac{x^n}{n!}$$

and the claim is that

1. $\| \frac{1}{n!} p^n \| \leq p^{-1}$ for all $n \geq 1$,
2. $\| \frac{1}{n!} p^n \| \to 0$ as $n \to \infty$.

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 $\| \frac{1}{n!} \| \leq \| \frac{1}{n!} \|$. \qed

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. $\log(\exp(x) - 1) = x$,
\[\exp(\log(1 + x)) = 1 + x,\]
\[\exp(nx) = \exp(x)^n,\]
\[\log((1 + x)^n) = n \log(1 + x).\]

**Warning 13.32.** Beware that the series defining the logarithm and exponential might sometimes converge for \(x \notin A_0\), but this case, Proposition 13.31 need not hold.

As an explicit example, consider
\[\log(-1) = \log(1 - 2) = \sum_{n \geq 1} \frac{(-2)^n(-1)^{n+1}}{n}.\]

In the field of 2-adic numbers, this is a convergent series. In formal power series, we have
\[((1 + X)^2 - 1) = (2X + X^2) = 2 \cdot (X)\]
(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 \((p\text{-adic})\) completed group algebra is the limit
\[\mathbb{Z}_p[[G]] := \lim_{N \nearrow G} \mathbb{Z}_p[G/N]\]
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,
\[\mathbb{Z}_p[G/N] = \lim_{\varphi} \mathbb{Z}/p^n[G/N].\]

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 3.18 that we have a canonical basis of open neighbourhoods of the identity given by the lower \(p\)-series we will denote by
\[G_k = P_k(G).\]
As a consequence, $Z_p[G]$ can be written as a sequential limit. To see this, notice that since $G_k$ are open, we have canonical projection maps

$$Z_p[G] \to Z_p[G/G_k] \to \mathbb{Z}/p^k[G/G_k]$$

**Lemma 14.2.** Let $G$ be a finitely generated pro-$p$ group. Then

$$Z_p[G] = \lim_{\leftarrow k} \mathbb{Z}/p^k[G/G_k]$$

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 $x \in Z_p[G]$ be non-zero, so that it has a non-zero image along

$$Z_p[G] \to Z_p[G/N]$$

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 $G_k \leq N$. Then we have a factorization

$$Z_p[G] \to \mathbb{Z}/p^c[G/G_c] \to \mathbb{Z}/p^a[G/N]$$

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. \hfill \Box

We would like to apply the theory of complete normed algebra developed in previous lectures to $Z_p[G]$. To do so, we will equip the group algebra $Z_p[G]$ with a norm such that $Z_p[G]$ 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 $Z_p$ 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

$$Z_p[G] \simeq \lim_{\leftarrow k} Z_p[G]/I_k,$$

where

$$I_k := (G_k - 1) + p^kZ_p[G]$$

and

$$(G_k - 1) := \ker(Z_p[G] \to Z_p[G/G_k]).$$

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

$$J = I_1 = (G - 1) + pZ_p[G] \subseteq Z_p[G].$$

It coincides with the kernel of the composite

$$Z_p[G] \to Z_p \to F_p$$

and is often called the augmentation ideal.

**Proposition 14.4.** For each $k \geq 1$, we have

1. $J^k \supseteq I_k$,
2. $I_k \supseteq J^{k[G/G_k]}$.

In particular, taking either $J^k$ or $I_k$ as a basis of open neighbourhoods of $Z_p[G]$ 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 $(G_k - 1) \subseteq J^k$. This is the equivalent to showing that the $G$-action on $Z_p[G]/J^k$ 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) $x^{-1}y^{-1}xy^8$ 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 $u^p \in J^{(k-1)p} \subseteq J^k$ 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 $J^{k[G/G_k]} \subseteq I_k$. Since $G/G_k$ is a finite $p$-group, there exists a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_p[G/G_k]$ such that the action factors through the upper unitriangular subgroup

$$U_{[G/G_k]}(\mathbb{F}_p) \subseteq GL_{[G/G_k]}(\mathbb{F}_p)$$

(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

$$J^{k[G/G_k]} \subseteq ((G_k - 1) + p\mathbb{Z}_p[G])^k \subseteq (G_k - 1) + p^k\mathbb{Z}_p[G] = I_k.$$

\[\square\]

**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 $x = \sum \lambda_i g_i$ 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

$$\mathbb{Z}_p[G]/((G_k' - 1) + p^{k'}\mathbb{Z}_p[G]) \cong \mathbb{Z}/p^{k'}[G/G_k'].$$

It follows from Proposition 14.4 that $x$ is not contained in $J^{k[G/G_k]}$, ending the argument. \[\square\]

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

$$\|0\| = 0,$$

$$\|x\| = p^n \text{ if } x \in J^n \setminus J^{n+1},$$

**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 \( G \to \mathbb{Z}_p[G] \) is a homeomorphism onto its image.

Proof. For the first part, observe that we have an identification
\[
\hat{\mathbb{Z}}_p[G] \cong \varprojlim \mathbb{Z}_p[G]/J^k \cong \varprojlim \mathbb{Z}_p[G]/I_k \cong \mathbb{Z}_p[J_G],
\]
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 \( \mathbb{Z}_p[J_G] \) with a completion with respect to a norm, it equips the completed group algebra with its own norm which we will 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 \( J \mathbb{Z}_p[J_G] = \ker(\mathbb{Z}_p[G] \to \mathbb{F}_p) \).

We will 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 will require a little bit of notation, which we introduce first.

Notation 14.9. For the rest of the lecture, \( G \) will be a powerful, finitely generated pro-\( p \)-group. We fix a choice \( g_1, \ldots, g_m \) 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 \( (\alpha) = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m \) is a multi-index, its degree is given by \( \deg(\alpha) = \alpha_1 + \ldots + \alpha_m \).

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
\[ x = \sum_{(\alpha) \in \mathbb{N}^m} \lambda_\alpha b^{(\alpha)} \]
where \( \lambda_\alpha \in \mathbb{Z}_p \) 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

\[ g^{(\beta)} = \sum_{\alpha} \binom{\beta}{\alpha} g^{(\alpha)}, \]

where the sum is taken over all multi-indices \((\alpha)\) and similarly

\[ b^{(\beta)} = \sum_{\alpha} (-1)^{\deg(\beta) - \deg(\alpha)} \binom{\beta}{\alpha} b^{(\alpha)} \]

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

\[ b^{(\beta)} = (g_1 - 1)^{\alpha_1} \cdots (g_m - 1)^{\alpha_m}. \]

\[ \square \]

Notation 14.12. If \(k \geq 1\), we write

\[ T_k = \{(\alpha) \in \mathbb{N}^m \mid \alpha_i < p^{k-1} \text{ for all } i\} \]

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. \[ \square \]

Proof of Theorem 14.10. Consider the map of topological abelian groups

\[ \prod_{\alpha \in \mathbb{N}^m} \mathbb{Z}_p \cong \text{map}(\mathbb{N}^m, \mathbb{Z}_p) \to \mathbb{Z}_p[G] \]

given by

\[ (\lambda_\alpha) \mapsto \sum_{\alpha} \lambda_\alpha b^{(\alpha)}. \]

Since \(\|b^{(\alpha)}\| \to 0\) when \(\deg(\alpha) \to \infty\), 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 \(\mathbb{Z}_p[G] = \lim \mathbb{Z}_p[G/G_k]\) as topological rings. We deduce that the image is the whole completed group algebra, as needed.

