IWASAWA ALGEBRAS

SIMON WADSLEY

Lecture 1

1. Introduction

Recall the following famous result in Number Theory.

Theorem 1.1. *Suppose that p is a odd prime. If x, y and z are integers such that $x^p + y^p = z^p$ then $xyz = 0$.*

One possible approach to trying to prove this is to begin by factorising the equation in $\mathbf{Q}[\zeta_p]$ where $\zeta_p = e^{2\pi i/p}$ denotes a primitive p-th root of 1 in $\mathbb{C}$.

Before we discuss this we should recall some notation. If F is a finite field extension of $\mathbf{Q}$ then its ring of integers is denoted $\mathcal{O}_F$. A fractional ideal in F is then a non-zero finitely generated $\mathcal{O}_F$-submodule of F. If I and J are two fractional ideals then their product $IJ = \{\sum x_i y_i \mid x_i \in I, y_i \in J\}$ is a fractional ideal. Since $\mathcal{O}_F$ is a Dedekind domain the set of fractional ideals of F forms an abelian group with respect to this product.

The ideal class group $C_F = \mathrm{Cl}(\mathcal{O}_F)$ (also known as the Picard group of $\mathcal{O}_F$) is then defined to be the group of fractional ideals in F modulo the subgroup of principal fractional ideals. Although any abelian group can arise as the ideal class group of a Dedekind domain, $\mathrm{Cl}(\mathcal{O}_F)$ is known to always be finite. When $\mathrm{Cl}(\mathcal{O}_F) = 1$, $\mathcal{O}_F$ is a UFD.

In 1850 Kummer was able to prove that if $C_{\mathbf{Q}(\zeta_p)}$ has order coprime to p then Theorem 1.1 is true. However there are infinitely many primes where this is not the case (the first being 37). These latter are known as the irregular primes.

In the 1950s Iwasawa studied the following situation. For an odd prime p he considered for each $n \geqslant 1$ a primitive p^n-root of 1 called ζ_{p^n} and then defined $F_n = \mathbf{Q}(\zeta_{p^{n+1}})$ giving a tower of Galois extensions over $\mathbf{Q}$,

$$F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots .$$

Given $\sigma \in \mathrm{Gal}(F_n/\mathbf{Q})$, $\sigma(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^{\chi(\sigma)}$ for some $\chi(\sigma) \in (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$. This defines a group homomorphism

$$\chi_n \colon \mathrm{Gal}(F_n/\mathbf{Q}) \to (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times.$$

It can be shown that for each n, $\mathcal{O}_{F_n} = \mathbf{Z}[\zeta_{p^{n+1}}]$, F_n is Galois of degree $p^n(p-1)$ over $\mathbf{Q}$ and each χ_n is a group isomorphism.

Taking $F_\infty = \bigcup F_n$ then $F_\infty/\mathbf{Q}$ is an infinite Galois extension with Galois group $G = \mathrm{Gal}(F_\infty/\mathbf{Q}) = \varprojlim \mathrm{Gal}(F_n/\mathbf{Q})$ and the χ_n patch to an isomorphism $\chi \colon G \to \mathbf{Z}_p^\times$ called the cyclotomic character. Here $\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^m\mathbf{Z}$ as rings and $\mathbf{Z}_p^\times \cong \mathbf{Z}_p \times C_{p-1}$ as groups.

The question that Iwasawa addressed is how the groups $A_n = C_{F_n}[p^\infty]$, that is the Sylow p-subgroups of the ideal class groups, grow with n in the tower.

Theorem 1.2 (Iwasawa, 1958)**.** *For any prime p, there are natural numbers λ, μ and c such that for any sufficiently large n*

$$\log_p |A_n| = \lambda n + \mu p^n + c.$$

For each n the action of $G_n = \mathrm{Gal}(F_n/\mathbf{Q})$ on F_n induces an action of G_n on C_{F_n} and so on A_n. That is we may view A_n as a $\mathbf{Z}[G_n]$-module. Since A_n is a finite abelian p-group this action factors through $(\mathbf{Z}/p^N\mathbf{Z})[G_n]$ for N sufficiently large and so even $\mathbf{Z}_p[G_n]$ acts on A_n.

Now there are norm maps $A_m \to A_n$ for $m > n$ coming from

$$I \mapsto \prod_{\sigma \in \mathrm{Gal}(F_m/F_n)} I^\sigma.$$

These make $A_\infty = \varprojlim A_n$ into a module over the *Iwasawa algebra* $\mathbf{Z}_p[[G]] = \varprojlim \mathbf{Z}_p[G_n] \cong Z_p[[T]][\overleftarrow{C}_{p-1}]$. Here $\Lambda = \mathbf{Z}_p[[T]]$ is a power series ring in one variable over $\mathbf{Z}_p$. In particular it is a commutative Noetherian integral domain of dimension 2.

Fact 1.3. Using class field theory one can show A_∞ is finitely generated and torsion as a Λ-module.

One can also prove the following using commutative algebra.

Proposition 1.4. *If M is a finitely generated torsion Λ-module M there is a Λ-module map*

$$M \to \bigoplus_{i=1}^{t} \Lambda/p^{a_i}\Lambda \oplus \bigoplus_{j=1}^{s} \Lambda/f_j\Lambda$$

with finite kernel and cokernel where the $a_i \in \mathbf{N}$ and the f_j are monic elements of $\mathbf{Z}_p[T]$.

Then to prove Theorem 1.2 we take $M = A_\infty$ in the Proposition and then $\mu = \sum a_i$ and $\lambda = \sum \deg f_j$. The idea is that because Λ is so well-behaved studying A_∞ is easier than directly studying each of the pieces A_n that make it up. But then A_n can be recovered from A_∞.

One can play similar games with more general families of field extensions or covering spaces and the action of related Galois groups on cohomology groups associated to the these extensions/covernings.

In this course we will focus on the algebraic (and p-adic analytic) background to this kind of arithmetic set up which turns out to be interesting from a ring-theoretic and representation theoretic point of view apart from the arithmetic applications; i.e. we will be more interested in results like Proposition 1.4 than Fact 1.3.

I should note that almost all the material in this course and more can be found in Lazard's monumental paper 'Groupes analytiques p-adiques' Publications Mathématiques de l'IHÉS, Volume 26 (1965), p. 5-219.

To prepare the lectures I've also used an exposition of Lazard's material by Schneider in his book p-adic Lie groups published by Springer in 2011, and unpublished lecture notes by Ardakov for a similar course to this one given in Oxford in 2016.

2. Filtrations

2.1. **Ring filtrations.**

Definition 2.1. A *(descending) filtration* on a ring R is a function

$$v\colon R \to \mathbf{R}^{\geqslant 0} \cup \{\infty\}$$

such that for all $r, s \in R$:

(a) $v(r-s) \geqslant \min(v(r), v(s))$;
(b) $v(rs) \geqslant v(r) + v(s)$;
(c) $v(1) = 0$ and
(d) $v(0) = \infty$.

We say that the pair (R, v) is a *filtered ring*. We say that the filtration v is *separated* if $v^{-1}(\infty) = \{0\}$.

Remarks 2.2.

(1) Notice that condition (c) in Definition 2.1 follows from condition (b) unless $v(r) = \infty$ for all $r \in R$.
(2) Similarly condition (d) in Definition 2.1 follows from condition (b) unless $v(r) = 0$ for all $r \in R$.

Example 2.3. Let $p \in \mathbf{Z}$ be prime and let $v_p\colon \mathbf{Z} \to \mathbf{R}^{\geqslant 0} \cup \{\infty\}$ be given by

$$v_p(n) = \sup\{k \in \mathbf{N}_0 \mid p^k \text{ divides } n\}.$$

Then $(\mathbf{Z}, v_p)$ is a separated filtration.

Lecture 2

Exercise 2.4. Suppose that $M_n(R)$ denotes the ring of $n \times n$ matrices with coefficients in a filtered ring (R, v) and let $v_n\colon M_n(R) \to \mathbf{R}^{\geqslant 0} \cup \{\infty\}$ be given by

$$v_n(A) = \min_{1 \leqslant i,j \leqslant n} \{v(A_{ij})\}.$$

Show that v_n is a filtration on $M_n(R)$. Moreover v_n is separated if and only if v is separated.

Remark 2.5. For any filtered ring (R, v) there is a family of two-sided ideals of R given by $(R_\lambda = \{r \in R \mid v(r) \geqslant \lambda\})_{\lambda \in \mathbf{R}^{\geqslant 0}}$. This family satisfies the following three conditions:

$$R_0 = R;$$

$$R_\lambda = \bigcap_{\mu < \lambda} R_\mu \text{ for all } \lambda \in \mathbf{R}^{\geqslant 0}$$

and

$$R_\lambda R_\mu \subseteq R_{\lambda+\mu} \text{ for all } \lambda, \mu \in \mathbf{R}^{\geqslant 0}.$$

In fact any family of additive subgroups $(R_\lambda)_{\lambda \in \mathbf{R}^{\geqslant 0}}$ of R satisfying these three conditions corresponds to a filtration on R via $v(r) = \sup\{\lambda \in \mathbf{R}^{\geqslant 0} \mid r \in R_\lambda\}$.

Example 2.6. Let M denote the free monoid on X and Y so that elements of M consist of finite (possibly empty) strings w of Xs and Ys and the binary operation is given by concatenation. We write $\ell(w)$ for the length of a string w so

$$\ell(X) = \ell(Y) = 1 \text{ and } \ell(uv) = \ell(u) + \ell(v) \text{ for any two strings } u, v \in M.$$

Let $\mathbf{Z}[M]$ denote the free associative ring on two generators so that $\mathbf{Z}[M]$ may be viewed as a free $\mathbf{Z}$-module on M and multiplication is given by the $\mathbf{Z}$-bilinear extension of multiplication in M. Let $v\colon \mathbf{Z}[M] \to \mathbf{R}^{\geqslant 0} \cup \{\infty\}$ be given by

$$v\left(\sum_{m\in M} c_m m\right) = \inf \ell(m)$$

where the infinum is taken over the (finite) set of m such that $c_m \neq 0$.[1] Then v is a separated filtration on $\mathbf{Z}[M]$.

Definition 2.7. If (R, v) and (S, w) are filtered rings then a *morphism of filtered rings* from (R, v) to (S, w) is a ring homomorphism $f\colon R \to S$ with $w(f(r)) \geqslant v(r)$ for all $r \in R$.

2.2. **Topology and completion.** A filtration v on a ring R induces a topology on R; a subset of R is open if and only if it is a union of cosets $r + R_\lambda$. This makes R into a topological ring — that is the addition and multiplication maps $R \times R \to R$ are both continuous. Moreover if $f\colon R \to S$ is a morphism of filtered rings (R, v) to (S, w) then f is continuous with respect to the induced topologies.

Definition 2.8. The *completion* of a filtered ring (R, v)

$$\widehat{R} = \varprojlim R/R_\lambda = \left\{ (r_\lambda + R_\lambda)_{\lambda\in\mathbf{R}^{\geqslant 0}} \in \prod_{\lambda\in\mathbf{R}^{\geqslant 0}} R/R_\lambda \mid (\forall \mu < \lambda) r_\lambda + R_\mu = r_\mu + R_\mu \right\}$$

is a ring when equipped with pointwise operations. Moreover there is a natural ring homomorphism $R \to \varprojlim R/R_\lambda$ given by $r \mapsto (r + R_\lambda)$.

We say that a filtered ring (R, v) is *complete* if the natural map $R \to \widehat{R}$ is a isomorphism.

Exercise 2.9. Show that $\widehat{R}$ has a separated filtration

$$\widehat{v}((r_\lambda + R_\lambda)_{\lambda\geqslant 0}) = \inf\{\lambda \mid r_\lambda \notin R_\lambda\} = v(r_\mu) \text{ whenever } r_\mu \notin R_\mu$$

with respect to which it is complete. Show moreover the natural map $\iota_R\colon (R, v) \to (\widehat{R}, \widehat{v})$ is then a morphism of filtered rings and ι_R is injective precisely if v is separated.

Examples 2.10.

(1) If $R = \mathbf{Z}$ with the p-adic filtration then $\widehat{R}$ is the ring of p-adic integers $\mathbf{Z}_p$
(2) If $R = \mathbf{Z}[M]$ with M the free monoid on X and Y with the filtration given in Example 2.6 then $\widehat{R}$ is isomorphic to the Magnus algebra $\mathfrak{M}$ of associative (not commutative) formal power series in X and Y with coefficients in $\mathbf{Z}$. Elements of $\mathfrak{M}$ are formal sums $\sum_{m\in M} c_m m$ and $\mathfrak{M}_n = \{\sum_{m\in M} c_m m \mid c_m = 0 \text{ whenever } \ell(m) < n\}$.

2.3. **Associated graded rings.**

Definition 2.11. An $(\mathbf{R}^{\geqslant 0})$-*graded ring* is a ring A equipped with a decomposition $A = \bigoplus_{\lambda\in\mathbf{R}^{\geqslant 0}} A_\lambda$ as a direct sum of abelian groups such that $A_\lambda A_\mu \subset A_{\lambda+\mu}$ for all $\lambda, \mu \in \mathbf{R}^{\geqslant 0}$.

[1] Recall $\inf \emptyset = \infty$.

Definition 2.12. If (R, v) is a filtered ring let $R_{\lambda^+} = \{r \in R \mid v(r) > \lambda\}$ and $\mathrm{gr}_\lambda R = R_\lambda / R_{\lambda^+}$ for $\lambda \geqslant 0$. The *associated graded ring* is the graded ring

$$\mathrm{gr}\, R = \bigoplus_{\lambda \in \mathbb{R}^{\geqslant 0}} \mathrm{gr}_\lambda R$$

with multiplication the bilinear extension of

$$\mathrm{gr}_\lambda R \times \mathrm{gr}_\mu R \to \mathrm{gr}_{\lambda+\mu} R;$$

$$(r + R_{\lambda^+})(s + R_{\mu+}) = rs + R_{(\lambda+\mu)^+}.$$

Lecture 3

Example 2.13. If $\mathbf{Z}$ is given the p-adic filtration then

$$\mathrm{gr}\, \mathbf{Z} = \oplus_{i=0}^{\infty} \mathbf{F}_p t^i = \mathbf{F}_p[t]$$

where t^i has degree i.

Proof. $(\mathbf{Z})_\lambda = (p^n)$ when $n - 1 < \lambda \leqslant n$ so $\mathrm{gr}_\lambda \mathbf{Z} = 0$ for $\lambda \notin \mathbf{Z}^{\geqslant 0}$ and $\mathrm{gr}_n \mathbf{Z} = (p^n)/(p^{n+1})$ for $n \in \mathbf{Z}^{\geqslant 0}$. Moreover if $t = p + (p)^2 \in (\mathrm{gr}\, \mathbf{Z})_{1^+}$ then $t^n = p^n + (\mathbf{Z})_{n^+} \in \mathrm{gr}_n \mathbf{Z}$ is non-zero. □

Definition 2.14. If $A = \oplus_{\lambda \in \mathbf{R}^{\geqslant 0}} A_\lambda$ and $B = \oplus_{\lambda \in \mathbf{R}^{\geqslant 0}} B_\lambda$ are graded rings. Then $f \colon A \to B$ is a *graded ring homomorphism* if it is a ring homomorphism such that $f(A_\lambda) \subset B_\lambda$ for all $\lambda \in \mathbf{R}^{\geqslant 0}$.

Exercise 2.15. Prove that for any filtered ring (R, v) there is an isomorphism of graded rings $\mathrm{gr}\, R \cong \mathrm{gr}\, \widehat{R}$. In particular $\mathrm{gr}\, \mathbf{Z}_p \cong \mathbf{F}_p[t]$.

Exercise 2.16. Show that if (R, v) is a filtered ring and $M_n(R)$ is given the filtration v_n given in Exercise 2.4 then there is an isomorphism of graded rings $\mathrm{gr}\, M_n(R) \cong M_n(\mathrm{gr}\, R)$.

Notation 2.17. If (R, v) is a filtered ring and $r \in v^{-1}(\mathbf{R}^{\geqslant 0})$ then we'll write $\sigma(r) = r + R_{v(r)^+}$. If $v(r) = \infty$ then we write $\sigma(r) = 0$. We call $\sigma(r)$ the *symbol* of r in $\mathrm{gr}\, R$.

2.4. **Filtrations on groups.**

Definition 2.18. A *filtration* on a group G is a function $\omega \colon G \to \mathbf{R}^{>0} \cup \{\infty\}$ such that, for all $x, y \in G$,

(a) $\omega(xy^{-1}) \geqslant \min(\omega(x), \omega(y))$;
(b) $\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y)$.

A *filtered group* is a group G equipped with a filtration ω.

Lemma 2.19. *Suppose that (G, ω) is a filtered group. Then*

(i) $\omega(e_G) = \infty$*; and for all* $x, y \in G$
(ii) $\omega(x) = \omega(x^{-1})$*;*
(iii) $\omega(y^{-1}xy) = \omega(x)$*;*
(iv) $\omega(xy) = \min(\omega(x), \omega(y))$ *whenever* $\omega(x) \neq \omega(y)$*;*
(v) if H is a subgroup of G then ω restricts to a filtration on H.

Proof. (i) Take $x = y = e_G$ in Definition 2.18(b) to get $\omega(e_G) \geqslant 2\omega(e_G) > 0$. So $\omega(e_G) = \infty$.

(ii) Take $x = e_G$ in Definition 2.18(a) to get $\omega(y^{-1}) \geqslant \min(\omega(e_G), \omega(y)) = \omega(y)$ and use symmetry.

