Diplomarbeit

Filtrations of p-adic analytic Galois groups of local fields

Angefertigt am
Mathematischen Institut

Vorgelegt der
Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

Januar 2008
Cornelius Probst
Wiesbaden

Contents

Preface

Fundamental in Geometry, analytic groups were introduced to the domain of Number Theory in the middle of the last century. Their theory has greatly advanced since, and has produced valuable results and challenging conjectures alike.

The basic idea for a number theoretic account of Lie groups[1] however is simple. We proceed exactly as in the real case and only replace $\mathbb{R}$ by $\mathbb{Q}_p$, the field of p-adic numbers. We thus consider a topological space G, locally homeomorphic to $\mathbb{Q}_p^d$, with an additional structure as topological group whose operations are (p-adic) analytic functions in the local coordinates.

Group-theoretic aspects of Lie theory. It is a distinctive feature of p-adic Lie groups that they can be characterised in purely *algebraic* terms (see [2]). Indeed, there is a close connection to profinite groups, established by the fundamental result that G is a p-adic Lie group if and only if it contains an open *uniform* subgroup H. This last statement's essence is that H is a pro-p group, with topological basis given by the open subgroups $H_n = H^{p^n}$. For all n, their quotients "uniformly" satisfy $H_n/H_{n+1} \simeq \mathbb{F}_p^d$, where d is the *dimension* of H (as well as of G).

Let K denote a p-adic number field, ie. a local field of characteristic 0. We give two typcial examples for the appearance of p-adic analytic groups:

(i) *Galois groups of (cyclotomic) $\mathbb{Z}_p$-extensions.* The p-adic integers $H = \mathbb{Z}_p$ are the simplest example of an infinite analytic group, because $\mathbb{Z}_p$ is itself already a uniform group. For any K as above, there exists an extension field K_∞ with $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$. In fact, K_∞ can be chosen as *cyclotomic* field, ie. as subfield of $K(\zeta_{p^\infty}) = \cup_n K(\zeta_{p^n})$.

(ii) *Galois representations on torsion points of Elliptic Curves.* Let E denote an elliptic curve, defined over K. The set $E[n]$ of n-torsion points on $E(\overline{K})$ has an (abstract) group structure $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ has a natural action on $E[n]$, which gives a representation

$$\rho_n \colon G_K \longrightarrow \mathrm{Aut}\big(E[n]\big) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

[1] We use the names "analytic group" and "Lie group" interchangeably.

If we set $n = p^r$ and let r grow, the sets $E[n]$ and the representations ρ_n fit together and give a p-adic representation

$$\rho : \ G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p).$$

The group $\mathrm{GL}_d(\mathbb{Z}_p)$ is not pro-p and in particular not uniform; we will however see in Section 1.3 that it contains a such one as open subgroup. It follows that $\mathrm{GL}_d(\mathbb{Z}_p)$ is indeed a p-adic Lie group, non-commutative and of dimension d^2.

Number-theoretic aspects of Lie groups. A distinctively number-theoretic property of the field K is its non-archimedean valuation v_K. For any Galois extension L/K, this valuation gives rise to the *ramification filtration* $G(r)_{r\geq -1}$ of the group $G = \mathrm{Gal}(L/K)$. This filtration[2] forms a topological basis of (not necessarily open) subgroups of G, and also reflects certain arithmetic properties of the extension L/K. For Galois subextensions $L/K'/K$, its relation to the ramification filtrations on $\mathrm{Gal}(L/K')$ and $\mathrm{Gal}(K'/K)$ can be described by explicit formulae.

We reconsider the first example, and put $p > 2$ and $K = \mathbb{Q}_p$ for brevity. The extension $L = \mathbb{Q}_p(\zeta_{p^\infty})/K$ is totally ramified and p-adic analytic, because its Galois group

$$G = \mathrm{Gal}(L/K) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

has $H = \mathrm{Gal}(L/\mathbb{Q}_p(\zeta_p)) \simeq \mathbb{Z}_p$ as open uniform subgroup. In the notation of the first example, this means $L = K'_\infty$, ie. L is the cyclotomoic $\mathbb{Z}_p$-extension of $K' = \mathbb{Q}_p(\zeta_p)$.

How are the subgroups $H_n = H^{p^n}$ of H (as p-adic Lie group) related to its subgroups $H(r)$ occuring as ramification filtration? In Section 5.4, a few results from Number Theory will suffice to show the simple relation $H_n = H(e_{K'} \cdot n + 1)$, where $e_{K'} = v_{K'}(p) = p - 1$ is the absolute ramification index of K'. We may return to G and stipulate a filtration by setting $G_0 = G$, and $G_n = H_{n-1}$ for $n \geq 1$. On the other hand, each ramification group $H(r)$ is equal to $G(s)$, for some s, by means of the explicit formulae mentioned above. We now have an even simpler relation, namely $G_n = G(e_K \cdot n)$, with $e_K = v_p(p) = 1$.

Sen's Theorem. It was conjectured by Serre [10] and eventually proven by Sen [8] that the essence of this relation holds for any totally ramified Galois extension L/K of local number fields such that $G = \mathrm{Gal}(L/K)$ is p-adic analytic, and of dimension > 0. An obvious shortcoming of the above example is the arbitrary choice of a filtration (G_n), which we will account for by introducing the class of *Lie filtrations* of G. For any such Lie filtration $(G_n)_{n\in\mathbb{N}}$, Sen's Theorem states the inclusions

$$G(ne + c) \subset G_n \subset G(ne - c)$$

[2]We understand as filtration of a group G a family of subsets $(G_i)_{i\in I}$, with $G_i \supset G_j$ for $i \leq j$ and $\cap_i G_i = 1$. We will have $I = \mathbb{N}$ for all filtrations except for+ the ramification filtration, where we require $I = [-1, \infty) \subset \mathbb{R}$.

where c is a constant, $n \geq 0$ any integer and $G(r) = G$ for $r < -1$.

The rather dense proof of Sen's Theorem as in [8] however builds upon an analytic characterisation of p-adic Lie groups as suggested by Lazard [5]. This paper attempts to give a more detailed and easily accessible proof, using the familiar algebraic language of [2]. This approach will result in minor terminological differences (spelt out in Section 4.4), but we account for these by introducing the notion of "uniform equivalence of filtrations in scaling s." A welcome side-effect of this technical concept is a cleaner and more intuitive strategy for Sen's proof.

Structure of this paper. This paper is divided into three principal parts.

(i) Part I introduces the group-theoretic language and objects required for the algebraic characterisation of p-adic analytic groups. The key concepts are those of uniform groups, their lower p-series and their dimension. In a brief addendum, we discuss elementary concepts of p-adic analysis, and define two fundamental p-adic analytic functions, namely the Exponential and the Logarithm. This first part's primary reference is [2], containing all details and proofs.

(ii) Part II explains the fundamental concepts of Lie theory. However, we proceed "backwards" and introduce Lie algebras (as free $\mathbb{Z}_p$-modules) first, which gives a close connection to the first part. We then proceed in the usual way, and define p-adic manifolds, Lie groups and their associated Lie algebras (as $\mathbb{Q}_p$-vector spaces). We discuss the algebraic characterisation of p-adic Lie groups as in [2], and conclude with a sketch of the original formulation in [5]. A third reference for this part is [12].

(iii) Part III is concerned with ramification in Lie groups, and Sen's Theorem in particular. We start with a number-theoretic survey on extensions of complete non-archimedean fields (eg. local ones), and define the *ramification filtration* of their Galois groups. Chapter 6 discusses filtrations in a more general context, and defines the class of *Lie filtrations* mentioned above. This allows to finally give a precise statement of Sen's Theorem. Its subsequent proof is very technical, but gives a valuable corollary for the study of "deeply ramified" fields. These will briefly be touched in Chapter 7. References for this last and other applications of Sen's Theorem are [1], [10], [13] and [4]. Direct references for the number-theoretic set-up in Chapter 5 are [11], [3] and [6].

Acknowledgements. This paper was submitted as Diploma Thesis in Mathematics at the University of Bonn. It was supervised by Professor Otmar Venjakob (now University of Heidelberg), and I wish to sincerely thank him for his continued support and his helpful suggestions.

Part I.

Profinite groups and p-adic analysis

1. Profinite group theory

This chapter presents elementary notions from profinite group theory. One of the most important concepts is the lower p-series, a natural filtration on pro-p groups. As a main result, we have that in finitely generated powerful pro-p groups, this filtration takes a particularly simple form – the slogan will be that "every commutator is a p-th power". A fundamental theorem by Serre gives further insight and implies that the topology of these groups is already determined by their algebraic structure. Imposing a regularity condition on certain finite quotients of a powerful group will lead to uniform groups. These allow to define a dimension theory for pro-p groups of finite rank.

While also of group theoretic interest, we primarily study uniform groups as an easily manageable tool in the algebraic treatment of p-adic Lie groups and Lie algebras. These objects were however first described in the more analytic language of filtered groups (cf. [5]). We summarize this approach in section 4.4.

1.1. Profinite and pro-p groups

Definition 1.1. A *profinite group* is a compact, Hausdorff topological group G whose open subgroups form a fundamental system of neighbourhoods of the identity.

Proposition 1.2. ([2], 1.2) *Let G be a profinite group.*

(i) Every open subgroup of G is closed, has finite index in G, and contains an open normal subgroup.

(ii) A closed subgroup $H \subset G$ is itself a profinite group, and every open subgroup of H is of the form $H \cap K$, where K is some open subgroup of G. H is open if and only if it has finite index in G.

(iii) Let N be a closed normal subgroup. Providing G/N with its quotient topology makes it a profinite group. The natural projection $G \to G/N$ is a closed and open map.

The family of quotients (G/N) of G by open normal subgroups N is a projective system together with the natural projections. Any quotient is finite by the Proposition above and provided with the discrete topology. The projective limit $\varprojlim G/N$ carries the subspace topology induced from the product topology on $\prod G/N$. The term "profinite groups" comes from their alternative characterisation as *pro*jective limits of *finite* groups:

Proposition 1.3. ([2], 1.3) *If G is a profinite group, we have an algebraic and topological isomorphism*

$$G \simeq \varprojlim G/N,$$

where N runs through all open normal subgroups. Conversely, the projective limit of any projective system of finite groups is a profinite group.

Example. (i) Galois groups are profinite groups (finite groups carrying the discrete and infinite groups the Krull topology). Conversely, it can be shown that every profinite group appears as Galois group of a suitable field extension.

(ii) The profinite completion of a (topological) group is usually explained as passing to the space of Cauchy series (which are defined as sequences of elements in G whose differences eventually end up in arbitrarily small, normal neighbourhoods of the neutral element) modulo equivalence. These groups can just as well be thought of as profinite with regard to the (projective) system of normal neighbourhoods.

We will mostly deal with topological groups rather than just abstract ones. We thus need a more suitable notion of finiteness, and agree to call a profinite group G *(topologically) finitely generated* if there is an (algebraically) finitely generated set whose closure is G.

Similarly, a profinite group G is a *pro-p group* if every quotient G/N by an open normal subgroup is a p-group. Since every open subgroup of a profinite group contains an open normal subgroup, any subgroup of a pro-p group has p-power index. A closed subgroup of a pro-p group is pro-p again; and we can set forth what we have seen in Proposition 1.3:

Proposition 1.4. ([2], 1.12) *A topological group is a pro-p group if and only if G is (topologically and algebraically) isomorphic to a projective limit of (finite) p-groups.*

Example. (i) $\mathbb{Z}_p$ is a pro-p group, generated by 1 and thus a *procyclic group*.

(ii) Sylow subgroups of profinite groups: A closed subgroup H of a profinite group G is called a *p-Sylow group* if it is a maximal pro-p subgroup. Such groups exist for each prime p.

(iii) Every p-adic Lie group is "locally" a pro-p group: it always contains an open normal (and even uniform) pro-p subgroup. These notions will become clear later.

The frequent appearance of the ring $\mathbb{Z}_p$ in the examples is not coincidental. There is the general phenomenon of *p-adic exponentiation*:

Lemma 1.5. ([2], 1.24) *Let G be a pro-p group and g an element of G. If we take two sequences (a_i), (b_i) of integers that converge to the same limit in $\mathbb{Z}_p$, then the sequences $\left(g^{a_i}\right)$ and $\left(g^{b_i}\right)$ both converge in G, and their limits are equal, too.*

We can hence make the following

Definition 1.6. Let G be a pro-p group, $g \in G$ and $\lambda \in \mathbb{Z}_p$. We define

$$g^\lambda = \lim_{n\to\infty} g^{a_n},$$

where (a_n) is a sequence of integers converging p-adically to λ.

Proposition 1.7. *With g, $h \in G$ and λ, $\mu \in \mathbb{Z}_p$, the operation of "p-adic exponentiation" satisfies:*

(i) $g^{\lambda+\mu} = g^\lambda g^\mu$ *and* $g^{\lambda\mu} = (g^\lambda)^\mu$.

(ii) If $gh = hg$, *then* $(gh)^\lambda = g^\lambda h^\lambda$.

(iii) The map $\lambda \mapsto g^\lambda$ *defines a continuous homomorphism of* $\mathbb{Z}_p$ *into* G. *Its image* $g^{\mathbb{Z}_p}$ *is the closure of* $\langle g \rangle$ *in* G.

1.2. The lower p-series in finitely generated pro-p groups

For a finite group G, the *Frattini subgroup* $\Phi(G)$ is defined as the intersection of all (proper) maximal subgroups. $\Phi(G)$ is a characteristic subgroup, and if G is a p-group, we have $G/\Phi(G) \simeq \mathbb{F}_p^d$, where d is the number of generators of G. We wish to investigate the properties of the profinite analogue.

Definition 1.8. The *Frattini subgroup* of a profinite group G is the intersection of all maximal *open* subgroups of G.

Results on profinite groups are often proved by taking quotients with open normal subgroups (which gives access to results from finite group theory) and "lifting" those results back to apply topological arguments. The following result is a useful example for this:

Proposition 1.9. ([2], 1.13) *Let G^p designate the subgroup of G generated by p-th powers and $[G,G]$ the subgroup generated by the commutators $[g,h] = ghg^{-1}h^{-1}$. If G is a pro-p group, we have $\Phi(G) = \overline{G^p[G,G]}$.*

Proof: It is well-known that in finite p-groups, any maximal (proper) subgroup is normal and has index p. The same is true for general pro-p groups if we restrict ourselves to *open* subgroups. So let M be a maximal proper open subgroup. Since the topology on G can be given by open *normal* subgroups, we can find an open normal subgroup $N \lhd_o G$ contained in M, and such that M/N is a maximal subgroup of the finite p-group G/N. By the correspondence of (normal) subgroups under a group

homomorphism and the classical result from finite p-groups, we conclude that $M \lhd G$ and $(G : M) = p$.

The quotient G/M is thus abelian and annihilated by p. M must thus both contain the derived group and the p-th powers, i.e. $M \supset G^p[G, G]$. Since this holds for arbitrary M, we have

$$\Phi(G) = \bigcap M \supset G^p[G, G]$$

Additionally, since $\Phi(G)$ is closed, we even have $\Phi(G) \supset \overline{G^p[G, G]}$.

For the reverse direction, we need the obvious fact that for a closed normal subgroup $N \lhd_c G$ and $N \subset \Phi(G)$, we have $\Phi(G/N) = \Phi(G)/N$. Now consider the group $Q = G/\overline{G^p[G, G]}$. This is a pro-$p$ group, so its normal subgroups intersect in the identity. If $N \lhd_o Q$, then Q/N is a finite elementary abelian p-group, which means $\Phi(Q/N) = 1$. Therefore $\Phi(Q) \subset \bigcap_{N \lhd_o Q} N = 1$, and by the first inclusion

$$\Phi(G)/\overline{G^p[G, G]} = \Phi(Q) = 1$$

□

As intersection of infinitely many subsets, there is no elementary reason for $\Phi(G)$ to be open again. The following result provides a useful criterion:

Proposition 1.10. ([2], 1.14, 1.20) *A pro-p group G is finitely generated if and only if $\Phi(G)$ is open in G. In this situation, we have $\Phi(G) = G^p[G, G]$.*

We now introduce a fundamental filtration on any pro-p group:

Definition 1.11. The *lower p-series* for a pro-p group G is defined as:

$$G = P_0(G) \supset P_1(G) = \overline{G^p[G, G]} \supset \ldots \supset P_n(G) \supset P_{n+1}(G) = \overline{P_n(G)^p[P_n(G), G]} \supset \ldots$$

We write G_n for $P_n(G)$ when this is not leading to confusion. It is immediate that $G_{n+1} \supset \Phi\big(G_n\big)$ for every n. If G is *finitely generated*, then the groups G_n form a basis of the topology of G (cf. [2], 1.16(iii)). This result is highly useful for a more refined study of pro-p groups, and we will see later that the succesive quotients G_n/G_{n+1} in the above series of characteristic subgroups carry valuable information.

The following relation between the lower p-series and the commutator is easily verified, but essential for our later discussion of Sen's Theorem:

Lemma 1.12. ([2], 1.16, (ii)) *In a pro-p group G, we have $[G_n, G_m] \subset G_{n+m+1}$ for all n, m.*[1]

[1] The result in [2] reads as $[G_n, G_m] \subset G_{n+m}$, which is due to a different numbering of the lower p-series. Similar (minor) deviations will apply for a few other results.

In the light of Proposition 1.10, we focus on finitely generated pro-p groups. The central result is a conversion to Proposition 1.2:

Theorem 1.13 (Serre)**.** ([2], 1.17) *If G is a finitely generated pro-p group, then every (abstract) subgroup of finite index in G is open.*

Let G still denote a finitely generated pro-p group. It can be shown that $G_{n+1} = G_n^p[G_n, G]$ (cf. [2], 1.20) for each n; and, by Proposition 1.10, that the lower p-series consists of *open* subgroups. For finitely generated pro-p groups, taking the closure as in Proposition 1.9 is thus superfluous and Definition 1.11 may be simplified correspondingly. Theorem 1.13 (in combination with the fact that the G_n form a topological basis) enables us to state a remarkable corollary:

Proposition 1.14. ([2], 1.21) *Every algebraic homomorphism from a finitely generated pro-p group G to a profinite group is continuous. In particular, any automorphism is also a topological automorphism. The topology of G is thus completely determined by its algebraic structure.*

1.3. Powerful and uniform groups and their dimension

For a (topologically) finitely generated group G, let $\mathrm{d}(G)$ denote the minimal cardinality of a generating set. It is a strong property to have $\mathrm{d}(H) \leq \mathrm{d}(G)$ for any closed subgroup H of G. We will see that finitely generated *powerful* groups meet this demand, and that their lower p-series eventually consists of *uniform* groups. The latter allow to devise a dimension theory; and the following result is preparatory for this:

Proposition 1.15. ([2], 3.11) *The rank of a profinite group G is defined as*

$$\begin{aligned}\mathrm{rk}(G) &= \sup\{\mathrm{d}(H)\colon\ H \text{ is a closed subgroup of } G\}\\ &= \sup\{\mathrm{d}(H)\colon\ H \text{ is a closed subgroup of } G, \text{ and } \mathrm{d}(H) < \infty\}\\ &= \sup\{\mathrm{d}(H)\colon\ H \text{ is an open subgroup of } G\}\\ &= \sup\{\mathrm{d}(G/N)\colon\ N \text{ is a normal open subgroup of } G\}\end{aligned}$$

The numbers $\mathrm{rk}(G)$ and $\mathrm{d}(G)$ will agree for (finitely generated) *powerful* groups:

Definition 1.16. A pro-p group G (not necessarily finitely generated) is *powerful* if p is odd and $G/\overline{G^p}$ is abelian, or if $p = 2$ and $G/\overline{G^4}$ is abelian.

For any group G and any normal subgroup N, the quotient G/N is abelian if and only if $N \supset [G, G]$. Thus, for p odd, the above definition may be streamlined to $\overline{G^p} \supset [G, G]$. In analogy to Proposition 1.4, a topological group is powerful if and only

if it is the projective limit of a surjective system of finite powerful p-groups (cf. [2], 3.3).

One of the most important properties of *finitely generated* powerful groups is that every element of G^p is already a p-th power (cf. [2], 3.4):

$$G^p = \{x \in G : x = g^p \text{ for some } g \in G\}$$

By induction, this carries on to subgroups of higher powers of p. Similar to previous results, the following theorem is deduced by examining the finite quotients G/G^{p^n}:

Theorem 1.17. ([2], 3.6, 3.8) *Let G be a* finitely generated *powerful p-group.*

(i) For each n, we have $G_{n+1} = G_n^p = \{x \in G : x = g^{p^{n+1}} \text{ for some g} \in G\} = \Phi(G_n)$.

(ii) For each n, the p-th power map $x \mapsto x^p$ induces a homomorphism from G_n/G_{n+1} onto G_{n+1}/G_{n+2}.

(iii) If H is a closed subgroup, we have $\mathrm{d}(H) \leq \mathrm{d}(G)$ and $\mathrm{rk}(G) = \mathrm{d}(G)$ in particular.

We see immediately that the open normal subgroups G_n are again finitely generated powerful groups. Property (i) is often phrased as: "In a finitely generated powerful group, commutators are p-th powers". Property (iii) in turn can be made more precise:

Proposition 1.18. ([2], 3.13) *Let G be a pro-p group. Then G has finite rank if and only if G is finitely generated and has a powerful open subgroup.*

By Theorem 1.17, the lower central series

$$G_0 = G \supset G_1 = \overline{G^p[G_0, G]} \supset \ldots \supset G_n \supset G_{n+1} = \overline{G_n^p[G_n, G]} \supset \ldots$$

can be simplified for finitely generated powerful groups to

$$G_0 = G \supset G_1 = G^p \supset \ldots \supset G_n = G^{p^n} \supset \ldots$$

By definition of the rank in 1.15, even a finite group has positive rank. We will rule out finite pro-p groups (except for the trivial group) by controlling the size of the quotients G_n/G_{n+1}, and arrive at the

Definition 1.19. A pro-p group is *uniform* if G is powerful, finitely generated and all successive quotients G_n/G_{n+1} have the same size.