Now suppose that \(G\) is uniform; we will show that expressions in monomials are unique. Suppose by contradiction that we have

\[ \sum_{\alpha} \lambda_\alpha b^{(\alpha)} = 0 \]

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 $S \subseteq \mathbb{N}^m$ such that $T_k \subseteq S$ and
\[
\| \sum_{\alpha \in S} \lambda_\alpha b^{(\alpha)} \| \leq p^{-|G/G_k|},
\]
so that
\[
\sum_{\alpha \in S} \lambda_\alpha b^{(\alpha)} \in j^{[G/G_k]}.
\]
We then have
\[
(14.2) \quad \sum_{T_k} \lambda_\alpha b^{(\alpha)} = \sum_{S} \lambda_\alpha b^{(\alpha)} - \sum_{S \smallsetminus T_k} \lambda_\alpha b^{(\alpha)}.
\]
Since any element of $(G-1)^{[G/G_k]}$ acts trivially on $F_p[G/G_k]$ as we observed in the proof of Proposition 14.4, we have $j^{[G/G_k]} \subseteq (G_k - 1) + p\mathbb{Z}_p[G]$ and $J \cap (G_k - 1) + p\mathbb{Z}_p[G] = (G_k - 1) + p\mathbb{Z}_p[G]$.

Since $b^{(\alpha)}$ for $\alpha \in T_k$ form a $F_p$-basis of $F_p[G/G_k]$ by Lemma 14.13, this implies that $\lambda_\alpha \equiv 0 \mod p$ for $\alpha \in T_k$. As $k$ was arbitrary, we deduce that $\lambda_\alpha \equiv 0 \mod p$ for all $\alpha$, which contradicts our assumption. □

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 $\mathbb{Z}_p[J]_{G_k}$ 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 15.8.

The following is the main result of today’s lecture:

**Theorem 15.1.** Let $G$ be a uniform group with minimal set of generators $g_1, \ldots, g_m$. Then for any element
\[
\sum \lambda_\alpha b^{(\alpha)} \in \mathbb{Z}_p[G]
\]
we have
\[
\| \sum \lambda_\alpha b^{(\alpha)} \| = \sup\{ \| p^{-\deg(\alpha)} \lambda_\alpha \| \} = \sup\{ \| p^{-\deg(\alpha)} \| \lambda_\alpha \| \},
\]
where the right hand side is the standard norm of Definition 14.6 and the sum and suprema are taken over $\alpha \in \mathbb{N}^m$.

The proof of Theorem 15.1 will require some preliminaries. Throughout this lecture, $G$ will be a powerful group and we write
\[
J = \ker(\mathbb{Z}_p[G] \to \mathbb{F}_p) = (G - 1) + p\mathbb{Z}_p[G] \]
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

$$\|0\| := 0,$$

$$\|x\| := p^{-n} \text{ if } x \in J^n \setminus J^{n+1},$$

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

$$J_{k+1,1} := p J^k + J^{k+2} \subseteq J^{k+1}.$$ 

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

$$[x, g] := xg - gx = x(g - 1) - (g - 1)x$$

and since $g - 1 \in J$, the bracket defines a linear map

$$[-, g] : J^k / J^{k+1} \rightarrow J^k / J^{k+2}.$$ 

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 $b_1$ and $p$ (which is central), we can assume that $x = b_1$. We have

$$[b_1, g] = [g_1, g] = g g_1 g^{-1} g - 1 = g g_1 (z^p - 1)$$

where we use that since $G$ is powerful we can write $g_1 g^{-1} g$ for some $z \in G$. Since $(z - 1)^p \equiv z^p - 1 \mod p$ 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 $g_1 g^{-1} g \in G_3$ and hence $g_1 g^{-1} g - 1 \in J_3$ by Proposition 14.4.

For $k > 1$, we argue by induction. Any element of $J^k$ can be written as a linear combination $x = uwv + u \in J^k$ and $w \in J$. Then

$$[w, g] = uv g - gw v = uv g - u g v + u v g - g uv = u[v, g] + [u, g]v$$

and the result follows from the inductive assumption applied to $[v, g]$ and $[u, g]$. \qed

**Lemma 15.3.** Let $G$ be powerful with a set of generators $g_i$ and associated elements $b_i = g_i - 1$. Then

$$J^k = \sum_{\alpha} p^{k - \deg(\alpha)} Z_p [b(\alpha)] + J^{k+1},$$

where the sum is taken over $\alpha \in \mathbb{N}^m$ 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

$$J^{k+1} + W_k \subseteq J^k.$$ 

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

$$Z_p [G] = \sum_{\alpha \in T_2} b(\alpha) + \text{ker} (Z_p [G] \rightarrow Z_p [G / G_2]),$$

where $T_2 = \{\alpha \in \mathbb{N}^m \mid \alpha_i < p\}$. Since

$$\text{ker} (Z_p [G] \rightarrow Z_p [G / G_2]) \subseteq J^2$$
For the right summand, observe that by Lemma 15.2 we have
\[ Z_p[G] = Z_p \cdot 1 + \sum_{\deg(\alpha) = 1} Z_p b^{(\alpha)} + J^2. \]
Since the latter two summands are contained in \( J \), intersecting this equality with \( J \) we obtain
\[ J = (J \cap Z_p \cdot 1) + \sum_{\deg(\alpha) = 1} Z_p b^{(\alpha)} + J^2 = W_1 + J^2, \]
since \( J \cap Z_p \cdot 1 = Z_p \cdot p \), 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 \( p, b \) and \( pW_{k-1} \subseteq W_k \), we only have to verify the inequality
\[ \| p^{k-\deg(\alpha)} b^{(\alpha)} b_i \|_{W_k + J^{k+1}} \]
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
\[ p^{k-\deg(\alpha)} b^{(\alpha)} b_m = p^{k-\deg(\alpha')} b^{(\alpha')} \in W_k. \]
As usual, the difficulty lies in the group algebra not being commutative.

Let \( f = (\alpha_1, \ldots, \alpha_i, 0, \ldots) \) and \( b = (\ldots, 0, \alpha_{i+1}, \ldots, \alpha_m) \) be the division of \( \alpha \) into the “front” and “back” parts, so that \( b^{(\alpha)} = b^{(f)} b^{(b)} \). Then
\[ p^{k-\deg(\alpha)} b^{(\alpha)} b_i = p^{k-\deg(\alpha)} b^{(f)} b^{(b)} b_i = p^{k-\deg(\alpha)} b^{(f)} b^{(b)} + p^{k-\deg(\alpha)} b^{(f)} [b^{(b)}, b_i]. \]
The left summand is \( p^{k-\deg(\alpha)} \) 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
\[ [b^{(b)}, b_i] \in p^{\deg(b)} + J^{\deg(b)+2} \]
and thus
\[ p^{k-\deg(\alpha)} b^{(f)} [b^{(b)}, b_i] \in p^{k-\deg(\alpha)} J^{\deg(\alpha)} + J^{k+1}. \]
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.