(iii)

$$\begin{aligned}\omega(y^{-1}xy) &= \omega(x(x^{-1}y^{-1}xy)) \\ &\geqslant \min(\omega(x^{-1}), \omega(x^{-1}y^{-1}xy) \text{ (Definition 2.18(a))} \\ &\geqslant \min(\omega(x), \omega(x) + \omega(y)) = \omega(x). \text{ (Definition 2.18(b) and part (ii))}\end{aligned}$$

Thus $\omega(ghg^{-1}) \geqslant \omega(h)$ for all $g, h \in G$. So writing $x = y^{-1}(yxy^{-1})y$ we see $\omega(x) \geqslant \omega(y^{-1}xy)$.

(iv) WLOG $\omega(x) > \omega(y)$. Then

$$\omega(y) \geqslant \min(\omega(x^{-1}), \omega(x^{-1}y)) \geqslant \min(\omega(x), \omega(y)) = \omega(y).$$

(v) is immediate. □

Definition 2.20. As for ring filtrations we say that a filtration ω is *separated* if $\omega^{-1}(\infty) = \{e_G\}$.

Proposition 2.21. *Suppose that (R, v) is a filtered ring. Let*

$$G = \{x \in R \mid x \text{ is a unit and } v(x-1) > 0\}.$$

Then G is a group under the ring multiplication and

$$\omega \colon G \to \mathbf{R}^{>0} \cup \{\infty\}; \qquad \omega(x) = v(x-1)$$

defines a filtration on G. Moreover ω is separated if v is separated.

Proof. First $v(1-1) = v(0) = \infty$ so $1 \in G$.

Next if $x, y \in G$ then as

$$xy^{-1} - 1 = (x-1) - (y-1) - (xy^{-1} - 1)(y-1)$$

we see that

$$v(xy^{-1}-1) \geqslant \min(v(x-1), v(y-1), v(xy^{-1}-1)+v(y-1)) = \min(v(x-1), v(y-1))$$

so $xy^{-1} \in G$ and $\omega(xy^{-1}) \geqslant \min(\omega(x), \omega(y))$. Similarly

$$x^{-1}y^{-1}xy - 1 = x^{-1}y^{-1}((x-1)(y-1) - (y-1)(x-1))$$

gives $\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y)$. The last part is immediate. □

Example 2.22. $M_n(\mathbf{Z}_p)$ has a separated filtration on it induced from the p-adic filtration on $\mathbf{Z}_p$ as in Exercise 2.4. This induces a separated filtration on

$$GL_n^1(\mathbf{Z}_p) = \ker(GL_n(\mathbf{Z}_p) \to GL_n(\mathbf{F}_p))$$

via Proposition 2.21.

Notation 2.23. Given a filtered group (G, ω) and $\lambda > 0$ we write

$$\begin{aligned}G_\lambda &= \{x \in G \mid \omega(x) \geqslant \lambda\} \text{ and} \\ G_{\lambda^+} &= \{x \in G \mid \omega(x) > \lambda\}.\end{aligned}$$

Lemma 2.24. *For any filtered group (G, ω) and $\lambda > 0$, G_λ and G_{λ^+} are normal subgroups of G. Moreover G_λ/G_{λ^+} is contained in the centre of G/G_{λ^+}.*

Proof. The statements that G_λ and G_{λ^+} are normal subgroups of G follow immediately from Exercise 2.19. For the last part we see that for any $x, y \in G$

$$\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y) > \omega(x)$$

so $x^{-1}y^{-1}xy \in G_{\omega(x)^+}$ and $xyG_{\omega(x)^+} = yxG_{\omega(x)^+}$ ie $xG_{\omega(x)^+}$ is central. □

It is also straightforward to see that

(a) $G = \bigcup_{\lambda>0} G_\lambda$
(b) $x^{-1}y^{-1}xy \in G_{\lambda+\mu}$ for all $x \in G_\lambda$ and $y \in G_\mu$ with $\lambda, \mu \in \mathbf{R}^{>0}$ and
(c) $G_\lambda = \bigcap_{\mu<\lambda} G_\mu$ for all $\lambda \in \mathbf{R}^{>0}$.

Moreover any family $(G_\lambda)_{\lambda\in\mathbf{R}^{>0}}$ of subgroups of G satisfying properties (a)-(c) determines a filtration on G via $\omega(x) = \sup\{\lambda \mid x \in G_\lambda\}$.[2]

Lecture 4

Aside on group commutators. We recall some general group theoretic facts. For x, y in a group we write $x^y = y^{-1}xy$ for the conjugate of x by y (on the right) and $(x, y) = x^{-1}y^{-1}xy = x^{-1}x^y$ for the commutator of x and y.

Exercise 2.25. Suppose that G is a group and $x, y, z \in G$.

(1) $(xy, z) = (x, z)^y(y, z)$;
(2) $(x, yz) = (x, z)(x, y)^z$;
(3) $(x^y, (y, z))(y^z, (z, x))(z^x, (x, y)) = e_G$.

Notation 2.26. If G is a group and H and K are subgroups of G we write (H, K) to denote the subgroup of G generated by commutators (h, k) with $h \in H$ and $k \in K$.

Definition 2.27. The *lower central series* for G is defined recursively: $\gamma_1(G) = G$; $\gamma_n(G) = (G, \gamma_{n-1}(G))$ for $n \geqslant 2$. We say that G is *nilpotent* if there is some $n \geqslant 1$ such that $\gamma_n(G) = \{e_G\}$.

Exercise 2.28. Show that $\omega\colon G \to \mathbf{R}^{>0}\cup\{\infty\}$ given by $\omega(x) = \sup\{n \mid x \in \gamma_n(G)\}$ defines a filtration on G. Show moreover that $\gamma_{n+1}(G)$ is the smallest normal subgroup of G such that $\gamma_n(G)/\gamma_{n+1}(G)$ is contained in the centre of $G/\gamma_{n+1}(G)$ for all $n \geqslant 1$.

Theorem 2.29. *[Hall–Petrescu Formula; P. Hall 1932, Lazard 1953] Let G be a group, $x, y \in G$ and $n \in \mathbf{N}$. Then*

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \cdots c_{n-1}^n c_n$$

for some $c_i \in \gamma_i(G)$

Exercise 2.30. Verify this for $n \leqslant 4$.

[2]Something similar is true for the family G_{λ^+}.

2.5. **The associated graded Lie algebra of a filtered group.** In this section we suppose that G is a group equipped with a filtration ω.

Definition 2.31. The *associated graded group* of G

$$\operatorname{gr} G = \bigoplus_{\lambda \in \mathbf{R}^{>0}} G_\lambda / G_{\lambda^+}.$$

We will write $\operatorname{gr}_\lambda G$ for the λ-component G_λ/G_{λ^+} of $\operatorname{gr} G$.

Notation 2.32. As for associated graded rings for $g \in \omega^{-1}(\mathbf{R}^{>0})$, we write $\sigma(g) = gG_{\omega(g)^+}$.

We note that by Lemma 2.24 each component $\operatorname{gr}_\lambda G$ is an abelian group. Thus we may view itself $\operatorname{gr} G$ as an abelian group. The goal of this section is to explain how to give $\operatorname{gr} G$ the structure of a $\mathbf{Z}$-Lie algebra in a way that only depends on the pair (G, ω). Moreover the Lie bracket

$$[-,-]\colon \operatorname{gr} G \times \operatorname{gr} G \to \operatorname{gr} G$$

will respect the grading in the sense that $[a, b] \in \operatorname{gr}_{\lambda+\mu} G$ whenever $a \in \operatorname{gr}_\lambda G$ and $b \in \operatorname{gr}_\mu G$. We will say that $\operatorname{gr} G$ is a graded Lie algebra.[3]

Definition 2.33. For any $\lambda, \mu > 0$ let

$$[-,-]\colon \operatorname{gr}_\lambda G \times \operatorname{gr}_\mu G \to \operatorname{gr}_{\lambda+\mu} G$$

be given by

$$[xG_{\lambda^+}, yG_{\mu^+}] = (x, y)G_{\lambda+\mu^+}.$$

Proposition 2.34. *The* $\mathbf{Z}$*-bilinear extension of* $[-,-]$ *to* $\operatorname{gr} G$ *makes* $\operatorname{gr} G$ *into an* $\mathbf{Z}$*-Lie algebra.*

Proof. First we check that $[-,-]$ is well-defined on $\operatorname{gr} G$. Suppose that xG_{λ^+}, yG_{μ^+} are homogeneous elements of $\operatorname{gr} G$. Then $(x, y) \in G_{\lambda+\mu}$ by condition (b) for a filtration on a group. Moreover if $l \in G_\lambda$ and $m \in G_\mu$ then

$$(xl, y) = (x, y)^l (l, y) \in (x, y)(l, y)G_{\lambda+\mu^+}$$

and

$$(x, ym) = (x, m)(x, y)^m \in (x, y)(x, m)G_{\lambda+\mu^+}$$

by Exercise 2.25 and the centrality of $G_{\lambda+\mu}/G_{\lambda+\mu^+}$ in $G/G_{\lambda+\mu^+}$ (Lemma 2.24). Moreover $(l, y) \in G_{\lambda+\mu^+}$ (resp. $(x, m) \in G_{\lambda+\mu^+}$) if $l \in G_{\lambda^+}$ (resp. $m \in G_{\mu^+}$).

Thus each map $\operatorname{gr}_\lambda G \times \operatorname{gr}_\mu G \to \operatorname{gr}_{\lambda+\mu} G$ is a well defined $\mathbf{Z}$-bilinear map.

Next we see that

$$[\sigma(x), \sigma(x)] = 0$$

since $(x, x) = e_G$ and

$$[\sigma(x), \sigma(y)] = -[\sigma(y), \sigma(x)]$$

since $(x, y)^{-1} = (y, x)$. Thus $[-,-]$ extends to an alternating $\mathbf{Z}$-bilinear form on $\operatorname{gr} G$.

Suppose now that additionally $z \in G$. Then the Jacobi identity

$$[\sigma(x), [\sigma(y), \sigma(z)]] + [\sigma(y), [\sigma(z), \sigma(x)]] + [\sigma(z), [\sigma(x), \sigma(y)]] = 0$$

holds on homogeneous elements by Exercise 2.25(3) and Lemma 2.19 and thus by multilinearity on the whole of $\operatorname{gr} G$. □

[3]Warning: this isn't always what is meant by this term!

Exercise 2.35. Let R be a commutative ring and let G denote the group of 3×3 upper-unitriangular matrices with entries in R

$$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in R \right\}$$

equipped with the filtration coming from the lower central series as in Exercise 2.28. Show that G is nilpotent and $\operatorname{gr} G$ is an R-Lie algebra $RX \oplus RY \oplus RZ$ (free of rank 3 as an R-module) with

$$\operatorname{gr}_1 G = RX \oplus RY \text{ and } \operatorname{gr}_2 G = RZ,$$

$[X, Y] = Z$ and $[X, Z] = [Y, Z] = 0$.

Exercise 2.36. Suppose now that $R = \mathbf{Z}_p$ and

$$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in pR \right\}$$

with the filtration ω induced by restricting the one in Example 2.22.

Show that $\operatorname{gr} G = \oplus_{n \in \mathbf{N}} \operatorname{gr}_n G$ is an $\operatorname{gr} \mathbf{Z}_p = \mathbf{F}_p[t]$-Lie algebra,

$$\operatorname{gr}_n G = \mathbf{F}_p t^n X \oplus \mathbf{F}_p t^n Y \oplus \mathbf{F}_p t^n Z \text{ for } n \geqslant 1$$

with tX, tY and tZ free generators all of degree 1, $[tX, tY] = t^2 Z$ and $[tX, tZ] = [tY, tZ] = 0$.

Lecture 5

3. p-valued groups

3.1. **Definitions and basic properties.** We will be most interested in special filtrations of groups called p-valuations. The reason for this will become apparent later.

Definition 3.1. Let p be a prime. A separated filtration ω on a group G is called a *p-valuation* if for all $g \in G$

(a) $\omega(g) > \frac{1}{p-1}$ and
(b) $\omega(g^p) = \omega(g) + 1$.

Lemma 3.2. *If G has a p-valuation ω then for all $\lambda > 0$*

(i) $G_\lambda / G_{\lambda^+}$ has exponent p;
(ii) G/G_λ is a p-group and
(iii) G is torsion-free.

Proof. (i) Suppose $gG_{\lambda^+} \in G_\lambda / G_{\lambda^+}$. Then $\omega(g) \geqslant \lambda$ so $\omega(g^p) \geqslant \lambda + 1 > \lambda$ and so $(gG_{\lambda^+})^p = e$.

(ii) Choose $n \in \mathbf{N}$ such that $n > \lambda$. For any $g \in G$, $\omega(g^{p^n}) = \omega(g) + n > \lambda$. So $(gG_\lambda)^{p^n} = 1$.

(iii) Suppose for contradiction that $g \in G \backslash \{e\}$ and $g^n = e$. Write $n = p^a m$ for $(m, p) = 1$. Then $\omega(g^{p^a}) = \omega(g) + a < \infty$. So we may choose $\mu > \omega(g^{p^a})$

Now $(g^{p^a})^m = e$ so, as G/G_μ is a p-group and $(m, p) = 1$, we see that $g^{p^a} G_\mu = G_\mu$ ie $g^{p^a} \in G_\mu$ and $\omega(g^{p^a}) \geqslant \mu$ contrary to the choice of μ. □

Exercise 3.3. Show that if ω is a p-valuation on G and $g \in \gamma_n(G)$ then $\omega(g) > n/(p-1)$. Show moreover that if $g \in \gamma_n(< x, y >)$ and $n \geqslant 2$ then $\omega(g) > \frac{n-1}{p-1} + \max\{\omega(x), \omega(y)\}$.

Proposition 3.4. *Suppose that (R, v) is a separated filtered ring such that $v(pr) = v(r)+1$ for all $r \in R$ and that (G, ω) is obtained from (R, v) as in Proposition 2.21. Then ω restricts to a p-valuation on $G_{1/(p-1)^+}$.*

Proof. That ω restricts to a separated filtration on $G_{1/(p-1)^+}$ satisfying condition (a) for a p-valuation is immediate from Proposition 2.21.

Suppose that $x \in G_{1/(p-1)^+}$. We must show $\omega(x^p) = \omega(x) + 1$. Now

$$x^p - 1 = (1 + (x-1))^p - 1 = \sum_{i=1}^{p} \binom{p}{i} (x-1)^i$$

But $v(p(x-1)) = \omega(x) + 1$ and for $2 \leqslant i \leqslant p-1$

$$v\left(\binom{p}{i}(x-1)^i\right) = 1 + v\left(p^{-1}\binom{p}{i}(x-1)^i\right) \geqslant 1 + i\omega(x) > \omega(x) + 1.$$

Finally $v((x-1)^p) \geqslant p\omega(x) > \omega(x) + 1$.[4] Thus $\omega(x^p) = v(x^p - 1) = \omega(x) + 1$ as required. □

Example 3.5. Recall the filtration on $GL_n^1(\mathbf{Z}_p)$ as in Example 2.22. For $p > 2$,

$$GL_n^1(\mathbf{Z}_p)_{1/(p-1)^+} = GL_n^1(\mathbf{Z}_p)$$

so this group has a p-valuation on it. For $p = 2$

$$GL_n^2(\mathbf{Z}_p) = \ker\left(GL_n(\mathbf{Z}_p) \to GL_n(\mathbf{Z}/p^2\mathbf{Z})\right)$$

has a p-valuation on it.

Since it is easy to verify that the restriction of a p-valuation to a subgroup is a p-valuation on the subgroup it follows that any subgroup of $GL_n^1(\mathbf{Z}_p)$ can be given a p-valuation for p odd and likewise any subgroup of $GL_n^2(\mathbf{Z}_p)$ when p is even. In particular in Exercise 2.36 the given ω is a p-valuation on the given group G.

3.2. **Finite rank p-valued groups.**

Lemma 3.6. *Suppose that G is a group with a p-valuation ω. Let $x, y \in G$, $n \in \mathbf{N}$ and $\omega(y) \geqslant \omega(x)$, then the following hold:*
(a) $\omega\left(y^{-p}x^{-p}(xy)^p\right) > \omega(y) + 1$; and
(b) $\omega(x^{-p^n}y^{p^n}) = \omega(x^{-1}y) + n$ for all $n \geqslant 0$.

Proof. (a) By the Hall–Petrescu formula (Theorem 2.29), there are $c_i \in \gamma_i(< x, y >)$ for $2 \leqslant i \leqslant p$ such that

$$y^{-p}x^{-p}(xy)^p = c_2^{\binom{p}{2}} \cdots c_{p-1}^p c_p.$$

Now by Exercise 3.3, for each $2 \leqslant i \leqslant p-1$

$$\omega(c_i) > \omega(y) \text{ and}$$
$$\omega(c_p) > \omega(y) + 1.$$

[4] this last inequality is equivalent to $\omega(x) > \frac{1}{p-1}$

Thus

$$\omega\left(c_2^{\binom{p}{2}}\cdots c_{p-1}^p c_p\right) > \omega(y)+1$$

since $v_p(\binom{p}{i}) \geqslant 1$ for $2 \leqslant i < p$.

