FIVE LECTURES ON ANALYTIC PRO-p GROUPS: A MEETING-GROUND BETWEEN FINITE p-GROUPS AND LIE THEORY

BENJAMIN KLOPSCH

Abstract. These notes were prepared for a series of lectures, given as part of an LMS-EPSRC Short Course on "Asymptotic Methods in Infinite Group Theory". The course was held at the University of Oxford in September 2007.

The notes were specifically written for the course in Oxford and there is likely to be room for corrections and improvements. Any form of feedback is welcome. Please send comments to the email address provided at the end of the notes.

1. Introduction: classifying finite p-groups

One of the great mathematical achievements of the last century is the classification of finite simple groups. Roughly speaking, the non-abelian finite simple groups comprise 26 sporadic groups and two infinite families, namely the alternating groups and the groups of Lie type. In particular, finite simple groups are highly structured and quite rare in occurrence. A rather weak quantification of 'rare' is the following: there are at most two non-isomorphic simple groups of any prescribed order.

At the opposite end of the vast spectrum of all finite groups lie the groups of prime-power order, finite p-groups for short. Here and throughout the letter p denotes a prime. Generally speaking, finite p-groups admit many normal subgroups. As all the composition factors of a finite p-group are cyclic of order p, the knowledge of them reveals nothing beyond the order of the particular group.

Indeed, there is a lot of flexibility in building finite p-groups from cyclic components by stepwise extension. In the 1960s Higman and Sims showed that the number of groups of order p^k is roughly of the size $p^{2k^3/27}$ as $k \to \infty$. Higman's famous PORC conjecture, which was formulated at the same time, concerns the precise numbers of groups of order p^k and remains a challenge to this day.

In 1993 Pyber used the classification of finite simple groups to prove that the number of groups of order at most n is roughly of the size $n^{2(\log_2 n)^2/27}$ as $n \to \infty$. In other words, 2-groups taken by themselves set the general pace as far as the asymptotic growth in the number of groups is concerned. As a consequence, classifying 2-groups seems to be about as ambitious as classifying finite groups without any restrictions at all – surely an impossible task!

Fortunately the story does not end there. In 1980 Leedham-Green and Newman formulated a series of conjectures, the so-called Coclass Conjectures, which constitute no less than a programme for the classification of all groups of prime-power order. The underlying idea is that, instead of staring at individual finite p-groups, one should suitably streamline them into infinite pro-p groups. A pro-p group

Date: December 19. 2008.

is a topological group which can be formed by taking an inverse limit of finite p-groups. In this way one can capture a whole family of finite p-groups in one single object and thus treat infinitely many groups of variable sizes simultaneously. The primary invariant for the classification which Leedham-Green and Newman proposed is the coclass of a finite p-group, which measures the difference between the order of the group and its nilpotency class. It fits well with the process of forming pro-p groups.

In fact, the Coclass Conjectures were all proved over a period of about ten years. This success story and similar advances in asymptotic group theory over the last twenty years both made use of and contributed to our general understanding of p-adic analytic pro-p groups. The aim of these notes is to introduce the reader to some of the concepts and techniques in the theory of compact p-adic Lie groups, with a view towards applications in general group theory. Concrete examples of such applications are discussed in the two accompanying lecture series "Strong approximation methods in infinite group theory" and "Zeta functions associated to infinite groups".

General references. The following books cover some of the selected material in greater detail. They also address related and more advanced topics.

- J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal, *Analytic Pro-p Groups*, Cambridge University Press, 1999.
- E.I. Khukhro, *p-Automorphisms of Finite p-Groups*, Cambridge University Press, 1998.
- G. Klaas, C.R. Leedham-Green, W. Plesken, *Linear Pro-p-Groups of Finite Width*, Springer Verlag, 1997.
- C.R. Leedham-Green and S. McKay, *The Structure of Groups of Prime Power Order*, Oxford University Press, 2002.
- J.S. Wilson, *Profinite Groups*, Oxford University Press, 1998.

The original source for much of the theory of p-adic analytic groups is Lazard's seminal paper *Groupes analytiques p-adiques*, Inst. Hautes Études Scientifiques, Publ. Math. (26), 389–603 (1965).

2. First Lecture

2.1. **Nilpotent groups.** Let G be a group and let $x, y \in G$. The *conjugate* of x by y is $x^y = y^{-1}xy$. Conjugation provides a natural action of G on itself, indeed it induces a homomorphism from G into its automorphism group $\mathrm{Aut}(G)$. The kernel of this homomorphism, which constitutes a normal subgroup of G, is called the *centre* of G and denoted by $\mathrm{Z}(G)$. The *upper central series* of G is the ascending series of normal subgroups

$$1 = \mathrm{Z}_0(G) \leq \mathrm{Z}_1(G) \leq \ldots, \quad \text{where } \mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G) = \mathrm{Z}(G/\mathrm{Z}_i(G)).$$

By and large we will be interested in filtrations of a group G which start at the top, such as the lower central series which we describe next. The *commutator* of x with y is $[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$. The subgroup generated by all commutators is called the *commutator subgroup* of G and denoted by $[G, G]$. This notation is easily adapted to a more general situation: if $H, K \leq G$, then we write $[H, K]$ to denote the subgroup of G which is generated by all commutators $[h, k]$ with $h \in H$ and $k \in K$. The group $[G, G]$ can be characterised as the smallest normal subgroup of G such that the corresponding quotient is abelian. The *lower central series* of G is the descending series of normal subgroups

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots, \quad \text{where } \gamma_{i+1}(G) = [\gamma_i(G), G].$$

A basic property of this sequence is that $[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G)$ for all $i, j \in \mathbb{N}$.

The group G is said to be *nilpotent* if its lower central series terminates in the trivial group 1 after finitely many steps; in this case the nilpotency class of G is the smallest non-negative integer c such that $\gamma_{c+1}(G) = 1$.[1]

Nilpotent groups can be thought of as close relatives of abelian groups. Nevertheless already the study of finite nilpotent groups can become exceedingly difficult from a purely group theoretic point of view. In fact, a finite group is nilpotent if and only if for each prime p it has a unique Sylow p-subgroup. Equivalently, a finite group is nilpotent if and only if it decomposes as a direct product of finite p-groups. Whereas finite abelian groups are completely classified, the theory of finite p-groups remains an active area of research with many open problems.

2.2. **Finite p-groups.** A *p-group* is a torsion group in which every element has p-power order. Accordingly, finite p-groups are precisely the groups of p-power order. We implicitly stated above that every finite p-group is nilpotent. This fact can easily be proved inductively from the following fundamental observation. Every non-trivial normal subgroup N of a finite p-group G intersects $\mathrm{Z}(G)$ non-trivially. In particular, the centre of a non-trivial finite p-group is non-trivial. This observation can be proved by analysing the possible orbit sizes in the action of G on N by conjugation; see Exercise 4.1. An interesting consequence is that every proper subgroup of a finite p-group G is properly contained in its normaliser.

It is easy to see that the maximal subgroups of a finite p-group G are precisely the subgroups of index p and hence normal in G. The intersection of all maximal subgroups of G is the *Frattini subgroup*, commonly denoted by $\Phi(G)$. The factor

[1] It can be shown that for any group G and for any natural number c the lower central series of G terminates in 1 after c steps if and only if the upper central series of G terminates in G after c steps.

group $G/\Phi(G)$ constitutes the largest elementary abelian quotient of the finite p-group G. In other words the Frattini subgroup can be described as $\Phi(G) = G^p[G,G]$, where G^p denotes the subgroup generated by all pth powers in G.

The Frattini subgroup of a finite p-group G plays a useful role in the context of generating sets. Let $X \subseteq G$. Then X generates G if and only if there is no maximal subgroup of G containing X. This shows that X generates G if and only if its image modulo $\Phi(G)$ constitutes a generating set of $G/\Phi(G)$. Being an elementary p-group, $G/\Phi(G)$ can be regarded as a finite dimensional vector space V over the finite prime field $\mathbb{F}_p$. The set X is a minimal generating set of G if and only if its image in V forms a basis for V. Thus all minimal generating sets of G have the same size, namely $\dim_{\mathbb{F}_p} V$.

2.3. **Lie rings.** Lie methods constitute an important tool in the study of groups. In particular this applies to p-groups and, more generally, pro-p groups. The basic idea is to capture a large part of the group structure in a Lie ring.

We recall that a *Lie ring* is a $\mathbb{Z}$-module L together with a bi-additive operation $[\cdot,\cdot] : L \times L \to L$ which is skew-symmetric and satisfies the Jacobi identity:

$$[x,x] = 0 \quad \text{and} \quad [[x,y],z] + [[y,z],x] + [[z,x],y] = 0 \quad \text{for all } x,y,z \in L.$$

Let R be a commutative ring, the most common case being that R is a field. If L has the additional structure of an R-module and if $[\cdot,\cdot]$ is bilinear with respect to scalar multiplication by elements of R, then L is called a *Lie algebra* over R. If R is a principal ideal domain and L is a free R-module of finite rank, one also uses the term *Lie lattice*. Standard examples of Lie algebras include matrix algebras. Let $d \in \mathbb{N}$. Then the set $\mathfrak{gl}_d(R)$ of $d \times d$ matrices over R, regarded as an R-module and endowed with the commutator bracket

$$[A,B] := AB - BA \quad \text{for all } A,B \in \mathfrak{gl}_d(R),$$

forms a Lie algebra over R. In fact, a theorem of Ado states that every finite dimensional Lie algebra over a field K of characteristic 0 is isomorphic to a Lie subalgebra of $\mathfrak{gl}_d(K)$ for a suitable degree d.

At first sight Lie rings perhaps appear to be more complicated objects than groups. However, one should think of a Lie ring essentially as a vector space. The extra structure, given by the Lie bracket, can be regarded as a simplified version of the group commutator. For instance, the group theoretic analogue of the Jacobi identity is the baffling Hall-Witt identity

$$[[x,y^{-1}],z]^y\,[[y,z^{-1}],x]^z\,[[z,x^{-1}],y]^x = 1$$

which holds in any group. Many of the concepts which we have introduced for groups, such as nilpotency, can be defined mutatis mutandis in the context of Lie rings. For instance, the centre of a Lie ring L is the Lie ideal $\mathrm{Z}(L) = \{x \in L \mid \forall y \in L : [x,y] = 0\}$. We trust that the reader will make the appropriate translations of this kind where necessary.

2.4. **Applying Lie methods to groups.** Next we describe a comparatively simple recipe for associating a Lie ring to a group G with respect to its lower central series. The procedure is particularly useful if G is residually nilpotent, i.e. if $\bigcap_{i\in\mathbb{N}} \gamma_i(G) = 1$. Form the direct sum $L = \bigoplus_{i=1}^{\infty} L_i$ of the abelian groups

$L_i := \gamma_i(G)/\gamma_{i+1}(G)$. Then commutation in G induces a natural binary operation $[\cdot,\cdot]_{\mathrm{Lie}}$ on L: it is defined on homogeneous elements $x\gamma_{i+1}(G) \in L_i$ and $y\gamma_{j+1}(G) \in L_j$ by

$$[x\gamma_{i+1}(G), y\gamma_{j+1}(G)]_{\mathrm{Lie}} := [x,y]\gamma_{i+j+1}(G) \in L_{i+j},$$

and can be uniquely extended to yield a bi-additive operation on all elements. As $[y,x] = [x,y]^{-1}$ for all $x, y \in G$, this binary operation on L is skew-symmetric. Moreover, the Hall-Witt identity can be used to show that $[\cdot,\cdot]_{\mathrm{Lie}}$ satisfies the Jacobi identity. Thus $L = \bigoplus_{i=1}^{\infty} L_i$ obtains the structure of a Lie ring. This Lie ring is graded in the sense that $[L_i, L_j] \subseteq L_{i+j}$ for all indices i, j. If all the homogeneous components L_i happen to have exponent p, we can regard L even as a Lie algebra over $\mathbb{F}_p$. An example of this construction is described in Exercise 4.3.

A more sophisticated way of constructing a Lie ring from a group is based on the so-called Hausdorff Formula which can be regarded as the centre piece of Lie theory.[2] Stated briefly, the Hausdorff Formula gives an expression for the formal power series

$$\Phi(X,Y) = \log(\exp(X)\cdot\exp(Y)) \in \mathbb{Q}\langle\langle X, Y\rangle\rangle$$

in non-commuting indeterminates X, Y. Here

$$\log(1+X) = \sum\nolimits_{n=1}^{\infty} (-1)^{n-1} X^n/n \quad \text{and} \quad \exp(X) = \sum\nolimits_{n=0}^{\infty} X^n/n!$$

denote the usual formal power series. The Hausdorff Formula enables one to translate between a Lie ring and a group via the logarithm and exponential functions. Classical and important instances of this procedure are the correspondences of Mal'cev and Lazard. These can be employed, in particular, to study finitely generated torsion-free nilpotent groups and finite p-groups of nilpotency class less than p. Without specifying further details at this point we formulate

Theorem 2.1 (Lazard's correspondence)**.** *The Hausdorff Formula and its inverse set up a correspondence between*

- *finite p-groups of nilpotency class less than p and*
- *nilpotent Lie rings of class less than p whose additive group is a finite p-group.*

The correspondence preserves such invariants as the orders and the nilpotency classes of the objects involved.

We give a simple illustration of Lazard's correspondence by describing the isomorphism classes of groups of order p^3 for odd primes p. Writing C_n to denote a cyclic group of order n, there are (up to isomorphism) precisely three abelian groups of order p^3, namely

$$G_1 = C_p \times C_p \times C_p, \quad G_2 = C_{p^2} \times C_p, \quad G_3 = C_{p^3}.$$

We claim that in addition to these there are (up to isomorphism) precisely two non-abelian groups of order p^3. Since the nilpotency class of a group of order p^3 is at most 2, by Lazard's correspondence it suffices to show that there are (up to isomorphism) precisely two nilpotent Lie rings of class 2 and order p^3. Clearly, the underlying additive group of such a Lie ring L cannot be cyclic. Moreover, the commutator Lie subring $[L, L]$ has to coincide with the centre $\mathrm{Z}(L)$. From

[2]Often the Hausdorff Formula is more decoratively referred to as the Baker-Campbell-Hausdorff Formula.

this one shows that each of the two non-cyclic abelian groups of order p^3 supports essentially one nilpotent Lie ring structure. The two resulting Lie rings and their corresponding groups can be realised in terms of matrices over $\mathbb{F}_p$ and $\mathbb{Z}/p^2\mathbb{Z}$, respectively; see Exercise 4.2. Representatives for the two isomorphism classes of non-abelian groups of order p^3 are also given by the following group presentations,

$$G_4 = \langle x, y, z \mid x^p = y^p = z^p = 1, z = [x, y], [z, x] = [z, y] = 1 \rangle,$$
$$G_5 = \langle x, y \mid x^{p^2} = y^p = 1, [x, y] = x^p \rangle.$$

In 'real life', Lazard's correspondence forms the starting point for the rather more sophisticated enumeration of finite p-groups of higher order, p^7 say.[3]

Note that the graded Lie rings associated to G_4 and G_5 with respect to their lower central series coincide. This illustrates that the first and simpler method which we presented above incurs a loss of information. The Lie rings which can be associated via the Hausdorff Formula to suitable pro-p groups are Lie lattices over the p-adic integers. It turns out that they do in fact determine the pro-p groups completely.

2.5. **Absolute values.** The traditional way to describe the size of a rational number is through the use of absolute values. An *absolute value* on a field K is a real-valued function $|\cdot| : K \to [0, \infty)$ which is non-degenerate, multiplicative and satisfies the triangle inequality; this means that for all $x, y \in K$ we have

(1) $|x| = 0$ if and only if $x = 0$,
(2) $|xy| = |x| \cdot |y|$,
(3) $|x + y| \leq |x| + |y|$.

The absolute value is *trivial* if $|x| = 1$ for all $x \neq 0$. For our purposes, the absolute value is said to be either *non-archimedean* or *archimedean* according to whether or not it satisfies the ultrametric triangle inequality

(3′) $|x + y| \leq \max\{|x|, |y|\}$.

The ordinary absolute value on $\mathbb{R}$, which is given by $|x|_\infty = \max\{x, -x\}$, restricts to an archimedean absolute value on $\mathbb{Q}$.

In addition there is an infinite family of non-archimedean absolute values on $\mathbb{Q}$, one for each prime p. Each rational number $x \neq 0$ can be written uniquely in the form

$$x = p^n \cdot \frac{a}{b} \quad \text{where } n, a, b \in \mathbb{Z} \text{ with } b > 0,\ \gcd(a, b) = 1,\ p \nmid ab.$$

We put

$$v_p(x) := n \quad \text{and} \quad |x|_p := p^{-n}.$$

Setting $v_p(0) := \infty$ and $|0|_p := 0$, we obtain the *p-adic absolute value* $|\cdot|_p$ on $\mathbb{Q}$. Intuitively, x is p-adically small if it is divisible by a large power of p. The map

[3] In 2005 O'Brien and Vaughan-Lee showed that for $p > 5$ the number of groups of order p^7 is precisely $3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455 + (4p^2 + 44p + 291)\gcd(p-1, 3) + (p^2 + 19p + 135)\gcd(p-1, 4) + (3p + 31)\gcd(p-1, 5) + 4\gcd(p-1, 7) + 5\gcd(p-1, 8) + \gcd(p-1, 9)$, if I copied everything correctly. In particular, this substantiates for $k = 7$ Higman's famous PORC conjecture which states that the precise number of groups of order p^k is given by a polynomial in p, depending on k and the residue class of p with respect to a suitable modulus $n(k)$. PORC stands for 'polynomial on residue classes'.

$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, which captures the same information, is called the *p-adic valuation* on $\mathbb{Q}$.

A theorem of Ostrowski states that, up to a suitable equivalence relation, the ordinary absolute value and the p-adic absolute values exhaust all possible non-trivial absolute values on $\mathbb{Q}$. They are linked by the curious adelic formula

$$|x|_\infty \prod_p |x|_p = 1 \quad \text{for all } x \in \mathbb{Q},$$

which is intimately linked with the Fundamental Theorem of Arithmetic; see Exercise 4.4.