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
\[ \| x \| = \sup_{\alpha} (p^{-\deg(\alpha)} \| \lambda_{\alpha} \|_p) \]
Since \( p, b_i \in J \), we have \( \| \lambda_{\alpha} b^{(\alpha)} \| \leq p^{-v(\lambda_{\alpha})-\deg(\alpha)} \), where \( v(\cdot) \) 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
\[ x = \sum_{\deg(\alpha) \leq c} p^{-c-\deg(\alpha)} u_{\alpha,c} b^{(\alpha)} + x' \]
with \( x' \in J^{c+1} \). Expanding \( x' \) similarly and continuing inductively, we obtain that
\[ x = \sum_{k \geq c} \left( \sum_{\deg(\alpha) \leq k} p^{k-\deg(\alpha)} u_{\alpha,c} b^{(\alpha)} \right). \]
which we can rewrite as
\[ x = \sum_{\alpha} \left( \sum_{k \geq c} p^{k - \deg(\alpha)} u_{\alpha,k} \right) p(\alpha). \]

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 \( p^{c - \deg(\alpha)} \| \lambda_{\alpha} \|_p < p^{-c} \) for each \( \alpha \); equivalently, that \( \| \lambda_{\alpha} \|_p < p^{d(\alpha) - c} \).

Since \( \| p^{k - \deg(\alpha)} u_{\alpha,k} \| < p^{-c} \) for \( k > c \), by (15.4) this can only happen if also
\[ \| p^{c - \deg(\alpha)} u_{\alpha,c} \| < p^{d(\alpha) - c}, \]
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 \( \| x \| = p^{-c} \).

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
\[ i : \mathbb{Z}_p[G] \to \mathbb{Q}_p[G]. \]

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
\[
J^k = \{ x \in \mathbb{Z}_p[G] \mid \|x\| \leq p^{-k} \} = \{ \sum_{\alpha \in \mathbb{N} \times m} \lambda_\alpha b(\alpha) \mid \|\lambda_\alpha\| \leq p^{\deg(\alpha)-k} \}
\]
From the second expression, we see that elements of the form
\[
p \cdot \deg(\alpha) \cdot b(\alpha)
\]
with \( \deg(\alpha) \leq k \) form a basis of the \( \mathbb{F}_p \)-vector space \( J^k/J^{k+1} \). Rephrasing things a little bit, the basis of \( J/J^2 \) is given by
\[
(15.5) \quad p, b_1, \ldots, b_m
\]
and the basis of \( J^k/J^{k+1} \) is given by monomials in these elements of length \( k \). In particular, the dimensions of these vector spaces are given by the same formula as in the case of a polynomial ring:

**Corollary 15.6.** Let \( G \) be a uniform group of dimension \( m \). Then
\[
\dim_{\mathbb{F}_p}(J^k/J^{k+1}) = \binom{m+k}{k} = \dim_{\mathbb{F}_p}(\{ p \in \mathbb{F}_p[x_0, \ldots, x_m] \mid p \text{ homogenous of degree } k \})
\]
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 \( \mathbb{F}_p \)-algebra which by Corollary 15.6 is in degree \( k \) of the same dimension as the graded polynomial ring \( \mathbb{F}_p[x_0, \ldots, x_m] \), 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
\[
\bar{p}, \bar{b}_1, \ldots, \bar{b}_m \in J/J^2
\]
of elements of (15.5). If these elements commute with each other, then we have an induced homomorphism of graded rings
\[
\mathbb{F}_p[x_0, \ldots, x_m] \to \text{gr}_J(\mathbb{Z}_p[G])
\]
defined by
\[
x_0 \mapsto \bar{p}
\]
and
\[
x_i \mapsto \bar{b}_i
\]
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 15.6. 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
\[
(15.6) \quad [\bar{b}_i, \bar{b}_j] \in \bar{p} \cdot \text{gr}(\mathbb{Z}_p[G])_1.
\]
This essentially shows the following:
Theorem 15.7. Let $G$ be a uniform group and consider the $\overline{p}$ adic filtration
\[ \cdots \subseteq \overline{p}^2 \cdot \text{gr}_J(\mathbb{Z}_p[G]) \subseteq \overline{p} \cdot \text{gr}_J(\mathbb{Z}_p[G]) \subseteq \text{gr}_J(\mathbb{Z}_p[G]) \]
on the associated graded of the $J$-adic filtration on the completed group algebra, where $\overline{p} \in J/J^2$ is the image of $p$. Then the associated graded of the $\overline{p}$-adic filtration is isomorphic as a bigraded ring to
\[ F_p[x_0, x_1, \ldots, x_m] \]
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 $\overline{p}$-adic.

Proof. The ring homomorphism is specified by
\[ x_0 \mapsto \overline{p}, \]
which is in $\overline{p}$-adic filtration one, and
\[ x_i \mapsto \overline{b}_i, \]
which is in $\overline{p}$-adic filtration zero. By (15.6) the bracket between $\overline{b}_i$ is zero in the associated graded of the $\overline{p}$-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 $\overline{p}$ and $\overline{b}_i$ we see that this map is surjective and injective by (a slight refinement of) the dimension count of Corollary 15.6. 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 15.8. 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
\[ \text{Ext}^s_{\mathbb{Z}_p[G]}(M,N) \]
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 $F_p[x_0, \ldots, x_m]$ has all three of these properties, and hence so does $\text{gr}_J(\mathbb{Z}_p[G])$ by Theorem 15.7 (note that the $\overline{p}$-adic filtration is complete by degree considerations). We deduce that the completed group algebra also has these three properties. \[ \square \]

Corollary 15.9. 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 $g_1, \ldots, g_k \in G$ 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 15.8, 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

$$E(X) = \sum_{n \geq 0} \frac{1}{n!} X^n$$

and logarithm

$$L(X) = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} X^n$$

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

$$\exp A_0 \leftrightarrow 1 + A_0: \log$$

An elementary calculation shows that in the ring $\mathbb{Q}_p[[X, Y]]$ of power series in two commuting variables, we have an equality

$$L(E(X)E(Y) - 1) = L(X) + L(Y).$$

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 $\mathbb{Q}_p[[X, Y]]$ be the power series ring in two non-commuting variables. The *Baker-Campbell-Hausdorff power series* $\Phi(X, Y) \in \mathbb{Q}_p[[X, Y]]$ is given by

$$\Phi(X, Y) := L(E(X)E(Y) - 1).$$

To get some practice in working with power series in non-commuting variables, let’s calculate the low degree terms. Since

$$E(X) = 1 + X + \frac{X^2}{2} + \text{terms of degree at least three}$$

and similarly for $E(Y)$, we have

$$E(X)E(Y) - 1 = X + Y + XY + \frac{X^2}{2} + \frac{Y^2}{2} + \text{terms of degree at least three}.$$  