By Lemma 1.12, each of these quotients is an abelian p-group, annihiliated by p-th powers, and thus isomorphic to $(\mathbb{Z}/p\mathbb{Z})^d$, for some d (which will turn out to be the *dimension* of G). We also have an immediate, yet important refinement of Theorem 1.17: the p-th power map $x \mapsto x^p$ induces the shift-isomorphism sh: $G_n/G_{n+1} \simeq G_{n+1}/G_{n+2}$.

Example. Let $\Gamma = \mathrm{GL}_d(\mathbb{Z}_p)$ denote the group of linear automorphisms of $\mathbb{Z}_p^d$, provided with the p-adic subspace topology from $\mathrm{Mat}_d(\mathbb{Z}_p)$. Γ is a closed and open subgroup, and thus compact and profinite. With $n \geq 1$, a basis of the neighbourhoods of 1 is given by the *congruence subgroups*

$$\begin{aligned}\Gamma_n &= \{\gamma \in \Gamma : \gamma \equiv 1 \bmod (p^n)\} \\ &= \ker\big(\Gamma \to \mathrm{GL}_d(\mathbb{Z}/p^n\mathbb{Z})\big)\end{aligned}$$

It follows that $(\Gamma : \Gamma_1) = (p^d - 1)(p^d - p)\dots(p^d - p^{d-1})$ and $(\Gamma_1 : \Gamma_n) = p^{d^2(n-1)}$, so Γ_1 is a pro-p group. We now set $G = \Gamma_1$ if p is odd, and $G = \Gamma_2$ if $p = 2$. By means of a suitable version of Hensel's Lemma, G can be shown to be a uniform group, with $G_n = \Gamma_{n+1}$ for odd p, and $G_n = \Gamma_{n+2}$ for $p = 2$ (cf. [2], 5.1). The quotients have constant size $(G_n : G_{n+1}) = p^{d^2}$, and $\mathrm{d}(G) = d^2$.

We continue with a few easy results that will prove useful for an algebraic characterisation of p-adic Lie groups.

Proposition 1.20. ([2], 4.2) *Let G be a finitely generated powerful pro-p group. Then G_n is uniform for all sufficiently large n.*

Proof: We denote each quotient's size by $|G_n : G_{n+1}| = p^{d_n}$. Because taking p-th powers acts as a surjective homomorphism between quotients (see Theorem 1.17 (i)), we have $d_1 \geq d_2 \geq \dots$. Hence there exists r such that $d_n = d_r$ for all $n \geq r$. By Theorem 1.17, we know that all G_n are finitely generated and powerful, and hence uniform for $n \geq r$. □

Corollary 1.21. ([2], 4.3) *A pro-p group of finite rank has a characteristic uniform subgroup.*

Proposition 1.22. ([2], 4.4) *Let G be a powerful finitely generated pro-p group with $\mathrm{d}(G) = d$. The following are equivalent:*

(i) *G is uniform.*

(ii) $\mathrm{d}(G_n) = \mathrm{d}(G)$ *for all n.*

(iii) $\mathrm{d}(H) = \mathrm{d}(G)$ *for every powerful open subgroup H of G.*

Proof: The "non-generators" within G_n are given by $\Phi(G) = G_{n+1}$, so by Theorem 1.17, we have

$$\mathrm{d}(G_n) = \mathrm{d}(G_n/G_{n+1}) \leq \mathrm{rk}(G) = d.$$

Any open powerful subgroup H contains some G_n (for the G_n are a basis of the topology), so we have

$$\mathrm{d}(G_n) \leq \mathrm{d}(H) \leq \mathrm{rk}(G) = d.$$

Now G is uniform if and only if $\mathrm{d}(G_n/G_{n+1}) = \mathrm{d}(G_1/G_2) = d$ for all n. □

Corollary 1.23. ([2], 4.6) *If H and I are open uniform subgroups of some pro-p group then $\mathrm{d}(H) = \mathrm{d}(I)$.*

Proof: For n large enough, we have $H_n \subset (H \cap I) \subset I$. By the last Proposition, $\mathrm{d}(I) = \mathrm{d}(H_n) = \mathrm{d}(H)$. □

Combined with Corollar 1.21, this allows to finally define the notion of dimension:

Definition 1.24. Let G be a pro-p group of finite rank. The *dimension* of G is

$$\dim(G) = \mathrm{d}(H),$$

where H is any open uniform subgroup of G. For a finite group G, we put $\dim(G) = 0$.

There are several deep relations between a uniform group G and the p-adic integers. The following result exhibits a map whose inverse function is a "chart" of G with values in $\mathbb{Z}_p$. We will refer to these values as (multiplicative) "coordinates of the second kind".

Proposition 1.25. *Let G be a uniform group and $(a_1, \ldots, a_d)$ a set of topological generators with $d = \mathrm{d}(G) = \dim(G)$. There is a homeomorphic mapping*

$$\phi\colon \mathbb{Z}_p^d \longrightarrow G, \quad (\lambda_1, \ldots, \lambda_d) \mapsto a_1^{\lambda_1} \ldots a_d^{\lambda_d}$$

We conclude with a collection of deeper results that are of interest in their own right.

Theorem 1.26. ([2], 4.5) *A finitely generated powerful pro-p group is uniform if and only if it is torsion-free.*

Theorem 1.27. ([2], 4.8) *Let G be a pro-p group of finite rank and N a closed normal subgroup of G. The concept of dimension behaves additively on short exact sequences:*

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

Corollary 1.28. ([2], 4.31) *Let G be a uniform group and $N \subset G$ a closed, normal subgroup. If G/N is uniform, then N is uniform, too.*

Proof: In the light of Theorem 1.26, we need to show that N is powerful. As G/N is torsion-free (by Theorem 1.26 again), it follows that $x^{p^n} \in N$ implies $x \in N$. This shows that $G^p \cap N = N^p$ and hence that N/N^p is abelian. For an odd prime p, this is just the requirement for N to be powerful. For $p = 2$, we modify the above in an obvious fashion to show that N/N^4 is abelian. □

2. p-adic analysis

This section explains elementary notions in ultrametric analysis. The concept of p-adic analytic functions is central, and we have as main result that on a suitable subset of a complete $\mathbb{Q}_p$-algebra, one can define p-adic versions of the analytic Exponential and Logarithm.

Definition 2.1. A *normed ring* is a ring A (not necessarily commutative) with a valuation $\|\cdot\| : A \to \mathbb{R}$ that satisfies

(i) $\|a\| \geq 0$, and $\|a\| = 0$ if and only if $a = 0$

(ii) $\|1\| = 1$, and $\|ab\| \leq \|a\| \cdot \|b\|$

(iii) $\|a + b\| \leq \max\{\|a\|, \|b\|\}$

for all elements $a, b \in A$. A normed ring is *complete* if it is complete as a metric space with the induced distance function $d(a, b) = \|a - b\|$. The normed ring $(A, \|\cdot\|)$ is a $\mathbb{Q}_p$*-algebra* (in the analytic sense) if it is an algebra over $\mathbb{Q}_p$ (in the algebraic sense) that satisfies $\|\lambda a\| = |\lambda|_p \ \|a\|$, where $|\cdot|_p$ denotes a p-adic norm of $\mathbb{Q}_p$.

Example. (i) $(\mathbb{Q}, |\cdot|_p)$ is a normed ring with completion $\mathbb{Q}_p$. The matrix ring $\mathrm{M}_n(\mathbb{Q}_p)$ with the maximum norm $\|A\| = \|(a_{ij})\| = \max\{|a_{ij}|_p\}$ is a complete $\mathbb{Q}_p$-algebra.

(ii) A generalisation of the p-adic valuation on $\mathbb{Z}$ is given as follows. Let $A = A_0 \supset A_1 \supset \ldots$ be a chain of ideals in A such that $\cap_{n\in\mathbb{N}} A_n = 0$ and $A_n A_m \subset A_{n+m}$ for all n, m. Now fix any real number $q > 1$ and define a norm on A by $\|0\| = 0$, $\|a\| = q^{-n}$ if $a \in A_n \backslash A_{n+1}$.

We yet need to define *non-commutative* power-series, which will serve as "local representation" of analytic functions.

Definition 2.2. The *ring of formal power series in the (non-commuting) variables* $X = (X_1, \ldots, X_n)$ is the set of all formal sums

$$\sum_{w\in W} \lambda_w w,$$

where W is the set of all words w in X and $\lambda_w \in \mathbb{Q}_p$. Declaring addition componentwise and multiplication by concatenation of words, this set is made into a $\mathbb{Q}_p$-algebra. We will denote this ring by $\mathbb{Q}_p\langle\langle X\rangle\rangle$.

For the rest of the chapter, let $\widehat{A}$ denote a complete $\mathbb{Q}_p$-algebra. In order to evaluate power series in a non-commutative normed ring, we will need a modified notion of convergent series:

Definition 2.3. Let I be an infinite, countable index set, and let $a, s \in \widehat{A}$.

(i) A family $(a_i)_{i\in I}$ *converges to* a (written as $\lim_{i\in I} a_i = a$) if for each $\varepsilon > 0$, there exists a finite subset $I' \subset I$ such that $\|a_i - a\| < \varepsilon$ for all $i \notin I'$.

(ii) The series $\sum_{i\in I} a_i$ *converges with sum* s, if for each $\varepsilon > 0$, there exists a finite set I' such that for all finite sets I'' with $I' \subset I'' \subset I$, we have $\|s - \sum_{i\in I''} a_i\| < \varepsilon$.

In fact, condition (ii) turns out to be analogous to absolute convergence in the real set-up (cf. [2], Prop. 6.9). Concepts from the real case such as double series, Cauchy multiplication and uniqueness of power series (cf. [2], 6.11, 6.12 and 6.13 resp.) can now be formulated. We can also evaluate formal power series:

Definition 2.4. The formal power series $F(X) = \sum_{w\in W} a_w w$ can be *evaluated at* $x = (x_1, \ldots, x_n) \in \widehat{A}^n$ if the series $\sum_{w\in W} a_w w(x)$ obtained by substituting x_i for X_i in each word w converges in $\widehat{A}$.

Most importantly, we can now define analytic functions:

Definition 2.5. We provide $\widehat{A}^n$ with its product topology and take an open, non-empty subset $D \subset \widehat{A}^n$. A map $f : D \to \widehat{A}$ is called *strictly analytic on* D if there exists $F(X) = \sum a_w w \in \mathbb{Q}_p\langle\langle X\rangle\rangle$ such that for all $x \in D$, we have

(i) $\lim_{w\in W} \big(|a_w| \cdot w\left(\|x_1\|, \ldots, \|x_n\|\right)\big) = 0$, and

(ii) $f(x) = F(X)$

It is a matter of persistent calculations to see that strictly analytic functions are continous ([2], Prop. 6.19). The by far most important example for our purposes are the p-adic Exponential and Logarithm, which are given by power series in one variable:

Proposition 2.6. ([2], 6.22) *Let*

$$\widehat{A}_0 = \begin{cases} \left\{x \in \widehat{A} : \|x\| \leq p^{-1}\right\} & \text{if } p \neq 2, \\ \left\{x \in \widehat{A} : \|x\| \leq 2^{-2}\right\} & \text{if } p = 2. \end{cases}$$

There are strictly analytic functions

$$\exp\colon \widehat{A}_0 \to 1 + \widehat{A}_0, \quad \log\colon 1 + \widehat{A}_0 \to \widehat{A}_0$$

that are given for all $x \in A_0$ by the power series:

$$E(X) = \sum_{n=0}^{\infty} \frac{1}{n!} X^n, \quad L(X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} X^n.$$

These functions have the following properties:

(i) $\log\big(\exp(x)\big) = x$

(ii) $\exp\big(\log(1+x)\big) = 1 + x$

(iii) $\log\big((1+x)^n\big) = n \cdot \log(1+x)$ *for each* $n \in \mathbb{Z}$

(iv) $\exp(n \cdot x) = \big(\exp(x)^n\big)$ *for each* $n \in \mathbb{Z}$

The definition of $\widehat{A}_0$ not only guarantees that $E(x)$ and $L(x)$ converge, but also ensures that their evaluation and composition commute. The following is an important combination of the two series and will later appear as an essential link between a Lie group and its associated Lie algebra.

Definition 2.7. The *Campbell-Hausdorff series* is defined as

$$\Phi(X, Y) = (L \circ P)(X, Y),$$

where $P(X, Y) = E(X)E(Y) - 1$ is a formal power series in $\mathbb{Q}_p\langle\langle X, Y\rangle\rangle$.

There is an elementary connection between the Campbell-Hausdorff series $\Phi(X, Y)$ on the one hand and the p-adic exponentiation and logarithm on the other hand:

Proposition 2.8. ([2], 6.27) *Let $x, y \in \widehat{A}_0$. Then both Φ and Ψ can be evaluated at (x, y), and $\Phi(x, y) = \log(\exp x \cdot \exp y)$.*

We conclude this chapter and throw a glance at the commutative case of power series in $\mathbb{Q}_p$. There is of course a natural epimorphism

$$\overline{\cdot} : \mathbb{Q}_p\langle\langle X\rangle\rangle \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Q}_p[\![X]\!]$$

with kernel generated by the commutators. Replacing the set of words in n variables with the set of monomials in these, we can repeat the definitions given before. The morphism $\overline{\cdot}$ is compatible with (non-)commutative evaluation on elements with commuting components:

Proposition 2.9. ([2], 6.34) *Let $F(X) \in \mathbb{Q}_p\langle\langle X\rangle\rangle$ and suppose that $F(x)$ exists for an $x = (x_1, \ldots, x_n) \in \widehat{A}^n$ with $x_i x_j = x_j x_i$. Then $\overline{F(X)}$ can be evaluated at x and $\overline{F}(x) = F(x)$.*

Corollary 2.10. ([2], 6.36) *Let $x, y \in \widehat{A}_0$ and suppose that $xy = yx$. Then*

$$\exp(x - y) = \exp(x)(\exp(y))^{-1}$$

Part II.

Lie theory

3. Lie algebras

A Lie algebra should be thought of as a "linear approximation" to a Lie group that is easier to understand but preserves valuable information. The precise treatment of this idea will be prepared in this section. We have as main result that (by means of the analytic map log) any uniform group G admits an associated *powerful* $\mathbb{Z}_p$-Lie algebra $\log(G)$. Conversely, any such powerful algebra $\mathfrak{g}$ can be realized as associated Lie algebra of some uniform group $\exp(\mathfrak{g})$. An equivalence of these two categories will be established in Theorem 3.10.

Definition 3.1. Let R be a commutative ring. A *Lie algebra* is an R-module $\mathfrak{g}$ with a bilinear mapping (the *Lie bracket*)

$$(\ ,\ ) : \mathfrak{g} \times \mathfrak{g} \longrightarrow \mathfrak{g}$$

that satisfies $(a,a) = 0$ and the *Jacobi identity* $\big((a,b),c\big) + \big((b,c),a\big) + \big((c,a),b\big) = 0$. A *Lie ideal* $\mathfrak{a} \subset \mathfrak{g}$ is an R-submodule that is closed under the Lie bracket, i.e. $(a,\lambda) \in \mathfrak{a}$ whenever $a \in \mathfrak{a}$ and $\lambda \in \mathfrak{g}$. A *morphism φ of Lie algebras* is a morphism of R-modules that satisfies $\varphi\big((a,b)\big) = \big(\varphi(a),\varphi(b)\big)$.

The category of Lie algebras over R is closed under taking quotients by an ideal, and the projection onto such a quotient is a morphism of Lie algebras. Any Lie ideal is thus the kernel of some Lie algebra morphism.

Example. Before diverting into the special case of uniform groups, we have a brief look at a general method to associate a Lie algebra (as a linear approximation) to a group G. We will revert to this in greater detail in section 4.4.

A *filtered group* (G,v) exhibits a valuation $v : G \to \mathbb{R} \cup \{\infty\}$ such that

(i) $v(g) > 0$ and $v(1) = \infty$

(ii) $v(gh^{-1}) \geq \min\{v(g), v(h)\}$

(iii) $v\big([g,h]\big) \geq v(g) + v(h)$

For each $x > 0$, there are normal subgroups $G_x = \{g \in G : v(g) \geq x\}$ and $G_{x+} = \{g \in G : v(g) > x\}$. The *graded group* $\mathrm{gr}(G) = \bigoplus G_x/G_{x+}$ is abelian by (iii). The maps $G_x \times G_y \to G_{x+y},\ x,y \mapsto [x,y]$ induce maps on the projections G_x/G_{x+} and G_y/G_{y+}, which can be extended by linearity to the whole of $\mathrm{gr}(G)$ to make it a Lie algebra.

An example for a filtered group is the first congruence subgroup

$$\begin{aligned}\Gamma_1 &= \{\gamma \in \mathrm{GL}_d(\mathbb{Z}_p) : \gamma \equiv 1 \bmod (p)\} \\ &= \ker\big(\mathrm{GL}_d(\mathbb{Z}_p) \to \mathrm{GL}_d(\mathbb{F}_p)\big)\end{aligned}$$

Any matrix $g = (g_{ij}) \in \Gamma_1$ can be written as $1 + x$, where $x = (x_{ij})$ has coefficients in $\mathfrak{m} = p\mathbb{Z}_p$. We define $v(g) = \inf\{v_p(x_{ij})\}$, and it can be checked easily (cf. [12], part I, chp. 2, 4) that v is in fact a valuation.

3.1. The $\mathbb{Z}_p$-Lie algebra of a uniform group

In this section, we will focus on Lie algebras of finite rank $d > 0$ over $R = \mathbb{Z}_p$. There are two ways to give any uniform group G of dimension d such a Lie algebra structure:

The algebraic approach. Extracting p^n-th roots defines an *abelian* group operation $+_G$ on G for $n \to \infty$. Keeping the topology, $(G, +_G)$ remains a uniform pro-p group. By a similar method, it inherits a Lie bracket from the original multiplication in G, and we denote this Lie algebra with $(G, +_G, (\ )_G)$.

The analytic approach. The completed group algebra $\mathbb{Z}_p[\![G]\!]$ is (topological) isomorphic to the completion of $\mathbb{Z}_p[G]$ with regard to a certain norm. This norm can be extended to $\mathbb{Q}_p[G]$ and makes it an (associative) $\mathbb{Q}_p$-Lie algebra. We denote its completion by $\widehat{A}$. G embeds *as a set* into a certain subset $1 + \widehat{A}_0 \subset \widehat{A}$, whereon the analytic function log is defined. The image $\log(G)$ is a Lie subalgebra of $\widehat{A}$ which we denote by $(\Lambda, +_{\mathrm{ind}}, [\ ]_{\mathrm{ind}})$.

It is a non-trivial result that Λ is closed under the induced Lie algebra operations. A convenient proof uses the algebraic construction of $(G, +_G)$, and establishes an isomorphism

$$\big(G, +_G, (\ )_G\big) \simeq \big(\Lambda, +_{\mathrm{ind}}, [\ ]_{\mathrm{ind}}\big)$$

of Lie algebras. We will see that this isomorphism is induced by the Logarithm, and that it provides G with with an *additive* system of coordinates, complementing the multiplicative "coordinates of the second kind" in Proposition 1.25.

The algebraic approach

By Proposition 1.17, the lower p-series of a finitely generated uniform group has the simple shape

$$G_0 = G \supset G_1 = G^p \supset \ldots \supset G_n = G^{p^n} \supset \ldots$$

It is then easy to see that each element $x \in G_n$ has a unique p^nth root in G. In other words, the map

$$G \longrightarrow G_n, \quad x \mapsto x^{p^n}$$

is a homeomorphism, with inverse map written as p^n-th roots. For each n, these define a new group structure on G:

$$+_n : \ G \times G \longrightarrow G, \quad (x, y) \mapsto x +_n y = (x^{p^n} y^{p^n})^{p^{-n}}$$

These operations are compatible with higher powers and invariant under multiplicative "disturbances" from within G_n. More precisely, for $x, y \in G$, we have $x +_m y \equiv x +_n y \pmod{G_{n+1}}$ for $m > n$, and $xu +_n yv \equiv x +_n y \pmod{G_n}$ for $u, v \in G_n$. We obtain a group structure on G as a limit of the operations $+_n$:

Proposition 3.2. ([2], section 4.3) *G becomes an abelian group under the operation $x +_G y = \lim_{n\to\infty} x +_n y$. For all $x, y \in G$, we have*

(i) If $xy = yx$, then $x +_G y = xy$.

(ii) For each interger m, $mx = x^m$.

(iii) For each $n \geq 0$, $p^n G = G_n$.

(iv) If $x, y \in G_n$, then $x +_G y \equiv xy \pmod{G_{n+1}}$.

There is some interplay between the multiplicative and additive structure on G. For instance, each G_n is also an additive subgroup, and the identity map $G_n/G_{n+1} \to G_n/G_{n+1}$ is an "isomorphism of quotients" between the multiplicative and additive structure. The following result proceeds in this direction, and introduces a mapping ψ that gives G "coordinates of the first kind".

Proposition 3.3. ([2], 4.16 and 4.17) *With the original topology, $(G, +_G)$ is a uniform pro-p group of dimension $d = \mathrm{d}(G)$. G has the structure of free $\mathbb{Z}_p$-module on the basis of the topological generators $\{a_1, \ldots, a_d\}$, and there is an isomorphism of $\mathbb{Z}_p$-modules*

$$\psi : G \longrightarrow \mathbb{Z}_p^d, \quad \lambda_1 a_1 +_G \ldots +_G \lambda_d a_d = g \mapsto (\lambda_1, \ldots, \lambda_d)$$

The loss of structural information under ψ is significant. More information can be transferred from G onto $(G, +_G)$ by defining a Lie bracket as follows: By Lemma 1.12, the commutator $[x^{p^n}, y^{p^n}]$ of p^nth powers is contained in G_{2n+1} for each n. This allows to extract p^{2n}th roots and to set $(x, y)_n = [x^{p^n}, y^{p^n}]^{p^{-2n}}$ (which lies in pG). By similar arguments as for the abelian operation "$+_G$" (cf. [2], 4.30 for details), the sequence $(x, y)_n$ can be shown to be Cauchy. We thus define $(x, y)_G$ as the limit $\lim_{n\to\infty}(x, y)_n$, and this operation makes $\big(G, +_G, (\ )_G\big)$ a Lie algebra over $\mathbb{Z}_p$.