2.6. **p-adic numbers.** The field $\mathbb{R}$ of real numbers can be regarded as the completion of $\mathbb{Q}$ with respect to the metric $d_\infty(x, y) = |x-y|_\infty$ induced by the ordinary archimedean absolute value. Formally, one could construct $\mathbb{R}$ by adjoining all the missing limits of Cauchy sequences in $\mathbb{Q}$ with respect to d_∞. Every element $\alpha \in \mathbb{R}$ is the limit of a Cauchy sequence $\alpha = \lim_{n\to\infty} x_n$ with $x_n \in \mathbb{Q}$, and the absolute value extends to $\mathbb{R}$ via $|\alpha|_\infty = \lim_{n\to\infty} |x_n|_\infty$. By a similar procedure, the ring operations, addition and multiplication, extend from $\mathbb{Q}$ to $\mathbb{R}$, and one obtains again a field with absolute value. In using the common decimal notation we tend to think of a real number α as the limit of a particular Cauchy sequence of the form

$$\alpha = \lim_{n\to\infty} x_n, \quad x_n = \lfloor \alpha \rfloor + \sum_{k=1}^{n} a_k \cdot 10^{-k},$$

where $\lfloor \alpha \rfloor$ denotes the integral part of α and the 'digits' a_k are taken from the set $\{0, 1, \ldots, 9\}$. We remark that base 10 is chosen by convention, not for any intrinsic mathematical reason.

Similarly we can form for each prime p the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to the metric $d_p(x, y) = |x - y|_p$ induced by the p-adic absolute value. In this case one has to adjoin all the missing limits of (equivalence classes of) Cauchy sequences with respect to d_p. Every element $\alpha \in \mathbb{Q}_p$ is the limit of a Cauchy sequence $\alpha = \lim_{n\to\infty} x_n$ with $x_n \in \mathbb{Q}$, and the absolute value is extended to $\mathbb{Q}_p$ by setting $|\alpha|_p = \lim_{n\to\infty} |x_n|_p$. Similarly one extends to $\mathbb{Q}_p$ the valuation map v_p and the ring operations, addition and multiplication. One then checks that $\mathbb{Q}_p$ is again a field with absolute value $|\cdot|_p$. The elements of $\mathbb{Q}_p$ are called *p-adic numbers*.

A convenient notation for explicit computations with p-adic numbers is the following. Every $\alpha \in \mathbb{Q}_p$ can be written uniquely as a series

$$\alpha = \sum_{k\in\mathbb{Z}} a_k p^k = \sum_{k=v_p(\alpha)}^{\infty} a_k p^k,$$

where the coefficients a_k are taken from the set $R_p := \{0, 1, \ldots, p-1\}$, $a_k = 0$ for $k < v_p(\alpha)$, and $a_{v_p(\alpha)} \neq 0$ if $\alpha \neq 0$. We remark that instead of R_p we could use any set of representatives for $\mathbb{Z}$ modulo $p\mathbb{Z}$.

A central feature of the real numbers $\mathbb{R}$ is that the field operations are continuous with respect to (the topology underlying) the metric associated to the absolute value $|\cdot|_\infty$. Section 3 contains a summary of basic notions in topology which we assume. As a topological space $\mathbb{R}$ is Hausdorff, locally-compact and

connected. Approximate computations in $\mathbb{R}$ can be performed by truncating the decimal representations of the numbers involved and verifying that errors do not pile up too much – the last bit can actually be quite tricky.

In a similar way the p-adic absolute value induces a metric and hence a topology on $\mathbb{Q}_p$. It is an inherent feature of the completion process that the field operations are continuous. As a topological space $\mathbb{Q}_p$ is Hausdorff, locally-compact and totally-disconnected. In fact, if we regard R_p as a finite discrete space and endow $\prod_{k\in\mathbb{Z}} R_p$ with the product topology, then the coordinate map

$$\mathbb{Q}_p \to \prod_{k\in\mathbb{Z}} R_p, \quad \alpha = \sum_{k\in\mathbb{Z}} a_k p^k = \sum_{k=v_p(\alpha)}^{\infty} a_k p^k \mapsto (a_k)$$

is a homeomorphism from $\mathbb{Q}_p$ onto the open subspace

$$\left\{ (a_k)_{k\in\mathbb{Z}} \in \prod\nolimits_{k\in\mathbb{Z}} R_p \mid \exists n \, \forall k < n : a_k = 0 \right\}.$$

Approximate computations in $\mathbb{Q}_p$ can be performed by truncating the standard representations of the numbers involved; the ultrametric triangle inequality guarantees that errors will not accumulate; see Exercise 4.4.

A *local field* is a field K, equipped with a non-trivial non-archimedean absolute value, such that K is locally-compact with respect to the induced topology. If K is a finite extension of $\mathbb{Q}_p$, then the p-adic absolute value $|\cdot|_p$ extends uniquely to an absolute value on K, and K becomes a local field. Conversely, it can be shown that every local field of characteristic 0 arises in this manner.

2.7. **p-adic integers.** Finally we describe a most notable difference between the archimedean field $\mathbb{R}$ and its counterparts, the non-archimedean p-adic fields $\mathbb{Q}_p$. The ultrametric triangle inequality implies that the open compact set

$$\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\} = \left\{ \sum\nolimits_{k=0}^{\infty} a_k p^k \mid a_k \in R_p \right\}$$

forms a subring of $\mathbb{Q}_p$. It is the topological closure of the ordinary integers $\mathbb{Z}$ in $\mathbb{Q}_p$, and its elements are called *p-adic integers*.

The structure of the ring of p-adic integers is quite simple. A short computation reveals that its group of units is given by

$$\mathbb{Z}_p^* = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p = 1\} = \left\{ \sum\nolimits_{k=0}^{\infty} a_k p^k \mid a_k \in R_p \text{ and } a_0 \neq 0 \right\}.$$

Moreover, the ideals of $\mathbb{Z}_p$ are principal and of the form $p^n\mathbb{Z}_p$: they line up neatly in a descending chain

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \ldots \supset 0.$$

The proper quotient rings of $\mathbb{Z}_p$ are the familiar finite rings $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. In Section 5 we describe how $\mathbb{Z}_p$ can be regarded as an inverse limit of these finite quotients. Intuitively, one should think of performing ring operations in $\mathbb{Z}_p$ as follows: do the operations in the ring $\mathbb{Z}_p/p^n\mathbb{Z}_p$, then let n tend to infinity.

2.8. **Preview: p-adic analytic pro-p groups.** As yet we have not even defined what we mean by a pro-p group. Nevertheless, skipping the theory that lies in between, we can already formulate a precise and hands-on description of the family of compact p-adic analytic groups and p-adic analytic pro-p groups, in particular.

A *topological group* is a group G which is also a topological space such that the group operations are continuous, i.e. such that the map $G \times G \to G, (g, h) \mapsto g^{-1}h$ is continuous. Let $d \in \mathbb{N}$, and consider the group $\mathrm{GL}_d(\mathbb{Z}_p)$ of all invertible $d \times d$ matrices over the ring $\mathbb{Z}_p$ of p-adic integers. The set $\mathrm{Mat}_d(\mathbb{Z}_p)$ of all $d \times d$ matrices carries a natural p-adic topology, namely the product topology induced from the p-adic topology on $\mathbb{Z}_p$. Matrix multiplication is easily seen to be continuous, and so is the process of forming the inverse of an invertible matrix. Hence $\mathrm{GL}_d(\mathbb{Z}_p)$, equipped with the subspace topology, becomes a topological group. We can now state

Theorem 2.2 (Lazard's characterisation of compact p-adic Lie groups)**.** *A compact topological group admits a p-adic analytic structure if and only if it is isomorphic to a closed subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for a suitable degree d.*

In fact, Lazard established a whole theory of p-adic analytic groups with much wider consequences. One of his key results is that the analytic structure of a p-adic analytic group is determined entirely by its topological group structure. This can be regarded as a positive solution to Hilbert's fifth problem for p-adic Lie groups.

As we will see, $\mathrm{GL}_d(\mathbb{Z}_p)$ is virtually a pro-p group. This means that $\mathrm{GL}_d(\mathbb{Z}_p)$ contains a subgroup of finite index which is a pro-p group. Theorem 2.2 implies that every compact p-adic analytic group is virtually a pro-p group.

We conclude this section with a concrete reformulation of Theorem 2.2 which applies more directly to pro-p groups. There is a natural ring homomorphism from $\mathbb{Z}_p$ onto the finite prime field $\mathbb{F}_p$. As $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$, this induces a surjective group homomorphism $\eta : \mathrm{GL}_d(\mathbb{Z}_p) \to \mathrm{GL}_d(\mathbb{F}_p)$. The kernel of η is the first congruence subgroup $\mathrm{GL}_d^1(\mathbb{Z}_p) = \{g \in \mathrm{GL}_d(\mathbb{Z}_p) \mid g \equiv 1 \pmod{p}\}$ of $\mathrm{GL}_d(\mathbb{Z}_p)$. The preimage under η of any Sylow p-subgroup of the finite group $\mathrm{GL}_d(\mathbb{F}_p)$ constitutes a Sylow pro-p subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$. One particular Sylow p-subgroup of $\mathrm{GL}_d(\mathbb{F}_p)$ is the group of upper uni-triangular matrices; according to the Sylow Theorems all other Sylow p-subgroups of $\mathrm{GL}_d(\mathbb{F}_p)$ are conjugate to this one.

Corollary 2.3. *A p-adic analytic pro-p group is a topological group which is isomorphic to a closed subgroup of a Sylow pro-p subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for a suitable degree d.*

3. Basic notions and facts from point-set topology

Pro-p groups and, more generally, profinite groups form a particular class of topological groups. For discussing their structure we require basic notions and facts from point-set topology. For the convenience of the reader I have listed the relevant prerequisites below.

A *topological space* $X = (X, \tau)$ is a set X together with a topology, given by a collection τ of *open* subsets of X, satisfying: (i) X and $\varnothing$ are open; (ii) the union of any family of open sets is open; (iii) the intersection of any two open sets is open. The complement in X of any open set is called a *closed* set. It is convenient to use the notation $A \subseteq_{\mathrm{o}} X$ (respectively $A \subseteq_{\mathrm{c}} X$) to indicate that a subset A is open (respectively closed) in X. Every metric space (X, d) with distance function d has an underlying topology: the open sets in this topology are the unions of 'open' balls $\{y \mid d(x, y) < r\}$, where $x \in X$ and $r \in \mathbb{R}$. The *discrete* topology on a set X is the topology in which every subset of X is open.

Let $\varphi : X \to Y$ be a map between topological spaces. The map φ is *continuous* if the preimage of any open set is open, i.e. if $B\varphi^{-1} \subseteq_{\mathrm{o}} X$ for all $B \subseteq_{\mathrm{o}} Y$. The map $\varphi : X \to Y$ is a *homeomorphism* if it is continuous, bijective and admits a continuous inverse.

Let X be a topological space. The *subspace topology* on a subset $Y \subseteq X$ is defined by declaring all intersections $Y \cap A$ with $A \subseteq_{\mathrm{o}} X$ to be open. This is the smallest topology which renders the natural inclusion $Y \to X$ continuous. The *quotient topology* on $Y := X/\sim$ with respect to an equivalence relation $\sim$ is defined by declaring a subset $B \subseteq Y$ open if its preimage in X under the natural projection is open. This is the smallest topology which renders the projection $X \to Y$ continuous.

If X_i, $i \in I$, is a family of topological spaces, then the *product topology* on the Cartesian product $X := \prod_{i \in I} X_i$ is defined by declaring a subset of X open if it is the union of basic open sets of the form $\prod_{i \in I} U_i$, where $U_i = X_i$ for almost all $i \in I$ and $U_i \subseteq_{\mathrm{o}} X_i$ for all $i \in I$. It is the smallest topology such that all canonical projections $X \to X_i$, $i \in I$, are continuous.

Let X be a topological space. The *closure* $\mathrm{cl}(A)$ of a subset $A \subseteq X$ is the intersection of all closed sets containing A; it constitutes the smallest closed set containing A. A subset $A \subseteq X$ is *dense* in X if its closure is equal to X. If $x \in A \subseteq_{\mathrm{o}} X$, then A is called an *open neighbourhood* of x. The space X is *Hausdorff* if any two distinct points have disjoint open neighbourhoods. The space X is *compact* if any covering $X = \bigcup\{U_i \mid i \in I\}$ of X by open subsets $U_i \subseteq_{\mathrm{o}} X$ admits a finite subcovering $X = \bigcup\{U_i \mid i \in J\}$, $J \subseteq I$ with $|J| < \infty$.[4] Equivalently, X is compact if for any non-empty family C_i, $i \in I$, of closed subsets of X having the finite intersection property

$$\bigcap\{C_i \mid i \in J\} \neq \varnothing \quad \text{for all } J \subseteq I \text{ with } 1 \leq |J| < \infty$$

one has $\bigcap\{C_i \mid i \in I\} \neq \varnothing$. The continuous image of a compact space is compact. A theorem of Tychonoff states that the product of any family of compact spaces is compact.

[4]The original notion 'kompakt' due to Hausdorff – and also adopted by Bourbaki – is reserved for spaces which are compact, in the given sense, and Hausdorff.

The space X is *locally-compact* if every point $x \in X$ has a local base of compact neighbourhoods, i.e. if for every open neighbourhood U of x there exist $V \subseteq_{\mathrm{o}} X$ and a compact subset $C \subseteq X$ such that $x \in V \subseteq C \subseteq U$. Every compact Hausdorff space is locally-compact; see Exercise 4.5.

The space X is *connected* if it cannot be partitioned into two proper open subsets, i.e. if for all $A \subseteq_{\mathrm{o}} X$ with $X \setminus A \subseteq_{\mathrm{o}} X$ one has $A = \varnothing$ or $A = X$. Equivalently, X is connected if every continuous map from X into the discrete space $\{0, 1\}$ is constant. The continuous image of a connected space is connected. The maximal connected subsets of X are called *connected components* of X. The connected components of X are closed and they partition X. The space X is *totally-disconnected* if all its connected components are one-point sets. A *path* from x to y in the space X is a continuous map φ from the unit interval $[0, 1]$ into X with $\varphi(0) = x$ and $\varphi(1) = y$. The space X is *path-connected* if any to points of X can be joined by a path. Every path-connected space is connected.

4. First set of exercises

This first set of exercises is also intended to serve as a bridge towards topics which will be covered in later sections. The reader is not necessarily expected to solve all parts of all exercises in the first go.

Exercise 4.1 (Finite p-groups)**.**
(a) Let N be a non-trivial normal subgroup of a non-trivial finite p-group G. Show that $\mathrm{Z}(G) \cap N \neq 1$. Conclude that $\mathrm{Z}(G) \neq 1$ and that G is nilpotent.
(b) Prove that the nilpotency class of a group of order p^n is at most $n-1$.
Construct a group of order p^p and nilpotency class $p-1$ along the following lines. Let V be a p-dimensional vector space over $\mathbb{F}_p$ with basis $e_1, \ldots, e_p$. Consider the linear map $\alpha : V \to V$, given by $e_i^\alpha = e_{i+1}$ for $i \in \{1, \ldots, p-1\}$ and $e_p^\alpha = e_1$. Observe that the 1-dimensional subspace U of V which is spanned by $e_1 + \ldots + e_p$ is invariant under α. Consider the semidirect product of V/U by $\langle \alpha \rangle$.
Remark: Groups of order p^n and nilpotency class $n-1$ are said to be of *maximal class*. In fact, they are the ones of coclass 1. The semidirect product of V by $\langle \alpha \rangle$ is isomorphic to the wreath product $C_p \wr C_p$.
(c) Let $n \in \mathbb{N}$ and write $n = n_0 + n_1 p + \ldots + n_r p^r$ with $0 \leq n_i < p$ for $i \in \{0, \ldots, r\}$. Determine $v_p(n!)$, i.e. the exponent of the highest p-power dividing $n!$, in terms of the numbers n_i. (*Hint:* First describe $v_p(n!)$ in terms of the numbers $\lfloor n/p^i \rfloor$.)
The *wreath product* $C_p \wr H$ of the cyclic group C_p with a finite group H is the semidirect product of the group algebra $\mathbb{F}_p[H]$ by H, with H acting by right multiplication. Let $k \in \mathbb{N}$ and observe that the iterated wreath product $W_k := C_p \wr (C_p \wr \ldots \wr C_p)$ of k cyclic groups of order p acts naturally on the finite p-regular rooted tree of length k, depicted below for $p = 3$ and $k = 2$.

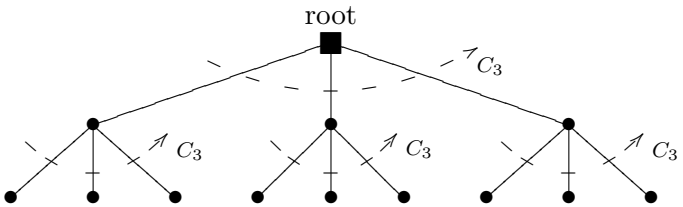

Figure 1. The wreath product $C_3 \wr C_3 \cong C_3 \ltimes (C_3 \times C_3 \times C_3)$ acts naturally on the rooted 3-regular tree of length 2. In this action the root vertex is fixed, and the action is recorded faithfully on the bottom layer of nine vertices. This describes an embedding of $C_3 \wr C_3$ into the symmetric group $\mathrm{Sym}(9)$.

By computing the order of W_k, prove that the Sylow p-subgroup of the symmetric group $\mathrm{Sym}(p^k)$ is isomorphic to W_k. Conclude that every finite p-group of order at most p^k embeds into W_k.
Can you guess the structure of a Sylow p-subgroup of the symmetric group $\mathrm{Sym}(n)$?

Exercise 4.2 (Groups and Lie rings of order p^3)**.**
(a) Determine up to isomorphism all groups of order p, p^2 and p^3.
(b) Determine up to isomorphism all Lie rings of order p and p^2. Can you find a Lie ring L of order p^3 which is perfect, i.e. which satisfies $L = [L, L]$?
(c) Show that the groups G_4 and G_5 of order p^3, which are defined in Section 2.4 by presentations, are isomorphic to the subgroups

$$\widetilde{G}_4 = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}, \quad \widetilde{G}_5 = \left\{ \begin{pmatrix} 1+pa & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/p^2\mathbb{Z} \right\}.$$

of $\mathrm{GL}_3(\mathbb{F}_p)$ and $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$, respectively.
Remark: The group $\widetilde{G}_4$ is the finite Heisenberg group over the field $\mathbb{F}_p$.
(d) Show that the sets

$$\widetilde{L}_4 = \left\{ \begin{pmatrix} 0 & a & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}, \quad \widetilde{L}_5 = \left\{ \begin{pmatrix} pa & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z}/p^2\mathbb{Z} \right\}.$$

form nilpotent Lie subrings of class 2 in $\mathfrak{gl}_3(\mathbb{F}_p)$ and $\mathfrak{gl}_2(\mathbb{Z}/p^2\mathbb{Z})$, respectively.
(e) Let $i \in \{4, 5\}$, and suppose that $p > 2$. Can you see how $\widetilde{L}_i$ and $\widetilde{G}_i$ are related to one another via the truncated exponential function $X \mapsto 1 + X + X^2/2$ and the truncated logarithm function $1 + X \mapsto X - X^2/2$?
Set up a bijection $\varphi : \widetilde{L}_i \to \widetilde{G}_i$ based on the truncated exponential function and work out a Lie expression in $x, y \in \widetilde{L}_i$ for the element $(x^\varphi \cdot y^\varphi)^{\varphi^{-1}}$.
Remark: This will constitute a first approximation to the Hausdorff Formula.