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 $(X + Y)^2 = X^2 + Y^2 + 2XY + YX$ 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 \((a_1, a_2) = a_1 a_2 - a_2 a_1\)), then the iterated bracket of length \(n\) is defined inductively as \[(a_1, a_2, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n).\]

**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 \(\mathbb{Q}(X, Y)\) 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
\[
L(X, Y) \to \langle X, Y \rangle
\]
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 \(\mathbb{Q}(X, Y)\) 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 \(\mathbb{Q}[X, Y]\), 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 \( \mathbb{Q}(X, Y) \) 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], \( \mathbb{Q}(X, Y) \) 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 \( \mathbb{Q}(X, Y) \) is exactly \( L(X, Y) \), so that they are all linear combinations of brackets in \( X, Y \). Passing to the completion \( \mathbb{Q}(X, Y) \), 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 \( I \subset \mathbb{Q}(X, Y) \) 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 will 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 \( T: A \to A \) is **bounded** if its **operator norm**

\[ \|T\| := \sup\left( \frac{\|Ta\|}{\|a\|} \mid a \in A, a \neq 0 \right) \]

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 \( A \to B(A) \) are the **left multiplication**, **right multiplication** and the **adjoint representation** denoted by

\[ a \mapsto l_a, \quad a \mapsto r_a, \quad a \mapsto ad_a \]

and defined by

\[ l_a(b) = ab, \quad r_a(b) = ba, \quad ad_a(b) = l_a(b) - r_a(b) = ab - ba = (a, b) \]

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

\[ l_{\exp(a)} = \exp(l_a), \]
\[ r_{\exp(a)} = \exp(r_a) \]

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 $ad : A \to B(A)$ 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

\[ \exp(r_a) \exp(r_b) = \exp(r_{\Phi(a,b)}) \]

(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

\[ \exp(\Phi(ad_a, ad_b)) = \exp(ad_a) \exp(ad_b) = l_{\exp(a)} r_{\exp(b)}^{-1} l_{\exp(b)} r_{\exp(b)}^{-1} = (l_{\exp(a)} l_{\exp(b)}) (r_{\exp(b)} r_{\exp(a)})^{-1}, \]

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

\[ l_{\exp(a)} r_{\exp(b)}^{-1} = \exp(l_{\Phi(a,b)}) \exp(r_{\Phi(a,b)})^{-1} = \exp(ad_{\Phi(a,b)}). \]

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

\[ \sum_{n \geq 1} u_n(ad_a, ad_b) = \sum_{n \geq 1} \lambda^n ad_{u_n(a,b)}. \]

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. \(\square\)
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 $\mathbb{Q}_p(X,Y,t)$ on three variables by the relations

\[
tX = Xt + X \\
tY = Yt + Y.
\]

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 $\mathbb{Q}_p(X,Y)$ as a subalgebra. As a consequence of (16), we have

\[
\text{ad}_t(X) = X
\]

and analogously for $Y$, from which we deduce that if $p(X,Y) \in \mathbb{Q}_p(X,Y)$ is homogeneous of degree $n$, then

\[
\text{ad}_t(p(X,Y)) = n \cdot p(X,Y).
\]

This algebra $A$ is specifically designed to be an enlargement of $\mathbb{Q}_p(X,Y)$ where the degree decomposition becomes an eigenspace decomposition for an operator $\text{ad}_t$ 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

\[
-n \cdot u_n(X,Y) = -\text{ad}_t(u_n(X,Y)) = \text{ad}_{u_n(X,Y)}(t) = u_n(\text{ad}_X, \text{ad}_Y)(t),
\]

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

\[-n \cdot u_n(X,Y) = \sum c_w w(\text{ad}_X, \text{ad}_Y)(t),
\]

where by $w(\text{ad}_X, \text{ad}_Y)$ we mean the element of the algebra of operators obtained by substituting $X \mapsto \text{ad}_X$ and $Y \mapsto \text{ad}_Y$. We claim that

\[w(\text{ad}_X, \text{ad}_Y)(t)
\]

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

\[w = Z_1 \cdots Z_n,
\]

where $Z_i \in \{X,Y\}$. Then

\[w(\text{ad}_X, \text{ad}_Y)(t) = \text{ad}_{Z_1} \cdots \text{ad}_{Z_n}(t) = \text{ad}_{Z_1} \cdots \text{ad}_{Z_{n-1}}(Z_n) = (Z_1, (Z_2, \ldots, (Z_{n-1}Z_n) \ldots)
\]

which since the bracket is anti-symmetric gives

\[w(\text{ad}_X, \text{ad}_Y)(t) = (-1)^n(Z_n, Z_{n-1}, \ldots, Z_1)
\]

which is an iterated bracket in $X,Y$ as claimed. \qed
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 will 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. \( \epsilon(n-1) + v(c_w) \to \infty \) as \( n \to \infty \).

**Proof.** We will 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 \( E(X)E(Y) - 1 \) is given by

\[
\sum_{i,j \geq 1} \frac{1}{i!j!} X^i Y^j.
\]

Applying the logarithm to calculate \( \Phi(X,Y) = \mathcal{L}(E(X)E(Y) - 1) \), we see that the terms of degree \( n \) are all sums of terms of the form

\[
\frac{(-1)^{k+1}}{k} \frac{1}{i_1!j_1! \ldots i_k!j_k!} X^{i_1} Y^{j_1} \ldots X^{i_k} Y^{j_k},
\]

where

1. \( 1 \leq k \leq n \),
2. \( i_l + j_l \geq 1 \) for all \( 1 \leq l \leq k \),
3. \( i_1 + j_1 + \ldots + i_k + j_k = n \).

Using **Lemma 13.29.**, we see that the \( p \)-adic valuation of a coefficient of such a term is given by

\[
v(\frac{(-1)^{k+1}}{k} \frac{1}{i_1!j_1! \ldots i_k!j_k!}) \geq -\frac{k-1}{p-1} - \sum_{1 \leq l \leq k} \left( \frac{i_l-1}{p-1} + \frac{j_l-1}{p-1} \right) \geq -\frac{n-1}{p-1},
\]

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 \( n \to \infty \). \( \square \)
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

$$g +_G h := \lim_{n \to \infty} (g^{p^n} h^{p^n})^{p^{-n}} ,$$

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

$$(g, h)_G := \lim_{n \to \infty} (g^{p^n} h^{p^n} g^{p^n} h^{p^n})^{p^{-2n}}.$$  

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 3.19, 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

$$g^{-1}h^{-1}gh \in G_3$$

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 [DDSM03, Lemma 4.28].

We will 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.

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 will write $G$ for a fixed uniform group. We assume that we are given a completed normed $\mathbb{Q}_p$-algebra and a continuous monomorphism $G \to A^\times$ into the group of units such that

$$G \leq 1 + A_0,$$

where

$$A_0 = \begin{cases} \{x \in A \mid \|x\| \leq \frac{1}{2} \} & p > 2 \\ \{x \in A \mid \|x\| \leq \frac{1}{4} \} & p = 2 \end{cases}.$$  

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 $g \in G$.