(b) An inductive argument reduces us to the case $n=1$. Note that

$$\omega(x^{-1}y) \geqslant \omega(x)$$

so we may apply (a) to the pair $(x, x^{-1}y)$ and see that

$$\omega((x^{-1}y)^{-p}x^{-p}y^p) > \omega(x^{-1}y)+1 = \omega\left((x^{-1}y)^p\right).$$

So by Lemma 2.19(iv) $\omega(x^{-1}y)+1 = \omega((x^{-1}y)^p) = \omega(x^{-p}y^p)$ □

Proposition 3.7. *If (G,ω) is a p-valued group there is a family of well-defined group homomorphisms*

$$P_\lambda\colon \operatorname{gr}_\lambda G \to \operatorname{gr}_{\lambda+1} G$$

given by $P_\lambda(xG_{\lambda^+}) = x^pG_{\lambda+1^+}$.

Moreover if $a \in \operatorname{gr}_\lambda G$ and $b \in \operatorname{gr}_\mu G$ then $[P_\lambda a, b] = P_{\lambda+\mu}[a,b]$.

Proof. If $x, y \in G_\lambda$ then $x^p, y^p, (xy)^p \in G_{\lambda+1}$ and $(xy)^pG_{\lambda+1^+} = x^py^pG_{\lambda+1^+}$ by Lemma 3.6(a). Moreover if $y \in G_{\lambda^+}$ then $y^p \in G_{\lambda+1^+}$. Thus each P_λ is a group homomorphism.

Let $a = xG_{\lambda^+} \neq 0$ and $b = yG_{\mu^+}$ and set $\nu = \lambda+\mu+1$ then

$$[Pa, b] = (x^p, y)G_{\nu^+}$$

and

$$P[a,b] = (x,y)^pG_{\nu^+}.$$

Now $(x^p,y) = x^{-p}(x^p)^y = x^{-p}(x^y)^p$. So we must show

$$(x,y)^{-p}(x^{-1})^p(x^y)^p \in G_\nu^+.$$

Now $\omega(x) = \omega(x^y) = \lambda$ and $\omega((x,y)) \geqslant \lambda+\mu > \omega(x)$. Since $x(x,y) = x^y$ we may use Lemma 3.6(a) this time applied to the pair $(x,(x,y))$ to deduce the result. □

We will write P for the degree 1 operator on $\operatorname{gr} G$ given by $\oplus P_\lambda$. Recall that $\mathbf{F}_p[t]$ can be viewed as the graded ring $\operatorname{gr}\mathbf{Z}_p$ where $\mathbf{Z}_p$ is given the p-adic filtration so that t has degree 1.

Lecture 6

Corollary 3.8. *If (G,ω) is a p-valued group then $\operatorname{gr} G$ is naturally a graded $\mathbf{F}_p[t]$-Lie algebra where t acts by P and has degree 1.*

Proof. $\operatorname{gr} G$ is a graded $\mathbf{Z}$-Lie algebra by Proposition 2.34. By Lemma 3.2 it has exponent p as an abelian group so is a graded $\mathbf{F}_p$-Lie algebra. Proposition 3.7 shows that defining $ta = P(a)$ for $a \in \operatorname{gr} G$ is a degree 1 operator such that $t[a,b] = [ta,b]$ for all $a, b \in \operatorname{gr} G$. Thus $p(t)[a,b] = [p(t)a,b]$ for all $p(t) \in \mathbf{F}_p[t]$ and $a, b \in \operatorname{gr} G$. Since $[-,-]$ is alternating it follows that it is $\mathbf{F}_p[t]$-bilinear. □

Lemma 3.9. *$\operatorname{gr} G$ is torsion-free as an $\mathbf{F}_p[t]$-module.*

Proof. Suppose that $0 \neq q(t) \in \mathbf{F}_p[t]$ and $0 \neq a \in \operatorname{gr} G$. We wish to show $qa \neq 0$.

We can write $q(t) = \sum_{i=0}^{m} q_i t^i$ with $q_i \in \mathbf{F}_p$ and $q_m \neq 0$ and $a = \sum_\lambda a_\lambda$ a finite sum with $a_\lambda \in \operatorname{gr}_\lambda G$. If μ is largest with $a_\mu \neq 0$ then the degree $\mu + m$ part of qa is $q_m t^m a_\mu$. Since $\operatorname{gr} G$ is a p-group and $q_m \in \mathbf{F}_p \backslash 0$, it thus suffices to show that $t^m a_\mu \neq 0$ ie that t acts injectively on $\operatorname{gr} G$.[5] Now if $a_\mu = xG_{\mu^+}$ then $\omega(x) = \mu$ and $ta_\mu = Pa_\mu = x^p G_{\mu+1^+}$. But $\omega(x^p) = \omega(x) + 1$ since ω is a p-valuation. Thus $Pa_\mu \neq 0$ as required. □

Definition 3.10. We say that a p-valued group (G, ω) has *finite rank* if $\operatorname{gr} G$ is finitely generated as an $\mathbf{F}_p[t]$-module. The *rank* of (G, ω) is then the minimal number of generators of $\operatorname{gr} G$ over $\mathbf{F}_p[t]$

Example 3.11. The computation in Example 2.36 shows that the pair (G, ω) there has rank 3.

Note that the structure theorem for modules over a principal ideal domain together with Lemma 3.9 gives that if (G, ω) is finite rank then $\operatorname{gr} G$ is in fact a free $\mathbf{F}_p[t]$-module of the same rank.

Exercise 3.12. Show that if (G, ω) has finite rank then $\operatorname{gr} G$ is free as a *graded* $\mathbf{F}_p[t]$-module. That is there are $\lambda_1, \dots, \lambda_n > 1/(p-1)$ and $x_i \in G_{\lambda_i}$ such that

$$\operatorname{gr} G = \oplus_{i=1}^{n} \mathbf{F}_p[t] x_i G_{\lambda_i^+}.$$

Lemma 3.13. *Suppose that (G, ω) is a finite rank p-valued group and $g_1, \dots, g_d \in G$ such that $\{\sigma(g_1), \dots, \sigma(g_d)\}$ spans $\operatorname{gr} G$ as an $\mathbf{F}_p[t]$-module.*

(a) For all $x \in G \backslash \{e\}$ there are integers $n_1, \dots, n_d$ such that $\omega(g_i) + v_p(n_i) = \omega(x)$ whenever $n_i \neq 0$ and $\sigma(x) = \sigma(g_1^{n_1} \cdots g_d^{n_d})$.

(b) $\omega(G \backslash \{e\})$ is a discrete subset of $\mathbf{R}$.

Proof. (a) Let $x \in G \backslash \{e\}$ so that $\sigma(x) \in \operatorname{gr} G \backslash \{0\}$. There are homogeneous elements $u_1, \dots, u_d \in \mathbf{F}_p[t]$ not all zero such that $\sigma(x) = \sum_{i=1}^{d} u_i \sigma(g_i)$. Moreover when $u_i \neq 0$ then we may assume $\deg u_i + \omega(g_i) = \omega(x)$. For each i we may choose $n_i \in \mathbf{Z}$ such that $u_i = \sigma(n_i)$ and then, whenever $n_i \neq 0$,

$$\omega(g_i^{n_i}) = \omega(g_i) + \deg(u_i) = \omega(x).$$

Moreover

$$\sigma(g_1^{n_1} \cdots g_d^{n_d}) = \sum_i \sigma(g_i^{n_i}) = \sum_i u_i \sigma(g_i) = \sigma(x).$$

(b) It follows from (a) that for $x \in G \backslash \{e\}$, $\omega(x) \in (\omega(g_1) + \mathbf{N}) \cup \cdots \cup (\omega(g_d) + \mathbf{N})$ which is a discrete subset of $\mathbf{R}$. □

Notation 3.14. If (R, v) is a complete filtered ring and $(r_n)_{n \geqslant 0}$ is a sequence in R such that $v(r_n) \to \infty$ as $n \to \infty$ then identifying R with $\widehat{R}$ we write

$$\sum_{n \geqslant 0} r_n = \left(\sum_{n=0}^{m_\lambda} r_n + R_\lambda \right)_{\lambda \geqslant 0}$$

where the m_λ are chosen so that $v(r_n) > \lambda$ for all $n > m_\lambda$.

[5] Note that the argument so far works for any graded $\mathbf{F}_p[t]$-module.

Exercise 3.15. Show that if r_n and s_n are two such sequences then so are (r_n+s_n) and $(\sum_{i+j=n} s_i r_j)$. Moreover

$$\left(\sum_{n\geqslant 0} r_n\right) + \left(\sum_{n\geqslant 0} s_n\right) = \sum_{n\geqslant 0}(r_n + s_n)$$

and

$$\left(\sum_{n\geqslant 0} r_n\right)\left(\sum_{n\geqslant 0} s_n\right) = \sum_{n\geqslant 0}\left(\sum_{i+j=n} r_i s_j\right).$$

Example 3.16. Suppose that $p > 2$ and $G = GL_n^1(\mathbf{Z}_p)$ with the p-valuation ω given in Example 2.22. Note that ω in $\mathbf{N}$-valued in this case and thus $\operatorname{gr} G$ is $\mathbb{N}$-graded. Moreover for each $m \in \mathbb{N}$

$$G_m = \{g \in G \mid \omega(g) \geqslant m\} = \{A \in M_n(\mathbf{Z}_p) \mid v(A-I) \geqslant m\} = I + p^m M_n(\mathbf{Z}_p)$$

since $(I + p^m A) = \sum_{i\geqslant 0}(-p^m A)^i$. Note moreover that if $E \in M_n(\mathbf{Z}_p)$

$$(I + p^m A + p^{m+1}E)(I + p^m A)^{-1} = I + p^{m+1}E'$$

for some $E' \in M_n(\mathbf{Z}_p)$ ie if $g, g' \in G_m$ are congruent as matrices mod p^{m+1} then $gG_{m+1} = g'G_{m+1}$. Thus we may consider the surjective map

$$\phi_m \colon p^m M_n(\mathbf{Z}_p) \to \operatorname{gr}_m G$$

such that $\phi_m(p^m A) = (1 + p^m A)G_{m+1}$. Since

$$(1+p^m A)(1+p^m B)G_{m+1} = (1+p^m(A+B)+p^{2m}AB)G_{m+1} = (1+p^m(A+B))G_{m+1}$$

we see that ϕ_m is a group homomorphism with kernel $p^{m+1}M_n(\mathbf{Z}_p)$. Thus $\phi = \oplus\phi_m$ defines an group isomorphism

$$\oplus_{m\geqslant 1} p^m M_n(\mathbf{Z}_p)/p^{m+1}M_n(\mathbf{Z}_p) \to \operatorname{gr} G.$$

Now the map $p^m M_n(\mathbf{Z}_p) \to M_n(\mathbf{F}_p)$ given by $p^m A \mapsto A + pM_n(\mathbf{F}_p)$ is a surjective group homomorphism with kernel $p^{m+1}M_n(\mathbf{Z}_p)$. So we obtain an isomorphism of $\mathbb{N}$-graded $\mathbf{F}_p$-spaces

$$\theta \colon tM_n(\mathbf{F}_p[t]) \to \operatorname{gr} G$$

given by linear extension of $\theta(t^m\overline{A}) = (I + p^m A)G_{m+1}$ where $A \in M_n(\mathbf{Z}_p)$ is any lift of $\overline{A} \in M_n(\mathbf{F}_p)$.

We claim that θ is even as isomorphism of $\mathbf{F}_p[t]$-Lie algebras where the Lie bracket on $tM_n(\mathbf{F}_p[t])$ is given by $[X, Y] = XY - YX$.

Lecture 7

First we note that, for $m \geqslant 1$ and $A \in M_n(\mathbf{Z}_p)$,

$$\begin{aligned} t\theta(t^m\overline{A}) &= t \cdot (I + p^m A)G_{m+1} = (I + p^m A)^p G_{m+2} \\ &= (I + p^{m+1}A)G_{m+2} = \theta(t^{m+1}\overline{A}) \end{aligned}$$

so θ is $\mathbf{F}_p[t]$-linear.

Next we prove that

$$\theta([t^m\overline{A}, t^l\overline{B}]) = [\theta(t^m\overline{A}), \theta(t^l\overline{B})]$$

for $l, m \geqslant 1$ and $\overline{A}, \overline{B} \in M_n(\mathbf{F}_p)$. By the last calculation it suffices to consider the case $m = l = 1$. That is

$$\begin{aligned}
[\theta(t\overline{A}), \theta(t\overline{B})] &= (1+pA)^{-1}(1+pB)^{-1}(1+pA)(1+pB)G_3 \\
&= (1-pA+p^2A^2)(1-pB+p^2B^2)(1+pA)(1+pB)G_3 \\
&= \left(1-p(A+B)+p^2(A^2+AB+B^2)\right)\left(1+p(A+B)+p^2AB)\right)G_3 \\
&= (1+p(A+B-A-B)+p^2(A^2+2AB+B^2-(A+B)^2)G_3 \\
&= (1+p^2(A^2+2AB+B^2-(A^2+AB+BA+B^2)))G_3 \\
&= (1+p^2(BA-AB))G_3 \\
&= \theta([t\overline{A}, t\overline{B}])
\end{aligned}$$

Thus we see that $\operatorname{gr} G \cong t\mathfrak{gl}_n(\mathbf{F}_p[t])$ has rank n^2 as an $\mathbf{F}_p[t]$-module.

Exercise 3.17. Show that if (G, ω) is a finite rank p-valued group and $H \leqslant G$ is a subgroup then $(H, \omega|_H)$ is a finite rank p-valued group.

3.3. **Complete p-valued groups.** As for filtered rings, we can define a topology on a filtered group.

Definition 3.18. If (G, ω) is a filtered group we give G a topology by declaring a subset open if and only if it is a union of cosets of the from gG_λ with $\lambda > 0$.

This makes G into a topological group; i.e. the multiplication map $G \times G \to G$; $(g, h) \mapsto gh$ and the inversion map $G \to G$; $g \mapsto g^{-1}$ are both continuous.[6]

We can also define the completion of a filtered group.

Definition 3.19. If (G, ω) is a filtered group then its *completion*

$$\widehat{G} = \varprojlim_{\lambda>0} G/G_\lambda = \{(g_\lambda G_\lambda)_{\lambda>0} \in \prod_{\lambda>0} G/G_\lambda \mid g_\lambda G_\mu = g_\mu G_\mu \text{ for all } \mu < \lambda\}.$$

We say that G is *complete* if the natural group homomorphism

$$G \to \widehat{G}; \quad g \mapsto (gG_\lambda)_{\lambda>0}$$

is an isomorphism.

Exercise 3.20.

(1) Show that $\widehat{G}$ has a separated filtration given by
$$\widehat{\omega}((g_\lambda G_\lambda)_{\lambda>0}) = \inf \omega(g_\lambda \mid g_\lambda \notin G_\lambda)$$
with respect to which it is complete.
(2) Show that the natural map $G \to \widehat{G}$ is injective if and only if ω is separated. Show that moreover that this map always induces a natural isomorphism $\operatorname{gr} G \to \operatorname{gr} \widehat{G}$.
(3) Show that if (R, v) is a complete filtered ring then the filtered group (G, ω) obtained as in Proposition 2.21 is complete.

Example 3.21. For any odd prime p if ω denotes the usual p-valutation on $GL_n^1(\mathbf{Z}_p)$ then $(GL_n^1(\mathbf{Z}_p), \omega)$ is a complete filtered group.

In the remainder of this section (G, ω) will be a complete p-valued group.

[6]Here $G \times G$ is given the product topology.

Lemma 3.22. *Suppose that $x \in G$ and $\lambda \in \mathbf{Z}_p$. There is a unique element $x^\lambda \in G$ such that for each $t > 0$, $x^\lambda G_t = x^{\lambda_t} G_t$ whenever $\lambda_t \in \mathbb{Z}$ and $v_p(\lambda - \lambda_t) \geqslant t$.*

Proof. Since G is complete with respect to the filtration, the natural map $G \to \varprojlim_t G/G_t$ is a bijection. Thus it suffices to show that there is a unique element $(x_t G_t)_{t>0}$ of $\varprojlim_t G/G_t$ such that $x_t G_t = x^{\lambda_t} G_t$ for any $\lambda_t \in \mathbf{Z}$ such that $v_p(\lambda - \lambda_t) \geqslant t$.

If $\lambda_t, \lambda_t' \in \mathbf{Z}$ such that $v_p(\lambda - \lambda_t) \geqslant t$ and $v_p(\lambda - \lambda_t') \geqslant t$, then $v_p(\lambda_t - \lambda_t') \geqslant t$ so $\omega(x^{\lambda_t - \lambda_t'}) \geqslant \omega(x) + t > t$. Thus $x^{\lambda_t} G_t = x^{\lambda_t'} G_t$ so the coset $x^{\lambda_t} G_t$ only depends on x, λ and t. That is there is a unique element $(x_t G_t)_{t>0}$ of $\prod_{t>0} G/G_t$ such that $x_t G_t = x^{\lambda_t} G_t$ for $\lambda_t \in \mathbf{Z}$ such that $v_p(\lambda - \lambda_t) \geqslant t$.

Now if $s > t$, $v_p(\lambda - \lambda_s) \geqslant s$ and $v_p(\lambda - \lambda_t) \geqslant t$ then $v_p(\lambda_s - \lambda_t) \geqslant t$ and $x^{\lambda_s} G_t = x^{\lambda_t} G_t$. Thus $(x_t G_t)_{t>0} \in \varprojlim_{t>0} G/G_t$ as required. □

Definition 3.23. When G is a complete p-valued group and $x \in G$ the function $\mathbf{Z}_p \to G$; $\lambda \mapsto x^\lambda$ given by Lemma 3.22 is called *p-adic exponentiation.*

Remark 3.24. The function $\lambda \mapsto x^\lambda$ is the unique continuous extension of the group homomorphism $\mathbf{Z} \to G$; $n \mapsto x^n$.