The analytical approach

The group algebra $\mathbb{Z}_p[G]$ of a pro-p group G gives rise to the projective system $(\mathbb{Z}_p[G/N])$, where N is an open normal subgroups and each component has the topology of a free $\mathbb{Z}_p$-module. The limit

$$\mathbb{Z}_p[\![G]\!] = \varprojlim \mathbb{Z}_p[G/N]$$

is the *completed group algebra of* G (or also *Iwasawa algebra of* G). We wish to rephrase its construction in analytic terms. Our first result is a slight reformulation of a theorem due to Lazard:

Proposition 3.4. ([5], II.2.2.2 and [2], pp138–141) *Let G be a finitely generated pro-p group. There exists a norm $\|\cdot\|$ on $\mathbb{Z}_p[G]$ such that the corresponding analytic completion $\widehat{\mathbb{Z}_p[G]}$ is topologically isomorphic to $\mathbb{Z}_p[\![G]\!]$.*

The norm $\|\cdot\|$ is constructed by a chain of ideals (see the example after Definition 2.1): Let $I = (G-1)\mathbb{Z}_p[G]$ denote the augmentation ideal of $\mathbb{Z}_p[G]$ and $J = I + p\mathbb{Z}_p[G]$ the kernel of the natural reduction $\mathbb{Z}_p[G] \to \mathbb{F}_p$. The powers of J are cofinal with another chain of ideals that determines the topology of $\mathbb{Z}_p[G]$, and hence so does (J^n).

For a *uniform* group G, it can be shown that every element of $\mathbb{Z}_p[G]$ is *uniquely* represented as a certain power series in the (fixed) topological generators of G (cf. [2], 7.5). This allows to place ourselves in the set-up of Proposition 2.6:

Proposition 3.5. ([2], 7.7) *Let G be a uniform pro-p group of finite rank d. Then $(\mathbb{Q}_p[G], \|\cdot\|) = A$ is a normed $\mathbb{Q}_p$-algebra. The norm on A induces the original topology on G and each element $g \in G$ satisfies $\|g-1\| \leq p^{-1}$.*

We keep the above assumption on G, and let $\widehat{A}$ denote the completion of A with regard to $\|\cdot\|$. $\widehat{A}$ is an associative algebra, and thus carries a natural Lie algebra structure by means of the commutator bracket. Setting

$$\widehat{A_0} = \begin{cases} \{x \in A : \|x\| \leq p^{-1}\} & \text{if } p \neq 2 \\ \{x \in A : \|x\| \leq 2^{-2}\} & \text{if } p = 2 \end{cases}$$

and possibly replacing G with G_1 for $p = 2$, we have $G - 1 \subset \widehat{A_0}$ under the canonical injection of G into $\widehat{A}$. Proposition 2.6 guarantees there is a mapping $\log : 1 + \widehat{A_0} \to \widehat{A_0}$, giving

$$\Lambda = \log(G) \subset \widehat{A_0}$$

We denote the restriction of the Lie algebra operations on $\widehat{A}$ to the subset Λ as $(\Lambda, +_{\mathrm{ind}}, [\ ]_{\mathrm{ind}})$. It is not clear that Λ is closed under these induced operations, for $\log : G \to \widehat{A_0}$ is *not* a group homomorphism. This is however true with G replaced by $(G, +_G)$, as the following result shows:

Lemma 3.6. *([2], 7.12) For $g, h \in G$ and $\lambda \in \mathbb{Z}_p$, we have*

$$\log g +_{\mathrm{ind}} \log h = \log(g +_G h), \quad \lambda \log g = \log g^\lambda$$
$$[\log g, \log h]_{\mathrm{ind}} = \log(g, h)_G$$

The following is now an immediate consequence:

Proposition 3.7. ([2], 7.13, 7.14) *$(\Lambda, +_{\mathrm{ind}}, [\ ]_{\mathrm{ind}})$ is a $\mathbb{Z}_p$-Lie subalgebra of $\widehat{A}$. It is denoted by $\log(G)$, since it is isomorphic (as Lie algebra) to $(G, +_G, (\ )_G)$ under the analytic map* log. *Both algebras are free $\mathbb{Z}_p$-modules of rank d.*

3.2. Powerful Lie algebras

By means of the Campbell-Hausdorff series, the process of assigning a Lie algebra to a uniform group can be reversed. However, we have to restrict ourselves to a certain kind of Lie algebras:

Definition 3.8. A Lie algebra $\mathfrak{g}$ over $\mathbb{Z}_p$ is *powerful* if there is an isomorphism $\phi : \mathfrak{g} \to \mathbb{Z}_p^d$ of $\mathbb{Z}_p$-modules for some d and

$$(\mathfrak{g}, \mathfrak{g}) \subset \begin{cases} p\,\mathfrak{g} & \text{if } p > 2, \\ 4\,\mathfrak{g} & \text{if } p = 2. \end{cases}$$

The isomorphism ϕ embeds $\mathfrak{g}$ into the algebra $\mathbb{Q}_p\,\mathfrak{g} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathfrak{g}$, and Proposition 2.8 enables to evaluate the Campbell-Hausdorff series Φ on this set. It can be shown that Φ maps the image of $\mathfrak{g}$ in $\mathbb{Q}_p\mathfrak{g}$ onto itself,[1] and we obtain:

Proposition 3.9. ([2], 9.8) *Let $\mathfrak{g}$ be a powerful Lie algebra. The operation $* : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, $x * y = \Phi(x, y)$ makes $\mathfrak{g}$ into a uniform pro-p group. If $\{a_1, \ldots, a_d\}$ is a $\mathbb{Z}_p$-basis for $\mathfrak{g}$, then $(\mathfrak{g}, *)$ is a group of dimension d, topologically generated by $\{a_1, \ldots, a_d\}$.*

Any abstract group homomorphism $f : G \to H$ of uniform groups is continuous by Proposition 1.14. As the Lie operations in L_G and L_H are defined by certain limits of the initial group operations, we see that $f : L_G \to L_H$ as a map of the underlying sets is already a Lie algebra morphism.

On the other hand, any morphism $f : \mathfrak{g} \to \mathfrak{h}$ of powerful Lie algebras is evidently continuous. For each $n \geq 1$, we have $f(u_n(x, y)) = u_n(f(x), f(y))$, where u_n is a Lie

[1] Two aspects are decisive: firstly, in $\mathbb{Q}_p\langle\langle X, Y\rangle\rangle$, the Campbell-Hausdorff series $\Phi(X, Y)$ is expressible as an infinite sum of *Lie elements* $u_n(X, Y)$. These are defined as certain sums of commutators (cf. [2], pp15–116 for details). This holds just as well for the Campbell-Hausdorff series in $\mathbb{Q}_p\,\mathfrak{g}$. Secondly, $\mathfrak{g}$ is powerful: this ensures that the Lie elements of $\mathbb{Q}_p\,\mathfrak{g}$ lie within $p\mathfrak{g}$ and $4\mathfrak{g}$, respectively, and that their sum converges within $\mathfrak{g}$.

element.[2] By continuity again we have $f\big((x) * (y)\big) = f(x) * f(y)$. Thus f is a group homomorphism from $(\mathfrak{g}, *)$ to $(\mathfrak{h}, *)$. This section's main result is:

Theorem 3.10. ([2], 9.10) *There is an equivalence of categories between uniform pro-p groups and powerful $\mathbb{Z}_p$-Lie algebras:*

$$\begin{array}{ccccc} \{\textit{Uniform groups}\} & & \{\textit{Powerful algebras}\} & & \{\textit{Powerful assoc. algebras}\} \\ G & \longrightarrow & L_G = (G, +_G, (\ )_G) & \xrightarrow{\sim} & \log(G) = (\Lambda, +_{\mathrm{ind}}, [\ ]_{\mathrm{ind}}) \\ (\mathfrak{g}, *) & \longleftarrow & \mathfrak{g} & \xrightarrow{\sim} & (\log(\mathfrak{g}), +_{\mathrm{ind}}, [\ ]_{\mathrm{ind}}) \end{array}$$

$$\exp$$

We conclude this section with a result that clarifies the role of Lie ideals:

Proposition 3.11. ([2], 7.15, 4.31) *Let G be a uniform group, and let $\mathscr{L} = \log(G)$ denote its $\mathbb{Z}_p$-Lie algebra. The following are equivalent:*

(i) $I \subset \mathscr{L}$ is a Lie ideal such that $\mathscr{L}/I$ is torsion-free.

(ii) $N = \exp(I)$ is uniform, closed and normal in G, and G/N is uniform.

[2] The statement follows from the definition of a Lie algebra morphism and the fact that $p^{2n}u_n(X, Y)$ is a $\mathbb{Z}_p$-linear combination of Lie monomials in X and Y. For the definition of Lie elements, see [2], pp15–116.

4. p-adic Lie groups

A p-adic Lie group is an ultrametric analogon to real and complex Lie groups. Although p-adic analytic manifolds share the formal definition of their real and complex counterparts, there is considerable discrepancy between the properties of the Lie groups. Structural reasons are the different topologies of the respective underlying spaces, and the prominence of discrete valuation rings in the ultrametric case.

The latter establishes a connection to the group theoretic results in Chapter 1 and leads to this section's main result, a general and very powerful characterisation of p-adic analytical groups due to Lazard:

Theorem 4.1. *A topological group G has the structure of a p-adic Lie group if and only if G has an open subgroup that is a powerful finitely generated pro-p group.*

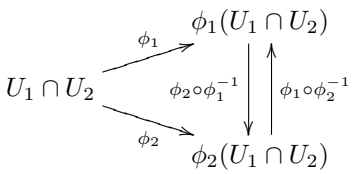
This result allows to define the dimension of a Lie group and its associated Lie algebra in *algebraic* terms. We explain the alternative definition as tangent space endowed with a Lie bracket and conclude with a brief summary of Lazard's more analytic approach via p-valuable groups.

4.1. Analytic manifolds and Lie groups over $\mathbb{Q}_p$

This first section reviews elementary concepts within the theory of p-adic Lie groups. The fundamental objects are *p-adic manifolds*:

Definition 4.2. (i) Let X be a topological space and U a (non-empty) open subset of X. A triple (U, ϕ, d) is a *chart* on X if ϕ is a homeomorphism from U onto an open subset of $\mathbb{Q}_p^d$. The dimension of the chart is d. The chart (U, ϕ, d) is a *global chart* if $U = X$.

(ii) Two charts (U_1, ϕ_1, d_1) and (U_2, ϕ_2, d_2) on X are *compatible* if the maps $\phi_2 \circ \phi_1^{-1}|_{\phi_1(U_1 \cap U_2)}$ and $\phi_1 \circ \phi_2^{-1}|_{\phi_2(U_1 \cap U_2)}$ are analytic functions on $\phi_1(U_1 \cap U_2)$ and $\phi_2(U_1 \cap U_2)$ respectively. (It can be shown that this entails $d_1 = d_2$.)



(iii) An *atlas* $\mathcal{A} = \{(U_i, \varphi_i, d_i)_{i\in I}\}$ of X is a set of pairwise compatible charts whose underlying spaces cover X. Two atlases $\mathcal{A}_1$ and $\mathcal{A}_2$ of X are *compatible* if every chart in $\mathcal{A}_1$ is compatible with every chart in $\mathcal{A}_2$. Equivalently, $\mathcal{A}_1$ and $\mathcal{A}_2$ are compatible if $\mathcal{A}_1 \cup \mathcal{A}_2$ is an atlas of X.

Compatibility of atlases is an equivalence relation (cf. [2], Prop. 8.7, or [12], section III.1). We can therefore make the following

Definition 4.3. (i) An *analytic manifold structure* on a topological space X is an equivalence class of compatible atlases. X is called a *analytic manifold* if such a structure exists.

(ii) A *morphism* (or *analytic function*) of manifolds is a continuous map $f : X \to Y$ of the underlying spaces that is "locally given by analytic functions". This means that there exist atlases $\mathcal{A}$ and $\mathcal{B}$ such that for each pair of charts, the composition

$$\phi(U \cap f^{-1}V) \xrightarrow{\phi^{-1}} U \xrightarrow{f} V \xrightarrow{\psi} \psi(V)$$

is analytic.

(iii) An open subset $O \subset X$ is given the *induced manifold structure* (or *submanifold* for brevity) by restriction of the charts to O. Also, the Cartesian product $X \times Y$ of the underlying spaces of two manifolds X and Y can be provided with the structure of a *product manifold* in the obvious way.

Because of the importance of $\mathbb{Z}_p$ as valuation ring, charts are often defined as maps to an open subset of $\mathbb{Z}_p$ rather than $\mathbb{Q}_p$. The first of the following examples shows that this is no restriction.

Example. (i) The space $X = \mathbb{Q}_p^d$ is covered by the open subsets $\{U_i = p^{-i}\mathbb{Z}_p^d\}$ with natural numbers i. These sets are homeomorphic to $\mathbb{Z}_p^d$ by the maps $\phi_i(x) = p^i x$, so the atlas $\mathcal{A} = \{(U_i, \phi_i, d)_{i\in\mathbb{N}}\}$ gives $\mathbb{Q}_p^d$ the structure of a p-adic manifold.

(ii) The group $X = \mathrm{GL}_d(\mathbb{Q}_p)$ is an open subgroup of $\mathrm{Mat}_d(\mathbb{Q}_p) = \mathbb{Q}_p^{d^2}$ and has a submanifold structure.
There is another (seemingly better-adapted) choice of atlas. The subgroup $U = 1 + p\,\mathrm{Mat}_d(\mathbb{Z}_p)$ is mapped to $\mathbb{Z}_p^{d^2}$ by $\phi(u) = u - 1$. This gives a chart (U, ϕ, d^2) of U, which we extend to the whole of X. For each $x \in X$, there is the open neighbourhood $U_x = xU$ of x and the map $\phi_x : U_x \to p\,\mathrm{Mat}_d(\mathbb{Z}_p)$, $u \mapsto x^{-1}u$. This yields $\mathcal{A} = \{(U_x, \phi_x, d^2),\ x \in X\}$ as atlas on X.

(iii) A uniform group G of dimension d can be given the structure of p-adic manifold in several ways. In Proposition 1.25 we introduced the "coordinates of the second kind" coming from the global chart $\phi^{-1}\colon G \longrightarrow \mathbb{Z}_p^d$, $g = a_1^{\lambda_1} \dots a_d^{\lambda_d} \mapsto (\lambda_1, \dots, \lambda_d)$.
The algebraic construction of a Lie algebra in section 3.1 (see Proposition 3.3)

exhibited the "coordinates of the first kind"; and the map $\psi : G \longrightarrow \mathbb{Z}_p^d,\ \lambda_1 a_1 + \ldots + \lambda_d a_d = g \mapsto (\lambda_1, \ldots, \lambda_d)$ gives another global chart.
The analytic approach featured $\log : G \to \Lambda \subset \widehat{A}$, a homeomorphism from G into a $\mathbb{Z}_p$-Lie algebra of dimension d. Choosing a $\mathbb{Z}_p$-basis for Λ, we obtain a map $\vartheta : \Lambda \to \mathbb{Z}_p^d$ and thus even another global chart $(G, \vartheta \circ \log, d)$. It is however immediate by Proposition 3.7 that the last two charts are compatible. In fact, we can choose $(\log a_1, \ldots, \log a_d)$ as $\mathbb{Z}_p$-basis for Λ.

The definition of a Lie group is now overdue:

Definition 4.4. A topological group G is a *Lie group* if G has the structure of an analytic manifold with the group operations being analytic functions. G is a *p-adic Lie group* if the manifold is p-adic analytic.

4.2. Characterisations of p-adic Lie groups

All the examples of p-adic manifolds considered above are in fact p-adic Lie groups. This is obvious for $X = \mathbb{Q}_p^d$, and fairly elementary for $\mathrm{GL}_d(\mathbb{Q}_p)$.[1] To show that *any* uniform group is a p-adic Lie group is both more general and more difficult. With regard to the atlas given by $\mathbb{Z}_p$-exponentiation, this is carried through in ([2], 8.18):

Proposition 4.5. ([2], 8.18) *Let G be topological group containing an open uniform subgroup. Then G is a p-adic Lie group.*

We wish to establish a converse result. While uniform groups have been key to exploring powerful p-groups, we have *standard groups* as their counterpart for Lie groups. There is a rigid connection between those two classes which will make our results on pro-p groups applicable to p-adic Lie groups.

Definition 4.6. Let G be a group of dimension d, and let X, Y denote sets of d variables $(X_1, \ldots, X_d)$ and $(Y_1, \ldots, Y_d)$, respectively. G is a *standard group* if it is (topological) isomorphic to the set $\{(g_1, \ldots, g_d) : g_i \in p\mathbb{Z}_p\}$ with group operation given by a formal group law $F(X, Y) \in \mathbb{Z}_p[\![X, Y]\!]$.[2]

We recall that a *formal group law* in d variables over a (commutative) ring R is a d-tuple $(F_i) = F$ of power series in the variables $X = (X_1, \ldots, X_d)$ and $Y = (Y_1, \ldots, Y_d)$

[1] Choose the atlas $\mathcal{A}$ defined as above. It is sufficient to check everything on U alone. Multiplication $(x, y) \mapsto xy$ is analytic since it is given by polynomials in the matrix entries. To show that $x \mapsto x^{-1}$ is analytic is tantamount to demonstrating that $\det(x)^{-1}$ is "expressible as power series" – which means in turn that it lies within $\mathbb{Z}_p$ for every $x \in U$. This is clear with Leibniz' formula for the determinant since $\mathbb{Z}_p$ is the discrete valuation ring of $\mathbb{Q}_p$.

[2] Our definition of "standard group" follows [12] and differs for $p = 2$ from the definition proposed in [2]. The latter approach enables a neater formulation of results at the prime 2, but would make the geometric approach to Lie algebras appear quite arbitrary.

such that

$$F(X,0) = X, \quad F(0,Y) = Y$$
$$F\big(U, F(V,W)\big) = F\big(F(U,V), W\big)$$

These properties ensure that the set above is in fact a group, with inverse $x^{-1} = \phi(x)$ given by the unique power series ϕ such that $F(X, \phi(X)) = 0 = F(\phi(X), X)$ (cf. [12], part II, ch. IV, 8 for details). On the other hand, by shrinking an analytic group G and choosing local coordinates, G can be understood as local neighbourhood of the origin in k^n with group structure given by a formal group law over k.

We have already encountered standard groups – in fact, any uniform group G contains a such one. As seen in Example (iii) above, G can be given the "coordinates of the fist kind" by means of the chart (G, ϕ, d). The image of $H = P_1(G)$ for p odd (and $H = P_2(G)$ for $p = 2$) under ϕ is then a standard group with formal group law the Campbell-Hausdorff series (cf. Theorem 3.10). This result can be generalised:

Proposition 4.7. ([2], 8.29 and [12], part II, ch. IV, 8) *Every p-adic Lie group G has an open subgroup that is a standard group.*

Conversely, any standard group is already a uniform group ([2], 8.31). We combine this result with Propositions 4.7 and 4.5 and obtain:

Theorem 4.8. ([2], 8.32) *Let G be a topological group. Then G is a p-adic Lie group if and only if G contains an open subgroup which is a uniform pro-p group.*

This also proves Theorem 4.1, for any finitely generated powerful groups eventually has uniform subgroups via its lower p-series (see Propostion 1.20). We have thus found an entirely algebraic formulation of the analytic concept of a p-adic Lie group. Applying our results on profinite groups, we can derive the following

Corollary 4.9. ([2], 8.34) *For a topological group G, the following are equivalent:*

(i) G is a compact p-adic Lie group.

(ii) G contains an open normal uniform pro-p subgroup of finite index.

(iii) G is a profinite group containing an open subgroup which is a pro-p group of finite rank.

Finally, we can clarify the notion of "dimension" for a p-adic Lie group and reconcile the analytic and algebraic characterisations:

Proposition 4.10. ([2], 8.36) *Let G be a p-adic Lie group. There exists an integer d (the dimension of G) such that any open pro-p subgroup of G has finite rank and (algebraic) dimension d. Moreover, every chart in an atlas of G has (analytic) dimension d.*

Morphisms in the category of p-adic Lie groups of dimension d should properly be thought of as group homomorphisms that additionally are morphisms of the underlying manifolds (ie. locally analytic). One of Cartan's theorems parallels Proposition 1.14 and allows to concentrate on continuous morphisms whenever Lie groups over $\mathbb{R}$ or $\mathbb{Q}_p$ are dealt with:

Proposition 4.11. ([2], 9.4 and [12], part II, chp. V, 9) *Let G_1 and G_2 be p-adic or real analytic groups. Then every continuous homomorphism $G_1 \to G_2$ is analytic.*

All these results indicate how restrictive it is for a topological group G to be p-adic analytic. In fact, there exists at most one structure as p-adic Lie group, and unless G is discrete, even the prime p is uniquely determined (cf. [2], 9.5). As a corollary, the various charts introduced in Example (i) and (ii) above are compatible and describe the *same* manifold structure on the respective group. We conclude with results on categorial properties of p-adic Lie groups:

Proposition 4.12. ([2], 9.6) *Let G be a p-adic Lie group.*

(i) Any closed subgroup H is a p-adic Lie group, and the inclusion $H \hookrightarrow G$ is analytic.

(ii) Any quotient G/N with a normal closed subgroup N is a p-adic Lie group again. The projection $G \to G/N$ is analytic.

Proposition 4.13. ([2], 9.7) *Let G be a Hausdorff topological group, and N a closed normal subgroup. If both N and G/N are p-adic Lie groups (with the induced and the quotient topologies respectively), then G is a p-adic Lie group as well.*

4.3. The Lie algebra of a Lie group

There are two ways to give precise meaning to the phrase "the Lie algebra of a (p-adic) Lie group G". The first approach uses the characterisation of Lie groups by uniform subgroups, and defines their Lie algebras as suitable $\mathbb{Q}_p$-saturations of $\mathbb{Z}_p$-algebras as constructed in section 3.1.