In terms of group commutators, we can write $(g, h)_G = \lim_{n \to \infty} [g^{p^n}, h^{p^n}]^{p^{-2n}}$. 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 will use, such as the additive bracket of a uniform group or a Lie bracket of a normed algebra.
Example 17.5. If $p$ is odd, then an example of a algebra satisfying the conditions of Nota-
tion 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 $\frac{1}{2}$, rather than $\frac{1}{4}$. 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 func-
tions $\exp A_0 \leftrightarrow 1 + A_0 \cdot \log$. Since $G \leq 1 + A_0$, the logarithm is well-defined on 
elements of the group. We will 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 $\log G \to A_0$ satisfies the following three identities for any 
g, h \in G, \lambda \in \mathbb{Z}_p$:

1. $\log(g + \lambda h) = \log(g) + \log(h),$
2. $\log(g^\lambda) = \lambda \log(g),$
3. $\log((g, h)\lambda) = (\log(g), \log(h)) = \log(g) \log(h) - \log(h) \log(g).$

Proof. Throughout the proof, we will 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

$A_0 \times A_0 \to A_0.$

Using the defining property $E(\Phi(X, Y)) = E(X) E(Y)$, 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 
$\log(g^n + h^n) = p^n \gamma + p^n \eta + \sum_{k \geq 2} p^{kn} u_k(\gamma, \eta).$

We then have 
$\log((g^n h^n)^\gamma) = \gamma + \eta + p^n \sum_{k \geq 2} p^{(k-1)n} u_k(\gamma, \eta).$

Since the logarithm is continuous, we deduce that 
$\log(g + \lambda h) = \gamma + \eta + \lim_{n \to \infty} p^n (\sum_{k \geq 2} p^{(k-1)n} u_k(\gamma, \eta)) = \gamma + \eta,$
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

$C(X, Y) := L(E(X)^{-1} E(Y)^{-1} E(X) E(Y))$
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
\[ \log((g, h)_G) = \lim_{n \to \infty} \left( \gamma, \eta \right) + p^n \left( \sum_{k \geq 3} p^{(k-3)n} v_k(\gamma, \eta) \right) = \left( \gamma, \eta \right) \]
which is what we wanted to show. \( \square \)

**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. \( \square \)

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
\[ \Phi(X, Y) = X + Y + \sum_{k \geq 2} u_k(X, Y) \]
Proof. Appyling the formal logarithm to the multiplication Lemma 17.13.

We see that the Baker-Campbell-Hausdorff series is associative in the sense that we have an equality when \( p \geq 2 \), 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 \( (L, L) \subseteq p^\infty \cdot L \), 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. \( u_k(l_1, l_2) \in p^k \cdot L \) for all \( k \geq 3 \).
3. \( u_k(l_1, l_2) \to 0 \) as \( k \to \infty \), 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

\[
(17.1) \quad l_1 \ast l_2 := \Phi(l_1, l_2) = l_1 + l_2 + \sum_{k \geq 2} u_k(l_1, l_2)
\]

Remark 17.12. Using properties (1) and (2) of \( u_k(l_1, l_2) \) outlined above, we see that

\[
l_1 \ast l_2 \equiv l_1 + l_2 \mod p
\]

and additionally

\[
l_1 \ast l_2 \equiv l_1 + l_2 + \frac{1}{2}(l_1, l_2) \mod 4
\]

when \( p = 2 \).

Lemma 17.13. The multiplication \( \ast \) 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 \( \ast \) of (17.1) is associative. To see that it makes \( L \) into a group, observe that immediately from the definition we see that

\[
l \ast 0 = 0 \ast l = l
\]

and

\[
l \ast (-l) = 0
\]

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 \( (L, \ast) \) with its \( p \)-adic topology is a uniformly powerful group.

Proof. Since \( (l, l) = 0 \) for any \( l \in L \), we have

\[
l^{\ast p} = p \cdot l.
\]

From bilinearity of the bracket we see that

\[
\{l^{\ast p} \mid l \in L\} = p \cdot L,
\]

the subset of \( \ast \)-\( p \)-th powers, is a \( \ast \)-subgroup. Since \( l_1 \ast l_2 \equiv l_1 + l_2 \mod p \),

\[
(L, \ast)/(p \cdot L, \ast)
\]

is abelian so that \( (L, \ast) \) is powerful when \( p > 2 \). When \( p = 2 \), we instead observe that

\[
l_1 \ast l_2 = l_1 + l_2 + \frac{1}{2}(l_1, l_2) \mod 4,
\]
so that
\[ l_1 \ast l_2 \ast -(l_2 \ast l_1) \equiv l_1 + l_2 + \frac{1}{2}(l_1, l_2) - l_2 - l_1 - \frac{1}{2}(l_2, l_1) \equiv (l_1, l_2) \equiv 0 \mod 4, \]
where we used the anti-symmetry of the bracket and the assumption that \((L, L) \subseteq 4 \cdot L\). We conclude that \((L, \ast)\) is powerful also when \(p = 2\).

Since \(l_1 \ast l_2 \equiv l_1 + l_2 \mod p\), 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 \((L, \ast)\) is finitely generated. To see that \((L, \ast)\) 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
\[ p^k L/p^{k+1} L = L^p / L^{p^k} \]
and the order of the left hand size does not depend on \(k\) by the assumption that \(L\) is free over \(\mathbb{Z}_p\), we deduce that \((L, \ast)\) is uniform. 

**Proof of Theorem 17.10.** By construction, both of the functors \(G \mapsto L(G)\) and \(L \mapsto (L, \ast)\) 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
\[ \exp : (L(G), \ast) \to (G, \cdot) \]
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 \(\mathbb{Q}_p[[X_1, \ldots, X_n]]\) 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 will often use the shorthand \(X\) to denote the variables \(X_1, \ldots, X_n\). In particular, we will write
\[ \mathbb{Q}_p[X] := \mathbb{Q}_p[[X_1, \ldots, X_n]]. \]
If \(I = (i_1, \ldots, i_n) \in \mathbb{N}^{\ast n}\) is a multi-index, we will write
\[ X^I := X_1^{i_1} \cdots X_n^{i_n} \]
so that a general power series can be uniquely expressed as
\[ f(X) = \sum_I a_I X^I = \sum_{(i_1, \ldots, i_n)} a_{(i_1, \ldots, i_n)} X_1^{i_1} \cdots X_n^{i_n} \]
with \(a_I \in \mathbb{Q}_p\). We call the number \(i_1 + \ldots + i_n\) the degree of a multi-index and denote it by \(\deg(I)\).
Recollection 18.2. If \( f(X) \) is a formal power series, we say that it can be evaluated at
\[
X = (x_1, \ldots, x_n) \in \mathbb{Q}_p^n
\]
if the sum
\[
f(x) := \sum_I a_I x^I = \sum_{(i_1, \ldots, i_n)} a_{i_1} x_1^{i_1} \cdots x_n^{i_n}
\]
converges. In this case, we call \( f(x) \) the value at \( x \).