Exercise 3.25. For any $x \in G$ and $\lambda \in \mathbf{Z}_p$, $\omega(x^\lambda) = \omega(x) + v_p(\lambda)$ and that $\sigma(x^\lambda) = \sigma(\lambda) \cdot \sigma(x)$.

Given any d-tuple $(g_1, \ldots, g_d)$ in a complete p-valued group G we have a continuous map

$$\mathbf{Z}_p^d \to G$$

given by

$$(\lambda_1, \ldots, \lambda_d) \mapsto g_1^{\lambda_1} \cdots g_d^{\lambda_d}.$$

We will often write this as $\lambda \mapsto g^\lambda$ for $\lambda = (\lambda_1, \ldots, \lambda_d) \in \mathbf{Z}_p^d$. This map is a group homomorphism if and only if the g_i pairwise commute.

Proposition 3.26. *Suppose that $(g_1, \ldots, g_d)$ is a d-tuple of non-identity elements in G. The following are equivalent:*
(a) $\sigma(g_1), \ldots, \sigma(g_d) \in \operatorname{gr} G$ are linearly independent over $\mathbf{F}_p[t]$;
(b) $\omega(g^\lambda) = \min\{\omega(g_i) + v_p(\lambda_i)\}$ for any $\lambda \in \mathbf{Z}_p^d$;.
(c) $\omega((g^\mu)^{-1} g^\lambda) = \min\{\omega(g_i) + v_p(\lambda_i - \mu_i)\}$ whenever $\lambda, \mu \in \mathbf{Z}_p^d$.

Note that (c) implies (b) is immediate since (b) is the special case where $\mu = 0$. Moreover if (c) holds then the map $\lambda \mapsto g^\lambda$ is injective since $\omega((g^\mu)^{-1} g_\lambda) < \infty$ whenever $\lambda \neq \mu$.

Lecture 8

Proof of Proposition 3.26. Throughout this proof we will write $x_i = \sigma(g_i)$ for each $i = 1, \ldots, d$.

Suppose (a) holds and $\lambda \in \mathbf{Z}_p^d \backslash 0$. Then

$$\omega(g^\lambda) \geqslant \min\{\omega(g_i^{\lambda_i})\} = \min\{v_p(\lambda_i) + \omega(g_i)\} = s,$$

say, by Exercise 3.25.

Writing

$$u_i(t) = \begin{cases} \sigma(\lambda_i) \in \mathbf{F}_p[t] & \text{if } \omega(g_i^{\lambda_i}) = s \\ 0 & \text{otherwise,} \end{cases}$$

we see that at least one $u_i \neq 0$ and so

$$\sum_i u_i x_i = g^\lambda G_{s^+} \neq 0$$

since $u_i x_i = \sigma(g_i^{\lambda_i})$ when $u_i \neq 0$ and the x_i are linearly independent over $\mathbf{F}_p[t]$. Thus $\omega(g^\lambda) = s$ and (b) holds.

Next suppose that (b) holds and $\sum u_i x_i = 0$ is a linear relation. We wish to show that all the $u_i = 0$. If not, then $s = \min\{\omega(g_i) + \deg(u_i)\}$ is finite. Since the x_i are homogeneous we may assume that the u_i are also homogeneous and $\omega(g_i) + \deg u_i = s$ whenever the left-hand side is finite. Let

$$\lambda_i = \begin{cases} a_i p^{n_i} \in \mathbf{Z}_p \text{ when } u_i = \overline{a_i} t^{n_i} \neq 0 \\ 0 \qquad\qquad \text{otherwise.} \end{cases}$$

Then $\omega(g^\lambda) = s$ by assumption and

$$g^\lambda G_{s^+} = \sum u_i . x_i = 0$$

yielding the desired contradiction. Thus (a) holds.

Suppose that (b) holds and $\lambda, \mu \in \mathbf{Z}_p^d$. Then let $s = \min\{\omega(g_i) + v_p(\lambda_i - \mu_i)\}$. We compute

$$\begin{aligned} (g^\mu)^{-1} g^\lambda G_{s^+} &= g_d^{-\mu_d} \cdots g_1^{-\mu_1} g_1^{\lambda_1} \cdots g_d^{\lambda_d} G_{s^+} \\ &= g_d^{-\mu_d} \cdots g_2^{-\mu_2} g_1^{\lambda_1 - \mu_1} g_2^{\lambda_2} \cdots g_d^{\lambda_d} \\ &= g_1^{\lambda_1 - \mu_1} g_d^{\mu_d} \cdots g_2^{-\mu_2} g_2^{\lambda_2} \cdots g_d^{\lambda_d} G_{s^+} \end{aligned}$$

since $g_1^{\lambda_1 - \mu_1} \in G_s$ and G_s / G_{s^+} is central in G/G_{s^+} by Lemma 2.24. Continuing in this fashion we see that

$$(g^\mu)^{-1} g^\lambda G_{s^+} = g^{\lambda - \mu} G_{s^+}.$$

By assumption $\omega(g^{\lambda-\mu}) = s$ so (c) holds. □

Definition 3.27. A d-tuple $(g_1, \ldots, g_d)$ is called an *ordered basis* for (G, ω) if the map $\mathbf{Z}_p^d \to G$; $\lambda \mapsto g^\lambda$ is a bijection (and so a homeomorphism since it always continuous, $\mathbf{Z}_p^d$ is compact and G is Hausdorff) and

$$\omega(g^\lambda) = \min\{v_p(\lambda_i) + \omega(g_i)\} \text{ for all } \lambda \in \mathbf{Z}_p^d.$$

Theorem 3.28. *Let (G, ω) be a complete p-valued group and $\{g_1, \ldots, g_d\} \subset G$. The following are equivalent*

(a) $\{\sigma(g_1), \ldots, \sigma(g_d)\}$ is a free generating set for $\operatorname{gr} G$ over $\mathbf{F}_p[t]$.
(b) $(g_1, \ldots, g_d)$ is an ordered basis for G.

Proof. Suppose first that (b) holds. Then by Proposition 3.26, $\{\sigma(g_1), \ldots, \sigma(g_d)\}$ is linearly independent and we must show that it spans. Consider $1 \neq g^\lambda \in G$, let $s = \omega(g^\lambda) = \min\{\omega(g_i) + v_p(\lambda_i)\}$ and

$$\{i_1 < \cdots < i_r\} = \{1 \leqslant i \leqslant d \mid \omega(g_i^{\lambda_i}) = s\}.$$

Then

$$\sigma(g^\lambda) = g_{i_1}^{\lambda_{i_1}} \cdots g_{i_r}^{\lambda_{i_r}} G_{s^+} = \sum_{j=1}^{r} \sigma(\lambda_{i_j}) \sigma(g_{i_j}).$$

Thus every homogeneous element of $\operatorname{gr} G$ is in the span of $\{\sigma(g_1), \ldots, \sigma(g_d)\}$ are we're done.

Conversely suppose (a) holds. By Proposition 3.26 it suffices to show that every element of G is of the form g^λ with $\lambda \in \mathbf{Z}_p^d$. That is if X is the image of the map $\mathbf{Z}_p^d \to G$; $\lambda \mapsto g^\lambda$ then we must show $X = G$. Since $\mathbf{Z}_p^d$ is compact and G is Hausdorff, X is closed. Let $h \neq e_G$ be in G. It suffices to show that for all $s \in \mathbf{R}^{>0}$ there is $x_s \in X$ such that $x_s G_s = hG_s$.[7]

We suppose for contradiction that there is some $s \in \mathbf{R}^{>0}$ such that there is no $x \in X$ with $xG_s = hG_s$. Since $\omega(G\backslash\{1\})$ is a discrete subset of $\mathbb{R}$ (Lemma 3.13(b)) there is some $t < s$ maximal such that we can find $x = g^\lambda \in X$ with $xG_t = hG_t$. Since $xG_u \neq hG_u$ for all $u > t$, $\omega(x^{-1}h) = t$. Thus by Lemma 3.13(a) there is some $\mu \in \mathbb{Z}^d$ such that $g^\mu = x^{-1}h$ and $\omega(g_i^{\mu_i}) = t$ whenever $\mu_i \neq 0$. Since G_t/G_{t^+} is central in G/G_{t^+} (Lemma 2.24) we obtain

$$g^{\lambda+\mu}G_{t^+} = g^\lambda g^\mu G_{t^+} = hG_{t^+}.$$

But the discreteness of $\omega(G\backslash\{1\})$ gives that $G_{t^+} = G_s$ for some $s > t$ contradicting the maximality of t. □

Remark 3.29. It follows that any complete p-valued group of finite rank has an ordered basis and so is compact and Hausdorff.

Exercise 3.30. If (G, ω) is as in Exercise 2.36 then the triple of matrices

$$\left(x = \begin{pmatrix} 1 & p & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & p \\ 0 & 0 & 1 \end{pmatrix} \; z = \begin{pmatrix} 1 & 0 & p \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$$

form an ordered basis. Rewrite $(x^{\lambda_1}y^{\lambda_2}z^{\lambda_3}) \cdot (x^{\mu_1}y^{\mu_2}z^{\mu_3})$ as $x^{\nu_1}y^{\nu_2}z^{\nu_3}$ for general $\lambda, \mu \in \mathbf{Z}_p^3$.

Exercise 3.31. Find an ordered basis for $(GL_n^1(\mathbf{Z}_p), \omega)$ where p is an odd prime and ω is an in Example 2.22.

Lecture 9

Proposition 3.32. *Suppose that $(g_1, \dots, g_d)$ is an ordered basis for G and, for $s \in \mathbb{R}$, let $n_i = n_i(s) = \inf\{n \in \mathbf{N}_0\} \mid g_i^{p^n} \in G_s\}$.*

(a) $(g_1^{p^{n_1}}, \dots, g_d^{p^{n_d}})$ is an ordered basis for $(G_s, \omega|_{G_s})$.
(b) $G/G_s = \{g^\lambda G_s \mid 0 \leqslant \lambda_i < p^{n_i}$ for $i = 1 \dots d\}$.
(c) $|G/G_s| = p^{n_1+\dots+n_d}$.

Proof. (a) Since $(g_1, \dots, g_d)$ is an ordered basis we see that, for $\lambda \in \mathbf{Z}_p^d$, $g^\lambda \in G_s$ if and only if $\omega(g_i) + v_p(\lambda_i) \geqslant s$ for each $1 \leqslant i \leqslant d$. This is easily seen to be equivalent to $v_p(\lambda_i) \geqslant n_i$ (that is p^{n_i} divides λ_i) for each such i. Thus every element of G_s can be written uniquely as $(g^{p^n\mu})$ with $\mu \in \mathbf{Z}_p^d$ and $n = (n_1, \dots, n_d) \in \mathbf{N}_0^d$. Moreover

$$\omega(g^{p^n\mu}) = \min\{\omega(g_i^{p^{n_i}}) + v_p(\mu_i)\}$$

as required.

(b) & (c) The function $\{\lambda \in \mathbf{Z}^d \mid 0 \leqslant \lambda_i < p^{n_i}\} \to G/G_s$ sending λ to $g^\lambda G_s$ is a bijection since, for $\lambda, \mu \in \mathbf{Z}_p^d$, $\omega((g^\mu)^{-1}g^\lambda) = \min\{\omega(g_i) + v_p(\lambda_i - \mu_i)\}$ by Proposition 3.26, and for all $\mu \in \mathbf{Z}_p^d$ there is a unique $\lambda \in \mathbf{Z}^d$ with $0 \leqslant \lambda_i < p^{n_i}$ and $v_p(\lambda_i - \mu_i) + \omega(g_i) \geqslant s$ for all i. □

[7] Since then h is in the closure of the set $\{x_s \mid s \in \mathbf{R}^{>0}\}$.

Corollary 3.33. *Any complete p-valued group of finite rank is an inverse limit of finite p-groups.*

Exercise 3.34. If g is an element of an ordered basis for a complete p-valued group (G, ω) then g is not a p-th power in G.

4. Universal objects

We want to recall the construction of some universal objects. First we recall the definition of a category.

Definition 4.1. A *category* $\mathcal{C}$ is a collection of *objects* $\mathrm{Ob}(\mathcal{C})$ together with a set of *morphisms* $\mathrm{Hom}_{\mathcal{C}}(A, B)$ for each pair $A, B \in \mathrm{Ob}(\mathcal{C})$ which have a compostion rule

$$\mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$$

for every triple of objects A, B and C written

$$(f, g) \mapsto g \circ f$$

such that if $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ and $h \in \mathrm{Hom}_{\mathcal{C}}(C, D)$ then

$$h \circ (g \circ f) = (h \circ g) \circ f;^{8}$$

and for every object A there is an identity morphism $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ such that

$$\mathrm{id}_A \circ f = f \text{ and } g \circ \mathrm{id}_A = g$$

whenever these compositions make sense.

Examples 4.2.

(1) **Set** is the category whose objects are all sets and $\mathrm{Hom}_{\mathbf{Set}}(A, B)$ is the set of functions $A \to B$.
(2) **Grp** is the category whose objects are all groups and $\mathrm{Hom}_{\mathbf{Grp}}(G, H)$ is the set of group homomorphisms $G \to H$.
(3) **Mon** is the category whose objects are all monoids (ie sets M with an associative binary operation and an identity e_M) $\mathrm{Hom}_{\mathbf{Mon}}(M, N)$ is the set of monoid homomorphisms (ie functions $f\colon M \to N$ such that $f(ab) = f(a)f(b)$ for all $a, b \in M$ and $f(e_M) = e_N$.
(4) **FiltGrp** is the category whose objects are all filtered groups (G, ω_G) and whose morphisms are filtered group homomorphisms; ie a group homomorphism $f\colon G \to H$ such that $\omega_H(f(g)) \geqslant \omega_G(g)$ for all $g \in G$. **CFiltGrp** is the subcategory whose objects are the complete filtered groups and morphisms as in **FiltGrp**.
(5) Similary **FiltRing** and **CFiltRing** are the categories of filtered rings/complete filtered rings and filtered ring homomorphisms.

Suppose that k is a commutative ring

(6) $\mathbf{Mod}_k$ is the category whose objects are k-modules and whose morphisms are k-linear maps — if k is a field we write $\mathbf{Vect}_k$.
(7) $\mathbf{Comm}_k$ is the category whose objects are all commutative k-algebras and whose morphisms are all k-algebra homomorphisms.
(8) $\mathbf{Ass}_k$ is the category whose objects are all associative k-algebras and whose morphisms are all k-algebra homomorphisms.

[8] i.e. composition is associative

(9) $\mathbf{Lie}_k$ is the category whose objects all all k-Lie algebras and whose morphisms are all k-Lie algebra homomorphisms.
(10) There are graded versions $\mathbf{grMod}_k$, $\mathbf{grComm}_k$, $\mathbf{grAss}_k$ and $\mathbf{grLie}_k$ of $\mathbf{Mod}_k$, $\mathbf{Comm}_k$, $\mathbf{Ass}_k$ and $\mathbf{Lie}_k$.

Definition 4.3. Suppose that $\mathcal{C}$ and $\mathcal{D}$ are categories. A *functor* $F\colon \mathcal{C} \to \mathcal{D}$ is a rule that assigns

- an object $FC \in \mathrm{Ob}(\mathcal{D})$ to every $C \in \mathrm{Ob}(\mathcal{C})$ and
- a morphism $F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$ to every $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ such that
- $F(gf) = F(g)F(f)$ whenever the compositon gf makes sense.
- $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for every object A in $\mathcal{C}$.

A functor F is *faithful* if $F\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(FA, FB)$ is injective for every pair of objects $A, B \in \mathrm{Ob}(\mathcal{C})$.

Examples 4.4. In any of the examples of categories above there is a faithful functor $\mathcal{C} \to \mathbf{Set}$ assigning an object to its underlying set and any morphism to its underlying function. Similarly for any commutative ring there are faithful functors $\mathbf{Comm}_k \to \mathbf{Mod}_k$, $\mathbf{Ass}_k \to \mathbf{Mod}_k$ and $\mathbf{Lie}_k \to \mathbf{Mod_k}$ sending objects to their underlying vector spaces and morphisms to their underlying linear maps. There is also a faithful functor $\mathbf{Ass}_k \to \mathbf{Mon}$ sending objects to their underlying multiplicative monoids and morphism to the underlying function viewed as a monoid homomorphism. There are also faithful 'inclusion' functors $\mathbf{CFiltGrp} \to \mathbf{FiltGrp}$ and $\mathbf{CFiltRing} \to \mathbf{FiltRing}$. We call all of these examples 'forgetful functors'.

Definition 4.5 (Universal property for a free object)**.** Suppose that $F\colon \mathcal{C} \to \mathcal{D}$ is a functor between two categories. For any object X in $\mathcal{D}$ we say that an object $U(X)$ in $\mathcal{C}$ together with a morphism $\iota \in \mathrm{Hom}_{\mathcal{D}}(X, FU(X))$ is *free on* X if for every object A in $\mathcal{C}$ and morphism $f \in \mathrm{Hom}_{\mathcal{D}}(X, FA)$ there is a unique morphism $g \in \mathrm{Hom}_{\mathcal{C}}(U(X), A)$ such that $f = F(g)\iota$.

We say that a morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is an isomorphism $A \to B$ if there is $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ such that $gf = \mathrm{id}_A$ and $fg = \mathrm{id}_B$.