Exercise 4.3 (The lower central series of the Nottingham group)**.**
The Nottingham group over $\mathbb{F}_p$ is the group G of formal power series

$$\mathbf{a} = t\left(1 + \sum\nolimits_{i=1}^{\infty} a_i t^i\right) = t + a_1 t^2 + a_2 t^3 + \ldots \quad \in t + t^2\mathbb{F}_p[\![t]\!]$$

with composition given by substitution: the product of $\mathbf{a}, \mathbf{b} \in G$ is defined as

$$\mathbf{a} \circ \mathbf{b} := \mathbf{a}(\mathbf{b}(t)) = t + (a_1 + b_1)t^2 + (a_2 + 2a_1b_1 + b_2)t^3 + \\ (a_3 + 3a_2b_1 + a_1b_1^2 + 2a_1b_2 + b_3)t^4 + \ldots$$

(a) Convince yourself that every element of G has an inverse with respect to the prescribed composition.
(b) Consider the elements $\mathbf{e}_i := t + t^{i+1} \in G$, $i \in \mathbb{N}$. Verify that $\mathbf{e}_i^\lambda \equiv t + \lambda t^{i+1}$ modulo t^{i+2} for $i \in \mathbb{N}$ and $\lambda \in \mathbb{Z}$. Prove that $\mathbf{e}_i \circ \mathbf{e}_j \equiv \mathbf{e}_j \circ \mathbf{e}_i$ modulo t^{i+j+1} and deduce that $[\mathbf{e}_i, \mathbf{e}_j] \equiv \mathbf{e}_{i+j}^{i-j}$ modulo t^{i+j+2} for all $i, j \in \mathbb{N}$.
(c) Show that for every $n \in \mathbb{N}$ the set $G_n := \{\mathbf{a} \in G \mid \mathbf{a} \equiv t \mod t^{n+1}\}$ forms a normal subgroup of index p^{n-1} in G. Show that $G_n = \langle \mathbf{e}_n \rangle G_{n+1}$ for $n \in \mathbb{N}$.
(d) Let $n \in \mathbb{N}$, and put $\Gamma_n := G/G_n$. Write e_i for the image of $\mathbf{e}_i$ in Γ_n. Show that every element $g \in \Gamma_n$ can be written uniquely in the form $g = e_1^{\lambda_1} e_2^{\lambda_2} \cdots e_{n-1}^{\lambda_{n-1}}$ with exponents $\lambda_i \in \{0, 1, \ldots, p-1\}$.
(e) Let $n \in \mathbb{N}$, and suppose that $p > 2$. Determine the commutator subgroup $[\Gamma_n, \Gamma_n]$ of Γ_n and show that it coincides with the Frattini subgroup. Conclude that e_1 and e_2 form a minimal generating pair for Γ_n.

(f) Suppose that $p > 2$. Work out the lower central series for Γ_{p+1} and determine the graded Lie ring associated to this group with respect to its lower central series, as described in Section 2.4.
(g) Suppose that $p > 2$. Work out the lower central series of Γ_{p+2}. Can you guess the general pattern of the lower central series of Γ_n as $n \to \infty$? See whether your guess is consistent with the following formula: for $n \geq 3$ the nilpotency class of Γ_n is equal to $(n-2) - \lfloor (n-3)/p \rfloor$.

Exercise 4.4 (Non-archimedean absolute values and p-adic numbers)**.**
(a) Prove that the adelic formula stated in Section 2.5 holds.
(b) Compute the standard representation $\sum_{k=0}^{\infty} a_k 3^k$ of -13 in the ring $\mathbb{Z}_3$ of 3-adic integers. Show that 5 has a multiplicative inverse in the ring $\mathbb{Z}_3$, by displaying the standard representation of such an element. Prove that 11 has no square root in $\mathbb{Z}_3$, but convince yourself that 7 does by computing the first five coefficients of the standard representation of a potential root.
Prove that 2 has no square root in $\mathbb{Q}_2$. Now suppose that $p > 2$. Convince yourself that 2 has a square root in $\mathbb{Q}_p$ if and only if it has one in $\mathbb{Z}_p$. Then show that 2 has a square root in $\mathbb{Z}_p$ if and only if 2 admits a square root modulo p. (*Hint:* Look at the quotient $\mathbb{Z}_p/p\mathbb{Z}_p$ to see that the condition is necessary. Now suppose that $x \in \mathbb{Z}_p$ satisfies $x^2 - 2 \equiv 0$ modulo p. Then $x^2 - 2 = pa$ for a suitable $a \in \mathbb{Z}_p$. Write $\tilde{x} = x + py$ with $y \in \mathbb{Z}_p$ to be specified. Since $2x \in \mathbb{Z}_p^*$, the congruence

$$p(2xy + a) \equiv x^2 + 2pxy + p^2y^2 - 2 = \tilde{x}^2 - 2 \equiv 0 \pmod{p^2}$$

can be solved for $y \in \mathbb{Z}_p$. Now continue inductively to find a Cauchy sequence $x, \tilde{x}, \ldots$ in $\mathbb{Z}_p$ whose limit gives a precise square root of 2.)
Remark: This procedure is a particular instance of Hensel's Lemma.
(c) Let $|\cdot|$ be a non-archimedean absolute value on a field K. Prove that for all $x, y \in K$ with $|x| \neq |y|$ the ultrametric triangle inequality specialises to $|x + y| = \max\{|x|, |y|\}$.
Suppose further that K is complete with respect to the metric $d(x, y) = |x - y|$ induced by the absolute value. Conclude that for any sequence $(a_n)_{n \in \mathbb{N}}$ in K the series $\sum_{n=1}^{\infty} a_n$ converges in K if and only if $|a_n| \to 0$ for $n \to \infty$. For which p does the harmonic series $\sum_{n=1}^{\infty} n^{-1}$ converge in $\mathbb{Q}_p$?
(d) Suppose that $p > 2$. Given that $v_p(n!) \leq (n-1)/(p-1)$ for all $n \in \mathbb{N}$, show that the exponential series $\exp(x) = \sum_{n=0}^{\infty} x^n/n!$ converges for all $x \in p\mathbb{Z}_p$. Deduce that the exponential series induces an isomorphism of topological groups from the additive group $p\mathbb{Z}_p$ onto the multiplicative group of one-units $1 + p\mathbb{Z}_p$.
Remark: Clearly, the additive groups $p\mathbb{Z}_p$ and $\mathbb{Z}_p$ are isomorphic. It can be shown that the subgroup $1 + p\mathbb{Z}_p$ of the abelian group $\mathbb{Z}_p^*$ admits a cyclic complement so that $\mathbb{Z}_p^* \cong \mathbb{Z}_p \times C_{p-1}$.
(e) Show that the additive group $\mathbb{Z}_2$ and the multiplicative group $1 + 2\mathbb{Z}_2$ are not isomorphic. Can you mend the situation by considering a subgroup of finite index in $1 + 2\mathbb{Z}_2$ and subsequently determine the structure of $\mathbb{Z}_2^*$?

Exercise 4.5 (Point-set topology and topological groups)**.**
(a) Show that $\mathrm{GL}_2(\mathbb{R})$, with respect to the natural topology, is a locally-compact, Hausdorff topological group. Is this group connected? If not, how many connected components does it have? (*Hint:* Think of determinants and canonical forms of matrices.)
Show that $\mathrm{GL}_2(\mathbb{Z})$ is a discrete subgroup of $\mathrm{GL}_2(\mathbb{R})$. Can you give an example of an infinite compact subgroup of $\mathrm{GL}_2(\mathbb{R})$? (*Hint:* Think of rotation matrices.) Does $\mathrm{GL}_2(\mathbb{R})$ admit any open compact subgroups?
(b) Let X, Y be topological spaces. Prove the following assertions from first principles. (i) If X is Hausdorff, then every compact subset of X is closed. (ii) If X is compact, then every closed subset of X is compact. (iii) If X is compact and Y is Hausdorff, then every continuous bijection $f : X \to Y$ is a homeomorphism. (iv) Every compact Hausdorff space is locally-compact.
(c) Regard C_p as a topological group, equipped with the discrete topology. Convince yourself that C_p is totally-disconnected, compact and Hausdorff. Using Tychonoff's Theorem and first principles, deduce that $G := \prod_{k\in\mathbb{Z}} C_p$ is a totally-disconnected, compact, Hausdorff topological group. Does G admit a finitely generated dense subgroup?
Let $V = \bigoplus_{k\in\mathbb{Z}} \mathbb{F}_p e_k$ be a vector space over $\mathbb{F}_p$ of countably infinite dimension. Show that the underlying abelian group of the dual space $\check{V} := \mathrm{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p)$ is isomorphic to G. What is the dimension of the $\mathbb{F}_p$-vector space $\check{V}$? Does G admit a countably generated dense subgroup?
(d) Let G be a topological group. Prove the following assertions from first principles. (i) For each $g \in G$, the maps $x \mapsto xg$, $x \mapsto gx$ and $x \mapsto x^g$ are homeomorphisms of G. (ii) If H is a subgroup of G and H is closed (respectively open), then every coset of H in G is closed (respectively open). (iii) Every open subgroup of G is closed. (iv) If H is a subgroup of G, then its closure $\mathrm{cl}(H)$ is also a subgroup of G. (v) If H is a subgroup of G and H contains a non-empty open subset of G, then H is open in G. (vi) The group G is Hausdorff if and only if $\{1\}$ is a closed subset of G. (*Hint:* To see that the condition is sufficient consider $x, y \in G$ with $x^{-1}y \neq 1$. In order to find disjoint open neighbourhoods of x and y, look at a suitable open neighbourhood of $(1, 1)$ in $G \times G$ which is fully contained in the preimage of $G \setminus \{x^{-1}y\}$ under the continuous map $(g, h) \mapsto g^{-1}h$.) (v) If N is a closed normal subgroup of G and G is Hausdorff, then G/N is Hausdorff with respect to the quotient topology.
(e) Show that $\mathrm{GL}_2(\mathbb{Q}_p)$, viewed as a topological group with respect to the natural topology, is totally-disconnected, locally-compact and Hausdorff. Prove that $\mathrm{GL}_2(\mathbb{Z}_p)$ is an open compact subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$.
Is $\mathrm{GL}_2(\mathbb{Z})$ a dense subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$? (*Hint:* Try to reduce a given matrix to the identity matrix modulo p^n by elementary row and column operations.) If not, determine the closure of $\mathrm{GL}_2(\mathbb{Z})$ in $\mathrm{GL}_2(\mathbb{Z}_p)$.

5. Second Lecture

5.1. **Powerful finite p-groups.** The theory of finite p-groups and, more generally, pro-p groups is very much governed by the interplay between commutators and pth powers. In some sense it is the right mixture of the two concepts that makes p-adic Lie groups work the way they do. An important class of finite p-groups, defined in terms of this interconnection, is the class of powerful finite p-groups, which was introduced by Mann, and developed by him and Lubotzky in the 1980s.[5]

Let G be a finite p-group. The group G is *powerful* if p is odd and G/G^p is abelian, or if $p = 2$ and G/G^4 is abelian. More generally, a subgroup $N \leq G$ is *powerfully embedded* in G if p is odd and $[N, G] \subseteq N^p$, or $p = 2$ and $[N, G] \subseteq N^4$.

Thus G is powerful if and only if it is powerfully embedded in itself; and if N is powerfully embedded in G, then $N \trianglelefteq G$ and N is powerful. When p is odd, G is powerful if and only if $\Phi(G) = G^p$; for $p = 2$ the equation $\Phi(G) = G^2$ always holds. Clearly, every abelian finite p-group is powerful, and one should think of 'powerful' as a generalisation of 'abelian'.

Proposition 5.1. *If G is a finite p-group and N is powerfully embedded in G, then N^p is powerfully embedded in G.*

Sketch of proof for $p > 2$. Let G be a finite p-group and let $N \leq G$ with $[N, G] \subseteq N^p$. It suffices to show that $[N^p, G] \subseteq [N, G]^p$. Passing to the quotient $G/[N, G]^p$, if necessary, we may assume that $[N, G]^p = 1$. Since G is nilpotent, we have $[K, G] \lneqq K$ for every non-trivial normal subgroup $K \trianglelefteq G$. Hence we may further assume that $[[N^p, G], G] = 1$. This implies that $[[N, G], G] \subseteq \mathrm{Z}(G)$.

Let $x \in N$ and $g \in G$. Then $[[x, g], x^i] \in \mathrm{Z}(G)$ for $i \in \{0, \ldots, p-1\}$, and

$$\prod_{i=0}^{p-1} [[x, g], x^i] = \prod_{i=0}^{p-1} [[x, g], x]^i = [[x, g], x]^{p(p-1)/2}.$$

Since p is odd and $[N, G]^p = 1$, this shows that

$$\begin{aligned} [x^p, g] &= [x, g]^{x^{p-1}} \cdot [x, g]^{x^{p-2}} \cdots [x, g] \\ &= [x, g] \, [[x, g], x^{p-1}] \cdot [x, g] \, [[x, g], x^{p-2}] \cdots [x, g] \\ &= [x, g]^p \prod_{i=0}^{p-1} [[x, g], x^i] \\ &= [x, g]^p \, [[x, g], x]^{p(p-1)/2} = 1. \end{aligned}$$

Hence $[N^p, G] = 1$, as wanted. □

The *lower p-series* of a group G is the descending series

$$G = P_1(G) \geq P_2(G) \geq \ldots, \quad \text{where } P_{i+1}(G) = P_i(G)^p [P_i(G), G].$$

A basic property of this sequence is that $[P_i(G), P_j(G)] \subseteq P_{i+j}(G)$ for all $i, j \in \mathbb{N}$. Now suppose that G is a finite p-group. Then $P_2(G) = \Phi(G)$ and, more generally,

[5] Another more classical class of finite p-groups, which is defined in terms of commutators and pth powers, comprises the regular p-groups, introduced by Hall in the 1930s. A finite p-group G is *regular* if for all $x, y \in G$ one has $(xy)^p \equiv x^p y^p$ modulo $\gamma_2(\langle x, y \rangle)^p$.

$P_{i+1}(G) \supseteq \Phi(P_i(G))$ for all i. The lower p-series of a powerful finite p-group behaves rather well.

Proposition 5.2. *Let $G = \langle a_1, \ldots, a_d \rangle$ be a powerful finite p-group. Writing $G_i := P_i(G)$ for $i \in \mathbb{N}$, the following assertions hold,*

(1) *G_i is powerfully embedded in G;*
(2) *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ for each $k \in \mathbb{N}$, and in particular $G_{i+1} = \Phi(G_i)$;*
(3) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle$;*
(4) *the map $x \mapsto x^{p^k}$ induces a homomorphism from G_i/G_{i+1} onto G_{i+k}/G_{i+k+1} for each $k \in \mathbb{N}$.*

Corollary 5.3. *If $G = \langle a_1, \ldots, a_d \rangle$ is a powerful finite p-group, then G decomposes as a product of its cyclic subgroups $\langle a_i \rangle$, i.e. $G = \langle a_1 \rangle \cdots \langle a_d \rangle$.*

Sketch of proof for $p > 2$. The assertions of the proposition and the corollary are established by induction, based on Proposition 5.1. As examples we give the proofs of parts (1) and (4).

(1) Since $G_1 = G$ is powerful, the group G_1 is powerfully embedded in G. Suppose that $i \geq 2$. By induction, G_{i-1} is powerfully embedded in G. Then $G_i = G_{i-1}^p[G_{i-1}, G] = G_{i-1}^p$, and Proposition 5.1 shows that G_i is powerfully embedded in G.

(4) Clearly, it suffices to consider the case $k = 1$. The argument above shows that G_i is powerful, $G_{i+1} = P_2(G_i) = G_i^p$ and $G_{i+2} = P_3(G_i)$. Changing notation, we may assume that $i = 1$. Furthermore, passing from G to G/G_3 we may assume that $G_3 = 1$ so that $[G, G] \subseteq G_2 \subseteq \mathrm{Z}(G)$ and $[G, G]^p \subseteq G_2^p \subseteq G_3 = 1$. As p is odd, we have for all $x, y \in G$,

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

Thus the map $x \mapsto x^p$ induces a homomorphism from G/G_2 onto G_2/G_3. □

For any group G let $d(G)$ denote the minimal cardinality of a generating set for G. The *rank* of a finite group G is defined to be $\mathrm{rk}(G) := \max\{d(H) \mid H \leq G\}$. If G is a finite p-group, then $d(G)$ is simply the dimension of $G/\Phi(G)$ as a vector space over $\mathbb{F}_p$, but there is no comparable general description of the more subtle invariant $\mathrm{rk}(G)$.

Theorem 5.4. *Let G be a powerful finite p-group. Then $\mathrm{rk}(G) = d(G)$, in other words $d(H) \leq d(G)$ for all $H \leq G$.*

Proof (by induction on $|G|$). Let $H \leq G$ and put $d := d(G)$. Write $G_i := P_i(G)$ for $i \in \mathbb{N}$, and put $d_2 := d(G_2)$. Proposition 5.2 shows that G_2 is powerful, hence by induction the group $K := H \cap G_2$ satisfies $d(K) \leq d_2$. Put $e := d(HG_2/G_2) \leq d$. Our aim is to find $h_1, \ldots, h_e \in H$ and $y_1, \ldots, y_{d-e} \in K$ such that

$$HG_2 = \langle h_1, \ldots, h_e \rangle G_2 \qquad \text{and} \qquad K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e} \rangle.$$

This will imply $H = \langle h_1, \ldots, h_e, y_1, \ldots, y_{d-e} \rangle$ and $d(H) \leq d$, as wanted.