Definition 18.3. Let \( V \subseteq \mathbb{Q}_p^n \) be an open subset. We say a function \( f: V \to \mathbb{Q}_p \)
\begin{enumerate}
\item is analytic at \( v \in V \) if there exists an open neighbourhood \( v' \in U \subseteq V \) and a formal power series \( F_v(X) \in \mathbb{Q}_p[[X]] \) such that for each \( v' \in U \), \( F_v \) can be evaluated at \( v' - v \) and
\[F_v(v' - v) = f(v').\]
\item is locally analytic if it is analytic at \( v \) for all \( v \in V \).
\end{enumerate}
More generally, we say that function \( f: V \to \mathbb{Q}_p^m \) is locally analytic if each of its coordinate functions is analytic.

Remark 18.4. It is clear from the definition that a function \( f: V \to \mathbb{Q}_p \) is analytic at \( v \in V \) if and only if the function \( g(x) := f(v + x) \) 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 \( f: V \to \mathbb{Q}_p \) be analytic at \( v \in V \) and let
\[F(X) = \sum_I a_I X^I\]
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
\[|a_I| p^{-\deg(I) \cdot N} \to 0\]
as \( \deg(I) \to \infty \).

Proof. Choose an \( N \geq 0 \) such that
\[f(v + (p^N, \ldots, p^N)) = F(p^N, \ldots, p^N) = \sum_I a_I p^{\deg(I) \cdot N}.\]
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.

Corollary 18.6. If \( f: V \to \mathbb{Q}_p \) 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.

Lemma 18.7. Let \( f: V \to \mathbb{Q}_p \) be analytic at \( v \) and let \( F, G \in \mathbb{Q}_p[[X]] \) 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 \( H \in \mathbb{Q}_p[[X]] \) is a formal power series such that \( H(x) = 0 \) for \( x \) in some neighbourhood of zero in \( \mathbb{Q}_p^n \), 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.
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 avoid 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

$$b: \mathbb{Z}_p \to \mathbb{Z}_p$$

given by

$$b(x) = \begin{cases} 1 & \parallel x \parallel = 1 \\ 0 & \parallel x \parallel < 1 \end{cases}$$

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 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, $V \subseteq \mathbb{Q}_p^n$ is open, and $\phi: U \to V$ 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

$$\phi_\alpha^{-1}(U_\alpha \cap U_\beta) \xrightarrow{\phi_\beta^{-1}} U_\alpha \cap U_\beta \xrightarrow{\phi_\beta} \phi_\beta(U_\alpha \cap U_\beta)$$

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 $f: M \to N$. 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 $V \subseteq \mathbb{Q}_p^n$ is an open subset, then it can be made into a $p$-adic manifold by declaring the identity $id: V \to V$ 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 $L \cong \mathbb{Z}_p^n \subseteq \mathbb{Q}_p^n$ 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 $m: G \times G \to G$,
2. the inverse map $(-)^{-1}: G \to G$

are both locally analytic.

Using the $p$-adic analogue of the implicit function theorem, see [DDMS03, 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 $GL_n(\mathbb{Q}_p)$ is a $p$-adic analytic Lie group of dimension $n^2$ with respect to the manifold structure inherited as an open subset of $M_n(\mathbb{Q}_p) \cong \mathbb{Q}_p^n$. 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 $U \subseteq G$ is an open subgroup, then $U$ is also $p$-adic analytic (with respect to the open submanifold structure). In particular, $GL_n(\mathbb{Z}_p) \leq GL_n(\mathbb{Q}_p)$ 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 $\cdot \cdot : \mathbb{Z}_p \times L \to L$ 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 $G$, it is enough to verify that the multiplication $\cdot : L \times L \to L$ and the inverse $-id: L \to L$ 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, $-id$ is linear and hence locally analytic. \qed
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 \textit{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
   \[
   (-)g^g : (gHg^{-1}) \cap H \to H
   \]
   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 over of $G$. If $G$ is $p$-adic analytic in a way compatible with the inclusion, then for any $t_\alpha$ the map
   \[
   t_\alpha \cdot : H \to t_\alpha H
   \]
   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
   \[
   t_\alpha H \times t_\beta H \to t_\gamma H
   \]
   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
   \[
   H \times H \to H
   \]
   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. \hfill \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

$$
\phi \colon U \to p^{k} \cdot \mathbb{Z}_{p}^{\times n}
$$

centered at the identity; that is, such that $\phi(e) = 0$. By assumption, the product $m \colon G \times G \to G$ is locally analytic, so that the induced function

$$
(\mathbb{Z}_{p}^{\times n})^{2} \ni (\phi \times \phi)(m^{-1}(U) \cap U \times U) \to \phi(U) = \mathbb{Z}_{p}^{\times n}
$$

can be expanded around zero into a collection of power series

$$
F_{i}(X, Y) \in \mathbb{Q}_{p}[X, Y]
$$

where $1 \leq i \leq n$ in variables $X_{1}, \ldots, X_{n}$ and $Y_{1}, \ldots, Y_{n}$.

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 ring. An $n$-dimensional formal group law over $R$ is a collection of power series

$$
F(X, Y) = (F_{1}(X, Y), \ldots, F_{n}(X, Y)) \in R[X, Y]^{\times n}
$$

in variables $X = (X_{1}, \ldots, X_{n})$ and $Y = (Y_{1}, \ldots, Y_{n})$ such that

1. $F(0, Y) = Y$ (left unitality),
2. $F(0, Y) = Y$ (left unitality)
3. $F(F(X, Y), Z) = F(X, F(Y, Z))$ (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

$$
F_{i}(X_{1}, \ldots, X_{n}, 0, \ldots, 0) = X_{i}
$$

and the last one that

$$
F_{i}(F_{1}(X, Y), \ldots, F_{n}(X, Y), Z_{1}, \ldots, Z_{n}) = F_{i}(X_{1}, \ldots, X_{n}, F_{1}(Y, Z), \ldots, F_{n}(Y, Z)).
$$

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 $F(X, Y)$ be an $n$-dimensional formal group law over a ring $R$. Then $F_i(X, Y) = X_i + Y_i + \text{terms of degree two and above}$ for each $1 \leq i \leq n$.

Proof. By right unitality, we have $F_i(X_1, \ldots, X_n, 0, \ldots, 0) = X_i$ so that $F_i(X, Y) = X_i + \text{terms divisible by } Y_k$ for some $1 \leq k \leq n$. Similarly, by left unitality we have $F_i(X, Y) = Y_i + \text{terms divisible by } X_k$ for some $1 \leq k \leq n$. Combining these two together yields the desired statement. \qed

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 $F(X, Y)$ over the $p$-adic integers; ie. $F_i(X, Y) = \sum_{I, J} a_{i, I, J} X^I Y^J \in \mathbb{Z}_p[X, Y]$, where $I, J$ are multi-indices. In this case, given $x_1, \ldots, x_n, y_1, \ldots, y_n \in p \cdot \mathbb{Z}_p$, the series $F_i(x, y) = \sum_{I, J} a_{i, I, J} x^I y^J$ is convergent for each $1 \leq i \leq n$. Since $F$ is a formal group law, this produces an associative multiplication $S \times S \to S$ with $0 = (0, \ldots, 0)$ as a two-sided unit, where $S = p \cdot \mathbb{Z}_p^n$.