Examples 4.6.

(1) Given a commutative ring k and the forgetful functor $\mathbf{Mod}_k \to \mathbf{Set}$ a free object on a set X is a k-module M together with an injective function $\iota\colon X \to M$ whose image is a free generating set.[9] We can construct such a free module as the set $k[X]$ of functions $X \to k$ which take non-zero values at only finitely many $x \in X$ with the natural k-linear structure and $\iota\colon X \to k[X]$ sending x to the indicator function of x.
(2) In Example 2.6 we constructed the free monoid and the free associative k-algebra on the set $\{X, Y\}$. These constructions generalise to any set.
(3) Given the forgetful functor $\mathbf{Ass}_k \to \mathbf{Mon}$ a free-associative k-algebra on a monoid M is the monoid algebra whose underlying k-module is $(k[M], \iota)$, the free k-module on M and whose multiplication is given by k-bilinear extension of the multiplication on the basis $\iota(M)$ — $\iota(a)\iota(b) = \iota(ab)$ for a, b in M. Note that ι can then be viewed as a monoid homomorphism from M to the underlying monoid of $k[M]$. In the case that a monoid M happens to be a group this gives the group algebra of M.

[9] ie it is a linearly independent spanning set.

Lecture 10

(4) Given the forgetful functors **CFiltRing** $\to$ **FiltRing** (resp. **CFiltGrp** $\to$ **FiltGrp**) a free complete filtered ring (resp. group) on a filtered ring R (resp. group G) is the completion $\widehat{R}$ (resp. $\widehat{G}$) together with the natural map $R \to \widehat{R}$ (resp. $G \to \widehat{G}$). The ring case is the content of Example Sheet 1 Q5. The group case is similar.

Lemma 4.7. *If $(U(X), \iota)$ and $(U'(X), \iota')$ are both free on X then there is a unique isomorphism $f\colon U(X) \to U'(X)$ such that $\iota' = F(f)\iota$.*

Proof. The universal property for $(U(X), \iota)$ applied to the morphsim ι' gives a unique morphism $f\colon U(X) \to U'(X)$ such that $\iota' = F(f)\iota$ that we must show is an isomorphism. Similarly the universal property for $(U'(X), \iota')$ applied to ι gives a unique morphism $g\colon U(X') \to U(X)$ such that $\iota = F(g)\iota'$. Then

$$\iota = F(g)F(f)\iota = F(gf)\iota \text{ and } \iota' = F(fg)\iota'.$$

The universal property for $(U(X), \iota)$ applied to ι gives that there is a unique morphism $h \in \mathrm{Hom}_{\mathcal{C}}(U(X), U(X))$ such that $\iota = h\iota$ but both $F(gf)$ and $\mathrm{id}_{FU(X)}$ satisfy this equation. Thus $F(fg) = \mathrm{id}_{FU(X)} = F(\mathrm{id}_{U(X)})$ so $fg = \mathrm{id}_{U(X)}$ since F is faithful. By symmetry $gf = \mathrm{id}_{U'(X)}$ as required. □

Remark 4.8. In general given a functor $F\colon \mathcal{C} \to \mathcal{D}$ and $X \in \mathrm{Ob}(\mathcal{D})$, a free object $U(X)$ on X need not exist but when one does the Lemma tells us that they are uniquely determined up to unique isomorphism (provided that the morphism $\iota\colon X \to FU(X)$ is considered part of the data.

Example 4.9. Given the forgetful functor $\mathbf{Ass}_k \to \mathbf{Mod}_{\mathbf{k}}$ the free associative algebra on a k-module V can be constructed as follows. Let $T^n(V) = V^{\otimes n}$ ie $T^0(V) = k$, $T^1(V) = V$ and $T^n(V) = T^{n-1}(V) \otimes_k V$ for $n \geqslant 2$. Then $\bigoplus_{n \geqslant 0} T^n(V)$ is the underlying k-module for the free associative k-algebra $k\langle V\rangle$ on V and the multiplication is given by k-bilinear extension of

$$(v_1 \otimes \cdots \otimes v_n) \cdot (w_1 \otimes \cdots \otimes w_m) = (v_1 \otimes \cdots v_n \otimes w_1 \otimes \cdots w_m)$$

and $\iota_V\colon V \to k\langle V\rangle$ is given by the natural inclusion map $V \to T^1(V) \to T(V)$: if R is an associative k-algebra and $f\colon V \to R$ is a k-linear map there is a unique k-algebra map $g\colon k\langle V\rangle \to R$ such that $f = g\iota$ given by linear extension of

$$g(v_1 \otimes \cdots \otimes v_n) = f(v_1) \cdots f(v_n).$$

If instead we consider the forgetful functor $\mathbf{grAss}_k \to \mathbf{grMod}_{\mathbf{k}}$ we can construct the free graded associative algebra on a graded vector space in a similar fashion: if $V = \oplus V_\lambda$ we define a grading on each $T^n(V)$ via

$$T^n(V)_\lambda = \bigoplus_{\lambda_1 + \cdots + \lambda_n = \lambda} V_{\lambda_1} \otimes \cdots V_{\lambda_n}.$$

Example 4.10. There is a forgetful functor from $\mathbf{Ass}_k \to \mathbf{Lie}_k$ that sends an associative k-algebra R to the k-Lie algebra with the same k-module and Lie bracket $[r, s] = rs - sr$. Then the free associative algebra on a k-Lie algebra $\mathfrak{g}$ is the *universal enveloping algebra* $U(\mathfrak{g})$. This can be constructed by taking the free associative algebra $k\langle\mathfrak{g}\rangle$ on the k-module underlying $\mathfrak{g}$ and modding out by the ideal generated by all elements $xy - yx - [x, y]$ for $x, y \in \mathfrak{g}$ i.e.

$$U(\mathfrak{g}) = k\langle\mathfrak{g}\rangle/(xy - yx - [x, y] \mid x, y \in \mathfrak{g})).$$

The k-Lie algebra map $\iota_{\mathfrak{g}}$ is given by the natural map that is the composite

$$\mathfrak{g} \to k\langle\mathfrak{g}\rangle \to U(\mathfrak{g}).$$

Exercise 4.11. Show that if $\mathfrak{g}$ is a graded k-Lie algebra then the grading on $k\langle\mathfrak{g}\rangle$ induces a grading on $U(\mathfrak{g})$ making it free on $\mathfrak{g}$ with respect to the forgetful functor $\mathbf{grAss} \to \mathbf{grLie}$.

Exercise 4.12. Show that if $f\colon A \to B$ is a morphism of rings there is a functor from $\mathbf{Mod}_B \to \mathbf{Mod}_A$ that sends a B-module M to its underlying abelian group together with the map $A \times M \to M$; $(a, m) \mapsto f(a)m$ and sends a morphism in $\mathbf{Mod}_B$ to its underlying function in $\mathbf{Mod}_A$ viewed as an A-linear map. Show that, with respect to this functor, given an A-module N, $B \otimes_A N$ together with the A-linear map $N \to B \otimes_A N$; $n \mapsto 1 \otimes n$ is the 'free B-module on N'.

5. The group ring

In this section we suppose that $\mathcal{O}$ is a complete discrete valuation ring with uniformiser p (so that $k = \mathcal{O}/p\mathcal{O}$ is a field of characteristic p) and (G, ω) will denote a p-valued group of finite rank. $\mathcal{O}[G]$ will denote the group algebra of G with coefficients in $\mathcal{O}$ i.e. the free associative $\mathcal{O}$-algebra on the monoid G and $k[G]$ the corresponding group algebra with coefficients in k.

We filter $\mathcal{O}$ p-adically and then we say that an $\mathcal{O}$-algebra R is *filtered* if has ring filtration v such that $v(pr) \geqslant v(r) + 1$ for all $r \in R$.

Notation 5.1. For $\lambda \geqslant 0$ let

$$\mathcal{O}[G]_\lambda = \mathcal{O} \cdot \{p^r(g_1 - 1)\cdots(g_s - 1) \mid r + \sum_{i=1}^{s} \omega(g_i) \geqslant \lambda \text{ for } g_1, \ldots, g_s \in G\}.$$

Lemma 5.2. *The family $(\mathcal{O}[G]_\lambda)_{\lambda \geqslant 0}$ defines a filtration v on $\mathcal{O}[G]$ making it into a filtered $\mathcal{O}$-algebra. Moreover we may view $\operatorname{gr}\mathcal{O}[G]$ as a graded $k[t]$ algebra via*

$$t.\alpha + \mathcal{O}[G]_{\lambda^+} = p\alpha + \mathcal{O}[G]_{\lambda+1^+}$$

Proof. We can easily check that $\mathcal{O}[G]_0 = \mathcal{O}[G]$, $\mathcal{O}[G]_\lambda = \bigcap_{\mu<\lambda} \mathcal{O}[G]_\mu$ for all $\lambda \geqslant 0$ and $\mathcal{O}[G]_\lambda \mathcal{O}[G]_\mu \subseteq \mathcal{O}[G]_{\lambda+\mu}$ for all $\lambda, \mu \geqslant 0$. So by Remark 2.5

$$v(r) = \sup\{\lambda \geqslant 0 \mid r \in \mathcal{O}[G]_\lambda\}$$

defines a ring filtration.

Now $p \in \mathcal{O}[G]_1$ so $v(pr) \geqslant 1 + v(r)$ for all $r \in \mathcal{O}[G]$ and $\mathcal{O}[G]$ is thus a filtered $\mathcal{O}$-algebra. It follows that $\operatorname{gr}\mathcal{O}[G]$ is a k-algebra and the given action of t does define a graded k-linear map on $\operatorname{gr}\mathcal{O}[G]$ of degree 1 commuting with the ring multiplication. □

Exercise 5.3. Show that there is a natural functor F from the category of filtered $\mathcal{O}$-algebras and filtered $\mathcal{O}$-algebra homomorphisms to **FiltGrp** given on objects by

$$F((R, v)) = (\{x \in R \mid x \text{ is a unit and } v(x - 1) > 0\}, \omega)$$

where $\omega(x) = v(x - 1)$ such that $(\mathcal{O}[G], v)$ is free on G with respect to F.

Lecture 11

Proposition 5.4. *The family of functions* $\varphi_\lambda\colon \operatorname{gr}_\lambda G \mapsto \operatorname{gr}_\lambda \mathcal{O}[G]$ *given by*

$$gG_{\lambda^+} \to (g-1) + \mathcal{O}[G]_{\lambda^+}$$

induce a map $\varphi = \bigoplus \varphi_\lambda$ *of graded* $\mathbf{F}_p[t]$*-Lie algebras where the Lie structure on* $\operatorname{gr}\mathcal{O}[G]$ *is given by commutators.*

Proof. If $\omega(g) = \lambda$ then $g - 1 \in \mathcal{O}[G]_\lambda$ so φ_λ is well-defined. If also $\omega(h) = \lambda$ then

$$gh - 1 = (g-1)(h-1) + (g-1) + (h-1) \in (g-1) + (h-1) + \mathcal{O}[G]_{\lambda^+}$$

since $v((g-1)(h-1)) \geqslant 2\lambda > \lambda$ so φ_λ is a group homomorphism for each $\lambda > 0$ and $\varphi = \oplus\varphi_\lambda$ is an graded $\mathbf{F}_p$-linear map.

Next $\varphi(t\sigma(g)) = g^p - 1 + \mathcal{O}[G]_{\lambda+1^+}$ whereas $t\varphi(\sigma(g)) = p(g-1) + \mathcal{O}[G]_{\lambda+1^+}$. Thus to see that φ is $\mathbf{F}_p[t]$-linear we must show that $(g^p-1)-p(g-1) \in \mathcal{O}[G]_{\lambda+1^+}$. But

$$\begin{aligned} g^p - 1 - p(g-1) &= (1 + (g-1))^p - 1 - p(g-1) \\ &= \sum_{i=2}^{p} \binom{p}{i} (g-1)^i. \end{aligned}$$

Since $v(p) = 1$ and $v((g-1)^i) \geqslant i\lambda$ we see that

$$v(p(g-1)^i) \geqslant 2\lambda + 1 > \lambda + 1 \text{ for } 2 \leqslant i < p.$$

Moreover $\lambda > 1/(p-1)$ by definition of a p-valuation so

$$v((g-1)^p) \geqslant p\lambda > \lambda + 1$$

and so $\sum_{i=2}^{p} \binom{p}{i}(g-1)^i \in \mathcal{O}[G]_{\lambda+1^+}$ as required — since $v_p\left(\binom{p}{i}\right) = 1$ for $2 \leqslant i < p$.

Finally if $\omega(g) = \lambda$ and $\omega(h) = \mu$ then

$$\varphi([\sigma(g), \sigma(h)]) = (g,h) - 1 + \mathcal{O}[G]_{\lambda+\mu^+}$$

and

$$\begin{aligned} [\varphi(\sigma(g)), \varphi(\sigma(h))] &= (g-1)(h-1) - (h-1)(g-1) + \mathcal{O}[G]_{\lambda+\mu^+} \\ &= gh - hg + \mathcal{O}[G]_{\lambda+\mu^+}. \end{aligned}$$

So to see that φ is a Lie-algebra map we must show

$$v\left((g,h) - 1 - (gh - hg)\right) > \lambda + \mu.$$

Now

$$\begin{aligned} (g,h) - 1 - (gh - hg) &= (g^{-1}h^{-1} - 1)(gh - hg) \\ &= (g^{-1}h^{-1} - 1)([g-1, h-1]). \end{aligned}$$

But $v(g^{-1}h^{-1} - 1) \geqslant \min\{\lambda, \mu\} > 0$ and $v([g-1, h-1]) \geqslant \lambda + \mu$ so we're done. □

Proposition 5.5. *The graded* $\mathbf{F}_p[t]$*-Lie algebra map* $\varphi\colon \operatorname{gr} G \to \operatorname{gr}\mathcal{O}[G]$ *in Proposition 5.4 extends to a surjective graded* $k[t]$*-algebra homomorphism*

$$\varphi\colon U_{k[t]}(k \otimes_{\mathbf{F}_p} \operatorname{gr} G) \to \operatorname{gr}\mathcal{O}[G]$$

Proof. That $\operatorname{gr} G \to \operatorname{gr} \mathcal{O}[G]$ extends to a graded $k[t]$-algebra homomorphism

$$\varphi\colon U_{k[t]}(k \otimes_{\mathbf{F}_p} \operatorname{gr} G) \to \operatorname{gr} \mathcal{O}[G]$$

follows immediately from the universal properties for $k \otimes_{\mathbf{F}_p} -$ and $U(-)$. Now $\operatorname{gr} \mathcal{O}[G]$ is generated an a $k[t]$-algebra by $\{(g-1) + \mathcal{O}[G]_{\omega(g)^+} \mid g \in G\}$ by the definition of the filtration:

$$p^r(g_1 - 1)\cdots(g_s - 1) + \mathcal{O}[G]_{\lambda^+} = t^r \cdot \varphi(\sigma(g_1))\cdots\varphi(\sigma(g_s))).$$

Since these are all in the image of φ it is indeed surjective. □

We will show that in fact this map φ is an isomorphism whenever G is a complete p-valued group of finite rank. To this end we fix a complete p-valued group (G, ω) of finite rank and an ordered basis $(g_1, \ldots, g_d)$ for it.

Notation 5.6. For $1 \leqslant i \leqslant d$ write $x_i = \sigma(g_i) \in \operatorname{gr} G \subseteq U_{k[t]}(k \otimes_{\mathbf{F}_p} \operatorname{gr} G)$ and $b_i = g_i - 1 \in \mathcal{O}[G]$. Then given $\alpha \in \mathbf{N}_0^d$ write

$$\mathbf{b}^\alpha = b_1^{\alpha_1} \cdots b_d^{\alpha_d} \in \mathcal{O}[G]$$

We also recall the notation from Proposition 3.32: for $s \in \mathbf{R}^{\geqslant 0}$,

$$n_i(s) = \inf\{n \mid g_i^{p^n} \in G_s\}.$$

Lemma 5.7. *The image of* $\{\mathbf{b}^\alpha \mid 0 \leqslant \alpha_i < p^{n_i(s)}\}$ *in* $\mathcal{O}[G/G_s]$ *is an* $\mathcal{O}$*-module basis.*

Proof. If $\beta \in \{\alpha \in \mathbf{N}_0^d \mid 0 \leqslant \alpha_i < p^{n_i}\}$ then

$$g^\beta = (1 + b_1)^{\beta_1} \cdots (1 + b_d)^{\beta_d} = \sum_{\alpha \in \mathbf{N}_0^d} \binom{\beta}{\alpha} \mathbf{b}^\alpha$$

where $\binom{\beta}{\alpha}$ denotes the image of $\prod_{i=1}^d \binom{\beta_i}{\alpha_i}$ in $\mathcal{O}$. Since $\binom{\beta}{\alpha} = 0$ unless $\alpha_i \leqslant \beta_i$ for all i, Proposition 3.32 gives that the given set spans $\mathcal{O}[G/G_s]$. As it has size $|G/G_s|$ and $\mathcal{O}[G/G_s]$ is a free $\mathcal{O}$-module of this rank it must also be linearly independent. □

Corollary 5.8. *The set* $\{\mathbf{b}^\alpha \mid \alpha \in \mathbf{N}_0^d\}$ *is linearly independent in* $\mathcal{O}[G]$.