According to Proposition 5.2, the map $x \mapsto x^p$ induces a homomorphism π from G/G_2 onto G_2/G_3. Both groups are elementary p-groups, so we may regard them

as vector spaces over $\mathbb{F}_p$. Basic linear algebra allows us to bound the dimension of the image $(HG_2/G_2)\pi$ over $\mathbb{F}_p$:

$$\begin{aligned}\dim((HG_2/G_2)\pi) &= \dim(HG_2/G_2) - \dim(\ker\pi \cap HG_2/G_2)\\ &\geq \dim(HG_2/G_2) - \dim(\ker\pi)\\ &= \dim(HG_2/G_2) - (\dim(G/G_2) - \dim(G_2/G_3)\\ &= e - (d - d_2)\\ &= d_2 - (d - e).\end{aligned}$$

Let $h_1, \ldots, h_e \in H$ such that $HG_2 = \langle h_1, \ldots, h_e\rangle G_2$. Observe that $\Phi(K) \subseteq \Phi(G_2) = G_3$. Hence the subspace of $K/\Phi(K)$ spanned by the cosets of $h_1^p, \ldots, h_e^p$ has dimension at least $\dim((HG_2/G_2)\pi) \geq d_2 - (d - e)$. Since $\dim(K/\Phi(K)) = d(K) \leq d_2$, we find $d - e$ elements $y_1, \ldots, y_{d-e} \in K$ such that

$$K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e}\rangle\Phi(K) = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e}\rangle.$$

□

The naive converse of the theorem is false, but a more complex statement is true: every finite p-group admits a powerful normal subgroup of index bounded by a function of $\mathrm{rk}(G)$.

Theorem 5.5. *Let G be a non-trivial finite p-group of rank $r := \mathrm{rk}(G)$, and write $\lambda(r) := \lceil \log_2(r)\rceil$ if p is odd, $\lambda(r) := \lceil \log_2(r)\rceil + 1$ if $p = 2$. Then G admits a powerful characteristic subgroup of index at most $p^{r\lambda(r)}$.*

This result can be see as an invitation into the world of pro-p groups. Indeed, it can be translated to characterise pro-p groups of finite rank as virtually powerful pro-p groups; see Section 5.7. Pro-p groups are special kinds of profinite groups, and we shall not delay their introduction any longer.

5.2. **Profinite groups as Galois groups.** The fundamental theorem of Galois theory sets up a correspondence between the intermediate fields of a finite Galois extension $L|K$ and the subgroups of the associated Galois group $G(L|K)$. In fact, it generalises to infinite Galois extensions, with an interesting twist.

Consider a general Galois extension $L|K$, i.e. a separable splitting field L for a (possibly infinite) family of polynomials over a ground field K. Then L is the union $L = \bigcup\{L_i \mid i \in I\}$ of its finite Galois subextensions $L_i|K$. The set $\{L_i \mid i \in I\}$ is partially ordered by the inclusion relation. It has the property that for all L_i, L_j there exists L_k such that $L_k \supseteq L_i$ and $L_k \supseteq L_j$; just think in terms of splitting fields. Writing $i \succeq j$ whenever $L_i \supseteq L_j$, the last observation can be stated as follows: for all $i, j \in I$ there exists $k \in I$ such that $k \succeq i$ and $k \succeq j$.

The Galois group $G(L|K)$ is, of course, defined as the group of all automorphisms of L which fix K element-wise. Every automorphism $\alpha \in G(L|K)$ is uniquely determined by its restrictions $\alpha|_{L_i}$, $i \in I$, and the normality of $L|K$ and its subextensions $L_i|K$ guarantees that each of the restriction maps $\varphi_i : G(L|K) \to G(L_i|K)$ is onto. Clearly, there is a certain compatibility condition that the restrictions of α to the various L_i satisfy, namely $(\alpha|_{L_i})|_{L_j} = \alpha|_{L_j}$ whenever $L_i \supseteq L_j$. Writing $\varphi_{ij} : G(L_i|K) \to G(L_j|K)$ for the natural restriction map whenever $L_i \supseteq L_j$, the compatibility condition can be rephrased as: $\varphi_i\varphi_{ij} = \varphi_j$

whenever $i \succeq j$. A similar conditions in terms of the restrictions alone can be stated as: $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ whenever $i \succeq j \succeq k$.

We are now ready to describe the Galois group $G := G(L|K)$. Writing $G_i := G(L_i|K)$, the coordinate map

$$\varphi : G \to \prod\nolimits_{i\in I} G_i, \quad g \mapsto (g\varphi_i)_{i\in I}$$

induces an isomorphism from G onto the group

$$G\varphi = \left\{ (g_i)_{i\in I} \in \prod\nolimits_{i\in I} G_i \mid g_i\varphi_{ij} = g_j \text{ whenever } i \succeq j \right\}.$$

But what happens to the Galois correspondence? It turns out that only certain subgroups of G correspond to intermediate fields of $L|K$. To describe why this is so and which subgroups play a role in the Galois correspondence we equip G with the *Krull topology*. Regarding each of the finite Galois groups G_i as a discrete topological group, the product $\prod_{i\in I} G_i$ naturally becomes a topological group which is totally-disconnected, compact and Hausdorff. The subgroup $G\varphi$ is easily seen to be closed, so its isomorphic twin G becomes a totally-disconnected, compact, Hausdorff topological group. We have seen how the structure of G is determined by its finite images G_i. In Section 5.3 we will formalise this process to see that G is the inverse (or projective) limit of the inverse system $(G_i; \varphi_{i,j})$ of finite groups, and thus G becomes a profinite group.

If M is an intermediate field of the extension $L|K$ then the set G^M of all $g \in G$ which fix M element-wise can be described in terms of the restrictions of automorphisms to (the normal closures of) finite subextensions of M. Indeed, G^M can be written as the intersection of closed open subgroups of G and thus forms a closed subgroup with respect to the Krull topology. The Galois correspondence for finite Galois extensions then readily generalises to yield

Theorem 5.6 (Fundamental theorem of Galois theory)**.** *The Galois group G of a (typically infinite) Galois extension $L|K$ is a profinite group with respect to the Krull topology. There is an inclusion-reversing correspondence between the lattice of all closed subgroups of G and the lattice of all intermediate fields of $L|K$.*

It can be shown that every profinite group is isomorphic to the Galois group of a suitable Galois extension. One of the fundamental problems in number theory is to describe the finite extensions of a given local field K, such as $K = \mathbb{Q}_p$. This is equivalent to understanding the absolute Galois group $G(\overline{K}|K)$, where $\overline{K}$ denotes the separable closure of K. Local class field theory provides a rather explicit and very satisfying description of all abelian extensions, i.e. Galois extensions with abelian Galois groups: the lattice of abelian extensions of the local field K has a precise reflection in the multiplicative group K^* via the norm residue symbol. In 1982 Jannsen and Wingberg gave a description of the full Galois group $G(\overline{K}|K)$ of a local field of characteristic 0 in terms of generators and relations. A quite different and far-reaching approach is described by the Langlands Conjectures.

5.3. **Profinite groups as inverse limits.** The description of Galois groups in terms of their finite factors can be formalised as follows. A *directed set* is a partially ordered set $I = (I, \preceq)$ such that for all $i, j \in I$ there exists $k \in I$ such that $k \succeq i$ and $k \succeq j$. An *inverse system* $(G_i; \varphi_{ij})$ of groups (or other mathematical structures

such as sets, rings, topological spaces, etc.) over I consists of a family of groups (or sets, ...) G_i, $i \in I$, and homomorphisms (or maps, ...) $\varphi_{ij} : G_i \to G_j$ whenever $i \succeq j$, satisfying the natural compatibility conditions

$$\varphi_{ii} = \mathrm{id}_{G_i} \quad \text{and} \quad \varphi_{ij}\varphi_{jk} = \varphi_{ik} \quad \text{for all } i, j, k \in I \text{ with } i \succeq j \succeq k.$$

The *inverse limit* of the inverse system $(G_i; \varphi_{ij})$ is the group (or set, ...)

$$\varprojlim G_i := \Big\{ (g_i)_{i \in I} \in \prod\nolimits_{i \in I} G_i \mid g_i \varphi_{ij} = g_j \text{ whenever } i \succeq j \Big\}$$

together with the natural coordinate maps $\varphi_i : G \to G_i$. It is the (unique) solution to an appropriate universal problem; see Exercise 6.3. In the special, but important case where $I = \mathbb{N}$ and $\preceq$ is the ordinary order-relation $\leq$ we can think of the inverse limit pictorially as the 'limit object' to a chain of homomorphisms

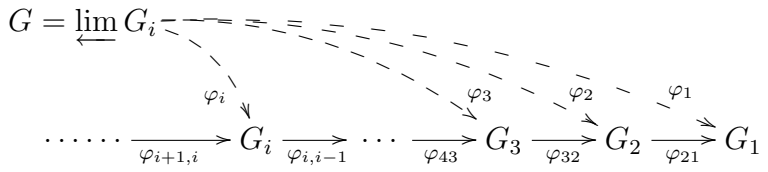

FIGURE 2. Pictorial description of the inverse limit G of an inverse system $(G_i; \varphi_{ij})$ of groups (or sets, ...).

If the G_i are finite groups, we give each of them the discrete topology, and $\prod_{i \in I} G_i$ the product topology. Then $\varprojlim G_i$ with the induced topology becomes a totally-disconnected, compact, Hausdorff topological group. Such a group is known as a *profinite group*, which is short for projective limit of finite groups.

Every finite group is a profinite group. As we have seen in the previous subsection natural examples of infinite profinite groups are given by Galois groups. The simplest such is perhaps the absolute Galois group $G(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ of a finite field $\mathbb{F}_q$. From field theory we know that $\mathbb{F}_q$ has precisely one extension of any given finite degree and that all these extensions are Galois with cyclic Galois group. The corresponding inverse system consists of the cyclic groups $G_n \cong \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, with φ_{mn} given by the natural projections $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ whenever $n \mid m$. The inverse limit of this inverse system is the procyclic group $\hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$.

In fact, $\hat{\mathbb{Z}}$ can be regarded as a profinite ring, simply by going through the same construction, considering each $\mathbb{Z}/n\mathbb{Z}$ not simply as a group but as a ring. There is an interesting connection between $\hat{\mathbb{Z}}$ and the rings of p-adic integers: $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ as topological rings; see Exercise 6.1.

5.4. **Profinite groups as profinite completions.** An impressively fruitful theme in infinite group theory builds upon the following unassuming question: how do the finite images of an infinite group affect its structure? A group G is *residually finite* if the intersection of all its finite-index subgroups is trivial. Residually finite groups are the groups whose structure one can hope to understand in terms of finite images, and they form quite a large class. For instance, every finitely generated linear group is residually finite.

Let Γ be any group. It is convenient to use the notation $H \leq_{\mathrm{f}} \Gamma$ to indicate that H is a subgroup of finite index in Γ. Note that the finite quotients of Γ form a natural inverse system Γ/N, $N \trianglelefteq_{\mathrm{f}} \Gamma$, with φ_{MN} given by the natural projection $\Gamma/M \to \Gamma/N$ whenever $M \subseteq N$. The inverse limit of this inverse system is the *profinite completion* $\hat{\Gamma} := \varprojlim \Gamma/N$ of Γ. There is a natural map from the original group into its profinite completion, namely

$$\vartheta : \Gamma \to \hat{\Gamma}, \quad g \mapsto (gN)_{N \trianglelefteq_{\mathrm{f}} \Gamma}.$$

If Γ is residually-finite, then ϑ is injective. Typically, $\Gamma\vartheta$ is strictly contained in $\hat{\Gamma}$, but it always forms a dense subgroup. The notation $\hat{\mathbb{Z}}$ is no coincidence: the procyclic group $\hat{\mathbb{Z}}$ can be regarded as the profinite completion of the infinite cyclic group.

5.5. **Profinite groups as topological groups.** Profinite groups are topological groups which are totally-disconnected, compact and Hausdorff. Indeed, it can be shown that the converse holds. But for our purposes the following characterisation is perhaps more useful: a profinite group is a compact Hausdorff topological group G such that every open neighbourhood of the neutral element 1 contains an open subgroup. This means that the open subsets of a profinite group G are precisely those sets which can be written as unions of cosets gN of open normal subgroups $N \trianglelefteq_{\mathrm{o}} G$.

Profinite groups are typically quite large, i.e. uncountable, and therefore rather unwieldy as abstract groups. But our interest is mainly focused on closed subgroups. So group theoretic notions and constructions should be employed with a topological twist. Often it is agreed implicitly that this approach is being taken.

For instance, let G be a profinite group and $X \subseteq G$. Then X is said to *generate* G (topologically) if X generates a dense subgroup of G. Accordingly, G is *finitely generated* (as a topological group), if it admits a finite (topological) generating set. We denote by $d(G)$ the minimal cardinality of a (topological) generating set for G. In order to check whether a given subset X generates a profinite group G, it suffices to show that X generates G modulo every open normal subgroup $N \trianglelefteq_{\mathrm{o}} G$; see Exercise 6.3. Thus one has $d(G) = \sup\{d(G/N) \mid N \trianglelefteq_{\mathrm{o}} G\}$.

The *Frattini subgroup* $\Phi(G)$ of a profinite group G is the intersection of all maximal proper open subgroups of G. Since every open subgroup is closed, it follows that $\Phi(G)$ is a closed subgroup of G. Furthermore, one can show that $X \subseteq G$ generates G if and only if X generates G modulo $\Phi(G)$.

Every open subgroup of a profinite group G has finite index in G. A recent theorem of Nikolov and Segal, relying on the classification of finite simple groups, states that in a finitely generated profinite group G every finite-index subgroup is open; see Exercise 6.5. So in the case of finitely generated profinite groups, the topology is uniquely determined by the algebraic structure of the group.

5.6. **Pro-p groups.** A *pro-p group* is a topological group which is isomorphic to the inverse limit of finite p-groups. Every group Γ admits a *pro-p completion* $\hat{\Gamma}_p$, which is the pro-p group arising from the inverse system of finite quotients Γ/N where N runs through all normal subgroups of p-power index in Γ.

Let G be a pro-p group. Then every closed subgroup of G is a pro-p group and any quotient of G by a closed normal subgroup is a pro-p group. In particular,

the index of any open subgroup of G is a power of p; see Exercise 6.5. The Frattini subgroup of G is equal to the closure of the abstract Frattini subgroup, i.e. $\Phi(G) = \mathrm{cl}(G^p[G,G])$. In particular, one has $d(G) = \dim_{\mathbb{F}_p} G/\Phi(G)$.

The category of pro-p groups is quite large. Our main focus will be on the class of pro-p groups of finite rank (which are the same as p-adic analytic pro-p groups), but we give a variety of examples.

(1) The additive group of p-adic integers $\mathbb{Z}_p$ is the most basic infinite pro-p group. It plays a similar role as the infinite cyclic group in abstract group theory; see Exercise 6.1.
(2) The Sylow theorems for finite groups carry over to profinite groups: every pro-p subgroup of a profinite group G is contained in a maximal pro-p subgroup, and any two maximal pro-p subgroups of G are conjugate in G; see Exercise 6.4. Maximal pro-p subgroups of G are called *Sylow pro-p subgroups*.
(3) Matrix groups over $\mathbb{Z}_p$ are virtually pro-p groups; see Exercise 6.2. According to Lazard, they constitute the class of compact p-adic Lie groups. Typical examples of p-adic analytic pro-p groups are the Sylow pro-p subgroups of $\mathrm{GL}_d(\mathbb{Z}_p)$.
(4) Let $d \in \mathbb{N}$ and F a free group on d generators. Then the pro-p completion $\hat{F}_p$, known as a *free pro-p group*, can be seen to be a free object (on d generators) in the category of pro-p groups.
(5) The *Nottingham group* over $\mathbb{F}_p$, which was introduced in Exercise 4.3 is a finitely generated pro-p group. It is virtually isomorphic to the automorphism group of a local field of characteristic p. The Nottingham group has remarkable properties, e.g. it can be shown that every finitely generated pro-p group embeds into it as a closed subgroup.

Next we return our attention to the concept of powerful groups, which we introduced in Section 5.1.

5.7. **Powerful pro-p groups.** Let G be a pro-p group. The group G is *powerful* if p is odd and $G/\mathrm{cl}(G^p)$ is abelian, or if $p = 2$ and $G/\mathrm{cl}(G^4)$ is abelian. More generally, a subgroup $N \leq_{\mathrm{c}} G$ is *powerfully embedded* in G if p is odd and $[N,G] \subseteq \mathrm{cl}(N^p)$, or $p = 2$ and $[N,G] \subseteq \mathrm{cl}(N^4)$. Thus G is powerful if and only if G is powerfully embedded in itself; and if N is powerfully embedded in G, then $N \trianglelefteq_{\mathrm{c}} G$ and N is powerful.

The *lower p-series* of a topological group G is the descending series

$$G = P_1(G) \geq P_2(G) \geq \ldots, \quad \text{where } P_{i+1}(G) = \mathrm{cl}(P_i(G)^p[P_i(G),G]).$$

A basic property of this sequence is that $[P_i(G), P_j(G)] \subseteq P_{i+j}(G)$ for all $i,j \in \mathbb{N}$. Proposition 5.2 easily translates into

Proposition 5.7. *Let $G = \mathrm{cl}\langle a_1, \ldots, a_d\rangle$ be a finitely generated powerful pro-p group. Writing $G_i := P_i(G)$ for $i \in \mathbb{N}$, the following assertions hold,*

(1) *G_i is powerfully embedded in G;*
(2) *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ for each $k \in \mathbb{N}$, and in particular $G_{i+1} = \Phi(G_i)$;*
(3) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \mathrm{cl}\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}}\rangle$;*
(4) *the map $x \mapsto x^{p^k}$ induces a homomorphism from G_i/G_{i+1} onto G_{i+k}/G_{i+k+1} for each $k \in \mathbb{N}$.*

Corollary 5.8. *If $G = \langle a_1, \dots, a_d \rangle$ is a powerful pro-p group, then G decomposes as a product of its procyclic subgroups $\mathrm{cl}\langle a_i \rangle$, i.e. $G = \mathrm{cl}\langle a_1 \rangle \cdots \mathrm{cl}\langle a_d \rangle$.*

The *rank* of a profinite group G is defined to be $\mathrm{rk}(G) := \sup\{d(H) \mid H \leq_{\mathrm{o}} G\}$. It can be shown that

$$\mathrm{rk}(G) = \sup\{d(H) \mid H \leq_{\mathrm{c}} G\} = \sup\{\mathrm{rk}(G/N) \mid N \trianglelefteq_{\mathrm{o}} G\};$$

see Exercise 6.3. Theorems 5.4 and 5.5 translate readily into

Theorem 5.9 (Characterisation of pro-p groups of finite rank)**.** *A pro-p group has finite rank if and only if it is finitely generated and virtually powerful.*

Moreover, if G is a finitely generated powerful pro-p group, then $\mathrm{rk}(G) = d(G)$.