The more traditional second approach demands additional conceptual effort. We introduce a Lie algebra as tangent space of G at the unit, endowed with a Lie bracket that comes from the quadratic part of a formal group law (which represents multiplication in G). We are rewarded with a more comprehensive understanding of formal groups and their place within Lie theory, and with a more precise geometric interpretation of Lie algebras as linear approximations.

The algebraic definition

Let G be a p-adic Lie group. We know from Theorem 4.8 that G has an open uniform subgroup. If H_1 and H_2 are two such groups, their intersection $H = H_1 \cap H_2$ has finite index in both H_1 and H_2. The associated Lie algebra L_H thus has the same rank as L_{H_1} and L_{H_2}. In analogy with the real case, we would like to end up with a Lie algebra over $\mathbb{Q}_p$. By equality of their ranks over $\mathbb{Z}_p$, the localized modules $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_H$ and $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_{H_{i=1,2}}$ respectively are each vector spaces of the same dimension over $\mathbb{Q}_p$. This gives an isomorphism

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_{H_1} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_H = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_{H_2}$$

of $\mathbb{Q}_p$-vector spaces, and we can hence give the following

Definition 4.14. Let G be a p-adic Lie group. The *Lie algebra of* G is

$$\mathcal{L}(G) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_H,$$

where H is any open uniform subgroup.

It follows that the dimension of a Lie group G coincides with the rank of the $\mathbb{Z}_p$-algebra L_H and the dimension of $\mathcal{L}(G)$ as $\mathbb{Q}_p$-vector space, where H is any open uniform subgroup of G:

$$\dim(G) = \dim(H) = \mathrm{rk}_{\mathbb{Z}_p}(L_H) = \dim_{\mathbb{Q}_p}\big(\mathcal{L}(G)\big)$$

A similar passage to the "local situation" allows to associate a Lie algebra morphism $\mathcal{L}(f) = f^*$ to a morphism f of Lie groups. With this operation, $\mathcal{L}$ becomes a functor from the category of p-adic Lie groups to the category of finite-dimensional $\mathbb{Q}_p$-Lie algebras (cf. [2], 9.11).

Its properties however might appear unsatisactory. Evidently, $\mathcal{L}$ cannot be invertible, since it only depends on a "small" open subgroup of G. This contrasts to the results of section 3.2, where we had to "shrink" the category of $\mathbb{Z}_p$-Lie algebras to establish an equivalence to uniform groups. The above process of saturating the Lie algebras L_H overcompensates for this, and a strict equivalence of categories would now require to consider certain equivalence classes of Lie groups. Details are spelt out in [2], pp231–234.

The geometric definition

We obtain a more general – and in many aspects more suitable – notion of Lie algebra by abandoning uniform groups. Their role will be filled by formal groups: Under a sufficiently small chart around the unit, the group law on a Lie group G turns into a

formal group law on k^d, which then gives rise to a Lie bracket on a suitable space. For fields of characteristic 0, this is ultimately justified by an equivalence of categories

$$(k\text{-Lie algebras }) \simeq (\text{Formal groups over } k\ )$$

(cf. [12], part II, chp. V, 6, Thm. 3). For $k = \mathbb{Q}_p$, formal groups additionally appear as standard subgroups in every p-adic Lie group. This makes some results easier to access than in the real or complex case. As an example, any finite-dimensional $\mathbb{Q}_p$-algebra can be shown to be the Lie algebra of some p-adic Lie group with little conceptual effort (cf. [12], part II, chp. V, 4).

Let x be a point of an analytic manifold X, defined over any complete field k. The *local ring* $\mathcal{O}_{X,x} = \mathcal{O}_x$ consists of germs of analytic functions at x, and the set of functions vanishing at x is its maximal ideal $\mathfrak{m}_x$. By composition of functions, any chart (U, ϕ, d) around x induces an isomorphism $\overline{\phi} : \mathcal{O}_{k^d,0} \to \mathcal{O}_x$, where $\mathcal{O}_{k^d,0}$ is isomorphic to the (local) ring of convergent power series in d variables, with coefficients in k.

By the natural embedding of constant functions, $\mathcal{O}_x$ is a k-algebra and admits a decomposition $\mathcal{O}_x = k \oplus \mathfrak{m}_x$. The action on $\mathfrak{m}_x$ thus determines any k-derivation of $\mathcal{O}_x$, and allows to identify the vector space $T_xX = (\mathfrak{m}_x/\mathfrak{m}_x^2)^*$ of k-linear forms on $\mathfrak{m}_x$ with the space of k-derivations of $\mathcal{O}_x$. We call T_xX the *tangent space* of X at x, and can think of it as the set of all points on lines tangent to X at x.

For an analytic group $X = G$, the tangent space T_1G at the identity can be given a natural Lie algebra structure. By choosing a chart (U, ϕ, d) at the identity, we give G "local coordinates", and the group law thus induces a formal group law $F(X, Y)$ on k^d, convergent on a sufficiently small ball around 0. We recall that any such law F expands to $X + Y + B(X, Y) + O(3)$, where B is a bilinear form. F thus gives rise to a Lie bracket $[X, Y]_F = B(X, Y) - B(Y, X)$ on k^d. (See [12], part II, chp. IV, 7 for any details.)

The morphism ϕ however also induces an isomorphism of the tangent spaces $\widetilde{\phi} : T_1G \to T_0k^d = k^d$. This allows to define a Lie bracket for $x, y \in T_1G$ by

$$\widetilde{\phi}\big[x, y\big] = \big[\widetilde{\phi}x, \widetilde{\phi}y\big]_F$$

This definition does not depend on the choice of chart (see [12], part II, chp. V, 1). In this more general set-up, $T_1G = \mathcal{L}(G)$ is the *Lie algebra of G*. This definition of $\mathcal{L}$ is again functorial, and compatible with Definition 4.14.

In the situation of Theorem 3.10, the mutual passage between a Lie group and its Lie algebra was carried through with the logarithm and the Campbell-Hausdorff series (which contained the exponential). There is a corresponding, however quite technical result in the general set-up. As a preparatory result to deeper results (e.g. Lie's Third Theorem), it can be shown that any finite-dimensional k-Lie algebra $\mathfrak{g}$ is the Lie algebra of an analytic *group chunk* G (which is a slight generalisation of a Lie group). The group chunk in question can be constructed by a formal group law F whose definition leans heavily on the Campbell-Hausdorff series. In fact, we get the

Campbell-Hausdorff group chunk $\mathrm{CH}(\mathfrak{g})$ which is mapped back to G under a formal isomorphism exp that satisfies $\mathcal{L}(\exp) = \mathrm{id}$. We refer to [12], part II, chp. V, 4 & 7 for details.

With the definition as tangent space in mind, there is an abundance of results that underline the nature of $\mathcal{L}(G)$ as linear approximation to G. For instance, we have the following "local-to-global" principle:

Proposition 4.15. ([12], part II, chp. V, 7, Cor. 1) *The p-adic Lie groups G and H have isomorphic open subgroups if their corresponding Lie algebras are isomorphic.*

More details on the relation between Lie groups and their Lie algebras can be found in ([12], part II, chp. V, 2). We conclude with a sanity check of the geometric approach.

Example. Generalising the example of $\mathrm{GL}_d(\mathbb{Q}_p)$ discussed above, the unit group R^* of a finite dimensional, associative k-algebra R is an analytic group (cf. [12], part II, chp. 4, 2). R^* is an *open* subgroup, so we have $T_1R^* = R$. Multiplication in R^* has the form

$$(1 + x)(1 + y) = 1 + x + y + xy$$

which corresponds to the formal group law $F(X, Y) = X + Y + XY$. As explained above, the Lie algebra structure on $R = T_1R^*$ is thus given by $[x, y] = xy - yx$.

4.4. Relation to Lazard's work: p-filtered groups

The original approach to p-adic Lie groups as proposed by Lazard (cf. [5]) is of a more analytic nature than the one just presented, and introduces objects that are related in a rather intricate way to powerful and uniform groups. We recall that a *filtered group* (G, v) exhibits a valuation $v : G \to \mathbb{R} \cup \{\infty\}$ such that

(i) $v(g) > 0$ and $v(1) = \infty$

(ii) $v(gh^{-1}) \geq \min\{v(g), v(h)\}$

(iii) $v\big([g, h]\big) \geq v(g) + v(h)$

For each $x > 0$, there are normal subgroups $G_x = \{g \in G : v(g) \geq x\}$ and $G_{x+} = \{g \in G : v(g) > x\}$ respectively. Morphisms of filtered groups (G, v) and (H, w) are group homomorphisms $\varphi : G \to H$ that satisfy $\varphi(G_x) \subset H_x$. The valuation v gives rise to a fundamental basis of neighbourhoods of the identity element, and thus makes G a topological group and φ as above a continous mapping. The induced topology is Hausdorff whenever $v(g) = \infty$ implies $g = 1$, and can be completed by passing to $\varprojlim G/G_x$.

Example. Let (A, w) be a filtered ring that contains $\mathbb{Z}$ such that w restricts to v_p on $\mathbb{Z}$. Any unit g can be written as $g = 1 + a$ with a non-unit a and $w(a) > 0$. The unit group A^* now becomes a filtered group by $v(g) = v(1 + a) = w(a)$. The effect of taking p-th powers of g can be described by comparing two numbers from a binomial expansion: g^p has valuation $\varphi(v(g)) = \min\{w(a) + 1, pw(a)\}$.

If A is also an algebra over a complete discrete valuation ring (with residue field of unequal characteristic), one can define analytic functions exp and log. The conditions for convergence are $w(x) \geq (p-1)^{-1}$ and $w(x-1) \geq (p-1)^{-1}$, respectively. This and the observation from the example above motivates a refined notion of filtered group:

A *p-valued group* is a filtered group such that

(iv) $v(g) < \infty$ for $x \neq 1$

(v) $v(g) > (p-1)^{-1}$

(vi) $v(g^p) = v(g) + 1$

The graded group $\mathrm{gr}(G) = \bigoplus G_x/G_{x+}$ of a p-valued group is a Lie algebra over $\mathbb{F}_p[\pi]$; the Lie bracket is induced by the group commutator (see the example after Definition 3.1) and multiplication by π corresponds to taking p-th powers. The conditions above guarantee that $\mathrm{gr}(G)$ is torsion-free and equal to 0 for $x \leq (p-1)^{-1}$.

Conditions (v) and (vi) prohibit that elements of valuation $\leq p/(p-1)$ have a pth root. This leads to define *p-saturated groups* as complete groups with pth roots for all elements with valuation above this threshold: whenever $v(g) > p/(p-1)$, then there exists h such that $h^p = g$ (cf. [5], III.2.1.6). A p-saturated group G with minimal set of (topological) generators $(g_1, \ldots, g_d)$ such that $v(g_i) + v(g_j) > p/(p-1)$ is called *strongly p-saturated*. This condition entails that any commutator is a p-th power, and G is thus powerful. In fact, the analytic and algebraic vocabulary agree at this stage: a p-valued group G is uniform if and only if it is strongly p-saturated (cf. [7], 4.3).

Lazard's characterisation of analytic groups has come into reach: If G is p-adic analytic (of dimension d) over $\mathbb{Q}_p$, then there exists an open, p-saturated subgroup S (of dimension d) with integral valuation v ([5], III.3.1.3).[3]

This valuation v is such that the topology induced on S coincides with the subspace topology of $S \subset G$. Furthermore, we have the equalities

$$S_n := S^{p^n} = \{s^{p^n} : s \in S\} = \begin{cases} \{s \in S : v(s) \geq n+1\} & \text{if } p > 2, \\ \{s \in S : v(s) \geq n+2\} & \text{if } p = 2. \end{cases}$$

We note that each S_n is indeed a sub*group* of S. The above equations justify the terminology in [8] to call the (S_n) "standard filtration" of S.[4]

[3] There is a converse for *compact* groups: G is a compact analytic group if and only if it contains an open, p-valuable pro-p subgroup H of finite index ([5], II.2.1.3 and III.3.2.2).

[4] We will not adopt this terminology and use it in this section only.

This terminology can be extended to the situation where S is an open subgroup of an analytic pro-p group H. We set $H_n = H^{p^n}$ as in the first two equations above,[5] and obtain the important relation

$$H_{n+e} \subset S_n \subset H_n,$$

where $p^e = (H : S)$. This shows again that the topology of an analytic pro-p group is determined by its algebraic structure, and that its topology has the sets of p^n-th powers as basis (cf. [5], III.3.1.4).

Definition 1.11 also provides H with the lower p-series $P_n(H)$. How does this series relate to H_n as above? Both series form a fundamental basis of the topology of H, so by the two formulations of Lazard's Theorem, both of them "run into" an open uniform subgroup $U \subset H$ and an open saturated subgroup $S \subset H$, respectively. (More precisely, this means that $P_c(H) \subset U$ and $H_c \subset S$ for some $c \in \mathbb{N}$ large enough.) On the uniform subgroup U, the lower p-series is now also given as p-th powers (cf. Theorem 1.17), and we conclude that

$$P_{n+c}(H) \subset H_n \subset P_{n-c}(H),$$

where $P_{n-c}(H) = H$ whenever $n - c < 0$. In the terminology of Chapter 6, this means that the "standard filtration" of an analytic pro-p group H is *uniformly equivalent in scaling 1* to its lower p-series $P_n(H)$. The expression "scaling 1" comes from the absence of a non-trivial multiplicative factor $s \cdot n$ to compare the two series.

[5] Note that H_n now only denotes the *set* of p^n-th powers – contrary to the case of powerful groups however, this is in general not a subgroup.

Part III.

Ramification in analytic groups

5. The ramification filtration of a Galois group

This chapter's fundamental object is a field K, complete with regard to a discrete, non-archimedean valuation. The behaviour of this valuation in extensions L/K may display "ramification", and we wish to examine this important aspect.

We will almost exclusively work under the assumption of different characteristics, ie. K is of characteristic 0, but $\mathrm{char}(k) = p > 0$ for the residue field k. If L/K is Galois with separable residue field extension l/k, we can describe the phenomenon of ramification in terms of the Galois group. This leads to the notion of *(higher) ramification groups*.

These groups will first be defined for finite extensions only. If the extension is abelian, this chapter's main result describes how p-th powers interact with the ramification filtration (this is Theorem 5.14). A neat formulation however requires to define an alternative numbering of the ramification groups. This is a rather intricate business, but allows to extend the notion of ramification groups to the infinite case.

The majority of our results is valid for fields more general than local ones, and it may be worthwhile to also keep the power series fields over $\mathbb{Q}_p$ in mind. Theorem 5.14 just mentioned will however be proved for local fields only; and we defer its generalisation to the case of perfect residue fields to Chapter 7.1. Main references for this chapter are [11], [6], [3].

5.1. Valuations and their extensions

By combined efforts from analysis and algebra, it is known that any complete valued field (K, v) admits a unique extension of its valuation to any algebraic extension field L/K. If v is a non-archimedean (exponential and normalized) valuation, the ring of integers $\mathcal{O}_K$ is a valuation ring and equal to the set of elements with non-negative valuation. Its unique maximal ideal $\mathfrak{p}_K$ is the set of elements with strictly positive valuation; and the residue field $\mathcal{O}_K/\mathfrak{p}_K$ of K is denoted by k.

If v is a discrete valuation, then $\mathcal{O}_K$ is a discrete valuation ring, with ideals given by $\mathfrak{p}_K^r = (\pi^r)$ for a prime element π. These ideals form a fundamental basis of the zero element, and so do the higher unit groups $U_r = 1 + \mathfrak{p}_K^r \subset \mathcal{O}_K^*$ for the unit in K^*. The quotients in these sequences satisfy $\mathfrak{p}_K^r/\mathfrak{p}_K^{r+1} \simeq U_r/U_{r+1} \simeq k$ for $r \geq 1$.

Let (K, v) be a field as above, with v discrete and non-archimedean. If (L, w) is a finite extension, we have the degree formula

$$[L : K] = e_{L/K} \cdot f_{L/K},$$

where $e_{L/K} = (w(L^*) : v(K^*))$ is the (relative) ramification index and $f_{L/K} = [l : k]$ the residue degree of the extension L/K. Let $(\lambda_1, \ldots, \lambda_{f_{L/K}}) \in \mathcal{O}_L$ denote representatives for a basis of l/k, and choose a prime element $(\pi_L) = \mathfrak{p}_L$ in $\mathcal{O}_L$. The set

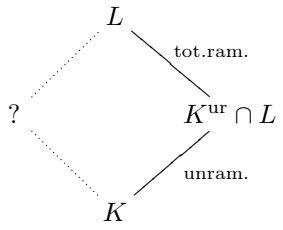
$$\left(\lambda_i \pi^j\right)$$

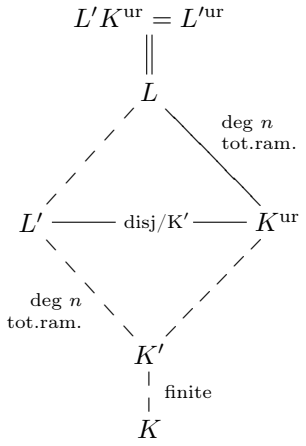
with $1 \leq i \leq f_{L/K}$ and $0 \leq j \leq e_{L/K} - 1$ is an $\mathcal{O}_K$-basis of the ring of integers $\mathcal{O}_L$ (and thus also a K-basis of L).

The extension L/K is *unramified*, if l/k is separable and $e_{L/K} = 1$. The composite of two unramified extensions is again unramified, and we define the *maximal unramified extension* K^{ur} as the composite of all unramified (finite) extensions of K. The extension K^{ur}/K is Galois, isomorphic to its residue field extension k^{sep}/k. The valuation of K extends uniquely to K^{ur}, although the latter field is in general of infinite degree over K and thus not necessarily complete.

For any extension L/K, the field $K^{\mathrm{ur}} \cap L$ is the maximal unramified subextension of L/K, with residue field $l \cap k^{\mathrm{sep}}$. If there is no such non-trivial extension, then L/K is called *totally ramified*. In this case, the corresponding residue field extension is trivial, and for L/K finite, the prime $\mathfrak{p}_K$ "ramifies totally" into $\mathfrak{p}_L^{[L:K]}$.

It is often desirable to split an extension L/K into an unramified and a completely ramified part. In general, it is only possible to first move to a maximal unramified intermediate field, which then admits L as totally ramified extension. The reverse procedure fails, for the composite of two totally ramified extensions is in general not totally ramified again.





With some amendments, the reverse decomposition becomes feasible for a certain class of extensions: If K has *perfect* residue field, then any finite extension L/K^{ur} of degree n splits into a totally ramified part of degree n and an unramified part, relative to some finite extension K'/K (cf. [11], chp. V, §4, Lemma 7).

5.2. Ramification groups: The lower numbering

We turn to the special situation of a finite Galois extension L/K whose residue extension l/k is separable and has characteristic $p > 0$. We write $v_L = w \cdot e_{L/K}$ for the normalized valuation on L and $v_K = v \cdot e_{L/K}$ for its restriction to K. The separability of l/k yields

Lemma 5.1. ([6], II, 10.4) *The valuation ring $\mathcal{O}_L$ is generated as $\mathcal{O}_K$-algebra by a single element $x \in \mathcal{O}_L$, ie.*

$$\mathcal{O}_L = \mathcal{O}_K[x].$$

This enables us to give the following

Definition 5.2. For $r \in [-1, \infty)$, the set

$$G(L/K)[r] = \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma x - x) \geq r + 1\}$$

is called the *r-th ramification group of $G = \mathrm{Gal}(L/K)$ in the lower numbering* (or simply *r-th lower ramification group* for brevity). If it is clear from the context we may omit the extension and simply write $G[r]$ for $G(L/K)[r]$.[1]

The condition above can easily be seen to be equivalent to $v_L(\sigma a - a) \geq r + 1$ for all $a \in \mathcal{O}_L$ and is thus independent of the choice of x. We collect a few observations on these ramification groups:

(i) *Filtration.* The $G[r]$ form a decreasing chain of normal subgroups. It is clear that $G[-1] = G$ and $G[n] = 1$ for some n large enough. The $G[r]$ thus form a

[1] As the name suggests, lower ramification groups are usually written G_r. We reserve this notation for the more frequently appearing lower p-series of a Lie group.

fundamental basis of open neighbourhoods of the unit in G (provided with the discrete topology).

(ii) *The group* $G[0]$. We recover that $G[0] = I(L/K)$, where

$$\begin{aligned} I(L/K) &= \{\sigma \in \mathrm{Gal}(L/K) : \sigma a \equiv a \bmod \mathfrak{p}_L, \text{ for all } a \in \mathcal{O}_L\} \\ &= \ker\big(G \to \mathrm{Aut}_\kappa(\lambda),\ \ \sigma \mapsto (a \bmod \mathfrak{p}_L \mapsto \sigma a \bmod \mathfrak{p}_L)\big) \end{aligned}$$

is the *inertia group* of $\mathrm{Gal}(L/K)$. It is a subgroup of order $e_{L/K}$ and thus a measure for the ramification in L/K. Furthermore, it "marks the border" between the unramified and totally ramified part in L/K: let $L' = K^{\mathrm{ur}} \cap K$ be the largest unramified subextension of L, and let $H = \mathrm{Gal}(L/L')$ denote its Galois group. The extension L/L' is totally ramified, with $H[r] = G[r]$ for $r \geq 0$. In this way, the study of ramification by means of the groups $G[r]$ is reduced to the case of totally ramified extensions L/K.

(iii) *The group* $G[1]$. The group $G[1] = R(L/K)$ is simply called *ramification group* of G and equal to

$$R(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \frac{\sigma a}{a} \equiv 1 \bmod \mathfrak{p}_L, \text{ for all } a \in L^*\}$$

It is the kernel of the canonical homomorphism $I(L/K) \longrightarrow \chi(L/K)$, where $\chi(L/K) = \mathrm{Hom}\big(v_L(L^*)/v_K(K^*),\ \lambda^*\big)$, and is the only p-Sylow subgroup of $I(L/K)$ (cf. [6], II.9 for details).