We claim that this multiplication actually makes $S$ into a group. To see this, observe that Lemma 19.4, we have
\begin{equation}
F(x, y) \equiv x + y \mod p.
\end{equation}
It follows that $F(x, -x) \equiv 0 \mod p$ so that $F(x, -x) \in p^2 \cdot \mathbb{Z}_p^n$. We then have
\begin{equation}
F(x, -x - F(x, -x)) = 0 \mod p^2.
\end{equation}
Proceeding inductively, we find an inverse of $x$ 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 $y$ is the $F$-inverse of $x \in p \cdot \mathbb{Z}_p^n$ in the sense that $F(x, y) = 0$, then $y \equiv -x \mod p^2 \cdot \mathbb{Z}_p^n$. More generally, if $x \in p^k \cdot \mathbb{Z}_p^n$, then $y \equiv -x \mod p^{k+1} \cdot \mathbb{Z}_p^n$.

The group structure on $p \cdot \mathbb{Z}_p^n$ 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
\begin{enumerate}
\item $p \cdot \mathbb{Z}_p^n$ if $p > 2$,
\item $4 \cdot \mathbb{Z}_2^n$ if $p = 2$.
\end{enumerate}
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 $p^{n(k-1)}$ (or $p^{n(k-2)}$ when $p = 2$). This in particular shows that a standard group is profinite. To see this, note that if $x \equiv y \mod p^k \cdot \mathbb{Z}_p^{\times n}$, then
$$F(x, -y) \equiv 0 \mod p^{k+1} \cdot \mathbb{Z}_p^{\times n}$$
which implies that $x, y$ 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
$$F(X, F(X, F(\ldots, X)\ldots)) = p \cdot X + \text{terms of degree two and higher}.$$ 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 $x, y \in p^k \cdot \mathbb{Z}_p^\times$, then
$$F(x, y) \equiv x + y \mod p^{2k} \cdot \mathbb{Z}_p^{\times n},$$
so that the $F$-multiplication agrees with addition modulo $p^2 \cdot \mathbb{Z}_p^\times$ for $p > 2$ and $p^3 \cdot \mathbb{Z}_p^\times$ 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 $p \cdot \mathbb{Z}_p^{\times n}$ (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. 

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 $H \subseteq G$ 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 $\phi : U \to p^k \cdot \mathbb{Z}_p^{\times n}$ in which the multiplication is expressed by a formal group law
$$F_i(X, Y) \in \mathbb{Q}_p = \sum_{i,j} a_{i,j}X^iY^j \in \mathbb{Q}_p[X, Y].$$
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
$$\|a_{i,j}p^{k'(\deg(i)+\deg(j))}\| \to 0$$
as \( \deg(I) + \deg(J) \to \infty \), 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 \( \phi: U \to p^k \cdot \mathbb{Z}_p^x \) to \( \psi := \frac{1}{p^k} \cdot \phi \), so that \( \psi: U \to \mathbb{Z}_p^x \). This changes the coefficients of the formal group law by

\[
a_{i,I,J} \mapsto a_{i,I,J} \cdot p^{(\deg(I) + \deg(J) - 1)}.
\]

Thus, by making this substitution, we can assume that \( k = 0 \) and that

\[
\|a_{i,I,J}\| \to 0.
\]

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 \( p^w \cdot \mathbb{Z}_p^x \) and then replacing it by \( \psi': = \frac{1}{p^w} \cdot \psi \), the above formula for the change of coefficients shows that they are all integral.

By construction, the preimage under the new chart \( \psi' \) of \( p \cdot \mathbb{Z}_p^x \) when \( p > 2 \) or \( p^2 \cdot \mathbb{Z}_p^x \) is a standard group, since it has multiplication defined by an integral formal group law.

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 \( H \subseteq G \) which is a uniform pro-\( p \)-group,
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.

**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

\[
v: G \setminus \{ e \} \to \mathbb{R}_{>0}
\]

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 [LMS7a] 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. □

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. □

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 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 consensed $G$-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. To a topological $G$-module, one can associate a sequence of groups

$$M \mapsto H^*(G, M)$$

We will 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

$$g \mapsto g \cdot m$$
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 $X : I \to \text{Mod}_G(\text{Ab})$ 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 $\lim \leftarrow X$ and colimit $\lim \rightarrow X$ calculated in the category of abelian groups have an induced action of $\tilde{G}$. Moreover, one verifies using Remark 20.2 that

1. the colimit $\lim \rightarrow X$ is again a discrete $G$-module,
2. the limit $\lim \leftarrow X$ is again a discrete $G$-module if the diagram $I$ is finite.

This implies the following:

**Proposition 20.3.** The category $\text{Mod}_G(\text{Ab})$ of discrete $G$-modules is Grothendieck abelian and the forgetful functor $\text{Mod}_G(\text{Ab}) \to \text{Ab}$ is an exact left adjoint.

**Warning 20.4.** Beware that a limit of discrete $G$-modules, calculated in abelian groups, need not be discrete. In terms of Proposition 20.3, 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

$$\mathbb{Z}_p[G] := \lim \leftarrow \mathbb{Z}_p[G/U],$$

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 20.3 can be identified with restriction of representations along the unique map $1 \to G$ from the trivial group. More generally, given a closed subgroup $H \leq G$, we have a restriction (ie. forgetful) functor

$$\text{res}^G_H : \text{Mod}_G(\text{Ab}) \to \text{Mod}_H(\text{Ab})$$

and this is also an exact left adjoint, as a consequence of Proposition 20.3. It will be useful to have an explicit description of the right adjoint, which we give now.

**Definition 20.5.** 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

$$\text{coind}^G_H(M) := \text{map}^H_{\text{cts}}(G, M) = \{ f : G \to M \mid f \text{ is continuous}, \forall h \in H, g \in G f(h \cdot g) = h \cdot f(g) \}$$

the module of continuous, $H$-equivariant maps, with $G$-action defined by

$$(g \cdot f)(g_0) := f(g_0 g).$$

The following is a fundamental property of coinduction.

**Lemma 20.6.** The coinduction functor $\text{coind}^G_H : \text{Mod}_H(\text{Ab}) \to \text{Mod}_G(\text{Ab})$ is exact and preserves filtered colimits.
Proof. One can show that the quotient map $G \to G/H$ (of topological spaces) admits a continuous section $\pi:G/H \to G$, 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 $G \to M$ is uniquely determined by its values at the set of representatives, any choice of a section $s$ determines an isomorphism of abelian groups

$$\text{coind}_{H}^{G}(M) \cong \text{map}_{cts}(G/H, M).$$

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. \qed

We recall the classical fact that restriction and coinduction functors form an adjunction of signature

$$\text{res}_{H}^{G}: \text{Mod}_{G}(Ab) \rightleftharpoons \text{Mod}_{H}(Ab): \text{coind}_{H}^{G}.$$

**Construction 20.7.** Suppose that $M$ is a $G$-module, $N$ is an $H$-module and that we have an $H$-equivariant map $\phi: M \to N$, which we can identify with a morphism $\text{res}_{H}^{G}(M) \to N$ in $\text{Mod}_{H}(Ab)$. We can then define a map $\psi: M \to \text{coind}_{H}^{G}(N)$ by

$$\psi(m)(g) = \phi(gm).$$

One then verifies that the construction $\phi \mapsto \psi$ define a natural isomorphism

$$\text{Hom}_{\text{Mod}_{H}(Ab)}(\text{res}_{H}^{G}(M), N) \cong \text{Hom}_{\text{Mod}_{G}(Ab)}(M, \text{coind}_{H}^{G}(N)).$$

**Remark 20.8.** 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 $\mathbb{Z}[G]$-module, 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.