The detailed proof of Theorem 5.5 also yields the following interesting 'local' description of pro-p groups of finite rank.

Theorem 5.10. *Let G be a pro-p group and $r \in \mathbb{N}$. If every open subgroup of G contains an open normal subgroup $N \trianglelefteq_{\mathrm{o}} G$ with $d(N) \leq r$, then G has finite rank.*

5.8. **Pro-p groups of finite rank – summary of characterisations.** There is a variety of other characterisations of the class of pro-p groups of finite rank. For instance, a pro-p group has finite rank if and only if it has polynomial subgroup growth; see Exercise 6.6. Considerably deeper, but most interesting is the result that a pro-p group has finite rank if and only if it admits the structure of a p-adic Lie group. By way of a short summary we record

Theorem 5.11 (Pro-p groups of finite rank – summary of characterisations)**.** *Let G be a pro-p group. Then each of the following conditions is necessary and sufficient for G to have finite rank:*

(1) *G is finitely generated and virtually powerful;*
(2) *there exists $r \in \mathbb{N}$ such that every open subgroup of G contains an open normal subgroup $N \trianglelefteq_{\mathrm{o}} G$ with $d(N) \leq r$;*
(3) *G has polynomial subgroup growth;*
(4) *G is isomorphic to a closed subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for suitable $d \in \mathbb{N}$;*
(5) *G is a p-adic analytic group.*

We conclude this section by stating an intriguing problem which aims at yet another interesting characterisation of pro-p groups of finite rank. A profinite group G is said to be *noetherian* if it satisfies the ascending chain condition on closed subgroups.[6] It is easily seen that a pro-p group G is noetherian if and only if every closed subgroup of G is finitely generated. Consequently, every pro-p group of finite rank is noetherian. In fact, if G is a pro-p group of finite rank, then there is a uniform bound on the lengths of chains of closed subgroups $1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$ with $|G_i : G_{i-1}| = \infty$ for all $i \in \{1, \dots, n\}$. This bound is given by the dimension of G; see Section 7.1.

The following rather natural problem, which was posed by Lubotzky and Mann, has been open for twenty years.

Problem. *Does every noetherian pro-p group have finite rank?*

[6] In point-set topology it is customary to call a topological space noetherian if it satisfies the ascending chain condition on open subsets, but this notion is of little use in the context of profinite groups: a non-discrete profinite group never satisfies the ascending chain condition on open subsets. This should be contrasted with the observation that every profinite group satisfies trivially the ascending chain condition on open subgroups.

6. Second set of exercises

Exercise 6.1 (Procyclic groups and p-adic exponentiation)**.**
(a) Recall that $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ is the profinite completion of $\mathbb{Z}$. Show that the ring $\mathbb{Z}_p$ of p-adic integers is isomorphic to the pro-p completion of the ring $\mathbb{Z}$.
(b) Show that the profinite ring $\hat{\mathbb{Z}}$ decomposes as $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.
(c) The profinite topology on $\mathbb{Z}$ is the topology whose open sets are the unions of cosets $a + b\mathbb{Z}$ with $a, b \in \mathbb{Z}$ and $b \neq 0$. Show that this agrees with the subspace topology coming from the inclusion $\mathbb{Z} \subseteq \hat{\mathbb{Z}}$. Note that every non-empty open subset of $\mathbb{Z}$ is infinite. Deduce from the equation $\{1, -1\} = \mathbb{Z} \setminus \bigcup\{p\mathbb{Z} \mid p \text{ prime}\}$ that there are infinitely many primes.
(d) Let G be a pro-p group. Let $g \in G$ and $\lambda = \sum_{k=0}^{\infty} a_k p^k \in \mathbb{Z}_p$. Write $\lambda_n := \sum_{k=0}^{n} a_k p^k$ to denote the partial sums, and show that the limit $\lim_{n\to\infty} g^{\lambda_n}$ exists. Denote this limit by g^λ, the *λth power* of g.
Let $g, h \in G$ and $\lambda, \mu \in \mathbb{Z}_p$. Convince yourself that p-adic exponentiation satisfies the common rules $g^{\lambda+\mu} = g^\lambda g^\mu$ and $g^{\lambda\mu} = (g^\lambda)^\mu$. Find a sufficient condition under which the equation $(gh)^\lambda = g^\lambda h^\lambda$ holds.
(e) Let G be a pro-p group and $g \in G$. Prove that p-adic exponentiation provides a surjective homomorphism $\mathbb{Z}_p \to \mathrm{cl}\langle g\rangle$, $\lambda \mapsto g^\lambda$.
Remark: A profinite group which is (topologically) generated by one element is called a *procyclic group*.
(f) Prove that a procyclic pro-p group is either finite and cyclic or isomorphic to $\mathbb{Z}_p$. Show more generally that a finitely generated abelian pro-p group G is isomorphic to $\mathbb{Z}_p^d \times F$ for some $d \in \mathbb{N}_0$ and a finite abelian p-group F. (*Hint:* Regard G as a finitely generated $\mathbb{Z}_p$-module.)

Exercise 6.2 (Explicit examples of pro-p groups)**.**
(a) Let $d \in \mathbb{N}$. Prove that $\mathrm{GL}_d(\mathbb{Z}_p)$ is virtually a pro-p group. Can you guess a candidate for an open powerful pro-p subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$? (*Hint:* Consider the first congruence subgroup $\mathrm{GL}_d^1(\mathbb{Z}_p) = \{g \in \mathrm{GL}_d(\mathbb{Z}_p) \mid g \equiv 1 \pmod p\}$.)
(b) The Heisenberg group over $\mathbb{Z}_p$ is the group of upper uni-triangular 3×3 matrices over $\mathbb{Z}_p$. Work out the lower p-series of this group. Is it a powerful pro-p group? If not, is it of finite rank?
(c) Suppose that $p > 2$. Consider the Nottingham group G over $\mathbb{F}_p$, which was introduced in Exercise 4.3. Convince yourself that G is a topological group with respect to the subspace topology, inherited from $\mathbb{F}_p[\![t]\!]$. Show that G is a two-generated pro-p group. Is it powerful? If not, is it of finite rank? (*Hint:* Consider the abelianisations of its natural subgroups $G_n := \{\mathbf{a} \in G \mid \mathbf{a} \equiv t \mod t^{n+1}\}$.)
(d) Construct surjective homomorphisms from $C_p \wr C_{p^{n+1}}$ onto $C_p \wr C_{p^n}$ for all $n \in \mathbb{N}$. (*Hint:* Realise $C_p \wr C_{p^n}$ as the semidirect product of $\mathbb{F}_p[X]/(X^{p^n} - 1)$ by $\langle x\rangle \cong C_{p^n}$, with x acting as multiplication by X. Then convince yourself that there is a natural projection $\mathbb{F}_p[X]/(X^{p^{n+1}} - 1) \to \mathbb{F}_p[X]/(X^{p^n} - 1)$.) Set up a corresponding inverse system and take the inverse limit. The resulting group is the pro-p wreath product $C_p \hat{\wr} \mathbb{Z}_p$. Show that this group is two-generated but has infinite rank.
Remark: In a loose sense, $C_p \hat{\wr} \mathbb{Z}_p$ can be regarded as the smallest pro-p group which is not p-adic analytic.

Exercise 6.3 (Profinite groups: generating sets, universal property, rank)**.**
(a) Let G be a profinite group and $X \subseteq G$. Show that $\mathrm{cl}(X) = \bigcap\{XN \mid N \trianglelefteq_{\mathrm{o}} G\}$. Deduce that X generates G if and only if X generates G modulo every open normal subgroup $N \trianglelefteq_{\mathrm{o}} G$.
(b) Prove that every open subgroup of a finitely generated profinite group is finitely generated. (*Hint:* Use the corresponding result for abstract groups, namely: every finite-index subgroup of a finitely generated group is finitely generated.)
(c) Let $(G_i; \varphi_{ij})$ be an inverse system of groups based on a directed set I. Let $G = \varprojlim G_i$, and let $\varphi_i : G \to G_i$ denote the ith coordinate map. Show that $(G; \varphi_i)$ is characterised by the following universal property: given a group H and homomorphisms $\vartheta_i : H \to G_i$, $i \in I$, such that $\vartheta_i \varphi_{ij} = \vartheta_j$ whenever $i \succeq j$, there is a unique homomorphism $\vartheta : H \to G$ such that $\vartheta_i = \vartheta \varphi_i$ for all $i \in I$. (*Hint:* Start by drawing a corresponding diagram.)
(d) Convince yourself that every profinite group G is isomorphic to the inverse limit $\varprojlim G/N$ of its (continuous) finite quotients G/N, $N \trianglelefteq_{\mathrm{o}} G$.
(e) Let G be a profinite group. Prove that $\mathrm{rk}(G) = \sup\{d(H) \mid H \leq_{\mathrm{c}} G\} = \sup\{\mathrm{rk}(G/N) \mid N \trianglelefteq_{\mathrm{o}} G\}$. For $N \trianglelefteq_{\mathrm{c}} G$ show that $\max\{\mathrm{rk}(N), \mathrm{rk}(G/N)\} \leq \mathrm{rk}(G) \leq \mathrm{rk}(N) + \mathrm{rk}(G/N)$. Deduce that, if G has an open subgroup of finite rank, then G itself has finite rank.

Exercise 6.4 (Profinite groups: Sylow theory and finite images)**.**
(a) Deduce from Tychonoff's Theorem the following set-theoretical principle which frequently allows one to deduce properties of a profinite group from properties of its finite quotients: the inverse limit $\varprojlim X_i$ of an inverse system of non-empty finite sets X_i, $i \in I$, is non-empty. (*Hint:* Enforce the compatibility conditions in finite portions.)
(b) Let G be a profinite group. A *Sylow pro-p subgroup* of G is a maximal pro-p subgroup. Deduce from the Sylow theorems for finite groups that (i) every pro-p subgroup of G is contained in a Sylow pro-p subgroup and that (ii) any two Sylow pro-p subgroups of G are conjugate. (*Hint:* Use part (a) and take advantage of the fact that a profinite group is a pro-p group if and only if all its open subgroups have p-power index; see Exercise 6.5.)
(c) Prove that two finitely generated profinite groups are isomorphic if and only if they have the same class of finite groups as their finite (continuous) homomorphic images. (*Hint:* Set up a suitable inverse system of isomorphisms between finite (continuous) quotients of the two groups and use part (a).)
Give an example of two non-isomorphic pro-p groups which have the same class of finite groups as their finite (continuous) homomorphic images.
(d) Let Γ be a group and denote by $G := \varprojlim_{N \trianglelefteq_{\mathrm{f}} \Gamma} \Gamma/N$ its profinite completion. Write $\vartheta : \Gamma \to G$ for the natural homomorphism $g \mapsto (gN)_N$. Show that ϑ induces an isomorphism $\Gamma/N \to G/\mathrm{cl}(N\vartheta)$ for each $N \trianglelefteq_{\mathrm{f}} \Gamma$. Prove that every open subgroup of G is of the form $\mathrm{cl}(H\vartheta)$ where $H \leq_{\mathrm{f}} \Gamma$.
Let Γ and Δ be finitely generated groups. Deduce from part (c) that their profinite completions $\hat{\Gamma}$ and $\hat{\Delta}$ are isomorphic if and only if Γ and Δ have the same class of finite groups as their finite homomorphic images.

Exercise 6.5 (Abstract finite-index subgroups of pro-p groups)**.**
(a) Give an example of a pro-p group admitting finite-index subgroups which are not open. (*Hint:* Your group cannot be finitely generated.)
(b) Let G be a pro-p group and $H \leq_{\mathrm{o}} G$. Show that $|G : H|$ is a power of p. (*Hint:* If $G = \varprojlim G_i$, think of G as subgroup of $\prod G_i$ and use that basic open subgroups of this latter group have p-power index.)
(c) Let G be a pro-p group and $H \leq_{\mathrm{f}} G$. Show that $|G : H|$ is a power of p. (*Hint:* Replacing H by its core in G, you may assume that H is normal in G. Write $|G : H| = m = p^r q$ with $p \nmid q$, and put $X := \{g^m \mid g \in G\}$. Note that $X \subseteq H$ and that X is closed. Let $g \in G$. Show that $g^{p^r} \in XN$ for every $N \trianglelefteq_{\mathrm{o}} G$. From $X = \bigcap\{XN \mid N \trianglelefteq_{\mathrm{o}} G\}$ conclude that $g^{p^r} \in X$. Deduce that $|G : H| = p^r$.)
(d) Let G be a finitely generated pro-p group. Prove that the abstract commutator subgroup $[G, G]$ is closed, using the following fact about (abstract) nilpotent groups: if $\Gamma = \langle a_1, \ldots, a_d\rangle$ is a nilpotent group, then every element of $[\Gamma, \Gamma]$ is equal to a product of the form $[x_1, a_1] \cdots [x_d, a_d]$ with $x_1, \ldots, x_d \in \Gamma$. (*Hint:* Suppose that $G = \mathrm{cl}\langle a_1, \ldots, a_d\rangle$ and consider $X := \{[g_1, a_1] \cdots [g_d, a_d] \mid g_1, \ldots, g_d \in G\}$. Show that X is closed and that $X \equiv [G, G]$ modulo any open normal subgroup of G. Conclude that $[G, G] = X$ is closed.)
(e) Let G be a finitely generated pro-p group. According to part (d), the abstract commutator subgroup $[G, G]$ is closed. Observe that the abstract Frattini subgroup $G^p[G, G]$ can be written as $\{g^p \mid g \in G\}[G, G]$ and hence show that $G^p[G, G]$ is closed. Deduce that $G^p[G, G] = \Phi(G)$.
(f) Let G be a finitely generated pro-p group and $H \leq_{\mathrm{f}} G$. Prove that H is open in G. (*Hint:* It is enough to prove the statement for normal subgroups. Arguing by induction on $|G : H|$, suppose that H is properly contained in G. Since $|G : H|$ is a p-power, $M := H\Phi(G) = HG^p[G, G]$ is a proper open subgroup of G. Note that M is finitely generated and apply induction to find that H is open in M.)

Exercise 6.6 (Pro-p groups with polynomial subgroup growth)**.**
Let G be a finitely generated pro-p group, and for every $n \in \mathbb{N}_0$ let σ_n denote the number of open subgroups of index at most p^n in G. The group G is said to have *polynomial subgroup growth* (PSG) if there exist $c, \alpha \in \mathbb{R}$ such that $\sigma_n \leq cp^{n\alpha}$ for all $n \in \mathbb{N}_0$.
(a) Show that σ_n is finite for every $n \in \mathbb{N}$.
(b) Show that, if G has finite rank, then G has PSG. – The remaining parts of the exercise are concerned with proving the converse.
(c) Let $r \in \mathbb{N}$, and let $N \trianglelefteq_{\mathrm{o}} G$ be maximal with the property $d(N) \geq r$. Show that N is equal to the centraliser of $N/\Phi(N)$ in G. (*Hint:* Write $C := \mathrm{C}_G(N/\Phi(N)) \trianglelefteq_{\mathrm{o}} G$ and assume for a contradiction that $N \subsetneqq C$. Choose an element xN of order p in $C/N \cap \mathrm{Z}(G/N)$ and put $M := \langle x\rangle N \trianglelefteq_{\mathrm{o}} G$. Deduce that $d(M) \geq d(N)$, in contradiction to $N \subsetneqq M$.)
(d) Let V be a vector space of dimension d over $\mathbb{F}_p$. Show that every p-subgroup G of $\mathrm{GL}(V)$ admits a chain of normal subgroups

$$G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{\lambda(d)} \supseteq G_{\lambda(d)+1} = 1$$

of length $\lambda(d) := \lceil \log_2(d) \rceil$ such that the quotients G_i/G_{i+1} of successive terms are elementary abelian. (*Hint:* It suffices to prove that a Sylow p-subgroup of $\mathrm{GL}(V)$ has a chain of normal subgroups of length $\lambda(d)$ such that the quotients

of successive terms are elementary abelian. All Sylow p-subgroups of $\mathrm{GL}(V)$ are isomorphic to the group of upper uni-triangular matrices of degree d over $\mathbb{F}_p$.)
Show that V contains at least $p^{(d-1)^2/4}$ subspaces of codimension $\lfloor d/2 \rfloor$.
(e) Let $r \in \mathbb{N}$, and let $N \trianglelefteq_{\mathrm{o}} G$ be maximal with the property $d := d(N) \geq r$. Show that $|G : N| \leq p^{(r-1)\lambda(d)}$ where $\lambda(d) := \lceil \log_2(d) \rceil$. (*Hint:* By part (c), G/N acts faithfully by conjugation on $N/\Phi(N) \cong \mathbb{F}_p^d$. Note that every normal subgroup of G/N can be generated by $r-1$ elements and use part (d).)
(f) Suppose that G has PSG and let $c, \alpha \in \mathbb{R}$ such that $\sigma_n \leq cp^{n\alpha}$ for all $n \in \mathbb{N}_0$. Show that there is a finite upper bound for the numbers $d(N)$ as N ranges over all open normal subgroups of G. (*Hint:* Let $r \in \mathbb{N}$, and suppose that $N \trianglelefteq_{\mathrm{o}} G$ is maximal with the property $d := d(N) \geq r$. By considering suitable subgroups of $N/\Phi(N)$ derive from parts (d) and (e) that G contains at least $p^{(d-1)^2/4}$ open subgroups of index at most $p^{(r-1)\lambda(d)+\lfloor d/2 \rfloor}$. Use the fact that G has PSG to show that d, and hence r, is bounded above in terms of c and α.)
(g) Deduce from (f) and Theorem 5.10: if G has PSG, then G has finite rank.

7. Third Lecture

7.1. **Uniformly powerful pro-p groups.** A finitely generate torsion-free powerful pro-p group is called a *uniformly powerful pro-p group*, or simply a *uniform pro-p group* for short. This concept and terminology is motivated by the following two results.