(iv) *The quotients.* The last statement is a consequence of the structure of the quotients $G[r]/G[r+1]$: for non-negative r, they can be embedded into the quotients U_L^r/U_L^{r+1} of the higher unit groups of L. For $r \geq 1$, the groups $G[r]/G[r+1]$ are thus abelian, and annihilated by p.

One of the most useful properties of the lower numbering is its smooth interaction with the process of replacing G by a subgroup (ie. changing the base field K):

Proposition 5.3. ([6], II, 10.3) *Let K' be an intermediate field of L/K. We have for all $r \geq -1$:*

$$G(L/K')[r] = G(L/K)[r] \cap G(L/K')$$

Any (integral) number n such that $G[n] \neq G[n+\varepsilon]$ for all $\varepsilon > 0$ is called a *jump* in the chain $(G[r])_r$. The last jump in the lower numbering is denoted by l_G, so that $G[l_G] \neq 1$, but $G[l_G + \varepsilon] = 1$ for all $\varepsilon > 0$. This section's main result is an upper bound for l_G.

Proposition 5.4. *Let L/K be an extension as above, ie. finite and Galois, but of characteristic 0. In this situation, the* absolute ramification index *of the field L is defined as $e_L = v_L(p)$. Let $G = \mathrm{Gal}(L/K)$ denote the Galois group of the extension. The last jump l_G in its ramification filtration is bounded by $e_L/(p-1)$, that is $G[r] = 1$ for $r > e_L/(p-1)$.*

Proof: We will not need to mention the residue field l of L any more, so we free up the notation and put $l = l_G$ for brevity. We claim that we can assume G to be totally ramified, and cyclic of degree p. Firstly, because of $e_L/(p-1) > 0$, we work inside of $G[1]$, which is the Galois group of a totally ramified subextension. Secondly, the last non-trivial ramification group $G[l]$ is an abelian p-group, and thus has a subgroup $H \simeq \mathbb{Z}/p\mathbb{Z}$. This group is the Galois group of some intermediate field, and by Proposition 5.3 above, the lower numbering of H is induced by the numbering on G. This means $H[r] = G[r] \cap H$, and we conclude that $l_H = l$.

We thus think of L/K as totally ramified and cyclic of order p. This means $e_L = p \cdot e_K$, and allows to choose a generator σ of $G = \mathrm{Gal}(L/K)$. We postpone the proofs of two supplementary results:

Lemma 5.5. *For any $a \in L$, we have $v_L\big((\sigma-1)a\big) \geq v_L(a) + l$, and equality if and only if $v_L(a)$ is prime to p.*

Let $P \in \mathbb{Z}[T]$ denote the polynomial determined by

$$1 + T + T^2 + \ldots + T^{p-1} = (T-1)^{p-1} + pP(T)$$

If we substitute $T = \sigma$, this gives the useful relation

$$\mathrm{tr}_{L/K}(a) = (\sigma-1)^{p-1}(a) + pP(\sigma)(a).$$

The second result examines the valuation of the last term on the right hand side:

Lemma 5.6. *The polynomial $P(\sigma)$ does not change the valuation of a, that is $v_L\big(P(\sigma)(a)\big) = v_L(a)$. In particular, we have $v_L\big(pP(\sigma)\big)(a) = e_L + v_L(a)$.*

With these two lemmas, we can derive the Proposition as follows: Assume l to be divisible by p, and choose $a \in L$ such that $v_L(a) = 1$. By Lemma 5.5 above, we have $v_L\big((\sigma-1)^{p-1}(a)\big) = (p-1)l+1$, which is not divisible by p. Neither is $v_L\big(pP(\sigma)(a)\big) = e_L+1$, for p already divides $e_L = e_K \cdot [L/K] = e_K \cdot p$. However, we have $v_L\big(\mathrm{tr}_{L/K}(a)\big) = p\, v_K\big(\mathrm{tr}_{L/K}(a)\big)$, which entails $e_L+1 = (p-1)l+1$ by the sharpened triangle inequality.

Now assume l to be prime to p, and choose $a \in L$ with $v_L(a) = l$. By the Lemma again, we have $v_L\big((\sigma-1)^{p-1}(a)\big) = (p-1)l + l = pl$, while $v_L\big(pP(\sigma)(a)\big) = e_L + l$ is prime to p. Since the number $v_L\big(\mathrm{tr}_{L/K}(a)\big)$ is still divisible by p, we must have $pl < e_L + l$. □

Proof of Lemma 5.5: Let $\pi = \pi_L$ be a uniformizing element of L. Since L/K is totally ramified, L admits a K-basis $(\pi^0, \pi^1, \ldots, \pi^{p-1})$ (cf. [6], II.6.8), and we can

choose π as generating element of $\mathcal{O}_L = \mathcal{O}_K[\pi]$. The map $(\sigma - 1) : L \to L$ is K-linear, and its action on π satisfies

$$v_L\big((\sigma-1)\pi^i\big) = \begin{cases} i + l & \text{if } 1 \le i \le p-1, \\ \infty & \text{if } i = 0. \end{cases}$$

This is clear for $i = 1$, for which we write the action on π as $\sigma\pi = \pi + u\pi^{l+1}$ with some unit $u \in \mathcal{O}_L^*$. It follows that

$$\sigma(\pi^i) = (\sigma\pi)^i = (\pi + u\pi^{l+1})^i \equiv \pi^i + (iu)\pi^{l+i} \mod (\pi^{l+i+1})$$

The factor (iu) is again a unit, for $1 \le i \le p-1$. This gives the above statement for all i.

Let $a = \sum_{i=0}^{p-1} \lambda_i \pi^i$ be an element of L, with $\lambda_i \in K$. We have

$$\begin{aligned} v_L(a) &\ge \min_{i\ge 0}\big(v_L(\lambda_i) + i\big) \\ v_L((\sigma-1)a) &\ge \min_{i\ge 1}\big(v_L(\lambda_i) + i + l\big) \end{aligned}$$

for the valuations of a and $(\sigma - 1)a$ respectively. However, each $v_L(\lambda_i)$ is divisible by p, so the $v_L(\lambda_i) + i$ are pairwise distinct. Thus there exist n and m such that

$$v_L(a) = v_L(\lambda_n) + n, \quad v_L\big((\sigma-1)a\big) = \begin{cases} v_L(\lambda_n) + n + l = v_L(a) + l & \text{if } n \ne 0, \\ v_L(\lambda_m) + m + l > v_L(a) + l & \text{if } n = 0. \end{cases}$$

It follows that $v_L((\sigma-1)a) \ge v_L(a) + l$. We have equality if and only if $n \ne 0$, which happens precisely when p is prime to $v_L(a)$. □

Proof of Lemma 5.6: We note that $P(1) = 1$, and thus write $P(T) = \sum_{i=1}^{p-1} c_i T^i$, with $\sum_{i=1}^{p-1} c_i = 1$. Moreover, we have

$$\frac{P(\sigma)(a)}{a} = \frac{c_1\sigma(a) + \ldots c_{p-1}\sigma^{p-1}(a)}{a} = c_1\frac{\sigma(a)}{a} + \ldots + c_{p-1}\frac{\sigma^{p-1}(a)}{a}$$

Since we are working within $G[1]$, we know that $\sigma^i(a)/a \equiv 1 \mod (\pi)$ for all powers of σ (see item (iii) in the list at this section's beginning). With the equation above, this implies

$$\frac{P(\sigma)(a)}{a} \equiv c_1 + \ldots + c_{p-1} = 1 \mod (\pi).$$

This means that $P(\sigma)(a)/a$ is a unit, ie. $v_L\big(P(\sigma)(a)\big) = v_L(a)$. □

We conclude this section with a widely used result in the study of higher ramification groups, namely the reduction to algebraically closed residue fields. Its proof is instructive, and centers around the concept of "ramification isomorphism".

Let L/K and L'/K' be finite Galois extensions as in Proposition 5.4, with residue field of characteristic p. We say that there is a *ramification isomorphism*, if there are isomorphisms

$$\mathrm{Gal}(L/K)[r] \simeq \mathrm{Gal}(L'/K')[r]$$

for each $r \geq 0$. The result mentioned now reads as:

Lemma 5.7. *Let L/K be as above, and assume additionally that the extension is* totally ramified*, with* perfect *residue field k. There exists an extension L'/K' as above, with algebraically closed residue field $\overline{k}$, such that there is a ramification isomorphism between L/K and L'/K'.*

Proof: The field K^{ur} has the desired residue field $\overline{k}$. Let $L' = LK^{\mathrm{ur}}$ denote the compositum of L and K^{ur}. One sees easily that $L' = L^{\mathrm{ur}}$. The fields L^{ur}, K^{ur} are however not complete, so we move on to $L' = \widehat{L^{\mathrm{ur}}}$ and $K' = \widehat{K^{\mathrm{ur}}}$, respectively. We claim that L'/K' has in fact the desired properties.

The first step is to compare the maximal unramified extensions to their completions. There is a ramification isomorphism between them, ie.

$$\mathrm{Gal}\big(L^{\mathrm{ur}}/K^{\mathrm{ur}}\big)[r] \simeq \mathrm{Gal}\big(L'/K'\big)[r]$$

for $r \geq 0$. Note that the left hand side is not covered by our definition of ramification groups, for we required *complete* fields in 5.2. This can however be relaxed to only demanding that the valuation of the base field has a unique continuation to the extension field (cf. [6], chp. II, §10). This is the case for K^{ur}, for it is a Henselian field (cf. [3], chp. II, 2).

K' does not contain any algebraic extension of K^{ur}: any such field would have the same residue field $\overline{k}$ as K^{ur}, and also be unramified – hence equal to K^{ur}. This shows the claimed isomorphism for $r = 0$. For $r \geq 1$, we observe that L^{ur} embeds as *dense* subset into L', and that all Galois automorphisms are *continuous* maps. Any $\sigma \in \mathrm{Gal}(L^{\mathrm{ur}}/K^{\mathrm{ur}})[r]$ thus extends uniquely to a continuous automorphism of L'/K', and lies in $\mathrm{Gal}(L'/K')[r]$.

The second step is to justify the isomorphisms

$$\mathrm{Gal}\big(L/K\big)[r] \simeq \mathrm{Gal}\big(L^{\mathrm{ur}}/K^{\mathrm{ur}}\big)[r]$$

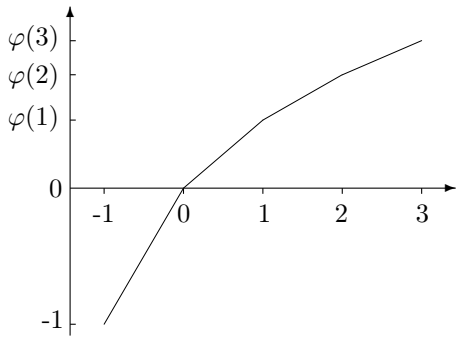
These follow "by definition" of the ramification groups, for the generator of $\mathcal{O}_{L^{\mathrm{ur}}}$ over $\mathcal{O}_{K^{\mathrm{ur}}}$ can be chosen from $\mathcal{O}_L$. This is a consequence of $L^{\mathrm{ur}} = LK^{\mathrm{ur}}$ as above, and the remark on any $\mathcal{O}_K$-basis of $\mathcal{O}_L$ in 5.1. We derive the assertion, for the valuations v_L and $v_{L^{\mathrm{ur}}}$ agree on L. □

5.3. Ramification groups: The upper numbering

The lower numbering displays a less desirable behaviour under taking quotients by a Galois subextension L'/K. Let $G = \mathrm{Gal}(L/K)$ as above, and $H = \mathrm{Gal}(L/L')$. Under the projection $G \longrightarrow G/H$, each $G[r]$ is mapped to some ramification group $(G/H)[s]$, but in general, we will have $r \neq s$. The change of numbering is intricate to describe. A central role is occupied by the function

$$\begin{aligned} \varphi_{L/L'} : [-1, \infty) &\longrightarrow [-1, \infty) \\ u &\mapsto \int_0^u \frac{dt}{(H[0] : H[t])} \end{aligned}$$

where $(H[0] : H[t])$ is to be understood as $1/(H[t] : H[0])$ for $-1 \leq t \leq 0$. We will also write φ_H for $\varphi_{L/L'}$, which is a continuous, piecewise linear and increasing function:



It enters the subject of ramification groups by Herbrand's Theorem:

Theorem 5.8 (Herbrand)**.** ([6], II, 10.7) *For all r, we have*

$$G[r]H/H = (G/H)[\varphi_H(r)]$$

Let us return to the extension L/K and consider the function $\varphi_G = \varphi_{L/K}$. Let $\psi_G = \psi_{L/K} = \varphi_{L/K}^{-1}$ denote its inverse function.

Definition 5.9. The *r-th ramification group in the upper numbering* is defined as

$$\mathrm{Gal}(L/K)(r) = G(r) = G[\psi_G(r)]$$

Just as in the case of the upper numbering, we may write $G(r)$ for $\mathrm{Gal}(L/K)(r)$ if this relation is clear from the context.[2] By means of the $G(r)$, the function ψ_G is

[2] We deviate again from the standard notation as G^r.

expressible as

$$\psi_G(u) = \int_0^u \big(G : G(t)\big)\mathrm{d}t,$$

which can be shown (by left-continuity of the lower filtration) on differences of the form $\psi(u+\varepsilon) - \psi(u)$. Both φ_G and ψ_G are transitive with regard to an intermediate extension (cf. [6], II, 10.8):

$$\varphi_G = \varphi_{G/H} \circ \varphi_H \quad \text{and} \quad \psi_G = \psi_H \circ \psi_{G/H}$$

This helps to discover the true merit of upper ramification groups: their numbering is invariant with regard to subextensions.

Proposition 5.10. ([6], II, 10.9) *As above, let L'/K be an intermediate Galois extension with $H = \mathrm{Gal}(L/L')$. We have*

$$G(r)H/H = (G/H)(r)$$

Another valuable property of the upper numbering is the possibility to generalize the concept of higer ramification groups to the case of an infinite Galois extension:

Definition 5.11. Let L/K be a (possibly infinite) Galois extension. We define the *higher ramification groups*

$$G(r) = \varprojlim (G/H)(r),$$

where H runs through the set of open subgroups of G. The family of subgroups $\big(G(r)_{r\geq -1}\big)$ is called *ramification filtration* of G.

It is immediate that $G(0) = G[0]$ in the case of a finite extension L/K; and it can be checked on finite intermediate extensions that the Galois theoretic properties of $G[0]$ carry over to $G(0)$ for an infinite extension. $G(0)$ is thus called "inertia group of G", and sometimes denoted by $I(L/K)$.

Each $G(r)$ is a closed normal subgroup in G, but it is by no means clear whether they are open. This is actually a direct corollary of Sen's Theorem – and thus a correct statement for an analytic Galois group of a totally ramified extension, with open pro-p subgroup of dimension ≥ 1.

5.4. Jumps in finite abelian extensions of local fields

For the rest of the section we assume that L/K is a finite Galois extension of *p-adic number fields*, ie. of local fields of characteristic 0. This entails $0 < v(p) = e_K = e < \infty$ for the absolute ramification index of K.

Jumps in the chain $(G(r))_r$ in the upper numbering are defined exactly as for lower ramification groups, with the last jump in the *upper* filtration denoted by u_G. Contrary

to the lower numbering, jumps do not need to be integers anymore (cf. [11], IV, §3, Exc. 2). It is remarkable that this conclusion yet holds for *abelian* extensions:

Proposition 5.12 (Hasse-Arf)**.** ([6], V, 6.3) *Let $G = \mathrm{Gal}(L/K)$ denote the Galois group of a finite* abelian *extension of local fields. Then all the jumps in the filtration $G(r)_{r\geq -1}$ are integers.*

This result is a consequence of a deep connection between the higher unit groups $U^r = 1 + \mathfrak{p}_K^r$ of a local field K and the higher ramification groups of its Galois group. It is known from Local Class Field theory that the *universal local Artin map*

$$(\quad, K) : K^* \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}})$$

induces the *relative local Artin map*

$$(\quad, L/K) : K^* \longrightarrow G = \mathrm{Gal}(L/K)$$

for every finite, abelian extension L/K. In this situation, we have the fundamental

Theorem 5.13. ([6], V, 6.2) *For any $r \geq 0$, the relative Artin map $(\quad, L/K)$ maps the unit groups U_K^r onto $G(L/K)(r)$.*

Our next result might be read with the notion of "p-filtered" group in mind. Up to the factor e, $G(1)$ will turn out to "almost" be such a group. All our further results rely on how p-th powers affect the ramification groups:

Theorem 5.14. *Recall that $e = e_K$ denotes the absolute ramification index of the base field K. For a finite abelian p-group $G = \mathrm{Gal}(L/K)$, the effect of p-th powers on its higher ramification groups is as follows:*

$$\begin{aligned} G(r)^p &\subset G(p \cdot r) \quad \text{if } r \leq \frac{e}{p-1} \\ G(r)^p &= G(r+e) \quad \text{if } r > \frac{e}{p-1} \end{aligned}$$

By Theorem 5.13, this follows immediately from

Proposition 5.15. ([3], chp. I, 5.7) *The higher unit groups satisfy:*

$$\begin{aligned} U_r^p &\subset U_{pr} \quad \text{if } r \leq \frac{e}{p-1} \\ U_r^p &= U_{e+r} \quad \text{if } r > \frac{e}{p-1} \end{aligned}$$

Proof: Let $1 + x$ be an element of U_r, and assume $v(x) = r$. For $p > 2$, we get:

$$(1+x)^p = 1 + \underbrace{p \cdot x}_{e+r} + \underbrace{\big(p(p-1)/2\big) \cdot x^2}_{e+2r} + \ldots + \underbrace{p \cdot x^{p-1}}_{e+(p-1)r} + \underbrace{x^p}_{p \cdot r}$$

with the respective valuations given underneath. Subtracting 1, we conclude

$$v\big((1+x)^p-1\big)\begin{cases}=v(x^p+px)=\min\{p\cdot r,e+r\} & \text{if } v(x^p)\neq v(p\cdot x),\\ \geq v(x^p+px) & \text{otherwise.}\end{cases}$$

This distinction holds as well for $p=2$, so we remove the above restriction on p.

We now note that $r\leq e/(p-1)$ if and only if $v(x^p)\leq v(p\cdot x)$, so we derive $U_r^p\subset U_{pr}$ in the first case. If conversely $r>e/(p-1)$, this means of course $U_r^p\subset U_{e+r}$.

It remains to show the inclusion $U_{e+r}\subset U_r^p$ for the latter case. The number p splits as $p=\gamma\pi^e$, so the element x can uniquely be written as $x=\alpha\gamma^{-1}\pi^r$ with a unit α. The calculation above gives

$$\begin{aligned}(1+x)^p=(1+\alpha\gamma^{-1}\pi^r)^p &\equiv 1+p\cdot\alpha\gamma^{-1}\pi^r\\ &\equiv 1+\alpha\pi^{r+e} \qquad \mod \pi^{r+e+1}\end{aligned}$$

The induced isomorphism $U_{r+e}/U_{r+e+1}\simeq U_r^p/U_{r+e+1}$ is applied repeatedly to give

$$U_{r+e}=U_r^p\cdot U_{r+e+1}=(U_r^pU_{r+e+1}^p)\cdot U_{r+e+2}=\dots$$

Any $b\in U_{r+e}$ thus expands as $b=u_1b_1=(u_1u_2)b_2=\dots$ with $u_i\in U_r^p$ and $b_i\in U_i$. The sequence $\big(\prod_{i=1}^n u_i\big)$ is Cauchy, since the U_i form a fundamental basis of neighbourhoods of the unit. The limit b lies within U_r^p, for this is a closed and thus complete set. □

Example: Ramification groups of cyclotomic local fields

We conclude this chapter and provide some illustration for the theory developed. Let $\zeta=\zeta_{p^n}$ denote a primitive p^n-th root of unity, and set $K=\mathbb{Q}_p$, $L=\mathbb{Q}_p(\zeta)$. The extension L/K is totally ramified of degree $(p-1)p^{n-1}$, and we wish to determine explicitly its ramification groups.

It is clear that $G[-1]=G[0]=G=\mathrm{Gal}(L/K)$, for $G[1]$ is the unique p-Sylow subgroup in G. There exist n different p-subgroups $G_m\subset G$, with $G_1=G[1]$ and $G_n=1$. If one of the G_m did not appear as ramification group, this would give a quotient $G[r]/G[r+1]$ of order $\geq p^2$, for some r. This contradicts Property (iv) after Definition 5.2, which implies that $G[r]/G[r+1]$ is either trivial or of order p.

Thus, each one of the n subgroups G_m occurs as $G[r]$, for some r. In other words, there are precisely n jumps j_m in the filtration $G[r]$, with $1\leq m\leq n$ as above. Moreover, we know that $j_1=0$, ie. $G[j_1]=G[0]=G=G_0$, and that

$$G[j_m]=G_{m-1}$$

for all m, with $\#G_m = p^{n-m}$. Our remaining objective is to determine the jumps j_m. There are several methods:

(i) *Elementary algebra.* Any $\sigma \in G$ acts as $\sigma\zeta = \zeta^s$ for some integer s. By $\sigma \mapsto \overline{s}$, this action gives an isomorphism $G = \mathrm{Gal}(L/K) \simeq (\mathbb{Z}/p^n\mathbb{Z})^*$, independent of the choice of ζ. We thus write $\sigma = \sigma_s$, and wish to know when σ_s "drops out" of the ramification groups. Obviously, this happens for some jump j_m with

$$\sigma_s \in G[j_m] - G[j_m + 1] \Longleftrightarrow \sigma_s \in G_{m-1} - G_m$$

Consider the right hand side first. Clearly $\sigma_s \in G_{m-1}$ if and only if $p^{m-1} | (s-1)$, and thus

$$\sigma_s \in G_{m-1} - G_m \Longleftrightarrow v_p(s-1) = m-1$$

Now consider the condition on the left. By definition of the ramification groups, we have that $\sigma_s \in G[j_m]$ if and only if $v_L(\zeta^s - \zeta) = v_L(\zeta^{s-1} - 1) \geq j_m + 1$. The valuation depends only on the multiplicity of p in $(s-1)$. We also note that $(\zeta - 1)$ is a prime in L, ie. has valuation 1. This means that $\sigma_s \in G[j_m]$ if and only if $p^{v_p(s-1)} \geq j_m + 1$, or equivalently

$$\sigma_s \in G[j_m] - G[j_m + 1] \Longleftrightarrow p^{v_p(s-1)} = j_m + 1$$

This gives $j_m = p^{m-1} - 1$, with $1 \leq m \leq n$.