Proof. Suppose that S is a finite subset of $\mathbf{N}_0^d$ such that there is a non-trivial linear relation $\sum_{\alpha \in S} \lambda_\alpha \mathbf{b}^\alpha = 0$ in $\mathcal{O}[G]$. We may choose $s \in \mathbf{R}^{\geqslant 0}$ large enough that if $\alpha \in S$ then $\alpha_i < p^{n_i(s)}$ for all i. Then the image of $\sum_{\alpha \in S} \lambda_\alpha \mathbf{b}^\alpha$ in $\mathcal{O}[G/G_s]$ gives a linear relation contradicting Lemma 5.7. □

Lemma 5.9. *If* H *is a finite* p*-group and* $J_H = \ker(k[H] \to k)$ *then* J_H *is nilpotent.*

Proof. By induction on $|H|$. Recall that $Z(H) \neq 1$ so we can pick $z \in Z(H)$ of order p. $H/\langle z\rangle$ is a p-group of order smaller than $|H|$ so by the induction hypothesis

$$J_{H/\langle z\rangle} = \ker(k[H/\langle z\rangle] \to k)$$

is nilpotent. i.e. there is some $N \geqslant 1$ such that $J_{H/\langle z\rangle}^N = 0$. It follows easily that $J_H^N \subset \ker(k[H] \to k[H/\langle z\rangle]) = k[H] \cdot (z-1)$. Now if $\alpha_1, \ldots \alpha_p \in K[H]$ then

$$\alpha_1(z-1)\cdots\alpha_p(z-1) = \alpha_1 \cdots \alpha_p (z-1)^p.$$

But $(z-1)^p = z^p - 1 = 0$ so $J_H^{Np} = 0$. □

Lecture 12

Corollary 5.10. *For all $m \in \mathbf{N}$ and $s \in \mathbb{R}^{>0}$ the kernel J of the augmentation homomorphism $(\mathcal{O}/p^m\mathcal{O})[G/G_s] \to k$ is nilpotent.*

Proof. The group G/G_s is a p-group by Proposition 3.32(c). Thus by Lemma 5.9 there is some $N \geqslant 1$ such that $J^N \subset (p)$. It follows that $J^{mN} \subset (p^m) = 0$. □

Corollary 5.11. *For all $m \in \mathbf{N}$ and $s \in \mathbb{R}^{>0}$ there is some $\lambda \in \mathbf{R}^{\geqslant 0}$ such that $\mathcal{O}[G]_\lambda \subset \ker(\psi_{s,m} \colon \mathcal{O}[G] \to (\mathcal{O}/p^m\mathcal{O})[G/G_s])$.*

Proof. Let $J = (p, g-1 \mid g \in G)$ an ideal in $\mathcal{O}[G]$. By Corollary 5.10 there is some $N \geqslant 1$ such that $\psi_{s,m}(J)^N = 0$. We take $\lambda = N(s+1)$.

Each $\alpha \in \mathcal{O}[G]_\lambda$ is an $\mathcal{O}$-linear combination of elements of the form

$$\alpha_j = p^r(h_1 - 1)\cdots(h_k - 1) \text{ with } h_i \in G \text{ and } r + \sum_{i=1}^{k} \omega(h_i) \geqslant \lambda.$$

It thus suffices to show that each such α_j lies in $\ker \psi_{s,m}$.

If $\omega(h_i) \geqslant s$ for some i then $\psi_{s,m}(h_i - 1) = 0$ so $\alpha_j \in \ker \psi_{s,m}$ as required. Similarly if $r \geqslant N$ then $p^r \in J^r \subset J^N \subset \ker \psi_{s,m}$ so $\psi_{s,m}(\alpha_j) = 0$.

Finally if $r < N$ and $\omega(h_i) < s$ for all i then $k > N$ so $\alpha_j \in J^N$ and $\alpha_j \in \ker \psi_{s,m}$.

So in all cases $\alpha_j \in \ker \psi_{s,m}$ and $\psi_{s,m}(\mathcal{O}[G]_\lambda) = 0$ as claimed. □

Notation 5.12. Now we let

$$B = \bigoplus_{\alpha \in \mathbb{N}_0^d} \mathcal{O}\mathbf{b}^\alpha \subset \mathcal{O}[G]$$

and define $u \colon B \to \mathbf{R}^{\geqslant 0} \cup \{\infty\}$ by

$$u\left(\sum r_\alpha b^\alpha\right) = \min\left\{ v_p(r_\alpha) + \sum_{i=1}^{d} \alpha_i \omega(g_i) \right\}$$

and write $B_\lambda = \{x \in B \mid u(x) \geqslant \lambda$. Notice that $v(x) \geqslant u(x)$ for all $x \in B$.

Lemma 5.13. *For all $\lambda < \mu$ in $\mathbf{R}^{\geqslant 0}$ the natural map*

$$B_\lambda / B_\mu \to \mathcal{O}[G]_\lambda / \mathcal{O}[G]_\mu$$

is surjective.

Proof. Since $x_1, \ldots, x_d$ is a spanning set for $\operatorname{gr} G$ over $\mathbf{F}_p[t]$, Proposition 5.5 tells us that $\sigma(b_1), \ldots, \sigma(b_d)$ generate $\operatorname{gr} \mathcal{O}[G]$ as an $\mathbf{F}_p[t]$-algebra. Thus

$$B_\lambda \to \mathcal{O}[G]_\lambda / \mathcal{O}[G]_{\lambda^+}$$

is surjective i.e. $B_\lambda + \mathcal{O}[G]_{\lambda^+} = \mathcal{O}[G]_\lambda$. Since $v(\mathcal{O}[G]\backslash 0)$ is a discrete subset of $\mathbb{R}$ there is some $\nu > \lambda$ such that $\mathcal{O}[G]_{\lambda^+} = \mathcal{O}[G]_\nu$. Then $B_\lambda + \mathcal{O}[G]_\nu = \mathcal{O}[G]_\lambda$. By induction on the number of values of $v(\mathcal{O}[G])$ between λ and μ we have

$$\mathcal{O}[G]_\nu = B_\nu + \mathcal{O}[G]_\mu.$$

Thus

$$\mathcal{O}[G]_\lambda = B_\lambda + B_\nu + \mathcal{O}[G]_\mu = B_\lambda + \mathcal{O}[G]_\mu$$

as required. □

Proposition 5.14. *$v(x) = u(x)$ for all $x \in B$.*

Proof. We know that $v(x) \geqslant u(x)$ for all $x \in B$. Suppose for contradiction that $v(x) > u(x)$ for some $x = \sum_{\alpha \in S \subset \mathbf{N}_0^d} r_\alpha \mathbf{b}^\alpha$ with S finite and $r_\alpha \neq 0$ for all $\alpha \in S$.

Choose $m \in \mathbf{N}$ and $s \in \mathbf{R}^{\geqslant 0}$ such that $m > v_p(r_\alpha)$ and $\alpha_i < p^{n_i(s)}$ for all $\alpha \in S$ and all $1 \leqslant i \leqslant d$. Then consider $\psi_{s,m} \colon \mathcal{O}[G] \to (\mathcal{O}/p^m\mathcal{O})[G/G_s]$.

By Lemma 5.11 there is some $\lambda > v(x)$ such that $\psi_{s,m}(\mathcal{O}[G]_\lambda) = 0$. Moreover by Lemma 5.13, $\mathcal{O}[G]_{v(x)} = B_{v(x)} + \mathcal{O}[G]_\lambda$.

So choose $y = \sum_{\alpha \in \mathbf{N}_0^d} s_\alpha \mathbf{b}^\alpha \in B_{v(x)}$ and $z \in \mathcal{O}[G]_\lambda$ such that $x = y + z$. Then $\psi_{s,m}(x) = \psi_{s,m}(y)$ and $u(y) \geqslant v(x) > u(x)$.

By Lemma 5.7 $\psi_{s,m}(\mathbf{b}^\alpha)$ with $\alpha \in S$ are linearly independent in $(\mathcal{O}/p^m\mathcal{O})[G/G_s]$ and so $r_\alpha \equiv s_\alpha \bmod p^m$ for all $\alpha \in S$. Since $v_p(r_\alpha) < m$ for all $\alpha \in S$,

$$v_p(s_\alpha) = v_p(r_\alpha) \text{ for all } \alpha \in S.$$

Thus

$$u(x) = \min_{\alpha \in S}\{v_p(r_\alpha) + \sum \alpha_i \omega(g_i)\} = \min_{\alpha \in S}\{v_p(s_\alpha) + \sum \alpha_i \omega(g_i)\} \geqslant u(y) > u(x)$$

the required contradiction. □

Theorem 5.15 (Poincaré–Birkhoff–Witt (PBW))**.** *Let $\mathfrak{g}$ be a Lie algebra over a commutative ring A and suppose that $x_1, \ldots, x_n$ is a spanning set for $\mathfrak{g}$ as an A-module. Then every element of $U(\mathfrak{g})$ is an A-linear combination of elements of the form $x_1^{k_1} \cdots x_n^{k_n}$ with $k_1, \ldots, k_n \in \mathbf{N}_0$. Moreover if $x_1, \ldots, x_n$ are a free generating set for $\mathfrak{g}$ over A so is $x_1^{k_1} \ldots x_n^{k_n}$ for $U(\mathfrak{g})$.*

Remark 5.16. We won't prove the PBW theorem but the first part is a straightforward consequence of the construction of $U(\mathfrak{g})$. The second part is more fiddly. There are other forms of it but this what we will need.

Theorem 5.17. *The morphism $\varphi \colon U_{k[t]}(k \otimes_{\mathbf{F}_p} \operatorname{gr} G) \to \operatorname{gr} \mathcal{O}[G]$ of graded $\mathbf{F}_p$-algebras is an isomorphism.*

Proof. Recall that $x_i = \sigma(g_i)$ and $x_1, \ldots, x_d$ is a basis for $\operatorname{gr} G$ as an $\mathbf{F}_p[t]$-module. So, by the PBW theorem, $U(k \otimes_{\mathbf{F}_p} \operatorname{gr} G)$ consists elements that are finite sums of the form $u = \sum_{\alpha \in \mathbf{N}_0^d} \lambda_\alpha x^\alpha$ with $\lambda_\alpha \in k[t]$. Moreover since φ is a map of graded algebras its kernel is also graded, so to prove that it is injective it suffices to show that no non-zero homogeneous elements lie in the kernel. That is we need only consider non-zero elements of the form $u = \sum \lambda_\alpha x^\alpha$ with each $\lambda_\alpha \in k[t]$ homogeneous and $\deg \lambda_\alpha + \sum \alpha_i \omega(g_i) = s$ is the same for all non-zero terms in the sum. Now $\varphi(\sum \lambda_\alpha x^\alpha) = \sum \lambda_\alpha \mathbf{b}^\alpha + \mathcal{O}[G]_{s^+}$ and we must show that such an element is not zero.

Pick $r_\alpha \in \mathcal{O}$ with $\sigma(r_\alpha) = \lambda_\alpha$ for each α. Then $\varphi(u) = \sum r_\alpha \mathbf{b}^\alpha + \mathcal{O}[G]_{s^+}$. By Proposition 5.14

$$s = u\left(\sum r_\alpha \mathbf{b}^\alpha\right) = v\left(\sum r_\alpha \mathbf{b}^\alpha\right)$$

so $\varphi(u) \neq 0$ as required. □

Lecture 13

6. The completed group ring

6.1. Inverse limits.

Definition 6.1. A *pre-ordered set* is a set I equipped with a binary relation $\leqslant$ that is

(a) reflexive ($a \leqslant a$ for all $a \in I$) and
(b) transitive ($a \leqslant b$ and $b \leqslant c$ implies $a \leqslant c$).

Definition 6.2. We say that a pre-ordered set $(I, \leqslant)$ is *directed* if it is non-empty and for any $a, b \in I$ there is some $c \in I$ such that $a \leqslant c$ and $b \leqslant c$ (ie every finite subset has an upper bound).

Examples 6.3.

(1) $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{R}$ are all directed pre-ordered sets with respect to their usual orders.
(2) If G is a group then the finite index subgroups are directed with respect to reverse inclusion i.e. $H \leqslant K$ precisely if $K \subseteq H$ — since if $H, K \leqslant G$ have finite index then $H \cap K$ has finite index.

Definition 6.4. Suppose that $\mathcal{C}$ is a category and $(I, \leqslant)$ is a pre-ordered set then an *inverse system* of shape $(I, \leqslant)$ in $\mathcal{C}$ is a family of objects $(C_a)_{a \in I}$ and morphisms $c_{bc} \colon C_c \to C_b$ whenever $b \leqslant c$ in I such that $c_{bc}c_{cd} = c_{bd}$ whenever $b \leqslant c \leqslant d$.

Example 6.5. If R is a filtered ring and $I = \mathbf{R}^{\geqslant 0}$ is given the usual ordering $\leqslant$ then the family of rings $(R/R_\lambda)_{\lambda \geqslant 0}$ together with the canonical surjections $R/R_\nu \to R/R_\mu$ for $\mu \leqslant \nu$ form an inverse system.

Definition 6.6. The *inverse limit* of an inverse system $C = (C_a, c_{bc})$ of shape $(I, \leqslant)$ in a category $\mathcal{C}$ is an object $\varprojlim_I C$ of $\mathcal{C}$ together with a family of morphisms $\pi_a \colon \varprojlim_I C \to C_a$ for each $a \in I$ such that $c_{bc}\pi_c = \pi_b$ whenever $b \leqslant c$ which satisfies the universal property:

- for any object D in $\mathcal{C}$ and family of morphims $\rho_a \colon D \to C_a$ for each $a \in I$ such that $c_{bc}\rho_c = \rho_b$ whenever $b \leqslant c$ there is a unique morphism
$$f \colon D \to \varprojlim_I C$$
such that $\pi_a f = \rho_a$ for all $a \in I$.

Note that this universal property is dual to the one for a free object.[10] It is possible to make this precise but we won't.

Exercise 6.7. Suppose I is a pre-ordered set and $C = (C_a, c_{bc})$ is an inverse system of shape I.

(a) Show that, if it exists, $\varprojlim_I C$ together with the family of morphisms
$$\left(\pi_a \colon \varprojlim_I C \to C_a\right)_{a \in I}$$
is uniquely determined up to unique isomorphism.
(b) Show that if I has a largest element t (i.e. $a \leqslant t$ for all $a \in I$) then $\varprojlim_I C = C_t$ and $\pi_a = c_{at}$ for all $a \in I$.
(c) More generally suppose that I is directed and $J \subset I$ such that for all $a \in I$ there is $j \in J$ with $a \leqslant j$[11] and consider the restriction of C to J i.e. the subfamily of objects $(C_j)_{j \in J}$ and morphisms $(c_{jk} \colon C_k \to C_j)_{j \leqslant k \in J}$. Show that if $\varprojlim_J C$ exists then so does $\varprojlim_I C$ and there is a canonical isomorphism $\varprojlim_J C \to \varprojlim_I C$.

[10] in the sense that the morphisms go the other way
[11] We say J is *cofinal* in I

Exercise 6.8. Suppose that I is a pre-ordered set and $\mathcal{C}$ is **Grp** or **Ring** and $C = (C_a, c_{bc})$ is an inverse system in $\mathcal{C}$. Show that

$$\varprojlim_I C \cong \{(x_a) \in \prod_{a\in I} C_a \mid c_{bc}(x_c) = x_b \text{ whenever } b \leqslant c\}$$

together with the projection maps $\pi_a((x_a)_{a\in I}) = x_a$ is the inverse limit of C.

In both of these cases $\varprojlim_I C$ is usually given the weakest topology such that all the projection maps π_a are continous when each object C_a is given the discrete topology. Then $\varprojlim_I C$ is a topological group/ring. In particular the inverse limits in Definitions 2.8 and 3.19 are consistent with Definition 6.6.

Lemma 6.9. *Suppose that S is a ring and $\{I_\alpha\}_{\alpha\in\mathcal{A}}$ and $\{J_\beta\}_{\beta\in\mathcal{B}}$ are two families of two-sided ideals in S that are directed with respect to reverse inclusion such that for all $\alpha \in \mathcal{A}$ there is $\beta \in \mathcal{B}$ such that $J_\beta \subseteq I_\alpha$ and for all $\beta \in \mathcal{B}$ there is $\alpha \in \mathcal{A}$ such that $I_\alpha \subseteq J_\beta$ then there is a natural isomorphism*

$$\varprojlim_{\mathcal{A}} S/I_\alpha \cong \varprojlim_{\mathcal{B}} S/J_\beta.$$

Proof. Consider $\mathcal{C} = \mathcal{A} \cup \mathcal{B}$ and for $\gamma \in \mathcal{C}$, let

$$K_\gamma = \begin{cases} I_\gamma & \text{if } \gamma \in \mathcal{A} \\ J_\gamma & \text{if } \gamma \in \mathcal{B}. \end{cases}$$

Then $\{K_\gamma\}_{\gamma\in\mathcal{C}}$ is directed with respect to reverse inclusion since if we have $K_{\gamma_1}, K_{\gamma_2}$ with $\gamma_1 \in \mathcal{A}$ and $\gamma_2 \in \mathcal{B}$ there is $\alpha \in \mathcal{A}$ such that $I_\alpha \subseteq J_{\gamma_2} = K_{\gamma_2}$ then, as I is directed, there is $\alpha' \in \mathcal{A}$ such that $K_{\alpha'} = I_{\alpha'} \subseteq I_{\gamma_1} \cap I_\alpha$. Then $K_\alpha \subseteq K_{\gamma_1} \cap K_{\gamma_2}$ the other cases are easier. Now by Exercise 6.7(c)

$$\varprojlim_{\mathcal{A}} S/I_\alpha \xrightarrow{\sim} \varprojlim_{\mathcal{C}} S/K_\gamma \xleftarrow{\sim} \varprojlim_{\mathcal{B}} S/J_\beta$$

as required. □

Exercise 6.10. Suppose that I and J are directed pre-ordered sets. Show that $I\times J$ is a directed pre-ordered set with respect to the relation $(i, j) \leqslant (i', j')$ precisely if $i \leqslant i'$ and $j \leqslant j'$. Assuming that all relevant inverse limits exist, show that if C is a diagram of shape $I \times J$ then $(\varprojlim_{\{i\}\times J} C)_{i\in I}$ has canonical maps making it a diagram of shape I and $(\varprojlim_{I\times\{j\}} C)_{j\in J}$ has canonical maps making it a diagram of shape J. Finally show that

$$\varprojlim_I \left(\varprojlim_{\{i\}\times J} C \right) \cong \varprojlim_{I\times J} C \cong \varprojlim_J \left(\varprojlim_{I\times\{j\}} C \right).$$

6.2. **Completing group algebras.**

Definition 6.11. We say that a topological group G is *profinite* if it is isomorphic to an inverse limit of finite groups. We say that is *pro-p* if is isomorphic to an inverse limit of finite p-groups.