Theorem 7.1 (Structure of finitely generated powerful pro-p groups)**.** *Let G be a finitely generated powerful pro-p group. Then the elements of finite order in G form a characteristic subgroup T of G. Moreover, T is a powerful finite p-group and G/T is a uniform pro-p group. In particular, G is virtually uniform.*

Proposition 7.2 (Properties of uniform pro-p groups)**.** *Let G be a finitely generated powerful pro-p group. Then the following are equivalent:*

(1) *G is uniform;*
(2) *for every $i \in \mathbb{N}$ the map $x \mapsto x^p$ induces an isomorphism from $P_i(G)/P_{i+1}(G)$ onto $P_{i+1}(G)/P_{i+2}(G)$;*
(3) *$d(H) = d(G)$ for every powerful open subgroup H of G.*

Let G be a pro-p group of finite rank. Then G contains an open uniform subgroup U. According to Proposition 7.2, the minimal number of generators for U does not depend on the particular choice of U and thus provides a useful invariant of G: the *dimension* of G is defined as $\dim(G) := d(U)$. One can show that

$$\dim(G) = \dim(N) + \dim(G/N) \qquad \text{for } N \trianglelefteq_{\mathrm{c}} G.$$

The algebraically defined dimension of G is, in fact, the same as the dimension of G regarded as a p-adic Lie group. A first indication that G carries the structure of a p-adic analytic manifold is given by

Proposition 7.3 (Multiplicative coordinate systems)**.** *Let U be a uniform pro-p group and $d = d(U)$. Then every minimal generating set $\{a_1, \ldots, a_d\}$ for U yields a homeomorphism*

$$\mathbb{Z}_p^d \to U, \quad (\lambda_1, \ldots, \lambda_d) \mapsto a_1^{\lambda_1} \cdots a_d^{\lambda_d}.$$

This proposition can easily be proved from Proposition 7.2 and Corollary 5.8. The algebraic properties of the multiplicative coordinate systems are, however, not so good. We therefore set out to describe uniform pro-p groups in terms of more useful coordinate systems.

7.2. **Associated additive structure.** Let G be a uniform pro-p group of dimension d, and write $G_n := P_n(G) = G^{p^{n-1}}$ for the terms of the lower p-series of G. Our aim is to define on G the structure of an abelian group isomorphic to $\mathbb{Z}_p^d$. The new addition is to be defined canonically in terms of the original group multiplication and such that the two compositions agree on all abelian subgroups of G.

We take our inspiration from the formal identity

$$\exp(X + Y) = \lim_{n \to \infty} \left(\exp(X/n) \exp(Y/n)\right)^n$$

which holds in the completed free associative algebra $\mathbb{Q}\langle\langle X, Y \rangle\rangle$ and can be traced back to the beginnings of Lie theory. Proposition 7.2 can be used to show that

every element $x \in G_{n+1}$ admits a unique p^nth root in G, which we shall denote by $x^{p^{-n}}$. Moreover, the groups G_n admit larger and larger abelian quotients G_n/G_{2n} as $n \to \infty$. These crucial observations allow us to define the sum of $x, y \in G$ as

$$x + y := \lim_{n\to\infty} (x^{p^n} y^{p^n})^{p^{-n}}.$$

Essentially, we superimpose the groups G_n, by mapping them onto the reference set G, and notice that their composition maps become more and more alike as $n \to \infty$. Careful, but elementary considerations lead to

Theorem 7.4 (Associated additive structure)**.** *Let G be a uniform pro-p group of dimension d, and let $\{a_1, \dots, a_d\}$ be a minimal generating set for G. Then the following hold:*

1. *G with the operation $+$ constitutes a free $\mathbb{Z}_p$-module on the basis $\{a_1, \dots, a_d\}$;*
2. *the operation $+$ agrees with the original multiplication on all abelian subgroups of G;*
3. *the terms of the lower p-series with respect to $+$ are the same as the ones for the original multiplication.*

In particular this implies:

- the neutral element of G with respect to $+$ equals the multiplicative identity element 1;
- inverses with respect to $+$ are the same as multiplicative inverses;
- p-adic exponentiation translates into scalar multiplication, i.e. $x^\lambda = \lambda x$ for all $x \in G$ and $\lambda \in \mathbb{Z}_p$.

A particularly useful consequence of the theorem is

Corollary 7.5. *Let G be a uniform pro-p group of dimension d. Then the action of* $\mathrm{Aut}(G)$ *on G is $\mathbb{Z}_p$-linear with respect to the $\mathbb{Z}_p$-module structure on $(G, +)$. Moreover,* $\mathrm{Aut}(G)$ *embeds into* $\mathrm{GL}_d(\mathbb{Z}_p)$ *as a closed subgroup.*

The corollary implies in particular that the automorphism group of a pro-p group of finite rank is virtually again a pro-p group of finite rank. Another immediate consequence is that every pro-p group G of finite rank which contains an open uniform subgroup U with $\mathrm{Z}(U) = 1$ is linear over $\mathbb{Z}_p$. In fact, this is a special instance of Lazard's characterisation of p-adic analytic groups as linear groups over $\mathbb{Z}_p$.

7.3. **Associated Lie structure.** Let G be a uniform pro-p group, and write $G_n := P_n(G) = G^{p^{n-1}}$ for the terms of the lower p-series of G. Since all free $\mathbb{Z}_p$-modules of a given dimension are isomorphic, the procedure of passing from the uniform pro-p group G to the associated $\mathbb{Z}_p$-module $(G, +)$ inevitably involves a certain loss of information. More information can be saved by defining yet another operation, namely a Lie bracket. The new operation is to be defined canonically in terms of group commutators.

Again, we take our inspiration from a formal identity, namely

$$\exp(XY - YX) = \lim_{n\to\infty} \big(\exp(X/n)^{-1} \exp(Y/n)^{-1} \exp(X/n) \exp(Y/n)\big)^{n^2}$$

which holds in the completed free associative algebra $\mathbb{Q}\langle\langle X, Y\rangle\rangle$ and is intimately linked with Lie theory. Accordingly, we define the Lie bracket of $x, y \in G$ as

$$[x, y]_{\mathrm{Lie}} := \lim_{n\to\infty} [x^{p^n}, y^{p^n}]^{p^{-2n}}.$$

The individual terms make sense as $[G_n, G_n] \subseteq G_{2n}$, but, of course, one needs to check that the sequence converges. Careful, but elementary considerations lead to

Theorem 7.6 (Associated Lie structure)**.** *Let G be a uniform pro-p group. With the operation $[\cdot,\cdot]_{Lie}$ the $\mathbb{Z}_p$-module $(G, +)$ becomes a $\mathbb{Z}_p$-Lie lattice.*

In the following we denote the $\mathbb{Z}_p$-Lie lattice associated to G by $L(G)$. The next proposition assures us that the assignment of a Lie lattice to a uniform pro-p group is well behaved with respect to the passage to subgroups or quotients.

Proposition 7.7. *Let G be a uniform pro-p group. Let $H \leq_{\mathrm{c}} G$ be a uniform subgroup, and let $N \trianglelefteq_{\mathrm{c}} G$ such that G/N is uniform. Then N is uniform and*

1. *$L(H)$ constitutes a Lie sublattice of $L(G)$;*
2. *$L(N)$ constitutes a Lie ideal of $L(G)$, the sets G/N and $L(G)/L(N)$ are equal and the natural epimorphism $G \to G/N$ of groups induces an epimorphism $L(G) \to L(G/N)$ of $\mathbb{Z}_p$-Lie lattices with kernel $L(N)$.*

Unlike the $\mathbb{Z}_p$-module $(G, +)$, the $\mathbb{Z}_p$-Lie lattice $L(G)$ actually captures all the information in the uniform pro-p group G. Indeed, our next task is to describe how the group multiplication can be recovered from the Lie bracket.

7.4. **The Hausdorff Formula.** As mentioned in Section 2.4, the Hausdorff Formula gives an expression for the formal power series

$$\Phi(X, Y) := \log(\exp(X) \cdot \exp(Y)) \in \mathbb{Q}\langle\langle X, Y\rangle\rangle$$

in non-commuting indeterminates X, Y. In order to state the precise formula, we first note that the associative algebra $\mathbb{Q}\langle\langle X, Y\rangle\rangle$ admits in $[A, B] := AB - BA$ a natural Lie bracket. Expressing exp and log as power series, one can effectively eliminate the associative multiplication by a careful analysis and express $\Phi(X, Y)$ completely in terms of Lie commutators: $\Phi(X, Y) = \sum_{n=1}^{\infty} u_n(X, Y)$ is the infinite sum of homogeneous terms $u_n(X, Y)$ where

$$u_n(X, Y) = \sum_{m=1}^{n} \sum_{\substack{a_i, b_i \geq 0 \text{ s.t.} \\ a_i + b_i > 0, \\ \sum (a_i + b_i) = n}} \frac{(-1)^{m-1}}{mn \cdot a_1! b_1! \cdots a_m! b_m!} [{}_{a_1}X_{,b_1}\, Y, \ldots, {}_{a_m}X_{,b_m}\, Y]$$

with $[{}_{a_1}X_{,b_1}\, Y, \ldots, {}_{a_m}X_{,b_m}\, Y] = [\underbrace{X, \ldots, X}_{a_1}, \underbrace{Y, \ldots, Y}_{b_1}, \ldots, \underbrace{X, \ldots, X}_{a_m}, \underbrace{Y, \ldots, Y}_{b_m}]$ and all commutators being left-normed. A computation of the first three homogeneous terms $u_i(X, Y)$ shows that

$$\Phi(X, Y) = X + Y + \frac{[X, Y]}{2} + \frac{[X, Y, Y] - [X, Y, X]}{12} + \ldots$$

As it stands the Hausdorff Formula is an identity in formal power series. Let us explain its meaning as such. Consider the completed free associative algebra $A := \mathbb{Q}\langle\langle x_1, \ldots, x_d\rangle\rangle$ in d non-commuting indeterminates. Write $M := (x_1, \ldots, x_d)$ for the maximal ideal of A. It is easily seen that the exponential map and the

logarithm map set up mutually inverse bijections between the sets M and $1+M$. For $d=1$ they even provide isomorphisms between the additive group M and the multiplicative group $1+M$. But for $d>2$ the groups M and $1+M$ are clearly not isomorphic: M is abelian, whereas $1+M$ is not. The situation can be saved by equipping M with the commutator Lie bracket: the Hausdorff Formula shows that the multiplicative group $1+M$ can be described entirely in terms of the Lie algebra M.

We want to use the Hausdorff Formula to recover a uniform pro-p group G from the associated $\mathbb{Z}_p$-Lie lattice $L(G)$. Naturally, this situation is more complicated. For instance, the question of convergence has to be considered more seriously.

7.5. **Applying the Hausdorff Formula.** A $\mathbb{Z}_p$-Lie lattice L is *powerful* if p is odd and $[L,L]\subseteq pL$, or if $p=2$ and $[L,L]\subseteq 4L$. It is easily seen that the Lie lattice $L(G)$ associated to a uniform pro-p group is powerful. It is also worth noting that for any $\mathbb{Z}_p$-Lie lattice L the sublattice pL (respectively $4L$) is powerful if p is odd (respectively $p=2$).

Let L be a powerful $\mathbb{Z}_p$-Lie lattice and let $x,y\in L$. A suitable analysis of the p-adic valuations of the rational coefficients which appear in the homogeneous components $u_n(X,Y)$ of the Hausdorff Formula shows that $u_n(x,y)\in L$ for all $n\in\mathbb{N}$. Moreover, the sequence $u_n(x,y)\to 0$ as $n\to\infty$. Consequently, the limit $\Phi(x,y):=\sum_{n=1}^{\infty}u_n(x,y)$ exists in L. The formal properties of the logarithm and exponential series imply

Theorem 7.8. *If L is a powerful $\mathbb{Z}_p$-Lie lattice, then the Hausdorff Formula induces a group structure on L, with multiplication given by $xy=\Phi(x,y)$. The resulting group is a uniform pro-p group.*

One can check that, if this construction is applied to the Lie lattice $L(G)$ associated to a uniform pro-p group G, one recovers the original group. The assignment $G\mapsto L(G)$ thus defines an equivalence between the category of uniform pro-p groups and the category of powerful $\mathbb{Z}_p$-Lie lattices.

This equivalence in turn induces a functor from the category of pro-p groups of finite rank (which is equal to the category of p-adic analytic pro-p groups) to the category of finite dimensional $\mathbb{Q}_p$-Lie algebras, taking G to $\mathfrak{L}(G):=\mathbb{Q}_p\otimes_{\mathbb{Z}_p}L(U)$ where U is any open uniform subgroup of G. Likewise the image under the functor of a homomorphism between two pro-p groups of finite rank only depends on its restriction to an open uniform subgroup.

8. Fourth Lecture

8.1. **The group $\mathrm{GL}_d(\mathbb{Z}_p)$ – an example.** Let $d \in \mathbb{N}$. In order to illustrate the abstract concepts introduced in Section 7 we discuss in some detail the group $\mathrm{GL}_d(\mathbb{Z}_p)$. Clearly, $\mathrm{GL}_d(\mathbb{Z}_p)$ can be regarded as a topological group with respect to the p-adic topology, i.e. with respect to the subspace topology induced from the natural topology on the space $\mathrm{Mat}_d(\mathbb{Z}_p)$ of all $d \times d$ matrices over $\mathbb{Z}_p$. The congruence subgroups

$$G_i := \mathrm{GL}_d^i(\mathbb{Z}_p) := \{g \in \mathrm{GL}_d(\mathbb{Z}_p) \mid g \equiv 1 \pmod{p^i}\}, \quad i \in \mathbb{N},$$

provide a natural filtration of $\mathrm{GL}_d(\mathbb{Z}_p)$. For each $i \in \mathbb{N}$ the ith congruence subgroup G_i is equal to the kernel of the natural projection $\mathrm{GL}_d(\mathbb{Z}_p) \to \mathrm{GL}_d(\mathbb{Z}/p^i\mathbb{Z})$ and hence forms an open normal subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$. Note that a matrix $x \in \mathrm{Mat}_d(\mathbb{Z}_p)$ is invertible if and only if it is invertible modulo p. This yields yet another description of the congruence subgroups: one has $G_i = 1 + p^i \mathrm{Mat}_d(\mathbb{Z}_p)$ for each $i \in \mathbb{N}$. In particular, it follows that

$$|G_0 : G_1| = |\mathrm{GL}_d(\mathbb{F}_p)| = (p^d - 1)(p^d - p) \cdots (p^d - p^{d-1}),$$
$$|G_1 : G_i| = p^{d^2(i-1)} \quad \text{for } i \geq 1.$$

Moreover, the groups G_i form a base of open neighbourhoods for the identity matrix in $\mathrm{Mat}_d(\mathbb{Z}_p)$ and thus determine completely the topology on $\mathrm{GL}_d(\mathbb{Z}_p)$: every open neighbourhood of 1 in $\mathrm{GL}_d(\mathbb{Z}_p)$ contains one of the open normal subgroups G_i. It follows that $\mathrm{GL}_d(\mathbb{Z}_p)$ is profinite and that G_1 is a pro-p group. Put $\varepsilon := 0$ if p is odd, $\varepsilon := 1$ if $p = 2$; and set $G := G_{1+\varepsilon}$.

Proposition 8.1. *The group $G = \mathrm{GL}_d^{1+\varepsilon}(\mathbb{Z}_p)$ is a uniform pro-p group and $\dim(G) = \mathrm{rk}(G) = d(G) = d^2$. Moreover, the lower p-series of G coincides with the natural congruence filtration, i.e. $P_i(G) = G_{i+\varepsilon} = \mathrm{GL}_d^{i+\varepsilon}(\mathbb{Z}_p)$ for all $i \in \mathbb{N}$.*

Sketch of proof for $p > 2$. As p is odd, we have $G = G_1$. An easy computation shows that every quotient G_i/G_{i+1} of successive terms of the congruence filtration G_i, $i \in \mathbb{N}$, constitutes an elementary p-group of rank d^2 which is central in G/G_{i+1}. Thus $P_i(G) \subseteq G_i$ for all $i \in \mathbb{N}$. Below we show that $G_2 = \{x^p \mid x \in G\}$. This implies that $P_2(G) = G_2 = G^p$, hence G is powerful. Next we conclude from Proposition 5.7 that $P_i(G)/P_{i+1}(G)$ is an elementary p-group of rank at most d^2 for every $i \geq 2$. In view of the inclusions $P_i(G) \subseteq G_i$, it follows that $P_i(G) = G_i$ for all $i \in \mathbb{N}$ and that G is uniform of dimension $\dim(G) = d^2$, as wanted.

It remains to prove that every element of G_2 is a pth power of an element of G. In other words, given $A \in \mathrm{Mat}_d(\mathbb{Z}_p)$ we are to solve

$$(1 + pX)^p = 1 + p^2 A \qquad \text{with } X \in \mathrm{Mat}_d(\mathbb{Z}_p).$$

We construct a solution X by means of successive approximations $X_i \in \mathrm{Mat}_d(\mathbb{Z}_p)$ modulo p^i, $i \in \mathbb{N}$, similarly as in Exercise 4.4. These approximations X_i will form a convergent sequence whose limit X will be an exact solution. Some care has to be taken, because matrix multiplication in general is not commutative. But we will construct each X_i so that it commutes with the given matrix A.

Set $X_1 := X_2 := X_3 := A$ and note that $(1 + pA)^p \equiv 1 + p^2 A$ modulo p^3. Now let $i \geq 4$ and suppose, inductively, that we have found a matrix X_{i-1}, commuting

with A, such that $(1+pX_{i-1})^p \equiv 1+p^2A$ modulo p^{i-1}. Then

$$(1+pX_{i-1})^p = 1+p^2A+p^{i-1}E \qquad \text{for some } E \in \mathrm{Mat}_d(\mathbb{Z}_p).$$

Observe that E commutes with A and X_{i-1}. Put $X_i := X_{i-1} - p^{i-3}E$. Then X_i commutes with A, and a short computation shows that, modulo p^i,

$$\begin{aligned}(1+pX_i)^p &= (1+pX_{i-1}-p^{i-2}E)^p \\ &\equiv (1+pX_{i-1})^p - p(1+pX_{i-1})^{p-1}p^{i-2}E \\ &\equiv 1+p^2A+p^{i-1}E-p^{i-1}E \\ &\equiv 1+p^2A.\end{aligned}$$

□

According to Section 7, there is a natural $\mathbb{Z}_p$-Lie lattice $L(G)$ associated to the uniform pro-p group G. Consider the $\mathbb{Z}_p$-Lie lattice $\mathfrak{gl}_d(\mathbb{Z}_p)$ of all $d \times d$ matrices over $\mathbb{Z}_p$, subject to the commutator Lie bracket. Similarly as the group $\mathrm{GL}_d(\mathbb{Z}_p)$, the Lie lattice $\mathfrak{gl}_d(\mathbb{Z}_p)$ admits a natural congruence filtration

$$\mathfrak{gl}_d^i(\mathbb{Z}_p) := \{x \in \mathfrak{gl}_d(\mathbb{Z}_p) \mid x \equiv 0 \pmod{p^i}\} = p^i\mathfrak{gl}_d(\mathbb{Z}_p), \quad i \in \mathbb{N}.$$

Put $\mathfrak{g} := \mathfrak{gl}_d^{1+\varepsilon}(\mathbb{Z}_p)$. Clearly, $\mathfrak{g}$ is a powerful $\mathbb{Z}_p$-Lie lattice.