(ii) *Use Hasse-Arf and Theorem 5.14.* Hasse-Arf shows that the sequence (j^m) of jumps in the upper numbering must be integral, and we know that its starts with $j^1 = 0$.

We consider the intermediate field $K' = \mathbb{Q}_p(\zeta_p)$, with $e_{K'} = p - 1$ and Galois group $H = \mathrm{Gal}\big(L/\mathbb{Q}_p(\zeta_p)\big)$. For $r \geq 1$, a simple calculation shows

$$\varphi_G(r) = \frac{\varphi_H(r) - 1}{p-1} + 1,$$

which gives

$$G(r) = H\big((r-1)(p-1) + 1\big).$$

Now H is a p-group, so Theorem 5.14 is applicable. It implies that the steps between jumps in H have uniform distance $e_{K'} = p-1$. The equation above gives $G(1) = H(1) = H$, and Hasse-Arf shows that 1 and p are the only candidates for the first jump in H. Proposition 5.4 excludes the latter, so the jumps in H occur at $m(p-1)+1$ with $1 \leq m \leq n-1$.[3] For G this translates to

$$j^m = m - 1.$$

The integration formula for ψ becomes a simple telescopic sum and immediately gives $\psi(j^m) = \psi(m-1) = p^{m-1} - 1$.

[3] This also shows the relation $H_n = H\big((n(p-1)+1\big)$ we referred to in the Preface.

m	j^m	j_m	*Ramification groups*		
1	0	0	G_0	=	$G(1) = G[1]$
				=	$\mathrm{Gal}(L/K)$
2	1	$p-1$	G_1	=	$\mathrm{Gal}(L/L_1)$
...	...	...	...		...
m	$m-1$	$p^{m-1}-1$	G_{m-1}	=	$G(j^m) = G[j_m]$
				=	$\mathrm{Gal}(L/L_{m-1})$
...	...	...	...		...
n	$n-1$	$p^{n-1}-1$	G_{n-1}	=	$\mathrm{Gal}(L/L_{n-1})$
–	–	–	G_n	=	1

6. Filtrations of analytic ramification groups

6.1. Statement of Sen's theorem and outline of its proof

We recall that a filtration of a group G is a family of subsets $(G_n)_{n\in I}$, with $G_n \supset G_m$ for $n \leq m$ and $\cap_n G_n = 1$. All filtrations now require $I = \mathbb{N}$, unless otherwise stated. A filtration (G_n) is *uniformly equivalent in scaling s* to another filtration (G^m) if $n \cdot s + O(1) = m$, that is: $G^{ns+c} \subset G_n \subset G^{ns-c}$ for some constant c.

The expression "equivalent" comes from the fact that both filtrations are *topologically* equivalent. We emphasize that "uniform equivalence" is an equivalence relation between filtrations if and only if we deal with scaling 1.

A filtration on a p-adic analytic group G is called *Lie filtration* if it agrees with the lower p-series on some open uniform subgroup $H \subset G$. This means there exists $r \in \mathbb{N}$ such that $P_n(H) = G_{r+n}$ for all $n \geq 0$.

The aim of this chapter is to prove

Theorem 6.1 (Sen)**.** *Let L/K be a totally ramified extension of local fields in characteristic 0, and let $e = e_K = v_K(p)$ denote the absolute ramification index of K. Assume that the Galois group $G = \mathrm{Gal}(L/K)$ is p-adic analytic, with $\dim(G) > 0$. Let (G_n) be a filtration on G that is uniformly equivalent in scaling 1 to some Lie filtration. (G_n) is then uniformly equivalent in scaling e to the ramification filtration $\big(G(n)\big)$. In other words, there exists a constant $c > 0$ such that*

$$G(ne + c) \subset G_n \subset G(ne - c)$$

for all n, with $G(r) = G$ for $r < 0$.

The definition of "Lie filtration" in [8] differs from the one given here, in that "uniform" is replaced by "p-saturated". The observations in Section 4.4 have shown that two filtrations of these kinds are uniformly equivalent in scaling 1 for an analytic pro-p group. The same holds for an analytic Galois group G as above, because G contains an open normal pro-p subgroup of finite index (cf. Corollary 4.9).

Outline of the proof

Section 6.2 Our first step is to reduce the problem to a uniform group G of dimension $d > 0$, with filtration $G_n = P_n(G)$ the lower p-series. This opens up the results developed in previous chapters.

Section 6.3 The essential idea to prove Sen's theorem is to study the sequence of quotients (G/G_n) together with their ultimate jumps (u_n) in upper numbering. As first approximation, we focus on the groups $A = G_n/G_{n+m}$ with $m \leq n+1$. These are *abelian* p-groups by Lemma 1.12, and Theorem 5.14 allows to describe the impact of p-th powers in terms of the ramification filtration.
Dependent on the size of u_A, this description takes two different forms. This leads to the distinction between *small* and *non-small* groups, and we derive a lower bound for u_A in the case of a small group.

Section 6.4 Non-small quotients are however of greater interest to us, for they allow to transfer knowledge of the u_A back to the u_n. Indeed, we will see that the ultimate jumps eventually increase uniformly by e, ie. there exists n_1 such that $u_{n+1} = u_n + e$ for all $n \geq n_1$. (This is Proposition 6.8.)
This gives the first inclusion in Sen's Theorem, ie. an inclusion of the form $G(ne+c) \subset G_n$ for some constant c. An obvious requirement is that there must be "enough" non-small quotients to have knowledge of the entire sequence u_n. (This is Proposition 6.13 & 6.8.)

Section 6.5 We use our results on Lie theory to establish the converse result. We will compare groups of the form G_{2n+1} and $G(ne+c)$, and discover they give rise to a projective system of certain quotients with limit $M \subset \mathscr{L} = \log(G)$. Sen's Theorem is immediate once we know that $p^{n_0}\mathscr{L} \subset M$ for some n_0.
For this latter statement, we need to replace M with its saturation within $\mathcal{L}(G) = \mathbb{Q}_p\mathscr{L}$. This saturation is a Lie ideal I, and corresponds to a uniform, closed and normal subgroup $N = \exp(I)$ of G. (This is Proposition 3.11.) A dimension argument now finishes the proof.

6.2. Reduction to uniform groups

Let L/K be a field extension with Galois group as described in Theorem 6.1. The theorem is trivial for any (finite) group G of dimension 0, so we assume $\dim(G) > 0$.

We recall that "uniform equivalence" is an equivalence relation between filtrations if and only if we deal with scaling 1. A filtration (G_n) is thus uniformly equivalent in scaling s to some fixed filtration if and only if this holds for all other filtrations that are uniformly equivalent in scaling 1 to (G_n). We conclude that it is sufficient to show Sen's Theorem for some Lie filtration. Let (G_n) be such a filtration, and denote by H

the uniform subgroup that the filtration eventually ends up in. It is immediate that we can skip finitely many groups to only consider the filtration

$$\big(G_0 = G,\ \ G_1 = H,\ \ G_n = P_{n-1}(H) \text{ for } n \geq 2\big)$$

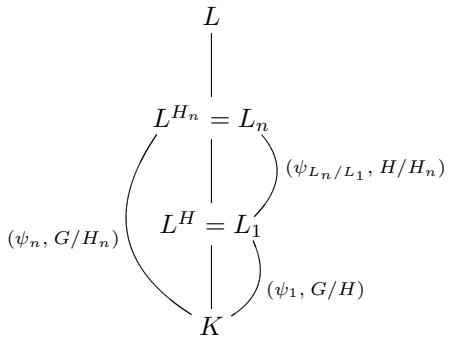
The open subgroup H corresponds to an intermediate extension L/L_1 such that L_1/K is finite with absolute ramification index $e_1 = e_{L_1} = v_{L_1}(p) = [L_1 : K]$. Suppose Sen's Theorem valid for H, that is: assume that the filtration $(P_n(H))$ is uniformly equivalent in scaling e_1 to $(H(n))$. To deduce the Theorem for G, we need to show that the ramification filtration on G is uniformly equivalent in scaling e_1/e to the ramification filtration on H.

$$\begin{array}{ccc} G_n & \overset{e}{\cdots\cdots\succ} & G(n) \\ \Big\downarrow{\scriptstyle 1} & & \Big\downarrow{\scriptstyle e_1/e} \\ P_n(H) & \underset{e_1}{- - \succ} & H(n) \end{array}$$

Lemma 6.2. *Recall the definition of $\psi_1 = \psi_{L_1/K}$ in Section 5.3.[1] For $r \geq 1$, we have*

$$G(r) \cap H = H\big(\psi_1(r)\big).$$

Proof: The groups $G(r)$ and H are closed in the profinite group G, and hence profinite as well. By definition of the (infinite) ramification groups as projective limits over their finite counterparts, we can check the assertion "componentwise".



It is sufficient to consider a (cofinal) system of open normal subgroups $(H_n)_{n\geq 2}$ that lie within $H = H_1$. The fixed field $L^{H_n} = L_n$ thus contains $L^H = L_1$ and is equipped with the function $\psi_{L_n/K} = \psi_n$. The assertion now follows with Theorem 5.8 and the transitivity relation $\psi_n = \psi_{L_n/L_1} \circ \psi_1$ (cf. [6], II, 10.8):

$$\begin{aligned} \big(G(r)H_n \cap H\big)/H_n &= \big(G/H_n\big)(r) \cap H/H_n = \big(G/H_n\big)\big[\psi_n(r)\big] \cap H/H_n \\ &= \big(H/H_n\big)\big[\psi_n(r)\big] = \big(H/H_n\big)\big[\psi_{L_n/L_1} \circ \psi_1(r)\big] = \big(H/H_n\big)\big(\psi_1(r)\big) \\ &= H\big(\psi_1(r)\big)H_n/H_n \end{aligned}$$

□

[1] The notation "e_1", "ψ_1" etc. comes from $H = G_1$ and will become clear when we consider a sequence of open subgroups.

Proposition 6.3. *The ramification filtration on G is uniformly equivalent in scaling e_1/e to the ramification filtration on H. More precisely, for $r > u_1$ we have*

$$G(r) = H\big(r \cdot e_1/e + (l_1 - u_1 \cdot e_1/e)\big),$$

where $u_1 = u_{G/H}$ is the ultimate jump in the upper numbering, and $l_1 = \psi_1(u_1)$ in the lower numbering of G/H.

Proof: By Proposition 5.10, we know that upper ramification groups are compatible with their quotients. This means $(G/H)(r) = G(r)H/H$ for all r, and hence $G(r) \subset H$ if and only if $r > u_1$. By the Lemma above, we conclude with the calculation of $\psi_1(r)$:

$$\begin{aligned}\psi_1(r) = \int_0^r \left(\frac{G}{H} : \frac{G}{H}(t)\right) \mathrm{d}t &= \int_0^{u_1} (\ldots)\mathrm{d}t + \int_{u_1}^r (\ldots)\mathrm{d}t \\ &= l_1 + (r - u_1) \cdot (G : H) \\ &= l_1 + (r - u_1) \cdot (e_1/e).\end{aligned}$$

□

6.3. A lower bound for jumps in small finite abelian groups

We place ourselves in the set-up of Theorem 5.14: let A denote the Galois group of a finite abelian extension of local fields, with order a power of p, and e_A the absolute ramification index of the base field. We wish to describe the ultimate jumps in such groups only in terms of the (abstract) group structure of A and the invariant e_A.

We call the group A *small* if the ultimate jump in the upper numbering is bounded above by

$$u_A \leq \frac{p}{p-1} \cdot e_A$$

One of this section's main results is a *lower* bound for small groups in terms of their p-torsion subgroups. We start by making ourselves familiar with the concept "small":

Lemma 6.4. *The group A is small if and only if $A(r)^p \subset A(pr)$ for all $r \geq 0$.*

Proof: Assume A as small. Due to Theorem 5.14 we have $A(r)^p \subset A(pr)$ for $r \leq \frac{1}{p-1} \cdot e_A$. For $r = \frac{1}{p-1} \cdot e_A + \varepsilon$ we have

$$\begin{aligned}A(r)^p = A(r + e_A) = A\left(\frac{e_A}{p-1} + \varepsilon + e_A\right) = A\left(\frac{p}{p-1} \cdot e_A + \varepsilon\right) \\ \subset A\big(u_A + \varepsilon\big) = 1.\end{aligned}$$

by first applying Theorem 5.14 and then that A is small.
Let conversely $A(r)^p \subset A(pr)$ be satisfied for all $r \geq 0$, and choose $\varepsilon > 0$. We have to show $A\Big(\frac{p}{p-1} \cdot e_A + \varepsilon\Big) = 1$. By assumption and Theorem 5.14 again, we have

$$A\left(\frac{p \cdot e_A}{p-1} + p \cdot \varepsilon\right) \supset A\left(\frac{e_A}{p-1} + \varepsilon\right)^p = A\left(\frac{p \cdot e_A}{p-1} + \varepsilon\right) \supset A\left(\frac{p \cdot e_A}{p-1} + p \cdot \varepsilon\right)$$

The implied equality $A\left(\frac{p \cdot e_A}{p-1} + p \cdot \varepsilon\right) = A\left(\frac{p \cdot e_A}{p-1} + \varepsilon\right)$ now shows $A\left(\frac{p \cdot e_A}{p-1} + \varepsilon\right) = 1$.
□

Any quotient of a small group is itself small, for the ramification index e_A stays the same. Conversely, the quotient of a non-small group stands a chance of becoming small. Indeed, the passage to a quotient admits a crucially easy description in this latter case:

Lemma 6.5. *Let $A_{(n)}$ denote the subgroup of elements $a \in A$ such that $a^n = 1$. We have:*

(i) $u_A \geq p^m \cdot u_{A/A_{(p^m)}}$ *for $m \geq 1$, if A is small,*

(ii) $u_A = u_{A/A_{(p)}} + e_A$, *if A not small.*

Proof: We have seen in section 5.3 that passing to a quotient is well-behaved under the upper numbering and satisfies $A(r)H/H = (A/H)(r)$. For $H = A_{(p^m)}$, this implies the relation

$$A(r) \subset A_{(p^m)} \Longleftrightarrow r > u_{A/A_{(p^m)}}$$

We can now prove the above statements:

(i) Because of $\big(A(u_A/p^m + \varepsilon)\big)^{p^m} \subset A(u_A + \varepsilon p^m) = 1$, we have $u_A/p^m + \varepsilon > u_{A/A_{(p^m)}}$.

(ii) If A is not small, we know by definition that $u_A > \frac{p}{p-1} \cdot e_A$, and thus have $u_A - e_A > \frac{1}{p-1} \cdot e_A$. By Theorem 5.14, this means $\big(A(u_A - e_A)\big)^p = A(u_A) \neq 1$. We thus have

$$u_{A/A_{(p)}} \geq u_A - e_A$$

Any $\varepsilon > 0$ gives $u_A - e_A + \varepsilon > \frac{1}{p-1} \cdot e_A$. It follows that $\big(A(u_A - e_A + \varepsilon)\big)^p = A(u_A + \varepsilon) = 1$, which altogether implies

$$u_A - e_A + \varepsilon > u_{A/A_{(p)}} \geq u_A - e_A$$

□

We will state the lower bound for the last jump in A in terms of the lower numbering. There is an obvious relation between l_A and u_A:

Lemma 6.6. *Regardless of whether A is small, we have*

$$l_{A/A_{(p^m)}} \leq u_{A/A_{(p^m)}}\big(A : A_{(p^m)}\big)$$

Proof: Recall the integral representation of $\psi_G = \phi_G^{-1}$ from the remarks after Definition 5.9. For any finite group G, we have

$$l_G = \psi_G(u_G) = \int_0^{u_G} \big(G(0) : G(t)\big)\mathrm{d}t \leq u_G \cdot |G|$$

Setting $G = A/A_{(p^m)}$, this translates into our proposition. □

We can now prove the desired estimate:

Proposition 6.7. *Suppose A is small. For $m \geq 1$, the last jump in the lower filtration satisfies:*

$$l_A \geq p^{m-1}(p-1) \cdot \Big(A_{(p^m)} : A_{(p)}\Big) \cdot l_{A/A_{(p^m)}}$$

Proof: This is a matter of persistent calculations:

$$\begin{aligned} l_A = \psi(u_A) = \int_0^{u_A} (A : A(t))\mathrm{d}t &\geq \int_{u_A/p+\varepsilon}^{u_A} \big(A : A(t)\big)\mathrm{d}t \\ &\geq (u_A - u_A/p - \varepsilon) \cdot \big(A : A(u_A/p+\varepsilon)\big) \\ &\geq \big(p^{-1}\,(p-1) \cdot u_A - \varepsilon\big) \cdot \big(A : A_{(p)}\big). \end{aligned}$$

The last inequality follows from $A(u_A/p+\varepsilon) \subset A_{(p)}$, which in turn follows from Lemma 6.4 by $A(u_A/p+\varepsilon)^p \subset A(u_A + p\cdot\varepsilon) = 1$.

We now apply Lemma 6.5 by replacing u_A with its lower estimate:

$$\begin{aligned} l_A &\geq \Big(p^{-1}\,(p-1) \cdot u_{A/A_{(p^m)}} \cdot p^m\Big) \cdot \big(A : A_{(p)}\big) \\ &= p^{m-1}\,(p-1) \cdot u_{A/A_{(p^m)}} \cdot \big(A : A_{(p)}\big) \\ &= p^{m-1}\,(p-1) \cdot \underbrace{\left(u_{A/A_{(p^m)}} \cdot \frac{|A|}{|A_{(p^m)}|}\right)}_{\geq\ l_{A/A_{(p^m)}} \text{ by 6.6}} \cdot \frac{|A_{(p^m)}|}{|A_{(p)}|} \\ &\geq p^{m-1}\,(p-1) \cdot l_{A/A_{(p^m)}} \cdot \Big(A_{(p^m)} : A_{(p)}\Big). \end{aligned}$$

□

6.4. Sen's Theorem: The first inclusion

We return to the situation described in Sen's Theorem 6.1 and additionally assume G uniform and of dimension $d > 0$, as explained in section 6.2. We recall that G has a filtration of open normal subgroups

$$G_0 = G \supset G_1 = \{x^p : x \in G\} \supset G_2 = \{x^p : x \in G_1\} \supset \dots$$

Each quotient G_n/G_{n+m} has size p^{md}. For $m \leq n+1$, it is abelian and isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^d$. The most important objects are the quotients G/G_n, for which we agree upon the following notation:

- With $n \geq 1$, let $u_n = u_{G/G_n}$ denote the last jump in G/G_n in the upper numbering. Correspondingly, $l_n = l_{G/G_n}$ denotes the last jump in the lower numbering. (u_n) is a strictly ascending sequence: $(G/G_n)(s) = 1 \Leftrightarrow G(s) \subset G_n$ tells us that it is ascending. We also have the inequalities $(G/G_{n+1})(u_n) \nsubseteq G_n/G_{n+1} \neq 1$. Thus, the group $(G/G_{n+1})(u_n)$ cannot be annihilated by p, ie. cannot be the last non-trivial group in the ramification filtration of G/G_{n+1}. This gives $u_{n+1} > u_n$.
- Being a Galois group in its own right, G/G_n comes with functions $\varphi_n = \varphi_{G/G_n}$ and $\psi_n = \varphi_n^{-1}$. Of course, we have $\psi_n(u_n) = l_n$.
- We denote the absolute ramification index of G_n by $e_n = e_{G_n}$. The condition that G belongs to a totally ramified extension translates into $e_n = e \cdot (G : G_n)$.

Let us assume there are "enough" non-small quotients: Proposition 6.13 will show that for any $m \geq \dim(G) + 3$, there always exists a non-small quotient G_n/G_{n+m}. We will see that this property is "hereditary", and also derive a result on the sequence (u_n) of ultimate jumps:

Proposition 6.8. *Suppose there are integers n_0 and $m \geq 2$ such that G_{n_0}/G_{n_0+m} is non-small and abelian. Let $n \geq n_0 + m$. If each quotient G_n/G_{n+2} is abelian, then none of them is small, and $u_{n+1} = u_n + e$ for every n.*

This "uniform rise" by e is the crucial ingredient to show the first inclusion in Sen's Theorem:

Corollary 6.9. *There exists an integer n_1 such that $u_n = u_{n_1} + (n - n_1)e$ for $n > n_1$. It follows that there is a constant c such that for every n, we have*

$$G(ne + c) \subset G_n.$$

Proof: We need to show that the requirements of Proposition 6.8 are fulfilled. By Lemma 1.12, the quotients G_n/G_{n+m} are abelian for $m \leq n+1$ and arbitrary n. Set $m = d + 3$. Since there are "enough" non-small quotients, there exists an abelian, non-small group G_{n_0}/G_{n_0+m} with $n_0 \geq d + 2$.