We want to define the cohomology groups of a profinite group as derived functors of the invariants functor

$$M \in \text{Mod}_{G}(Ab) \mapsto M^{G} \in \text{Ab}.$$

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

$$\text{Hom}_{\text{Mod}_{G}(Ab)}(\mathbb{Z}, M) \cong M^{G}.$$

This motivates the following definition.

**Definition 20.9.** 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

$$H^{n}(G, M) = \text{Ext}^{n}_{\text{Mod}_{G}(Ab)}(\mathbb{Z}, M)$$

in the category of discrete $G$-modules.

Continuous cohomology groups are often denoted with subscript “cts”, i.e. one writes

$$H^{n}_{\text{cts}}(G, M) = H^{n}(G, M)$$

to emphasize that this depends on the topology of $G$. To avoid clutter, we will omit the subscript, since there is no other kind of group cohomology we will consider in this course. Note that if $G$ is finite, then $\text{Mod}_{G}(Ab)$ is just the category of all $G$-representations in abelian groups and the above definition reduces to cohomology of finite groups in the usual sense.
We will now show that Definition 20.9 is equivalent to a construction of cohomology groups in terms of group cochains.

**Lemma 20.10** (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

\[
H^s(G, \text{coind}_H^G(M)) \cong H^s(H, M).
\]

**Proof.** Since \( \text{coind}_H^G(-) \) is exact by Lemma 20.6, the left hand side can be identified with derived functors of

\[
M \mapsto H^0(G, \text{coind}_H^G(M)).
\]

Thus, it is enough to construct the needed natural isomorphism when \( s = 0 \). We have an identification

\[
H^0(G, \text{coind}_H^G(M)) \cong (\text{map}_{cts}^G(G, M))^G
\]

and we observe that a function \( G \to M \) 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

\[
\text{map}_{cts}^H(G, M)^G \cong M^H.
\]

\( \square \)

**Construction 20.11** (Coinduction complex). The adjunction \( \text{res}_1^G \dashv \text{coind}_1^G \) induced by the inclusion of the trivial subgroup determines a monad \( S \simeq \text{coind}_1^G \circ \text{res}_1^G \) on \( \text{Mod}_G(\text{Ab}) \) and thus for any discrete \( G \)-module \( M \) we obtain an augmented cosimplicial object

\[
M \rightarrow S(M) \Rightarrow S^2(M) \Rightarrow \ldots
\]

This in turn determines a cochain complex of discrete \( G \)-modules of the form

\[
S(M) \rightarrow S^2(M) \rightarrow S^3(M) \rightarrow \ldots
\]

where the differentials are given by alternating sums of coboundary maps of (20.1), together with an augmentation map \( M \to S(M) \).

**Definition 20.12.** 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 20.11.

**Remark 20.13** (Explicit form of group cochains). By unwrapping the definition of coinduction, the complex of discrete \( G \)-modules of Construction 20.11 can be rewritten as

\[
\text{map}_{cts}(G, M) \rightarrow \text{map}_{cts}(G \times G, M) \rightarrow \text{map}_{cts}(G \times G \times G, M) \rightarrow \ldots
\]

Applying invariants, we see that the group cochain complex is of the form

\[
M \rightarrow \text{map}_{cts}(G, M) \rightarrow \text{map}_{cts}(G \times G, M) \rightarrow \ldots
\]

With enough patience, one can calculate that in these terms the differential

\[
d: C^s(G, M) \to C^{s+1}(G, M)
\]

is given by the formula

\[
(df)(g_1, \ldots, g_{s+1}) = g_1f(g_2, \ldots, g_{s+1}) + \sum_{1 \leq i < s} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{s+1}) + (-1)^{s+1} f(g_1, \ldots, g_s).
\]

**Proposition 20.14.** Let \( M \) be a discrete \( G \)-module. Then the groups \( H^s(G, M) \) of Definition 20.9 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 20.11 is split after applying $\text{res}^G_{G_1} \cdot \text{Mod}_G(\text{Ab}) \to \text{Ab}$, 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 $H^s(G, \text{coind}_G^G(M)) \cong \text{Ext}^s_{\text{Mod}_G}(\mathbb{Z}, \text{coind}_G^G(M))$ vanishes for $s > 0$. By Shapiro’s Lemma 20.10, this can be identified with $H^s(1, M) \cong \text{Ext}^s_{\text{Ab}}(\mathbb{Z}, M)$ which vanishes in positive degrees since $\mathbb{Z}$ is projective as an abelian group. □

Example 20.15 (Zeroth cohomology). After retracing the definitions, we see that the first differential $d : M \to \text{map}_{ct}(G, M)$ 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 20.16 (First cohomology). The second differential $d : \text{map}_{ct}(G, M) \to \text{map}_{ct}(G^2, M)$ 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 $f : G \to M$ 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 $G \to M$.

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 20.14 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 $H^1(G, M) \cong \text{Hom}_{\text{grp}}(G, M)$.

Another consequence of Proposition 20.14 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 20.17. For any $s \geq 0$, the functor $M \mapsto H^s(G, M)$ preserves filtered colimits.

Proof. This is immediate from Proposition 20.14, since taking cohomology of cochain complex, the invariants functor and coinduction all preserve filtered colimits, the last one by Lemma 20.6. □

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 $H^s(G/H, M^U) \to H^s(G, M^U) \to H^s(G, M)$ where the first arrow is functoriality in the group and the second one is induced by the inclusion $M^H \hookrightarrow M$. 
Proposition 20.18. For any discrete $G$-module $M$ and any $s \geq 0$, we have

$$\text{H}^s(G,M) \cong \varprojlim \text{H}^s(G/U, M^U).$$

where the colimit is taken over the (opposite of) the poset of open normal subgroups $U \trianglelefteq G$.

Proof. Since both sides commute with filtered colimits in $M$ by Corollary 20.17 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

$$\text{H}^s(G, M) \cong \varprojlim \text{H}^s(G/V, M).$$

By Proposition 20.14, we can calculate both sides by the group cochain complex, and the needed claim follows from the fact that

$$\text{map}_{cts}(G^s, M) \cong \varprojlim \text{map}((G/V)^s, M)$$

since any locally constant function $G^s \to M$ factors through $(G/V)^s$ for small enough $V$. □

References


[Hen98] Hans-Werner Henn, Centralizers of elementary abelian $p$-subgroups and mod-$p$ cohomology of profinite groups.


[Lee] John M Lee, Smooth manifolds


[Sch19] Peter Scholze, Condensed mathematics, Lecture notes based on joint work with D. Clausen. Available at Scholze’s webpage (2019).