Proposition 8.2. *The $\mathbb{Z}_p$-Lie lattice $L(G)$ associated to the uniform pro-p group $G = \mathrm{GL}_d^{1+\varepsilon}(\mathbb{Z}_p)$ is isomorphic to $\mathfrak{g} = \mathfrak{gl}_d^{1+\varepsilon}(\mathbb{Z}_p)$.*

Sketch of proof for $p > 2$. The correspondence between $G = \mathrm{GL}_d^1(\mathbb{Z}_p)$ and $\mathfrak{g} = \mathfrak{gl}_d^1(\mathbb{Z}_p)$ admits an explicit interpretation through the logarithm and the exponential map. For instance, one can check directly that the Lie bracket obtained in the construction of $L(G)$ is the same as the one of $\mathfrak{g}$, if one passes from one Lie lattice to the other by means of the logartihm and the exponential map.

Concretely, one may proceed as follows. A natural $\mathbb{Z}_p$-basis for $\mathfrak{g}$ is given by the p-multiples of the d^2 elementary matrices, i.e. by the matrices with one entry equal to p and all remaining entries equal to 0. One can explicitly compute the images of these basis elements in G under the exponential map. For any two basis elements $a, b \in \mathfrak{g}$ one can then verify that $\exp(ab-ba)$ is the same as the value which results from the corresponding limit formula, with input $x := \exp(a)$ and $y := \exp(b)$, provided in Section 7.3. □

8.2. **Just-infinite pro-p groups.** A profinite group is *just-infinite*, if it is infinite but admits no proper infinite quotients. It is easily seen that every just-infinite pro-p group is finitely generated and that every infinite finitely generated pro-p group has a just-infinite homomorphic image; see Exercise 9.3. Just-infinite pro-p groups play a similar role in the theory of pro-p groups as finite simple groups in the theory of finite groups. Many of the better known just-infinite pro-p groups are groups of Lie type, defined over $\mathbb{Z}_p$ or over the pro-p ring $\mathbb{F}_p[\![t]\!]$ of formal power series with coefficients in $\mathbb{F}_p$. In addition, there are several interesting exceptional examples of just-infinite pro-p groups, such as the Nottingham group; see Exercise 9.3. As yet no convincing proposal has been put forward for classifying just-infinite pro-p groups. In fact, one can construct uncountably many pairwise non-isomorphic just-infinite pro-p groups. So a first step would be to give a precise and sensible meaning to the word 'classification' in the given context.

Best understood among the just-infinite pro-p groups are the p-adic analytic ones. Every soluble just-infinite pro-p group is virtually abelian and hence p-adic analytic. Indeed, the soluble just-infinite pro-p groups are irreducible p-adic space groups, and they can be investigated by the methods developed to study pro-p groups of finite coclass. The non-soluble p-adic analytic just-infinite pro-p groups can be realised as open subgroups of the groups $\mathbf{G}_{\mathbb{Q}_p}$ of $\mathbb{Q}_p$-rational points of certain semisimple algebraic groups defined over the field $\mathbb{Q}_p$. It is this description which makes them accessible in a rather explicit way.

Indeed, the non-soluble p-adic analytic just-infinite pro-p groups can naturally be partitioned into commensurability classes, where two profinite groups are *commensurable* if they have isomorphic open subgroups. One can then show that within each commensurability class of non-soluble p-adic analytic just-infinite pro-p groups there is (up to isomorphism) a unique *maximal* representative G which has the property that every just-infinite pro-p group which is commensurable to G embeds as an open subgroup into G.

The maximal group G which is commensurable to a given non-soluble p-adic analytic just-infinite pro-p group H can be constructed as follows. To H one associates via an open uniform subgroup $U \leq_{\mathrm{o}} H$ the $\mathbb{Q}_p$-Lie algebra $\mathcal{L}(H) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L(U)$. This Lie algebra turns out to be the direct sum of p^e copies of a simple $\mathbb{Q}_p$-Lie algebra for a suitable $e \in \mathbb{N}_0$, with $e = 0$ corresponding to the most interesting case. The automorphism group of the Lie algebra $\mathcal{L}(H)$ can be regarded as an algebraic group $\mathbf{G}$ defined over $\mathbb{Q}_p$. We remark that the classification of simple $\mathbb{Q}_p$-Lie algebras and simple algebraic groups over $\mathbb{Q}_p$ can be used to obtain an overview of the groups that occur. Since H is non-soluble and just-infinite, it acts faithfully on $\mathcal{L}(H)$ and thus embeds into the group $\mathbf{G}_{\mathbb{Q}_p}$ of $\mathbb{Q}_p$-rational points. Being a pro-p group, H is contained in a Sylow pro-p subgroup G of $\mathbf{G}_{\mathbb{Q}_p}$. A suitable Sylow theorem implies that all Sylow pro-p subgroups of $\mathbf{G}_{\mathbb{Q}_p}$ are conjugate. From this one shows that G is a maximal just-infinite pro-p group within the commensurability class of H.

It can be shown that a non-soluble p-adic analytic just-infinite pro-p group is never isomorphic to a proper subgroup of itself. In contrast to this, the known just-infinite pro-p groups which are not p-adic analytic do admit proper subgroups which are isomorphic to the original groups. This leads to the interesting

Problem. *Suppose that G is a just-infinite pro-p group which is not isomorphic to any of its proper closed subgroups $H <_{\mathrm{c}} G$. Does it follow that G is p-adic analytic?*

8.3. **Potent filtrations and saturable pro-p groups.** In his seminal paper *Groupes analytiques p-adiques*, Lazard develops the theory of p-adic Lie groups from a class of groups which he calls 'groupes p-saturables'. These saturable pro-p groups include uniform pro-p groups, but form a strictly larger class. From a group theoretic perspective saturable pro-p groups are, however, not as comfortable to work with as uniform pro-p groups. Intuitively, a pro-p group G is saturable if we can associate to it a $\mathbb{Z}_p$-Lie lattice $L(G)$ via the limit process described in Section 7. Recently, González-Sánchez has developed a quite useful description of saturable pro-p groups in terms of potent filtrations.

Let G be a pro-p group, and let N be a closed normal subgroup of G. A *potent filtration* of N in G is a descending series N_i, $i \in \mathbb{N}$, of closed normal subgroups of G such that (i) $N_1 = N$, (ii) $\bigcap\{N_i \mid i \in \mathbb{N}\} = 1$, (iii) $[N_i, G] \subseteq N_{i+1}$ and $[N_{i,p-1}\, G] \subseteq N_{i+1}^p$ for all $i \in \mathbb{N}$. We say that N is *PF-embedded* in G if there exists a potent filtration of N in G. The group G is a *PF-group*, if G is PF-embedded in itself.

To ease notation, group theoretic constructs within topological groups will from now on be implicitly geared towards closed subgroups. For instance, if H, K are closed subgroups of a topological group G we interpret $[H, K]$ as the *closed* subgroup generated by all commutators $[h, k]$ with $h \in H$ and $k \in K$.

Some basic properties of PF-embedded subgroups, which are listed in the next Lemma, follow essentially from the Hall-Petrescu collection formula. This formula states that for elements x, y of any group G and $n \in \mathbb{N}$,

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} \cdots c_i^{\binom{n}{i}} \cdots c_{n-1}^n c_n \qquad \text{for suitable } c_i \in \gamma_i(G),\ i \in \{2, \ldots, n\}.$$

Lemma 8.3 (Properties of PF-embedded subgroups)**.** *Let G be a pro-p group, and let N, M be PF-embedded subgroups of G. Then*

(1) *NM, N^p and $[N,_k G]$ are PF-embedded in G for all $k \in \mathbb{N}$;*
(2) *$[N^p, G] = [N, G]^p$;*
(3) *$N^p = \{x^p \mid x \in N\}$;*
(4) *if G is torsion-free and $x^p \in N^p$, then $x \in N$; moreover, if $x, y \in N$ such that $x^p = y^p$, then $x = y$.*

González-Sánchez' characterisation of saturable pro-p groups is

Theorem 8.4 (Saturable pro-p groups as PF-groups)**.** *Let G be a torsion-free finitely generated pro-p group. Then G is saturable if and only if G – or equivalently $G/\Phi(G)^p$ – is a PF-group.*

In particular, if $\gamma_p(G) \subseteq \Phi(G)^p$, then G is saturable.

It is not difficult to check that every uniform pro-p group G satisfies $\gamma_p(G) \subseteq \Phi(G)^p$. Hence uniform pro-$p$ groups are saturable. In fact, if G is a torsion-free finitely generated pro-p group satisfying $\gamma_p(G) \subseteq \Phi(G)^p$, then the lower p-series of G provides a potent filtration; see Exercise 9.4.

8.4. **Lie correspondence.** One difficulty in working with uniform pro-p groups is that the property of being powerful is not inherited by subgroups in any coherent way; see Exercise 9.2. For instance, this causes problems, if one tries to set up a Lie correspondence for subgroups of a uniform pro-p group. The situation improves substantially if instead one works with saturable pro-p groups. Using Theorem 8.4, González-Sánchez and Klopsch recently proved

Theorem 8.5. *Every torsion-free p-adic analytic pro-p group of dimension less than p is saturable. On the other hand there exists a torsion-free p-adic analytic pro-p group of dimension p which is not saturable.*

This allows one to study torsion-free p-adic analytic pro-p groups of dimension less than p by means of $\mathbb{Z}_p$-Lie lattices, similarly as finite p-groups of nilpotency class less than p can be investigated based on the Lazard correspondence. In addition, González-Sánchez and Klopsch proved

Proposition 8.6. *Let G be a saturable pro-p group, and $H \leq_{\mathrm{c}} G$ with $\dim(H) \leq p$. Then H is saturable and hence corresponds to a Lie sublattice $L(H)$ of $L(G)$.*

This proposition gives a conceptually satisfying approach to setting up a Lie correspondence for subgroups of a saturable pro-p group. A similar correspondence in the context of uniform pro-p groups was originally discovered and proved by Ilani via ad-hoc type arguments.

Theorem 8.7 (Lie correspondence)**.** *Let G be a saturable pro-p group and let $L(G)$ be the associated saturable $\mathbb{Z}_p$-Lie lattice. Suppose that $K, H \subseteq_{\mathrm{c}} G$ are closed subsets, and denote them by $L(K)$, $L(H)$ when regarded as subsets of $L(G)$.*

1. *Suppose that H is a subgroup of G and that $\dim\langle x, y\rangle_{\mathrm{Grp}} \leq p$ for all $x, y \in H$. Then $L(H)$ is a Lie sublattice of $L(G)$. Moreover, if K is a normal subgroup of H, then $L(K)$ is a Lie ideal of $L(H)$.*
2. *Suppose that $L(H)$ is a Lie sublattice of $L(G)$ and that $\dim\langle x, y\rangle_{\mathrm{Lie}} \leq p$ for all $x, y \in L(H)$. Then H is a subgroup of G. Moreover, if $L(K)$ is a Lie ideal of $L(H)$, then K is a normal subgroup of H.*

Theorem 8.7 has natural applications, for instance to the subject of subgroup growth. Indeed, it forms the basis for studying the subgroup growth zeta functions of p-adic analytic pro-p groups, such as $\mathrm{GL}_d^1(\mathbb{Z}_p)$, via their associated Lie lattices. It remains a challenging problem to describe the subgroup growth of the analytic pro-p groups $\mathrm{GL}_d^1(\mathbb{Z}_p)$, $d \in \mathbb{N}$. At least for $p \geq d^2$ this problem 'reduces' to understanding the sublattice growth of the $\mathbb{Z}_p$-Lie lattice $\mathfrak{gl}_d^1(\mathbb{Z}_p)$.

9. Third set of exercises

Exercise 9.1 (The special linear groups $\mathrm{SL}_d(\mathbb{Z}_p)$)**.**
(a) Let $d \in \mathbb{N}$ and consider the topological group $\mathrm{SL}_d(\mathbb{Z}_p)$. Show that this group is virtually a pro-p group and display an open uniform subgroup, together with its lower p-series. Realise the associated powerful $\mathbb{Z}_p$-Lie lattice explicitly as a Lie sublattice of $\mathfrak{gl}_d(\mathbb{Z}_p)$.
(b) Show that every open neighbourhood of 1 in $\mathrm{SL}_2(\mathbb{Z}_p)$ contains an open subgroup which is not powerful.

Exercise 9.2 (The quaternion group $\mathrm{SL}_1(\Delta_p)$)**.**
Suppose that $p > 2$, and let $\rho \in \{1, 2, \ldots, p-1\}$ be a non-square modulo p. The 4-dimensional *quaternion algebra* over $\mathbb{Q}_p$ is the associative algebra

$$\mathbb{D}_p := \mathbb{Q}_p + \mathbb{Q}_p\mathbf{u} + \mathbb{Q}_p\mathbf{v} + \mathbb{Q}_p\mathbf{uv},$$

defined by the multiplication rules

$$\mathbf{u}^2 = \rho, \quad \mathbf{v}^2 = p, \quad \mathbf{uv} = -\mathbf{vu}.$$

The *reduced norm* and the *reduced trace* of an element $\mathbf{x} = \alpha+\beta\mathbf{u}+\gamma\mathbf{v}+\delta\mathbf{uv} \in \mathbb{D}_p$ are given by

$$\mathrm{N}(\mathbf{x}) = \alpha^2 - \rho\beta^2 - p\gamma^2 + \rho p\delta^2 \quad \text{and} \quad \mathrm{T}(\mathbf{x}) = 2\alpha.$$

We write $\mathrm{SL}_1(\mathbb{D}_p) := \{\mathbf{x} \in \mathbb{D}_p \mid \mathrm{N}(\mathbf{x}) = 1\}$ and $\mathfrak{sl}_1(\mathbb{D}_p) := \{\mathbf{x} \in \mathbb{D}_p \mid \mathrm{T}(\mathbf{x}) = 0\}$.
(a) Show that $\mathbb{D}_p$ is a skew field. (*Hint:* Use the norm map.)
(b) Prove that $\mathrm{SL}_1(\mathbb{D}_p)$ is a compact topological group. (*Hint:* Consider $\mathbf{x} = \alpha + \beta\mathbf{u} + \gamma\mathbf{v} + \delta\mathbf{uv} \in \mathbb{D}_p$ with $\mathrm{N}(\mathbf{x}) = 1$. Note that $v_p(\alpha^2 - \rho\beta^2)$ is even, while $v_p(p\gamma^2 - \rho p\delta^2)$ is odd. Conclude that $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_p$. Now use the fact that the norm map is continuous.)
Remark: The group $\mathrm{SL}_2(\mathbb{Q}_p)$, in contrast, is clearly not compact.
(c) Show that $\mathfrak{sl}_1(\mathbb{D}_p)$ is a 3-dimensional simple $\mathbb{Q}_p$-Lie algebra. Prove that $\mathfrak{sl}_1(\mathbb{D}_p)$ does not have any subalgebras of dimension 2. Conclude that $\mathfrak{sl}_1(\mathbb{D}_p)$ is not isomorphic to the Lie algebra $\mathfrak{sl}_2(\mathbb{Q}_p)$.
Remark: There are (up to isomorphism) precisely two 3-dimensional simple $\mathbb{Q}_p$-Lie algebras, namely $\mathfrak{sl}_1(\mathbb{D}_p)$ and $\mathfrak{sl}_2(\mathbb{Q}_p)$.
(d) Note that $\Delta_p := \mathbb{Z}_p + \mathbb{Z}_p\mathbf{u} + \mathbb{Z}_p\mathbf{v} + \mathbb{Z}_p\mathbf{uv}$ constitutes a $\mathbb{Z}_p$-order of $\mathbb{D}_p$, i.e. a $\mathbb{Z}_p$-subalgebra whose $\mathbb{Q}_p$-span is equal to the entire algebra $\mathbb{D}_p$. Show that Δ_p admits a unique maximal ideal $\mathfrak{p}$ which is generated by $\mathbf{v}$.
Remark: One can extend the p-adic valuation on $\mathbb{Q}_p$ uniquely to a valuation on the skew field $\mathbb{D}_p$. The element $\mathbf{v}$ is a uniformiser for this valuation, i.e. it plays a similar role as p does for the valuation on $\mathbb{Q}_p$.
(e) Write $\mathfrak{sl}_1(\Delta_p) := \mathfrak{sl}_1(\mathbb{D}_p) \cap \Delta_p$ and $\mathbf{i} := \frac{1}{2}\mathbf{u}$, $\mathbf{j} := \frac{1}{2}\mathbf{v}$, $\mathbf{k} := \frac{1}{2}\mathbf{uv}$. Note that $\mathfrak{sl}_1(\Delta_p) = \mathbb{Z}_p\mathbf{i}+\mathbb{Z}_p\mathbf{j}+\mathbb{Z}_p\mathbf{k}$ and work out the commutators $[\mathbf{i}, \mathbf{j}]$, $[\mathbf{i}, \mathbf{k}]$, $[\mathbf{j}, \mathbf{k}]$ in terms of the new basis $\mathbf{i}, \mathbf{j}, \mathbf{k}$.
(f) Note that $\mathfrak{sl}_1^2(\Delta_p) := p\,\mathfrak{sl}_1(\Delta_p)$ is powerful. Convince yourself that the corresponding uniform pro-p group, which is defined via the Hausdorff Formula, is equal to the group $\mathrm{SL}_1^2(\Delta_p) := \mathrm{SL}_1(\mathbb{D}_p) \cap (1 + p\Delta_p)$.
Conclude that $\mathrm{SL}_1(\mathbb{D}_p)$ is a 3-dimensional just-infinite compact p-adic analytic group which is not commensurable with $\mathrm{SL}_2(\mathbb{Z}_p)$.