Set $n_1 = n_0 + m$ for brevity. We recall that (u_n) is a strictly ascending sequence, and that $G(r) \subset G_n$ if and only if $r > u_n$. Proposition 6.8 implies that

$$u_n \quad \begin{cases} \leq u_{n_1} & \text{if } n \leq n_1, \\ = u_{n_1} + (n - n_1)e & \text{if } n > n_1. \end{cases}$$

This means $u_n < ne + u_{n_1}$ for all $n > 0$, and we conclude by setting $c = u_{n_1}$. □

The verification of the assumptions made above will be of a somewhat technical nature. We start with a general observation:

Lemma 6.10. *Let H be a finite p-group, but not necessarily abelian. Assume H is provided with the lower numbering from some Galois extension, and let $H_{(p)}$ denote the set of elements annihilated by p. Any subgroup A that contains $H_{(p)}$ has the same last jump as H, that is: $l_A = l_H$.*

Proof: The ramification groups of A are induced by H, ie. $A[r] = H[r] \cap A$. If we had $A[l_H] = 1$, this would mean $1 = H[l_H] \cap A \supset H[l_H] \cap H_{(p)}$. This contradicts $H[l_H] \subset H_{(p)}$, which must hold since the higher quotients are annihilated by p. □

We now compare the numbers e_n and l_n for ascending quotients:

Lemma 6.11. *Let $A = G_n/G_{n+m}$ with $m \geq 1$. We have:*

(i) $l_{n+m} = l_A$

(ii) $l_{n+1} = l_{G_n/G_{n+1}} = l_{A/A_{(p^{m-1})}}$

Proof: We have to apply Lemma 6.10 above: set $H = G/G_{n+m}$ and note that $H_{(p)} = G_{n+m-1}/G_{n+m}$. This immediately gives (i) and the first equality in (ii). The rest follows from

$$A/A_{(p^{m-1})} = \frac{G_n/G_{n+m}}{(G_n/G_{n+m})_{(p^{m-1})}} \simeq \frac{G_n}{G_{n+1}}.$$

□

Lemma 6.12. *Assume that $A = G_n/G_{n+m}$ is abelian and small. For $m \geq 2$, we have:*

$$\frac{l_{n+m}}{e_{n+m}} \geq (p-1)p^{m-(d+2)} \cdot \frac{l_{n+1}}{e_{n+1}}$$

Proof: We have $l_{n+m} = l_A$ by the Lemma above, and $e_{n+m} = e_{n+1} \cdot (G_{n+1} : G_{n+m})$ since we are dealing with a totally ramified extension. This gives:

$$\frac{l_{n+m}}{e_{n+m}} = p^{-(m-1)d} \cdot l_A \cdot \frac{1}{e_{n+1}}$$

Lemma 6.7 concludes the proof with the estimate

$$\begin{aligned} l_A &\geq (p-1)p^{m-2} \cdot \big(A_{(p^{m-1})} : A_{(p)}\big) \cdot l\Big(A/A_{(p^{m-1})}\Big) \\ &= (p-1)p^{m-2} \cdot \quad p^{(m-2)d} \quad \cdot l_{n+1} \end{aligned}$$

where $l_{n+1} = l\big(A_{(p^{m-1})} : A_{(p)}\big)$ is case (ii) in the above Lemma. □

We can now derive the first assumption: the property "small" does not always coincide with the property "abelian", and there are "enough" non-small quotients.

Proposition 6.13. *Assume there is $m \geq \dim(G) + 3 = d + 3$ such that G_n/G_{n+m} is abelian for n sufficiently large. Then not all of these latter quotients are small.*

Proof: We deduce from Lemma 6.12 that for small quotients, we would have

$$\frac{l_{n+m}}{e_{n+m}} \geq (p-1)p \cdot \frac{l_{n+1}}{e_{n+1}}$$

This contradicts Proposition 5.4, which says that l_n/e_n is bounded by $\frac{1}{p-1}$ for all n. □

For the second assumption, we firstly state a relation between the values of u_n and l_n. This allows to derive an estimate for the growth of the numbers u_n.

Lemma 6.14. *For $n, m \geq 1$, we have $u_{G_n/G_{n+m}} = l_n + (u_{n+m} - u_n)(G : G_n)$.*

Proof: $u = u_{G_n/G_{n+m}}$ has the property that $G_n(u) \nsubseteq G_{n+m}$, but $G_n(u+\varepsilon) \subset G_{n+m}$ for all $\varepsilon > 0$. Analogously, the number u_{n+m} has the property that $G(u_{n+m}) \nsubseteq G_{n+m}$, but $G(u_{n+m}+\varepsilon) \subset G_{n+m}$. Recall that $u_{n+m} > u_n$, so Proposition 6.3 (with $H = G_n$) is applicable and gives

$$G(u_{n+m}) = G_n(l_n + (u_{n+m} - u_n) \cdot (G : G_n)),$$

which is what we had to show. □

Corollary 6.15. *Suppose there are $n, m \geq 1$ such that $A = G_n/G_{n+m}$ is abelian. Then*

(i) $u_{n+1} - u_n < \frac{e}{p^{m-2}(p-1)}$, *if G_n/G_{n+m} is small,*

(ii) $u_{n+m} - u_{n+m-1} = e$, *if G_n/G_{n+m} is not small.*

Proof: This is a direct consequence of Lemma 6.5. Note that

$$A/A_{p^{m-1}} = \frac{G_n/G_{n+m}}{(G_n/G_{n+m})_{(p^{m-1})}} = \frac{G_n/G_{n+m}}{G_{n+1}/G_{n+m}} \simeq \frac{G_n}{G_{n+1}}$$
$$A/A_p = \frac{G_n/G_{n+m}}{(G_n/G_{n+m})_{(p)}} = \frac{G_n/G_{n+m}}{G_{n+m-1}/G_{n+m}} \simeq \frac{G_n}{G_{n+m-1}}$$

For the case (i), since A is small by assumption, we have $u = u_{G_n/G_{n+m}} \leq \frac{p}{p-1} \cdot e_n$. From Lemma 6.5 we derive $u \geq p^{m-1} \cdot u_{G_n/G_{n+1}}$. Now we apply Lemma 6.14 above to substitute the expression $u_{G_n/G_{n+1}}$. This yields the inequalities

$$\frac{p}{p-1} \cdot e_n \geq u \geq p^{m-1}\big(l_n + (u_{n+1} - u_n)(G : G_n)\big)$$

The result follows by $l_n > 0$ and $e_n = e \cdot (G : G_n)$.

For (ii), Lemma 6.5 yields $u = u_{G_n/G_{n+m-1}} + e_n$. This time, we have to plug in the expression from Lemma 6.14 for u and $u_{G_n/G_{n+m-1}}$ on both sides. Subtract l_n to get

$$(u_{n+m} - u_n) \cdot (G : G_n) = (u_{n+m-1} - u_n) \cdot (G : G_n) + e_n$$

We simplify to $(u_{n+m} - u_{n+m-1}) \cdot (G : G_n) = e_n$, and observe $e_n = e \cdot (G : G_n)$. □

We can now prove the second assumption made in this section's beginning:

Proposition 6.8: Suppose there are integers n_0 and $m \geq 2$ such that G_{n_0}/G_{n_0+m} is non-small and abelian. Let $n \geq n_0 + m$. If each quotient G_n/G_{n+2} is abelian, then none of them is small, and $u_{n+1} = u_n + e$ for every n.

Proof: Since G_{n_0}/G_{n_0+m} is non-small, case (ii) in the above Corollary implies $u_{n_0+m} = u_{n_0+m-1} + e$. If the quotient G_{n_0+m-1}/G_{n_0+m+1} were small, we would have the contradiction $u_{n_0+m} - u_{n_0+m-1} < e$ by case (i). The quotient G_{n_0+m-1}/G_{n_0+m+1} is thus non-small, and we deduce from case (ii) that $u_{n_0+m+1} - u_{n_0+m} = e$. We reiterate this procedure to get the assertion. □

6.5. Sen's Theorem: The second inclusion

For the reverse inclusion, we will study the relation between the groups $G(ne + c)$ and G_{2n+1} for $n \geq n_1$ as in Corollary 6.9. This choice of indices is due to Lemma 1.12 and the previous result $G(ne + c) \subset G_n$, because they imply that the quotient $G(ne + c)G_{2n+1}/G_{2n+1}$ is abelian.

Rather than in the non-abelian group G, we wish to work within its associated $\mathbb{Z}_p$-Lie algebra $\mathscr{L} = \log(L_G)$. By Proposition 3.3, $\mathscr{L}$ is a free $\mathbb{Z}_p$-module and carries a

profinite group structure. We aim to relate the sequence $G(ne+c)$ to some projective system within $\mathscr{L} = \varprojlim \mathscr{L}/p^n\mathscr{L}$.

We recall there is an equivalence of categories between powerful Lie algebras and uniform groups (cf. Theorem 3.10). Under this equivalence, p-th powers in G correspond to multiplication with p in $\mathscr{L}$, giving $G_n = \exp(p^n\mathscr{L})$ and $\log(G_n) = p^n\mathscr{L}$. We point out again that the analytic map log is *not* a group homomorphism, but only maps G_n onto $p^n\mathscr{L}$ as sets.

Theorem 3.10 (together with Lemma 1.12 and Proposition 3.2) now gives an isomorphism of abelian groups

$$G_n/G_{n+m} \simeq (\mathbb{Z}/p^m\mathbb{Z})^d \simeq p^n\mathscr{L}/p^{n+m}\mathscr{L}$$

for any $m \leq n+1$. Any subgroup $A \subset G_n/G_{n+m}$ thus corresponds to exactly one subgroup $B \subset p^n\mathscr{L}/p^{2n+1}\mathscr{L}$, which we denote by $B = \log(A)$ and $A = \exp(B)$.

The shift-isomorphism sh: $G_n/G_m \simeq G_{n+1}/G_{m+1}$ induced by p-th powers (see the remark after Definition 1.19) corresponds to an isomorphism $p^n\mathscr{L}/p^m\mathscr{L} \simeq p^{n+1}\mathscr{L}/p^{m+1}\mathscr{L}$. It is induced by multiplication with p and as well denoted by sh. With this notation, we have a commutative diagram

$$\begin{array}{ccccc}
\mathscr{L}/p^{n+1}\mathscr{L} & & \xrightarrow{\quad\pi\quad} & & \mathscr{L}/p^n\mathscr{L} \\
\Big\downarrow{\scriptstyle \exp\cdot\mathrm{sh}^{n+1}} & & & & \Big\downarrow{\scriptstyle \exp\cdot\mathrm{sh}^{n}} \\
G_{n+1}/G_{2n+2} & \xrightarrow{\pi} & G_{n+1}/G_{2n+1} & \xrightarrow{\mathrm{sh}^{-1}} & G_n/G_{2n}
\end{array}$$

where π denotes the canonical projection onto a smaller quotient. We can now construct the desired projective system:

Proposition 6.16. *For each $n \geq n_1$, let M_n denote the quotient*

$$M_n = \mathrm{sh}^{-n}\left(\log \frac{G(ne+c)G_{2n}}{G_{2n}}\right) \subset \frac{\mathscr{L}}{p^n\mathscr{L}}.$$

The quotients (M_n) form a projective system with surjective transition maps, and limit denoted by $M = \varprojlim_{n\geq n_1} M_n \subset \mathscr{L}$.

Proof: Recall from Corollary 6.9 that $n_1 \geq 6$ and $G(ne+c) \subset G_n$, so the definition makes sense. Using the above diagram, we need to check that M_{n+1} is mapped onto M_n. The interesting point is the shift-isomorphism sh^{-1}, for which we need the following result.

Lemma 6.17. *Let $n \geq n_1$ and c be as above. We have:*

$$G(ne+c)^p G_{2n+1} = G\big((n+1)e+c\big)G_{2n+1}$$

Proof of the Lemma: The definition of c in Proposition 6.9 means that $c = u_n - (n-n_1)e$ for $n \geq n_1$. Proposition 6.3 with $H = G_n$ gives:

$$\begin{aligned} G(ne+c) &= G\big(ne + u_n - (n-n_1)e\big) = G(u_n + n_1 e) \\ &= G_n\big((u_n + n_1 e)e_n/e + (l_n - u_n e_n/e)\big) \\ &= G_n(n_1 e_n + l_n) \end{aligned}$$

We set $\gamma = n_1 e_n + l_n > e_n/(p-1)$ for brevity. The quotient $G(ne+c)G_{2n+1}/G_{2n+1}$ is abelian by Lemma 1.12, so Theorem 5.14 is applicable:

$$\left(\frac{G_n(\gamma)^p G_{2n+1}}{G_{2n+1}}\right) = \left(\frac{G_n}{G_{2n+1}}(\gamma)\right)^p = \frac{G_n}{G_{2n+1}}(\gamma + e_n) = \frac{G_n(\gamma+e_n)G_{2n+1}}{G_{2n+1}}$$

Replacing n by $(n+1)$, the same calculation as above for $G(ne+c)$ now gives

$$G_n(\gamma + e_n) = G\big((n_1+1)e_n + l_n\big) = G\big((n+1)e + c\big).$$

□

Proposition 6.16 is now immediate:

$$\begin{aligned} M_{n+1} = \mathrm{sh}^{-n-1}\left(\log \frac{G\big((n+1)e+c\big)G_{2n+2}}{G_{2n+2}}\right) &\xrightarrow{\exp\cdot\mathrm{sh}^{n+1}} \frac{G\big((n+1)e+c\big)G_{2n+2}}{G_{2n+2}} \\ &\xrightarrow{\pi} \frac{G\big((n+1)e+c\big)G_{2n+1}}{G_{2n+1}} \underset{(6.17)}{=} \frac{G(ne+c)^p G_{2n+1}}{G_{2n+1}} \\ &\xrightarrow{\mathrm{sh}^{-1}} \frac{G(ne+c)G_{2n}}{G_{2n}} \xrightarrow{\mathrm{sh}^{-n}\cdot\log} M_n \end{aligned}$$

□

Let us assume that M is large enough to contain $\mathscr{L}$ up to multiplication by some power of p. This is sufficient to finish the proof of Sen's Theorem:

Proposition 6.18. *Assume that $p^{n_2}\mathscr{L} \subset M$ for some n_2, and let $n > n_2$. We then have*

$$G_{n+n_2} \subset G(ne+c).$$

Proof: With $n > n_2$, the assumption implies

$$\frac{p^{n_2}\mathscr{L}}{p^n\mathscr{L}} \subset \frac{M + p^n\mathscr{L}}{p^n\mathscr{L}} = M_n.$$

We apply $\exp \cdot \mathrm{sh}^n$ to translate this into $G_{n+n_2}/G_{2n} \subset G(ne+c)G_{2n}/G_{2n}$, which gives

$$G_{n+n_2} \subset G(ne+c)G_{2n}.$$

Any $g \in G_{n+n_2}$ can thus be written as $g = g_0 b_0$, with $g_0 \in G(ne+c)$ and $b_0 \in G_{2n}$. By the same argument (e.g. with $n' = 2n - n_2$ in place of n), we see that this last factor admits a representation as $b_0 = g_1 b_1$ with $g_1 \in G(ne+c)$ and $b_1 \in G_{2n+1}$. We thus have $g = (g_0 g_1) b_1$. Repeated performance gives a sequence (h_m) with components

$$h_m = \prod_{i=0}^{m} g_i$$

that lie within $G(ne+c)$, and a sequence (b_m) with $b_m \in G_{2n+m}$. The (h_m) converge towards g, for

$$h_m \cdot g^{-1} = h_m \cdot (h_m b_m)^{-1} = h_m b_m^{-1} h_m^{-1}$$

is an element of G_{2n+m} due to the normality of the G_n (which in turn form a basis of neighbourhoods for the unit). The group $G(ne+c)$ is complete as closed subset of G and thus contains the limit g. □

It is an immediate corollary that the ramification groups are open in G, and that we obtain the inclusion

$$G_n \subset G(ne+c)$$

for all n by suitably redefining the constant c. This proves Sen's Theorem. An immediate consequence is the following version of Theorem 5.14 for infinite Lie groups:

Proposition 6.19. *Let G be p-adic analytic as in Sen's Theorem 6.1 (ie. we drop the assumption that G is uniform for the moment). For any $r \in \mathbb{R}$ large enough, we have*

$$G(r)^p = G(r+e)$$

Proof: Proposition 6.3 shows that we can return immediately to our assumption of a uniform group G. The proof of Lemma 6.17 shows that there was nothing special about the constant c, and we can add any constant $a \geq 0$ to get

$$G(ne+c+a)^p \, G_{2n+1} = G\big((n+1)e+c+a\big) \, G_{2n+1}$$

Choose any a from the interval $[0, e]$ and set $c_1 = c + a$ for brevity. For $n > n_1$ sufficiently large, we have

$$\begin{aligned} G(ne+c_1) \;&\supset\; G\big(2ne-c\big) &&\supset G_{2n} \\ G\big((n+1)e+c_1\big) \;&\supset\; G\big((2n+1)e-c\big) &&\supset G_{2n+1} \end{aligned}$$

The first inclusions are due to the magnitude of n, the second inclusions follow from Sen's Theorem. The first line immediately implies $G(ne+c_1)^p \supset G_{2n+1}$, and the above

version of Lemma 6.17 then gives

$$G(ne+c_1)^p = G(ne+c_1)^p\, G_{2n+1} = G\big((n+1)e+c_1\big)G_{2n+1}$$
$$= G\big((n+1)e+c_1\big)$$

□

We conclude this chapter to prove the assumption $p^{n_2}M \subset \mathscr{L}$ in the above result. Since M is in general no subalgebra of $\mathscr{L}$, we first need to move on to a more suitable object.

Lemma 6.20. *Recall that $\mathbb{Q}_pM \subset \mathbb{Q}_p\mathscr{L} = \mathcal{L}(G)$ is the $\mathbb{Q}_p$-subspace spanned by M, and let $I = \mathbb{Q}_pM \cap \mathscr{L}$ denote the subset that lies within $\mathscr{L}$. Then I is a Lie ideal in $\mathscr{L}$, and the quotient module $\mathscr{L}/I$ is torsion-free.*

Proof: Any inner automorphism of G

$$(\cdot)^\tau : G \longrightarrow G, \quad g \mapsto (\tau^{-1}g\tau)$$

is also a $\mathbb{Z}_p$-Lie algebra automorphism of $\mathscr{L}$ (see the definition of the abelian group operation $+_G$ in Section 3.1). Since each subgroup $G(ne+c)$ is normal in G, each M_n and hence M is invariant under every τ. Hence, $\mathbb{Q}_pM$ is an invariant subspace of $\mathcal{L}(G) = \mathbb{Q}_p\mathscr{L}$ (which is an *associative* algebra and thus has the commutator as Lie bracket). This is enough for the first assertion: for $m \in M$ and $\lambda \in \mathcal{L}(G)$, we have

$$(m,\lambda) = m\lambda - \lambda m = \lambda(\underbrace{\lambda^{-1}m\lambda}_{\in \mathbb{Q}_pM} - m) \in \mathbb{Q}_pM$$

Intersecting with $\mathscr{L}$ preserves these properties and gives the first assertion. For the second, let $a \in \mathscr{L}$ and $\lambda \neq 0 \in \mathbb{Z}_p$ such that $\lambda a \in I = \mathbb{Q}_pM \cap \mathscr{L}$. Then $a = \lambda^{-1}(\lambda a) \in \mathbb{Q}_pM$, and hence $a \in \mathbb{Q}_pM \cap \mathscr{L} = I$. □

Lemma 6.21. *Let $N = \exp(I) \subset G$ denote the (closed) subgroup of G that corresponds to the Lie ideal I. The group N contains generators of $G(ne+c)$ modulo some open subgroup of G, and we have $G(ne+c) \subset G_{2n}N$.*

Proof: We have $M_n = (M + p^n\mathscr{L})/p^n\mathscr{L} \subset (I + p^n\mathscr{L})/p^n\mathscr{L}$ by definition. This yields:

$$\frac{G(ne+c)G_{2n}}{G_{2n}} = \exp\big(\mathrm{sh}^n \cdot M_n\big) \subset \exp\left(\mathrm{sh}^n \cdot \frac{I + p^n\mathscr{L}}{p^n\mathscr{L}}\right)$$
$$= \exp\left(\frac{p^nI + p^{2n}\mathscr{L}}{p^{2n}\mathscr{L}}\right) = \frac{N^{p^n}G_{2n}}{G_{2n}}$$

□

The quotient $\overline{G} = G/N$ is the Galois group of some intermediate extension L'/K, uniform by Proposition 3.11 and p-adic analytic under the projection $G \to G/N$ (Proposition 4.12). Its lower p-series is given by $P_n(\overline{G}) = \overline{G}_n = G_nN/N$.

If $\dim(N) = \mathrm{rk}_{\mathbb{Z}_p}(I) < \mathrm{rk}_{\mathbb{Z}_p}(\mathscr{L}) = \dim(G)$, then $\overline{G}$ has dimension > 0 by Theorem 1.27, and satisfies the observations made in Corollary 6.9. The sequence $\overline{u}_n = u_{\overline{G}/\overline{G}_n}$ thus "ascends by $\overline{e}$ eventually". The passage to the quotient group $\overline{G}$ however keeps the base field, which means $\overline{e} = e$. We thus have

$$\overline{u}_n = ne + \overline{c}$$

for some constant $\overline{c}$ and n larger than some $\overline{n_1}$. This is the decisive ingredient in proving our fundamental assumption:

Proposition 6.22. *There is a fixed number n_2 such that $p^{n_2}\mathscr{L} \subset M$.*

Proof: The assertion is immediate if $I = \mathscr{L}$: we would have $\mathbb{Q}_pM \supset \mathscr{L}$, and M is a (free and finitely generated) submodule of the free $\mathbb{Z}_p$-module $\mathscr{L}$. Let us assume $I \neq \mathscr{L}$ for a contradiction, that is $\dim(N) = \mathrm{rk}_{\mathbb{Z}_p}(I) < \mathrm{rk}_{\mathbb{Z}_p}(\mathscr{L}) = \dim(G)$.

For typographic reasons, let $u(A)$ denote u_A. The sequence $\overline{u}_n = u(\overline{G}/\overline{G}_n)$ denotes the last jumps in G/G_nN, and we have

$$\overline{u}_{2n} = u\big(\overline{G}/\overline{G}_{2n}\big) = u\left(\frac{G/N}{G_{2n}N/N}\right) = u\left(\frac{G}{G_{2n}N}\right)$$

The result $G(ne + c) \subset G_{2n}N$ in Lemma 6.21 thus translates to

$$\overline{u}_{2n} < ne + c$$

Combining this result with $\overline{u}_n = ne + \overline{c}$ for $n \geq \overline{n_1}$ as discussed above, we obtain

$$2ne + \overline{c} = \overline{u}_{2n} < ne + c$$

for all $n \geq \overline{n_1}$, which is a contradiction. □

7. Extensions and applications of Sen's Theorem

This chapter provides two supplements to the results obtained in Chapter 6. Firstly, we show that Sen's Theorem does not depend on finite residue fields but also holds in the case of *perfect* residue fields. Secondly, we give a brief summary of the relation between p-adic Lie groups and "deeply ramified" fields.