Exercise 6.12 (Optional)**.** Show that a profinite group is compact, Hausdorff and totally disconnected[12]. Show conversely that any compact Hausdorff, totally disconnected topological group is profinite.

[12]i.e. any connected subspace is a single point

Suppose that G is a profinite group. The set $\{N \mid N \trianglelefteq_o G\}$ of open normal subgroups of G forms a directed pre-ordered set under reverse inclusion and then for any commutative ring R there are natural maps $R[G/N_1] \to R[G/N_2]$ whenever $N_2 \leqslant N_1$.

Lecture 14

Definition 6.13. For any commutative ring R and profinite group G the *completed group ring with coefficients in* R is

$$RG = R[[G]] = \varprojlim_{N \trianglelefteq_o G} R[G/N].$$

If $R = \mathbf{Z}_p$ and G has an open normal subgroup N that can be given a p-valuation ω making (N, ω) into a complete p-valued group of finite rank then we call RG an *Iwasawa algebra*.

It is a theorem of Lazard that the profinite groups G with a finite index normal subgroup that can be viewed as a complete p-valued group are precisely the compact p-adic Lie groups; that is the compact locally analytic manifolds over $\mathbf{Q}_p$ with a group structure such that the group multiplication is locally analytic[13]. We've seen that a complete p-valued group has a global chart $\mathbf{Z}_p^d \to G$ given by an ordered basis. So the claim in one direction is that if $(g_1, \dots, g_d)$ is an ordered basis and

$$g^\lambda \cdot g^\mu = g^\nu$$

then each $\nu_i(\lambda, \mu) \colon \mathbf{Z}_p^{2d} \to \mathbf{Z}_p$ is given locally by convergent power series.

Note that G can be viewed as a subgroup of the group of units of RG under the family of maps $g \mapsto (gN)_{N \trianglelefteq_o G} \in \varprojlim R[G/N]$.

Definition 6.14. A *crossed product* of a ring S by a group G is a ring $S * H$ which contains S as a subring and contains a set of units $\overline{H} = \{\bar{h} \mid h \in H\}$ such that

- $S * H$ is a free left S-module on $H \to S * H$; $h \mapsto \bar{h}$ and
- for all $x, y \in H$, $\bar{x}S = S\bar{x}$ and $\bar{x}.\bar{y}S = \overline{xy}S$.

Example 6.15. If G is a group with normal subgroup N and R is a commutative ring then $R[G]$ can be viewed as a crossed product $R[N] * (G/N)$. The set $\overline{G/N}$ can be formed as the image of a set of coset representatives of N in G in the ring $R[G]$. Then all the conditions are straightforward to verify. Notice that it may not be possible to choose $\overline{G/N}$ to closed under multiplication.

Lemma 6.16. *If H is an open normal subgroup of a profinite group G then H has finite index. Moreover RG is a crossed product of RH by the finite group G/H.*

Proof. Since G is compact and the left cosets of H in G form a disjoint open cover of G, H must have finite index in G. Fix a set of coset representatives $x_1, \dots, x_k$ of H in G.

Let I be the set of open normal subgroups of G contained in H ordered by reverse inclusion. Now for each $N \in I$,

$$R[G/N] = \bigoplus_{i=1}^{k} R[H/N]x_i = R[H/N] * G/H.$$

[13] A locally analytic function is one that is locally given by convergent power series

Then

$$\varprojlim_I R[G/N] \cong \bigoplus_{i=1}^{k} (\varprojlim_I R[H/N])x_i \cong (\varprojlim_I R[H/N]) * (G/H).$$

Since $N \cap H \in I$ for each $N \trianglelefteq_o G$, I is cofinal in the set of open normal subgroups of G and $RG = \varprojlim_I R[G/N]$.

Similary if $K \trianglelefteq_o H$ then $\bigcap_{g\in G} gKg^{-1}$ is a finite intersection so lives in I and so I is cofinal in the set of open normal subgroups of H. So

$$RH = \varprojlim_I R[H/N]$$

and the result follows. □

The idea of these observations about crossed products is that a reasonable strategy for understanding RG and its representation theory is to first understand RH and its representation theory and then use the crossed product structure to deduce things about RG. In particular to understand Iwasawa algebras an important first case will be to understand the case where the group is complete p-valued of finite rank.

Theorem 6.17. *Let (G, ω) be a complete p-valued group of finite rank and recall the filtration on $\mathcal{O}[G]$ from Lemma 5.2. Then*

$$\mathcal{O}G \cong \varprojlim_{\lambda\in\mathbf{R}^{\geqslant 0}} \mathcal{O}[G]/\mathcal{O}[G]_\lambda.$$

Proof. Since $\mathcal{O}$ is p-adically complete and for $N \trianglelefteq_o G$, it follows from Exercise 6.10 that

$$\mathcal{O}G \cong \varprojlim_{N\trianglelefteq_o G} \left(\varprojlim_{m\in\mathbf{N}_0} (\mathcal{O}/p^m\mathcal{O})[G/N] \right) \cong \varprojlim_{\mathbf{N}_0\times\{N|N\trianglelefteq G\}} \mathcal{O}[G]/I_{m,N}$$

where $I_{m,N} = \ker(\mathcal{O}[G] \to (\mathcal{O}/p^m\mathcal{O})[G/N]) = (n-1, p^m \mid n \in N) \trianglelefteq \mathcal{O}[G]$.

Now for each $N \trianglelefteq_o G$ there is some $s \in \mathbf{R}^{\geqslant 0}$ such that $G_s \leqslant N$ since the G_s form a basis of open neighbourhoods of the identity. Thus by Lemma 5.11, for all $m \in \mathbf{N}_0$ there is some $\lambda \in \mathbf{R}^{\geqslant 0}$ such that $\mathcal{O}[G]_\lambda \subseteq I_{m,N}$.

Conversely given $\lambda \in \mathbf{R}^{\geqslant 0}$, if $m \in \mathbf{N}_0$ is bigger than λ then $I_{m,G_\lambda} \subseteq \mathcal{O}[G]_\lambda$ so we're done by Lemma 6.9. □

Definition 6.18. If R is a ring then an *ascending $\mathbf{N}_0$-filtration* is a family of additive subgroups $(F_nR)_{n\in\mathbf{N}_0}$ of R such that

- $1 \in F_nR$ for all $n \in \mathbf{N}_0$;
- $F_nRF_mR \subseteq F_{n+m}R$ for all $n, m \in \mathbf{N}_0$ and
- $R = \bigcup_{n\geqslant 0} F_nR$.

Given an ascending $\mathbf{N}_0$-filtration on R the *associated graded ring* of R is the $\mathbf{N}_0$-graded ring

$$\operatorname{gr} R = \bigoplus_{n\in\mathbb{N}_0} F_nR/F_{n-1}R$$

(where $F_{-1}R = 0$) with multiplication the bilinear extension of

$$\begin{aligned} (F_nR/F_{n-1}R) \times (F_mR/F_{m-1}R) &\to F_{n+m}R/F_{n+m-1}R \\ (r + F_{n-1}R, s + F_{m-1}R) &\mapsto rs + F_{m+n-1} \end{aligned}$$

Recall that a ring R is Noetherian if it is both left and right Noetherian and is a domain if it has no non-trivial zero-divisors.

Exercise 6.19. Suppse that R has either an ascending $\mathbf{N}_0$-filtration or a descending $\mathbf{R}^{\geqslant 0}$-filtration.

(1) Show that if $\operatorname{gr} R$ is a domain then R is a domain.
(2) Show that if $\operatorname{gr} R$ is Noetherian and, in the descending case R is complete with $v(\mathbf{R}^{\geqslant 0}\backslash\{0\})$ discrete and closed in $\mathbf{R}^{\geqslant 0}$, then R is Noetherian.

Lecture 15

Corollary 6.20. *If (G,ω) is a complete p-valued group of finite rank then $\mathcal{O}G$ is a Noetherian domain.*

Proof. By Theorem 6.17 and Exercise 2.15 we may filter $\mathcal{O}G$ so that it is complete and $\operatorname{gr}\mathcal{O}G \cong \operatorname{gr}\mathcal{O}[G]$. Moreover by Theorem 5.17 $\operatorname{gr}\mathcal{O}[G] \cong U_{k[t]}(k\otimes_{\mathbf{F}_p}\operatorname{gr} G) = U$. Now we may give U an ascending $\mathbf{N}_0$-filtration via $F_0U = k[t]$, $F_1U = k[t]+k[t]\operatorname{gr} G$ and $F_nU = (F_1U)^n$ for $n \geqslant 2$. Since $k\otimes_{\mathbf{F}_p}\operatorname{gr} G$ is a free $k[t]$-module of rank d say, the PBW Theorem gives that $\operatorname{gr} U \cong \operatorname{Sym}_{k[t]}(k\otimes_{\mathbf{F}_p}\operatorname{gr} G)$ a polynomial ring over $k[t]$ in d-variables. Since this is a Noetherian domain we may use Exercise 6.19 to deduce that U is a Noetherian domain and then that $\mathcal{O}G$ is a Noetherian domain since $\mathcal{O}G$ is complete with respect to its filtration. □

Exercise 6.21. Deduce that if $r,s\in\mathcal{O}G$ then $v(rs) = v(r)+v(s)$.

Corollary 6.22. *Any Iwasawa algebra $\mathbf{Z}_pG$ is Noetherian.*

Proof. G has an open normal subgroup N that can be viewed as a complete p-valued group of finite rank. By Lemma 6.16 $\mathbf{Z}_pG \cong \mathbf{Z}_pN * (G/N)$. By Corollary 6.20 $\mathbf{Z}_pN$ is a Noetherian domain. Since $\mathbf{Z}_pG$ is a finitely generated $\mathbf{Z}_pN$-module it follows that $\mathbf{Z}_pG$ is Noetherian — $\mathbf{Z}_pG$ is a finitely generated left/right $\mathbf{Z}_pN$-module and so every left/right ideal of $\mathbf{Z}_pG$ is finitely generated as a left/right $\mathbf{Z}_pN$-module and so also as a left/right $\mathbf{Z}_pG$-module. □

We can understand the $\mathcal{O}$-linear structure of $\mathcal{O}G$ when (G,ω) is complete p-valued of finite rank with ordered basis $(g_1,\dots,g_d)$. Recall that $b_i = g_i - 1 \in \mathcal{O}[G]$ and $\mathbf{b}^\alpha = b_1^{\alpha_1}\cdots b_d^{\alpha_d}$ for $\alpha\in\mathbf{N}_0^d$.

Proposition 6.23. *There is an $\mathcal{O}$-linear bijection*

$$\theta\colon \prod_{\alpha\in\mathbb{N}_0^d}\mathcal{O}\to\mathcal{O}G$$

given by

$$\theta((r_\alpha)_{\alpha\in\mathbf{N}_0^d}) = \left(\sum_{\sum_{i=1}^d \alpha_i\omega(g_i)\leqslant s} r_\alpha\mathbf{b}^\alpha + \mathcal{O}[G]_s\right)_{s\in\mathbf{R}^{\geqslant 0}} \in \varprojlim \mathcal{O}[G]/\mathcal{O}[G]_s \cong \mathcal{O}G.$$

Proof. Recall that by Proposition 5.14

$$v\left(\sum r_\alpha\mathbf{b}^\alpha\right) = \min_\alpha\left\{v_p(r_\alpha)+\sum_{i=1}^d\alpha_i\omega(g_i)\right\}$$

for any finite sum $\sum r_\alpha\mathbf{b}^\alpha$.

For $s \geqslant 0$, let S_s be the finite set $\left\{\alpha \in \mathbf{N}_0^d \mid \sum_{i=1}^d \alpha_i \omega(g_i) \leqslant s\right\}$. Since for $t > s$, $S_s \subset S_t$ and $v\left(\sum_{\alpha \in S_t \setminus S_s} r_\alpha \mathbf{b}^\alpha\right) > s$, it is straightforward to verify that θ is well-defined and $\mathcal{O}$-linear.

Moreover if $\theta((r_\alpha)_{\alpha \in \mathbf{N}_0^d}) = 0$ then $v(\sum_{\alpha \in S_s} r_\alpha \mathbf{b}^\alpha) \geqslant s$ for all $s \geqslant 0$. Thus

$$v_p(r_\alpha) \geqslant s - \sum_{i=1}^d \alpha_i \omega(g_i)$$

for all $\alpha \in \mathbf{N}_0^d$ and all $s \geqslant 0$ and so $v_p(r_\alpha) = \infty$ for all $\alpha \in \mathbf{N}_0^d$. It follows that θ is injective.

Now suppose that $(x_s)_{s>0} \in \varprojlim \mathcal{O}[G]/\mathcal{O}[G]_s$. By Lemma 5.13

$$\mathcal{O}[G] = \bigoplus_{\alpha \in \mathbf{N}_0^d} \mathcal{O}\mathbf{b}^\alpha + \mathcal{O}[G]_s$$

for each $s \geqslant 0$ and so we can find $x_{\alpha,s} \in \mathcal{O}$ such that $x_s = \sum_{\alpha \in S_s} x_{\alpha,s} \mathbf{b}^\alpha + \mathcal{O}[G]_s$.

If $t > s$ then $x_t + \mathcal{O}[G]_s = x_s + \mathcal{O}[G]_s$ so

$$\sum_{\alpha \in S_s} (x_{\alpha,s} - x_{\alpha,t}) \mathbf{b}^\alpha \in \mathcal{O}[G]_s$$

ie $v_p(x_{\alpha,t} - x_{\alpha,s}) \geqslant s - \sum \alpha_i \omega(g_i)$ for all $\alpha \in S_s$ and $t > s$.

Now given $\alpha \in \mathbf{N}_0^d$ we can choose s such that $\alpha \in S_s$ and then

$$v_p(x_{\alpha,t} - x_{\alpha,u}) \geqslant t - \sum \alpha_i \omega(g_i)$$

for all $u > t > s$ ie there is some $x_\alpha = \lim_{t \to \infty} x_{\alpha,t} \in \mathcal{O}$ since $\mathcal{O}$ is complete.

Now we can verify that $\theta((x_\alpha)_{\alpha \in \mathbf{N}_0^d}) + \mathcal{O}[G]_s = x_s$ for each $s \geqslant 0$ and so θ is surjective. □

Remark 6.24. We may view θ as an $\mathcal{O}$-module isomorphism $\mathcal{O}[[b_1, \ldots, b_d]] \to \mathcal{O}G$. This will not be a ring isomorphism in general as $\mathcal{O}G$ will not be commutative.

Examples 6.25.

(a) If $G = \mathbf{Z}_p^d$ with $\omega(\lambda) = \min_{1 \leqslant i \leqslant d}\{v_p(\lambda_i)\} + 1$ Then $\mathcal{O}G$ is isomorphic to the commutative formal power series ring $\mathcal{O}[[T_1, \ldots, T_d]]$ as claimed for $d = 1$ in Lecture 1.

(b) If (G, ω) is as in Exercise 2.36,

$$x = \begin{pmatrix} 1 & p & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & p \\ 0 & 0 & 1 \end{pmatrix} \text{ and } z = \begin{pmatrix} 1 & 0 & p \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

then writing $X = x - 1, Y = y - 1, Z = z - 1 \in \mathcal{O}G$ we can compute that

$$\mathcal{O}G = \left\{ \sum_{l,m,n \geqslant 0} \lambda_{lmn} X^l Y^m Z^n \mid \lambda_{lmn} \in \mathcal{O} \right\}$$

as an $\mathcal{O}$-module with multiplication such that Z is central and

$$(1+Y)(1+X) = (1+X)(1+Y)(1+Z)^{-p} \text{ ie}$$

$$YX = XY + (1 + X + Y + XY) \left(\sum_{j \geqslant 1} \binom{-p}{j} Z^j \right).$$

Exercise 6.26. Show that if G is a complete p-valued group of rank d and $k = \mathcal{O}/(p)$ as usual then there is a k-linear isomorphism $kG \cong \{\sum_{\alpha \in \mathbf{N}_0^d} x_\alpha \mathbf{b}^\alpha \mid x_\alpha \in k\}$.