Exercise 9.3 (Just-infinite pro-p groups)**.**
(a) Prove that every just-infinite pro-p group is finitely generated.
Remark: I do not know whether there are just-infinite profinite groups which are not finitely generated.
(b) Let G be a pro-p group of finite rank with open uniform subgroup $U \leq_{\mathrm{o}} G$. Prove that, if the associated $\mathbb{Q}_p$-Lie algebra $\mathcal{L}(G) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L(U)$ is simple, then G is just-infinite.
(c) Determine all abelian just-infinite pro-p groups. Show that every soluble just-infinite pro-p group is virtually abelian. Construct a soluble just-infinite pro-p group which is not abelian.
(d) Give an example of an infinite pro-p group which does not have any just-infinite quotients. (*Hint:* Your group cannot be finitely generated.)
In contrast, show that every infinite finitely generated pro-p group G admits a just-infinite quotient. (*Hint:* Consider an ascending chain $N_1 \subseteq N_2 \subseteq \ldots \subseteq G$ of closed normal subgroups of G such that G/N_i is infinite for all $i \in \mathbb{N}$, and assume for a contradiction that $M := \mathrm{cl}(\bigcup\{N_i \mid i \in \mathbb{N}\})$ is open in G. Conclude that M is finitely generated and derive a contradiction. Now apply Zorn's Lemma.)
(e) Consider the profinite group $G := \prod_p C_p$, where the product extends over all primes p. Prove that G is finitely generated, but does not admit any just-infinite quotient.
(f) Suppose that $p > 2$. Prove that the Nottingham group, introduced in Exercise 4.3, is hereditarily just-infinite, i.e. that every open subgroup of the Nottingham group is just-infinite.

Exercise 9.4 (Saturable pro-p groups)**.**
(a) Prove that every uniform pro-p group G satisfies $\gamma_p(G) \subseteq \Phi(G)^p$. Go on to show that, if G is a torsion-free finitely generated pro-p group satisfying $\gamma_p(G) \subseteq \Phi(G)^p$, then the lower p-series of G provides a potent filtration. Conclude from Theorem 8.4 that uniform pro-p groups are saturable.
(b) Let $d \in \mathbb{N}$ with $d \geq 3$, and let G be a Sylow pro-p subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$. Show that G is not uniform. (*Hint:* Show that the image of G in $\mathrm{GL}_d(\mathbb{F}_p)$ is not powerful.)
(c) Let $d \in \mathbb{N}$, and let G be the Sylow pro-p subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$. Determine the lower central series of G for the specific case $d = 3$ and guess the general pattern. (*Hint:* Take for G the group of matrices which are upper uni-triangular modulo p, and consider the commutators of elementary matrices.) Conclude from Theorem 8.4 that G is saturable for $d \leq p - 2$.
(d) Construct a torsion-free p-adic analytic pro-p group of dimension p which is not saturable. (*Hint:* Consider the semidirect product $G := A \ltimes M$ of the abelian groups $A = \langle \alpha \rangle \cong \mathbb{Z}_p$ and $M = \langle x_1, \ldots, x_{p-1} \rangle \cong \mathbb{Z}_p^{p-1}$, defined by

$$x_i^{\alpha} = \begin{cases} x_i x_{i+1} & \text{if } 1 \leq i \leq p-2, \\ x_{p-1} x_1^p & \text{if } i = p-1. \end{cases}$$

Assume for a contradiction that G admits a potent filtration G_i, $i \in \mathbb{N}$. Observe that $[M, {}_{p-1} G] = M^p$ and deduce that $M \subseteq G_i$ for all $i \in \mathbb{N}$ in contradiction to $\bigcap\{G_i \mid i \in \mathbb{N}\} = 1$.)

Exercise 9.5 (Haar measure and random generation)**.**
Every profinite group G is a compact topological group and as such it carries a normalised Haar measure μ which is invariant under both left and right multiplication. The measure is normalised in the sense that $\mu(G) = 1$. The Haar measure μ can be evaluated on Borel subsets, in particular on all closed subsets of G. Sometimes it is useful to think of μ as a *probability measure* on G. For $k \in \mathbb{N}$ it induces a probability measure on the direct product $G \times \ldots \times G$ of k copies of the group G; thus one can consider *random k-tuples* of elements in G.
(a) Let G be profinite group and $H \leq_c G$. Determine the measure $\mu(H)$ in terms of the index $|G : H|$.
(b) Let G be a finitely generated pro-p group, and put $d := d(G)$. For $k \in \mathbb{N}$ determine the probability that a random k-tuple of elements in G generates G.
(c) Let G be a pro-p group of finite rank so that, by Exercise 6.6, its subgroup growth is polynomially bounded: denoting by σ_n the number of subgroups of index p^n in G, there exist $c, \alpha \in \mathbb{R}$ such that $\sigma_n \leq cp^{n\alpha}$ for all $n \in \mathbb{N}_0$. Let $k \in \mathbb{N}$ with $k > \alpha + 1$. Deduce form the Borel-Cantelli Lemma that a random k-tuple of elements in G generates with probability 1 an open subgroup of G. (*Hint:* The Borel-Cantelli Lemma states that, if $X_i \subseteq_c G$, $i \in \mathbb{N}$, is a family of closed subsets of G such that $\sum_{i=1}^{\infty} \mu(X_i)$ converges, then the Borel set

$$X = \bigcap \{Y_n \mid n \in \mathbb{N}\}, \quad \text{where } Y_n := \bigcup \{X_i \mid i \in \mathbb{N} \text{ with } i \geq n\},$$

has measure 0. In order to apply this in the given situation note that a k-tuple fails to generate an open subgroup of G if and only if it is contained in infinitely many open subgroups of G.)

Exercise 9.6 (Hausdorff dimension)**.**
Let G be a pro-p group of finite rank, and write $G_n := G^{p^n}$ for $n \in \mathbb{N}$.
(a) Prove that

$$\dim(G) = \lim_{n\to\infty} \frac{\log_p |G : G_n|}{n}.$$

(*Hint:* Choose an open uniform subgroup U of G, and write $U_n := U^{p^n}$ for $n \in \mathbb{N}$. Then $G_c \subseteq U$ for some $c \in \mathbb{N}$. Use the estimates $|U : U_{n-c}| \leq |G : G_n| \leq |G : U_n|$ for $n \in \mathbb{N}$ with $n \geq c$.)
(b) Suppose that G is uniform and let H be a uniform subgroup of G. Prove that the *isolator* $\mathrm{iso}_G(H) := \{g \in G \mid \exists n \in \mathbb{N} : g^n \in H\}$ forms a uniform subgroup of G with $|\mathrm{iso}_G(H) : H| < \infty$. (*Hint:* Work in the associated $\mathbb{Z}_p$-Lie lattice $L(G)$ and translate back and forth between the groups and the Lie lattices.)
(c) Let $H \leq_c G$ be a closed subgroup of G. Prove that

$$\lim_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|} = \frac{\dim H}{\dim G}.$$

Remark: The limit on the left hand side is equal to the *Hausdorff dimension* of H in G with respect to (the metric induced by) the filtration G_n, $n \in \mathbb{N}$.
(*Hint:* Note that $|HG_n : G_n| = |H : H \cap G_n|$ for all $n \in \mathbb{N}$. Using similar arguments as in part (a), reduce to the situation where both G and H are uniform. Convince yourself that we can further assume that H is isolated in G, i.e. that $\mathrm{iso}_G(H) = H$. Employing the associated $\mathbb{Z}_p$-Lie lattices, prove the claim in this situation.)

10. Fifth Lecture

10.1. **Representation growth and Kirillov's orbit method.** Let G be a profinite group. For $n \in \mathbb{N}$ we denote by $r_n(G)$ the number of isomorphism classes of continuous irreducible n-dimensional complex representations of G. For a general profinite group, these numbers may very well be infinite, but there are interesting situations where they are all finite. Indeed, if G is finitely generated, then $r_n(G) < \infty$ for all $n \in \mathbb{N}$ if and only if G is FAb[7], i.e. if and only if $H/[H,H]$ is finite for every open subgroup $H \leq_{\mathrm{o}} G$. In this situation one takes an interest in the arithmetic sequence $r_n(G)$, $n \in \mathbb{N}$, which reflects the *representation growth* of the profinite group G. A useful tool is the *representation growth zeta function*

$$\zeta_G^{\mathrm{irr}}(s) := \sum\nolimits_{n=1}^{\infty} r_n(G) n^{-s},$$

which encodes the entire representation growth of G.

The *derived series* of G is the descending series G_i, $i \in \mathbb{N}_0$, of closed normal subgroups, defined by $G_0 := G$ and $G_i := [G_{i-1}, G_{i-1}]$ for $i \geq 1$. It is easy to see that, if G is a pro-p group, then G is FAb if and only if every term of its derived series is open in G. In particular, any non-soluble just-infinite pro-p group is FAb.

Now suppose that G is p-adic analytic and consider the $\mathbb{Q}_p$-Lie algebra $\mathcal{L}(G) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L(U)$ associated to G via an open uniform pro-p subgroup U. Then G is FAb if and only if $\mathcal{L}(G)$ is perfect, i.e. if and only if $\mathcal{L}(G) = [\mathcal{L}(G), \mathcal{L}(G)]$. This makes the representation growth of compact open subgroups of semisimple p-adic Lie groups a natural field of study, and the so-called orbit method provides a useful tool in this context.

Kirillov originally introduced the orbit method to study the unitary representations of nilpotent Lie groups in the 1960s, around the same time when Lazard developed his theory of p-adic Lie groups. The method is based on the 'experimental' fact that there exists a close connection between the unitary irreducible representations of a Lie group and the orbits in its co-adjoint representation. In the case of a connected, simply-connected nilpotent Lie group G with associated Lie algebra $\mathfrak{g}$, one obtains a natural correspondence between equivalence classes of irreducible unitary representations of G and G-orbits in the dual space of $\mathfrak{g}$. In the 1970s Howe showed that the orbit method can also be put to use in the context of compact p-adic Lie groups. More recently, Jaikin-Zapirain and others extended and applied the orbit method to solve problems in the subject of representation growth.

10.2. **The orbit method for saturable pro-p groups.** Let G be a saturable pro-p group and let $\mathfrak{g} := L(G)$ denote the associated $\mathbb{Z}_p$-Lie lattice. Continuous complex representations of G correspond to continuous complex characters. Thus we want to arrive at a description of the set $\mathrm{Irr}(G)$ of continuous irreducible complex characters of G.

In the following we will frequently use the fact that the underlying sets of G and $\mathfrak{g}$ are one and the same. We denote by $\mathrm{Irr}(\mathfrak{g}_+)$ the set of continuous irreducible characters of the additive group $\mathfrak{g}_+ := (\mathfrak{g}, +)$, which coincides with the set $\mathrm{Hom}_{\mathbb{Z}}^{\mathrm{cont}}(\mathfrak{g}_+, \mathbb{C}^*)$ of continuous homomorphisms from $\mathfrak{g}_+$ into the multiplicative group $\mathbb{C}^*$. Indeed, one should think of $\mathrm{Irr}(\mathfrak{g}_+)$ as the dual space of $\mathfrak{g}$.

[7]FAb sounds fabulous and is short for 'finite abelianisations'.

The adjoint action of G on $\mathfrak{g}$ which is given by conjugation, induces the so-called *co-adjoint action* of G on $\mathrm{Irr}(\mathfrak{g}_+)$: for $\omega \in \mathrm{Irr}(\mathfrak{g}_+)$ and $g \in G$ the element $\omega^g \in \mathrm{Irr}(\mathfrak{g}_+)$ is defined by setting

$$\omega^g(x) := \omega(x^{g^{-1}}) \quad \text{for all } x \in \mathfrak{g}.$$

Natural candidates for the irreducible characters of G arise in form of the class functions

$$\Phi_\Omega : G \to \mathbb{C}, \quad \Phi_\Omega(x) := |\Omega|^{-1/2} \sum\nolimits_{\omega \in \Omega} \omega(x),$$

where Ω runs through all orbits of the G-space $\mathrm{Irr}(\mathfrak{g}_+)$. Indeed, one easily verifies that these functions form an orthonormal set. In fact, they give rise to an orthonormal basis for the class functions of G modulo any open PF-embedded subgroup N.

In parallel we need to keep track of the degrees of the irreducible characters of G. For this purpose we introduce the notion of a radical. To $\omega \in \mathrm{Irr}(\mathfrak{g}_+)$ we associate the bi-additive and skew-symmetric map

$$b_\omega : \mathfrak{g} \times \mathfrak{g} \to \mathbb{C}^*, \quad b_\omega(x, y) := \omega([x, y]).$$

The *radical* of this map b_ω is

$$\mathrm{Rad}(\omega) := \mathrm{Rad}(b_\omega) = \{x \in \mathfrak{g} \mid \forall y \in \mathfrak{g} : b_\omega(x, y) = 1\}.$$

One can prove that the radical $\mathrm{Rad}(\omega)$ associated to $\omega \in \mathrm{Irr}(\mathfrak{g}_+)$ is, in fact, a Lie sublattice of $\mathfrak{g}$ and coincides as a set with a saturable subgroup of G, namely with the stabiliser $\mathrm{Stab}_G(\omega)$ of ω in G.

Theorem 10.1 (Orbit method for saturable pro-p groups)**.** *Let G be a saturable pro-p group with $\gamma_{p-2}(G) \subseteq G^p$. Then the continuous irreducible complex characters of G are parameterised by the orbits of the co-adjoint action of G on $\mathrm{Irr}(\mathfrak{g}_+)$:*

$$\mathrm{Irr}(G) = \{\Phi_\Omega \mid \Omega \text{ an orbit of the } G\text{-space } \mathrm{Irr}(\mathfrak{g}_+)\}.$$

Moreover, if Ω is the G-orbit of $\omega \in \mathrm{Irr}(\mathfrak{g}_+)$, then the degree of the corresponding irreducible character Φ_Ω is equal to $|\mathfrak{g} : \mathrm{Rad}(\omega)|^{1/2}$.

We remark that the theorem applies in particular to uniform pro-p groups, if $p \geq 5$, and that similar conclusions hold true for uniform pro-2 and pro-3 groups.

Corollary 10.2. *Let G be a saturable pro-p group, which satisfies $\gamma_{p-2}(G) \subseteq G^p$ and which is FAb. Then*

$$\zeta_G^{\mathrm{irr}}(s) = \sum_{\omega \in \mathrm{Irr}(\mathfrak{g}_+)} |\mathfrak{g} : \mathrm{Rad}(\omega)|^{-(s+2)/2}.$$

Proof. Based on the theorem, this is now an easy computation. Observe that the dimension of the representation corresponding to a continuous complex character

χ of G is equal to $\chi(1)$. Hence we have

$$\begin{aligned}\zeta_G^{\mathrm{irr}}(s) &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-s} \\ &= \sum_{\substack{\omega \in \mathrm{Irr}(\mathfrak{g}_+) \\ \Omega := \omega^G}} |\Omega|^{-1} \Phi_\Omega(1)^{-s} \\ &= \sum_{\omega \in \mathrm{Irr}(\mathfrak{g}_+)} |G : \mathrm{Stab}_G(\omega)|^{-1} |\mathfrak{g} : \mathrm{Rad}(\omega)|^{-s/2} \\ &= \sum_{\omega \in \mathrm{Irr}(\mathfrak{g}_+)} |\mathfrak{g} : \mathrm{Rad}(\omega)|^{-1-s/2}.\end{aligned}$$

□

10.3. **An application of the orbit method.** Based upon Corollary 10.2 Jaikin-Zapirain has shown that, for odd primes p, the representation growth zeta function $\zeta_G^{\mathrm{irr}}(s) := \sum_{n=1}^{\infty} r_n(G) n^{-s}$ of a FAb p-adic analytic pro-p group G is in fact a rational function in p^{-s}. For $p = 2$ the same assertion holds if one further assumes that G is uniform. It is a major challenge to find out more about these representation growth zeta functions. Of particular interest are the zeta functions associated to families of open pro-p subgroups of semisimple p-adic Lie groups, such as the principal congruence subgroups of the special linear groups $\mathrm{SL}_n(\mathbb{Z}_p)$.

Regarding the existence of functional equations Voll and Klopsch have recently proved a positive result in a global setting. For this they consider families of p-adic Lie groups whose associated Lie algebras share a common $\mathbb{Z}$-Lie sublattice.

Denote by $\mathbb{P}$ the set of all primes. Let L be a Lie lattice over $\mathbb{Z}$, and for $p \in \mathbb{P}$ let $L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ denote the localisation of L at p. Then for all $p \in \mathbb{P}$ and $k \in \mathbb{N}$, with $k \geq 2$ is $p = 2$, the $\mathbb{Z}_p$-Lie lattice $p^k L_p$ is powerful and thus corresponds to a uniform pro-p group which we denote by $G_{p,k}$.

Theorem 10.3. *Let L be a Lie lattice over $\mathbb{Z}$ such that $\mathbb{Q} \otimes_{\mathbb{Z}} L$ is a perfect $\mathbb{Q}$-Lie algebra of dimension d. For $p \in \mathbb{P}$ consider the family of FAb uniform pro-p groups $G_{p,k}$ corresponding to the family of powerful $\mathbb{Z}_p$-Lie lattices $p^k L_p$, where $k \in \mathbb{N}$, with $k \geq 2$ if $p = 2$.*

Then for almost all $p \in \mathbb{P}$ the representation growth zeta functions associated to the groups $G_{p,k}$, k as above, satisfy the functional equations

$$\zeta_{G_{p,k}}^{\mathrm{irr}}(s)|_{p \to p^{-1}} = p^{(1-2k)d} \zeta_{G_{p,k}}^{\mathrm{irr}}(s).$$

These functional equations are to be interpreted as follows. Consider $G_{p,k}$ for $p \in \mathbb{P}$ and $k \in \mathbb{N}$ as above. The zeta function $\zeta_{G_{p,k}}^{\mathrm{irr}}(s)$ is a rational function in p^{-s} whose coefficients can be expressed as polynomials in p and in the numbers $\nu(V)$ of $\mathbb{F}_p$-points of certain smooth projective $\mathbb{F}_p$-defined varieties V. The operation $p \to p^{-1}$ on such a number $\nu(V)$ is performed by inverting the Frobenius eigenvalues associated to V: the alternating sum of these complex numbers equals $\nu(V)$ in accordance with the Weil conjectures. In the simplest case the Frobenius eigenvalues are just powers of p, in agreement with our notation.

The proof of Theorem 10.3 is built on two main ideas. The first ingredient is the parameterisation of the irreducible characters of a FAb uniform pro-p group

G in terms of the orbits of the co-adjoint action of G. In a second step one takes advantage of the fact that the problem of counting co-adjoint orbits can be treated within the framework of generalised Igusa local zeta functions.

– The End –

Acknowledgements. In preparing the course and these notes I have made considerable use of several of the books listed at the end of Section 1 and I have included key results from selected research articles and preprints. Originality I can claim, in a limited sense, with regard to the overall exposition. Given the informal style of the notes I have not aimed for systematically attributing all results to their respective authors.

These notes were specifically written for the course in Oxford and there is likely to be room for corrections and improvements. All comments and suggestions sent to the email address below are welcome. Revised and supplemented versions of these notes will be made available on my homepage.

Department of Mathematics, Royal Holloway, University of London, Egham TW20 0EX, United Kingdom

E-mail address: Benjamin.Klopsch@rhul.ac.uk