7.1. Extension to perfect residue fields

We place ourselves in the situation of Chapter 6. The proof of Sen's Theorem 6.1 does not crucially rely on the residue field k of K to be finite. In this section, we will show that it is already sufficient to assume k perfect.

Theorem 7.1. *Let L/K be a totally ramified Galois extension of fields in characteristic 0, complete with regard to discrete, non-archimedean valuations, and with* perfect *residue field k of characteristic $p > 0$. With the remaining assumptions as in 6.1, Sen's Theorem holds in this situation as well.*

We keep the above assumptions on K and k for the entire section. We need to collect a few (somewhat loose) facts before we can prove the above result. The first one is concerned with the construction of a *finite* extension L/K as above:

(i) Let K' and k' denote fields with the above properties. Any extension k/k' of the residue fields gives rise to an unramified extension K/K', with residue field of K equal to k (cf. [3], chp. II, 5.5). If k/k' is algebraic, this requires lifting roots of certain polynomials. In the transcendent case $k' = k(X)$, one defines a suitable valuation on $K = K'(X)$ that sends X to zero.

(ii) Now assume the base field K already given. An extension L/K is totally ramified of degree n if and only if L is the splitting field of an Eisenstein polynomial $f(X) = X^n + a_1X^{n-1} + \ldots + a_n$ with coefficients $a_i \in \mathfrak{m}_K \subset \mathcal{O}_K$, but $a_n \notin \mathfrak{m}_K^2$. The primitive root α of f is a prime element of L, and generates the ring of integers, ie. $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. We refer to ([3], chp. II, 3.6) and ([11], chp. I, §6) for details.

Setting $K' = \mathbb{Q}_p$ in (i) shows that there exists a complete discrete valuation field of characteristic 0 with any given residue field of characteristic p and absolute ramification index 1.

This last result admits a more precise formulation, for any field k (perfect, of characteristic p) gives rise to the *Witt ring* $W(k)$. This ring is complete with regard to a discrete valuation, has k as its residue field, and is *absolutely unramified* in that p has valuation 1. We refer to ([11], chp. II, §5) and ([3], chp. I, 7 & 8, and chp. II, 5) for a full discussion, and only include the following results:

(i) *Uniqueness.* Let $\mathcal{O}$ be another complete discrete valuation ring with k as residue field, and let e denote the absolute ramification index of $\mathcal{O}$. Then there exists an injection $W(k) \to \mathcal{O}$, which makes $\mathcal{O}$ a free $W(k)$-module of rank e. This shows in particular that $W(k)$ is unique up to isomorphism (cf. [11], chp. II, §5, Thm. 3 & 4).

(ii) *Ring of integers.* The p-adic integers $\mathbb{Z}_p$ are contained in $W(k)$ for any k. Indeed, the Witt ring can be thought of as generalisation of $\mathbb{Z}_p$ to non-algebraic extensions. This is justfied by $W(\mathbb{F}_p) = \mathbb{Z}_p$, and the fact that $W(k)$ is always the ring of integers in its quotient field.

(iii) *Functorial properties.* Even if k is just a perfect *ring*, Witt rings can still be constructed. In this case, $W(-)$ is a functor with $\mathrm{Hom}(k, k') = \mathrm{Hom}\big(W(k), W(k')\big)$. One of the many implications for fields is as follows: Let K_1 and K_2 be as above, with absolute ramification index 1. If there is an isomorphism $\bar{\iota} : k_1 \to k_2$ of their residue fields, then there exists a field embedding $\iota : K_1 \to K_2$ with $\overline{\iota(a)} = \iota(\overline{a})$ for all $a \in \mathcal{O}_{K_1}$, and the image of K_1 in K_2 is uniquely determined (cf. [3], chp. II, 5.6).

We now return to the set-up of Theorem 7.1. The original finiteness condition for Sen's Theorem was only relevant in the context of Theorem 5.14, which described the effect of p-th powers with regard to the ramification filtration. Once this result is also available for extensions with perfect residue fields, the extension of Sen's Theorem as in 7.1 is immediate.

The essential ingredient for the proof of Theorem 5.14 was a result from Local Class Field Theory (namely 5.13). The desired generalisation of 5.14 (and of Sen's Theorem) is thus directly related to a suitable generalisation of Local Class Field Theory. Indeed, it is known that the results of Local Class Field Theory can be extended to fields K as in the above Theorem 7.1, once their residue field k is *quasi-finite*.[1] This means that k is perfect with algebraic closure $\overline{k}$, and that there is an isomorphism $\widehat{\mathbb{Z}} \longrightarrow \mathrm{Gal}(\overline{k}/k)$ given by the $\widehat{\mathbb{Z}}$-exponentiation of a fixed element $\sigma \in \mathrm{Gal}(\overline{k}/k)$.

Example. An obvious example for quasi-finite fields are the finite fields $k = \mathbb{F}_q$, with σ the Frobenius map $x \mapsto x^q$. A non-trivial example is the power series field $k = C((T))$ of an algebraically closed field C. The algebraic closure of k can be described as

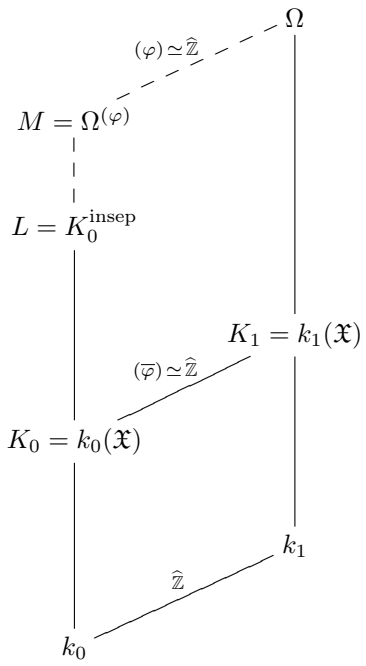
[1] Details on "Quasi-local Class Field Theory" can be found in [14] and [9].

the union of the cyclic extensions $k_n = C((T^{1/n}))$, with Galois groups generated by $\sigma_n : T^{1/n} \mapsto \zeta_n T^{1/n}$. The factors ζ_n are n-th roots of unity, and can be chosen such that they fit together and thus define an element σ for $\mathrm{Gal}(\overline{k}/k)$. If $C = \mathbb{C}$, one can choose $\sigma_n = \exp(2\pi i/n)$. Further details can be found in [11], chp. XIII, §2.

The following result shows that the above list of examples is by no means exhaustive:

Proposition 7.2. *Every algebraically closed field Ω occurs as closure of a quasi-finite subfield. This means there exists a quasi-finite subfield $M \subset \Omega$ with $\mathrm{Gal}(\Omega/M) \simeq \widehat{\mathbb{Z}}$.*

Proof: Let k_0 denote the prime field of Ω. Dependent on its characteristic, k_0 admits a $\widehat{\mathbb{Z}}$-extension k_1 by $\mathbb{F}_p^{\mathrm{sep}}$ or a subfield of $\mathbb{Q}^{\mathrm{ab}} = \cup_{n\geq 1} \mathbb{Q}(\zeta_n)$ (cf. [3], chp. 5, 1.2).



Let $\mathfrak{X}$ be a k_0-basis of transcendental elements in Ω. The field $K_0 = k_0(\mathfrak{X})$ then has $K_1 = k_1(\mathfrak{X})$ as $\widehat{\mathbb{Z}}$-extension. Its Galois group $\mathrm{Gal}(K_1/K_0) \simeq \widehat{\mathbb{Z}}$ is topologically generated by an element $\overline{\varphi}$ (an "abstract Frobenius").

Ω is algebraic over K_0, and is its algebraic closure. However, the extension does not need to be Galois, so we move on to the maximal inseparable extension $L = K^{\mathrm{insep}} = \Omega^{\mathrm{Aut}(\Omega/K_0)}$. By restriction to K_1, we have a continuous surjection

$$\mathrm{res}\colon \mathrm{Gal}(\Omega/L) \twoheadrightarrow \mathrm{Gal}(K_1/K_0) = (\overline{\varphi}) \simeq \widehat{\mathbb{Z}}$$

Choose a pre-image φ. The closed subgroup $H = (\varphi)$ of $\mathrm{Gal}(\Omega/L)$ generated by this element is procyclic, and thus has precisely $H^n = (\varphi^n)$ as open subgroups (cf. [6], IV, §2). The projection

$$\mathrm{pr}\colon H = (\varphi) \twoheadrightarrow (\overline{\varphi})/(\overline{\varphi^n}) \simeq \mathbb{Z}/n\mathbb{Z}$$

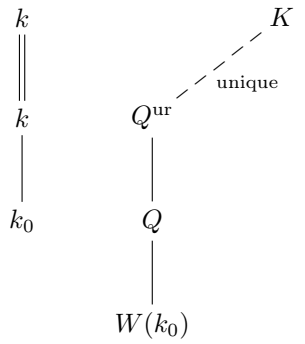
has an open subgroup as kernel, which then must be H^n by cardinality. By passage to the projective limit, this amounts to $H \simeq \widehat{\mathbb{Z}}$. We now set $M = \Omega^H$, and conclude by infinite Galois theory.

We can now prove the generalisation of Theorem 5.14 to the case of a perfect residue field k. The strategy is as follows: By Lemma 5.7, k can be assumed algebraically closed, so the above proposition gives a quasi-finite extension on the level of the residue fields. By means of the Witt ring, we can then construct a quasi-finite field extension L'/K' in characteristic 0, with the same ramification groups as L/K. Generalized Local Class Field Theory is then available and finishes the proof. As discussed above, the extension of Sen's Theorem as in 7.1 is a direct consequence.

Proposition 7.3. *The conclusion of Theorem 5.14 (where L/K is a* finite *extension) holds as well in the case of a perfect residue field k of characteristic $p > 0$, with all other requirements unchanged.*

Proof: By Lemma 5.7, we can assume that k is algebraically closed.

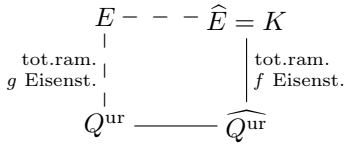
Proposition 7.2 then ensures the existence of a quasi-finite field $k_0 \subset k = \overline{k}$. The quotient field Q of the Witt ring $W(k_0)$ is a complete, discretely valued field of absolute ramification index 1. Its maximal unramified extension Q^{ur} has residue field isomorphic to k. By the functorial properties of the Witt ring (see (iii) above), there exists a unique embedding $Q^{\mathrm{ur}} \to K$.



On the other hand, by the uniqueness property of the Witt ring, $K/\widehat{Q^{\mathrm{ur}}}$ is a totally ramified extension of degree e. It is generated by the root of some Eisenstein polynomial $f \in \mathcal{O}_{\widehat{Q^{\mathrm{ur}}}}[X]$. We observe that this polynomial ring satisfies

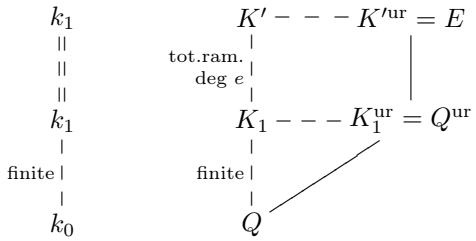
$$\mathcal{O}_{\widehat{Q^{\mathrm{ur}}}}/\widehat{\mathfrak{m}}[X] \simeq k[X] \simeq \mathcal{O}_{Q^{\mathrm{ur}}}/\mathfrak{m}[X]$$

with $\mathfrak{m} = \mathfrak{m}_{Q^{\mathrm{ur}}} \subset \mathcal{O}_{Q^{\mathrm{ur}}}$ for brevity. We can thus choose an Eisenstein polynomial $g \in \mathcal{O}_{Q^{\mathrm{ur}}}[X]$ with same reduction as f, and g then defines a totally ramified extension E/Q^{ur} of degree e such that $\widehat{E} = K$. In fact, $E \subset K$ is the maximal subextension that is algebraic over Q^{ur}, for it has the same absolute ramification index e as K, and the same algebraically closed residue field.



We want to move "one level lower" for an algebraic extension of Q. By ramification decomposition again, there exists an unramified finite extension K_1/Q and a totally

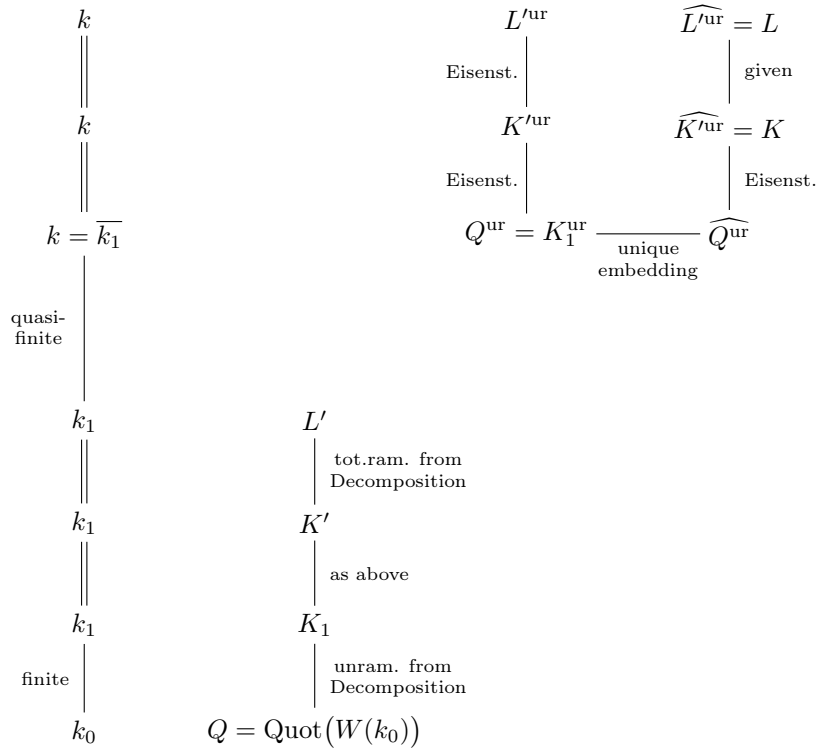
ramified extension K'/K_1 of degree e, such that $K'^{\mathrm{ur}} = E$:



It follows that K_1/Q has a finite residue field extension k_1/k_0; and k_1 is thus quasi-finite as well, which makes K'/K_1 a totally ramified extension of *quasi-local* fields, with $e_{K'} = e_K$.

We now repeat the entire procedure with K' in place of Q, and derive from the given extension L/K the existence of a totally ramified extension L'/K', with quasi-finite residue field k_1. With the same argument as at the beginning, the ramification groups of this extension coincide with those of L/K. This finishes the proof. □

We conclude this section with a (rather large) diagram to illustrate the entire construction above. The residue fields of the occuring fields are denoted in the first column (an "ordinate" in this sense). All vertical extensions are Galois, and finite except for k/k_1. For fields in characteristic 0, the different columns indicate a different "algebraic type": base field over the Witt ring, maximal unramified extension, and completion.



7.2. Deeply ramified fields

This section gives an outline of how Sen's theorem is applied in [1] to an arithmo-geometric problem. A certain class of fields plays an important part therein, namely the "deeply ramified" ones. We show that a field L (algebraic over $\mathbb{Q}_p$) is deeply ramified if there is a local field K such that L/K is a p-adic analytic Galois extension, with infinite inertia group.

Geometric background. Suppose A is an abelian variety, defined over $\mathbb{Q}_p$, and let $A[p^\infty]$ denote the p-primary subgroup of $A(\overline{\mathbb{Q}_p})$. The absolute Galois group $G = G_{\mathbb{Q}_p}$ has a natural action on this group. Now let L be any algebraic extension of $\mathbb{Q}_p$. In this situation, the Kummer homomorphism

$$\kappa_{A,L} : A(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(L, A[p^\infty])$$

is defined as follows: for a given point $P \in A(L)$ and representative $(p^{-n} \mod \mathbb{Z}_p)$, choose $Q \in A(\overline{\mathbb{Q}_p})$ such that $p^n Q = P$. Then $P \otimes (p^{-n} \mod \mathbb{Z}_p)$ is mapped to the class of the 1-cocycle φ, defined by $\varphi(\sigma) = \sigma(Q) - Q$ for all $\sigma \in G_L$.

An important question is whether the image of $\kappa_{A,L}$ admits a description solely in terms of the $G_{\mathbb{Q}_p}$-module $A[p^\infty]$. A satisfactory answer is known for all finite extensions, whereas in the infinite case, "deeply ramified" fields L have emerged as suitable objects to study (cf. [1], Prop. 4.3).

Relation to Lie groups. We recall from Chapter 5 that for any Galois group, its zero-th ramification group is equal to the inertia group I. This subgroup "contains all ramification", and the field fixed by it can be taken as base field for the examination of any higher ramification. The geometric situation above suggests to consider the absolute Galois group $G = G_{\mathbb{Q}_p}$ of the p-adic numbers. We then have $G(0) = \mathrm{Gal}\big(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\mathrm{ur}}\big)$, and each $r \geq 0$ defines a totally ramified extension K_r/K_0, where K_r is the field fixed by $G(r)$.

As above, let L be any algebraic extension of $\mathbb{Q}_p$. The field L is called *deeply ramified* if $L \not\subseteq K_r$ for all r. Intuitively, the upper numbering does not capture the "full amount" of ramification in L on any finite level, and the absolute ramification groups do not "shrink fast enough" to be ever contained in $G_L = \mathrm{Aut}_L(\overline{\mathbb{Q}_p})$.

This vague intuition can be made more precise by alternative definitions for deeply ramified fields. One method is to approximate L by means of finite extensions $F_n/\mathbb{Q}_p$, such that $L = \cup_n F_n$ and $F_n \subset F_{n+1}$. In this situation, L is deeply ramified if and only if $v_p\big(\delta(F_n/\mathbb{Q}_p)\big) \to \infty$ for $n \to \infty$, ie. if the different δ grows beyond all p-adic bounds.

This has an important consequence: in our definition of "deeply ramified", $\mathbb{Q}_p$ can always be replaced by any finite extension $K/\mathbb{Q}_p$, with the fields K_r altered accordingly. We then have $K_{-1} = K$, which was the motivation for the above notation. A similar remark applies for our sketch of the geometric background, where $\mathbb{Q}_p$ should be replaced by some local number field K. We refer to [1] for the general set-up, and in particular to Prop. 2.4, p. 143 and Lemma 2.12.

The classical example of a deeply ramified field is a field L which is a totally ramified $\mathbb{Z}_p$-extension of some field K, finite over $\mathbb{Q}_p$ (cf. [13]). We conclude this section to explain how Sen's Theorem provides a vast generalisation of this example:

Proposition 7.4. *Let K be a finite extension of $\mathbb{Q}_p$. Assume that L/K is a Galois extension with $J = \mathrm{Gal}(L/K)$ a p-adic analytic group. If the inertia group $I(L/K) = J(0)$ is infinite, then L is deeply ramified.*

Proof: We aim to show $L \not\subseteq K_r$, as explained in the definition above. Consider $L^{J(0)}$, the field fixed by the (closed) inertia group. We pass on to its completion K', and let $L' = LK'$ denote the compositum within an algebraic closure of K'. The extension L'/K' is totally ramified, and exhibits a ramification isomorphism

$$J'(r) = \mathrm{Gal}(L'/K')(r) \simeq \mathrm{Gal}(L/L^{J(0)})(r) = J(r)$$

by the infinite analogue of Lemma 5.7. Since $J(0)$ is closed in J, it is itself p-adic analytic, and so is J'.

However, J' has the additional virtue of being a group as required by Sen's Theorem (note that we need the generalised version of Theorem 7.1). One of the byproducts of this result was that the higher ramification groups $J'(r)$ are *open* and thus have finite index. By the ramification isomorphism above, the same holds for J. This gives $J(r) \neq 1$ for all r, because $J(0)$ is infinite. Combined with Proposition 5.10, this reads as

$$\frac{G_K(r)\, G_L}{G_L} \simeq \mathrm{Gal}(L/K)(r) = J(r) \neq 1$$

We conclude that $G_K(r) \nsubseteq G_L$ for all r. This means $K_r \not\supseteq L$ for all r, as desired. $\square$

Bibliography

[1] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields. *Invent. Math.*, 124(1-3):129–174, 1996.

[2] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[3] I. Fesenko. *Lectures on Local Fields*. School of Mathematical Sciences, University of Nottingham, `http://www.maths.nott.ac.uk/personal/ibf`.

[4] F. Laubie. Sur la ramification des extensions de Lie. *Compositio Math.*, 55(2):253–262, 1985.

[5] M. Lazard. Groupes analytiques p-adiques. *Inst. Hautes Études Sci. Publ. Math.*, (26):389–603, 1965.

[6] J. Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, 2002.

[7] P. Schneider and J. Teitelbaum. Algebras of p-adic distributions and admissible representations. *Invent. Math.*, 153(1):145–196, 2003.

[8] S. Sen. Ramification in p-adic Lie extensions. *Invent. Math.*, 17:44–50, 1972.

[9] J.-P. Serre. Sur les corps locaux à corps résiduel algébriquement clos. *Bull. Soc. Math. France*, 89:105–154, 1961.

[10] J.-P. Serre. Sur les groupes de Galois attachés aux groupes p-divisibles. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 118–131. Springer, Berlin, 1967.

[11] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[12] J.-P. Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006.

[13] J. T. Tate. $p-$*divisible groups*.. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.

[14] G. Whaples. The generality of local class field theory (Generalized local class field theory V). *Proc. Amer. Math. Soc.*, 8:137–140, 1957.