Lecture 16

Exercise 6.27. Show that $kG \cong \mathcal{O}G/(p)$. Let M be a finitely generated $\mathcal{O}G$-module and write $M[p^k] = \{m \in M \mid p^k m = 0\}$. Show that there is some $n \geqslant 0$ such that $M[p^k] = M[p^n]$ for all $k \geqslant n$, that $M[p^k]/M[p^{k-1}]$ is naturally a finitely generated kG-module for each $1 \leqslant k \leqslant n$ and that $M/M[p^n]$ is an $\mathcal{O}G$-module with no p-torsion elements.

It follows that many questions about finitely generated $\mathcal{O}G$-modules can answered by considering finitely generated kG-modules (i.e. those $\mathcal{O}G$-modules killed by p) and finitely generated $\mathcal{O}G[1/p]$-modules separately.

7. Centres of Iwasawa algebras

In this section k will denote a finite field of characteristic p and G will denote a profinite group. Our goal will be to compute $Z(RG)$ in the case G has a p-valuation with respect to which it is complete and $R = \mathbf{Z}_p$ or $R = k$. We will follow Ardakov 'The Centre of Completed Group Algebras of Pro-p Groups' (2004).

Definition 7.1. The category $\mathbf{G - Set^f}$ has objects finite sets X[14] equipped with a continous G-action $G \times X \to X$ and morphisms

$$\mathrm{Hom}_{\mathbf{G-Set^f}}(X, Y) = \{f \colon X \to Y \mid g.f(x) = f(gx) \text{ for all } g \in G, x \in X\}.$$

We may view this as a subcategory of the category of all topological G-sets with continuous action map.

Exercise 7.2. Show that an action $G \times X \to X$ on a finite set is continuous precisely if $\mathrm{Stab}_G(x)$ is an open subgroup of G for each $x \in X$.

For each object $X \in \mathbf{G - Set^f}$ we can form the permutation module $R[X]$ which is the free R-module with basis X and with G-action the R-linear extension of the G-action on the basis. A morphism $f \colon X \to Y$ in $\mathbf{G - Set^f}$ naturally induces a G-linear map $f \colon R[X] \to R[Y]$ sending the basis vector $x \in X$ to the basis vector $f(x) \in Y$.

Given an inverse system$(X_n, \pi_{n,m})$ in $\mathbf{G - Set^f}$ of shape $(\mathbf{N}, \leqslant)$ we can form the inverse limit $\varprojlim X_n$ in the category of all topological G-Sets with continuous G-action and $RX = \varprojlim R[X_n]$ in the category of all topological kG-modules. All of these spaces are compact and Hausdorff and indeed metrizable[15] In particular we give $kX = \varprojlim k[X_n]$ the metric

$$d((\alpha_n)_{n \in \mathbf{N}}, (\beta_n)_{n \in \mathbf{N}}) = p^{-\inf\{n \in \mathbf{N} \mid \alpha_n \neq \beta_n\}}.$$

We will compute $(kX)^G$ and $(\mathbf{Z}_p X)^G$ when G is a pro-p group and then apply this to the case where G acts on itself by conjugation and is complete p-valued.

---

[14] with the discrete topology

[15] We topologise $\mathbf{Z}_p X = \varprojlim_{n,m} \mathbf{Z}_p/(p^m)[X_n]$ with the weakest topology so that all maps $\mathbf{Z}_p X \to \mathbf{Z}_p/(p^m)[X_n]$ are continuous where the codomain is always discrete or equivalently so that all maps $\mathbf{Z}_p X \to \mathbf{Z}_p[X_n]$ are continuous where $\mathbf{Z}_p[X_n] \cong \mathbf{Z}_p^{|X_n|}$ is given the product topology with respect to the usual topology on $\mathbf{Z}_p$.

Notation 7.3. Given a set X with a G-action and a finite orbit $\mathcal{C} \subseteq X$ we write

$$[\mathcal{C}] = \sum_{x \in \mathcal{C}} x \in R[X]$$

for its *orbit sum*. We write

$$X^G = \{x \in X \mid gx = x \text{ for all } g \in G\}.$$

Exercise 7.4. If X is any set with a G-action then $R[X]^G$ is spanned by the orbit sums $[\mathcal{C}]$ as $\mathcal{C}$ ranges over all finite G-orbits in X.

Lemma 7.5. *Suppose that G is pro-p and $f\colon X \to Y$ is a morphism in $\mathbf{G-Set^f}$. Then under $f\colon k[X] \to k[Y]$ the image of $k[X]^G$ in $k[Y]$ is spanned by the orbit sums $[f(\mathcal{C})]$ where $\mathcal{C}$ ranges over the orbits of X such that $|f(\mathcal{C})| = |\mathcal{C}|$.*

Proof. It is easy to verify that if $\mathcal{C}$ is an orbit in X then $f(\mathcal{C})$ is an orbit in Y. Moreover if $y \in f(\mathcal{C})$ then

$$|\{x \in \mathcal{C} \mid f(x) = y\} = |\operatorname{Stab}_G(y)|/|\operatorname{Stab}_G(x)| = |\mathcal{C}|/|f(\mathcal{C})|.$$

This number is independent of the choice of $y \in f(\mathcal{C})$ and is always a power of p since G is pro-p.

Thus

$$f([\mathcal{C}]) = \frac{|\mathcal{C}|}{|f(\mathcal{C})|}[f(\mathcal{C})] = \begin{cases} [f(\mathcal{C})] & \text{if } |\mathcal{C}| = |f(\mathcal{C})| \\ 0 & \text{otherwise.} \end{cases}$$

The result follows immediately via Exercise 7.4. □

Proposition 7.6. *If G is pro-p and X is the inverse limit of an inverse system of shape $(\mathbf{N}, \leqslant)$ in $\mathbf{G-Set^f}$ then*

$$kX^G = \overline{k[X]^G}$$

Proof. Since the action of G on kX is continuous, kX^G is closed in kX and so $\overline{k[X]^G} \subset kX^G$.

Suppose that $\alpha = (\alpha_n)_n \in kX^G$. We will show that for each $r \in \mathbf{N}$ there is some $\beta \in k[X]^G$ such that $d(\alpha, \beta) < p^{-r}$ and so $\alpha \in \overline{k[X]^G}$ as required.

We fix $r \in \mathbf{N}$. Since the $\pi_n\colon kX \to k[X_n]$ are maps of G-spaces each $\alpha_n \in k[X_n]^G$. In particular we may write

$$\alpha_r = \sum_{\mathcal{C}} \lambda_{\mathcal{C}}[\mathcal{C}]$$

where the sum is over all G-orbits $\mathcal{C}$ in X_r.

We consider some orbit $\mathcal{C}$ such that $\lambda_{\mathcal{C}} \neq 0$. Since for all $n > r$ the map $\pi_{n,r}\colon k[X_n] \to k[X_r]$ sends $\alpha_n \in k[X_n]^G$ to α_r, by Lemma 7.5 we can find an orbit $\mathcal{C}_n$ in X_n such that $\pi_{n,r}(\mathcal{C}_n) = \mathcal{C}$ and $|\mathcal{C}| = |\mathcal{C}_n|$. Indeed we may inductively construct the $\mathcal{C}_n$ so that $\pi_{n,n-1}(\mathcal{C}_n) = \mathcal{C}_{n-1}$ for each $n > r$ (and $\mathcal{C}_r = \mathcal{C}$). Thus for $x_r \in \mathcal{C}$ we can find a unique $x_n \in \mathcal{C}_n$ such that $\pi_{n,r}(x_n) = x_r$. This family $(x_n)_{n \geqslant r}$ defines an element $x \in X = \varprojlim X_n$. The G-orbit $\mathcal{C}_\infty$ of x is $\varprojlim_{n \geqslant r} \mathcal{C}_n$ and has the same order as $\mathcal{C}$ by construction.

Repeating this construction for each orbit $\mathcal{C}$ in X_r with $\lambda_{\mathcal{C}} \neq 0$ we can then define $\beta = \sum \lambda_{\mathcal{C}}[\mathcal{C}_\infty] \in k[X]^G$. Then $\pi_s(\beta) = \alpha_s$ for all $s \leqslant r$ and so $d(\alpha, \beta) < p^{-r}$ as required. □

Lecture 17

Corollary 7.7. *If G and X are as in Proposition 7.6 then $(\mathbf{Z}_pX)^G = \overline{\mathbf{Z}_p[X]^G}$.*

Proof. Once again since the action of G on $\mathbf{Z}_pX$ is continuous, $(\mathbf{Z}_pX)^G$ is closed in $\mathbf{Z}_pX$ and so $\overline{\mathbf{Z}_p[X]^G} \subset (\mathbf{Z}_pX)^G$.

Let $q\colon \mathbf{Z}_pX \to \mathbf{F}_pX$ denote the reduction map mod p. Then for $\alpha \in (\mathbf{Z}_pX)^G$, $q(\alpha) \in \mathbf{F}_pX^G = \overline{\mathbf{F}_p[X]^G}$. Thus for each $n \geqslant 0$ we may find $\beta_n \in (\mathbf{F}_p[X])^G$ such that $d(q(\alpha), \beta_n) < p^{-n}$. For each such β_n we may find $\gamma_n \in \mathbf{Z}_p[X]^G$ such that $q(\gamma_n) = \beta_n$. Since $\mathbf{Z}_pX$ is compact and Hausdoff, by Bolzano–Weierstrass γ_n has a convergent subsequence with limit δ_0, say. Moreover as $\overline{\mathbf{Z}_p[X]^G}$ is closed it must contain δ_0. Then $q(\delta_0) = q(\alpha)$ by construction so

$$\alpha - \delta_0 \in (\mathbf{Z}_pX)^G \cap \ker q = (\mathbf{Z}_pX)^G \cap p\mathbf{Z}_pX = p(\mathbf{Z}_pX)^G$$

since $pr \in (\mathbf{Z}_pX)^G$ precisely if $r \in (\mathbf{Z}_pX)^G$. Thus we may write $\alpha = \delta_0 + p\alpha_1$ for some $\alpha_1 \in (\mathbf{Z}_pX)^G$. Repeating this argument we obtain α is equal to a convergent sum $\sum_{i\geqslant 0} p^i\delta_i$ with each $\delta_i \in \overline{\mathbf{Z}_p[X]^G}$. Thus $\alpha \in \overline{\mathbf{Z}_p[X]^G}$ as required. □

Theorem 7.8. *If (G, ω) is a complete p-valued group with centre Z then $Z(kG) = kZ$ and $Z(\mathbf{Z}_pG) = \mathbf{Z}_pZ$.*

Proof. Since $\mathbf{N}$ is cofinal in $\mathbf{R}^{\geqslant 0}$, $G = \varprojlim G/G_n$. Moreover G is pro-p by Lemma 3.2. Thus by Proposition 7.6

$$Z(kG) = (kG)^G = \overline{k[G]^G} = \overline{Z(k[G])}.$$

Similarly by Corollary 7.7

$$Z(\mathbf{Z}_pG) = (\mathbf{Z}_pG)^G = \overline{\mathbf{Z}_p[G]^G} = \overline{Z(\mathbf{Z}_p[G])}.$$

Thus it suffices to show that $Z(k[G]) = k[Z]$ and $Z(\mathbf{Z}_p[G]) = \mathbf{Z}_p[Z]$.

By Exercise 7.4, $Z(R[G])$ is spanned by all the finite orbit sums under the conjugation action. So it is equivalent to prove that all the finite conjugacy classes have order 1. Let $\mathcal{C}$ be a finite conjugacy class in G and $x \in \mathcal{C}$. Then $C_G(x)$ is a closed subgroup of finite index. Thus for all $y \in G$ there is some $n \in \mathbf{N}$ such that $y^{p^n} \in C_G(x)$ i.e.

$$y^{p^n} = xy^{p^n}x^{-1} = (xyx^{-1})^{p^n}.$$

But by Lemma 3.6(b) if $g, h \in G$ then $\omega(g^{-p^n}h^{p^n}) = \omega(g^{-1}h) + n$. Thus if $g^{p^n} = h^{p^n}$ then $g = h$. In particular we can deduce that $y = xyx^{-1}$ as required. □

8. The Campbell-Baker-Hausdorff formula

8.1. Coalgebras and Primitive elements.

Definition 8.1. Let k be a commutative ring. A *k-coalgebra* is a k-module C equipped with k-linear maps $\Delta\colon C \to C \otimes_k C$ (the *co-multiplication*) and $\epsilon\colon C \to k$ such that

(1) $(\Delta \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \Delta)\Delta$ (Δ is *co-associative*); and
(2) $(\epsilon \otimes \mathrm{id})\Delta = \mathrm{id} = (\mathrm{id} \otimes \epsilon)\Delta$ (ϵ is a *counit*).

A k-bialgebra A is a k-coalgebra (A, Δ, ϵ) such that A also has the structure of an (associative unital) algebra with respect to which Δ and ϵ are algebra homomorphisms.

Example 8.2. Let G be a group. Then we can define

$$\Delta\colon k[G] \to k[G] \otimes_k k[G]$$

to be the k-linear extension of the map $g \mapsto g \otimes g$ for $g \in G$ and

$$\epsilon\colon k[G] \to k$$

to be the k-linear extension of $g \mapsto 1$ for $g \in G$. Then $k[G]$ is a k-bialgebra.

Definition 8.3. In general we call c in a coalgebra C *grouplike* if $\Delta(c) = c \otimes c$.

Examples 8.4.

(a) Let G be a finite group. Then $k^G = \{f\colon G \to k\}$ is an k-algebra under pointwise operations. If we identify $k^G \otimes_k k^G$ with $k^{G\times G}$ and set $\Delta(f)(x,y) = f(xy)$ for $f \in k^G$ and $x, y \in G$ and $\epsilon(f) = f(e_G)$ then k^G is a bialgebra that is in some sense dual to $k[G]$.

(b) Let $\mathfrak{g}$ be a Lie algebra over k. Then the map $x \mapsto (x, x)$ defines a Lie algebra homomorphism $\mathfrak{g} \to \mathfrak{g} \times \mathfrak{g}$ that extends to a k-algebra homomorphism

$$\Delta\colon U(\mathfrak{g}) \to U(\mathfrak{g} \times \mathfrak{g}) \cong U(\mathfrak{g}) \otimes_k U(\mathfrak{g})$$

such that $\Delta(x) = x \otimes 1 + 1 \otimes x$ for $x \in \mathfrak{g}$. Moreover the trivial representation $\mathfrak{g} \to k$; $x \mapsto 0$ gives a k-algebra homomorphism $U(\mathfrak{g}) \to k$. Thus $U(\mathfrak{g})$ equipped with Δ and ϵ is a k-bialgebra.

Definition 8.5. In general we call c in a k-bialgebra C *primitive* if $\Delta(c) = 1 \otimes c + c \otimes 1$. The set of primitive elements is denoted $\mathcal{P}(C)$

Lemma 8.6. *If A is a k-bialgebra then $\mathcal{P}(A)$ is a k-Lie algebra under the commutator bracket $[a, b] = ab - ba$ with respect to the algebra structure on A.*

Proof. If $x, y \in A$ are primitive and $\lambda \in k$ then

$$\Delta(\lambda x) = \lambda\Delta(x) = \lambda x \otimes 1 + 1 \otimes \lambda x$$

and

$$\Delta(x + y) = \Delta(x) + \Delta(y) = (x + y) \otimes 1 + 1 \otimes (x + y)$$

so $\mathcal{P}(A)$ is a k-module. Moreover

$$\begin{aligned}\Delta(xy - yx) &= [\Delta(x), \Delta(y)]\\ &= (x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) - (y \otimes 1 + 1 \otimes y)(x \otimes 1 + 1 \otimes x)\\ &= (xy - yx) \otimes 1 - 1 \otimes (xy - yx)\end{aligned}$$

so $xy - yx$ is primitive. □

Lecture 18

At this point we need a generalisation of the form of the PBW theorem we had before.

Theorem 8.7 (PBW)**.** *If $\mathfrak{g}$ is a k-Lie algebra whose underlying k-module is free on a set X. Then the ascending $\mathbf{N}_0$-filtration on $U = U(\mathfrak{g})$ given by $F_0U = k$, $F_1U = k + \mathfrak{g}$ and $F_nU = (F_1U)^n$ for $n \geqslant 2$ (known as the PBW filtration) satisfies $\operatorname{gr} U(\mathfrak{g}) \cong \operatorname{Sym}(\mathfrak{g}) \cong k[X]$ the polynomial ring over k with variables in X.*

If X is finite this is just a rephrasing of Theorem 5.15.

Theorem 8.8. *Suppose that k is torsion free as an additive group and $\mathfrak{g}$ is a k-Lie algebra that is free as a k-module. Then $\mathcal{P}(U(\mathfrak{g})) = \mathfrak{g}$.*

Proof. First we notice that with respect to PBW-filtration on $U = U(\mathfrak{g})$ and the *tensor product filtration* on $U \otimes_k U$ given by

$$F_n(U \otimes_k U) = \sum_{l+m=n} F_l U \otimes_k F_m U \text{ for all } n \geqslant 0,$$

Δ is a filtered k-algebra homomorphism.

Thus Δ induces a graded algebra map $\operatorname{gr}\Delta\colon \operatorname{gr} U \to \operatorname{gr}(U \otimes_k U)$. If $x_1, \dots, x_n \in \operatorname{gr}_1 U$ then

$$\operatorname{gr}\Delta(x_1 \cdots x_n) = \prod_{i=1}^{n} \operatorname{gr}\Delta(x_i) = \prod_{i=1}^{n} (x_i \otimes 1 + 1 \otimes x_i).$$

So writing $\mu\colon \operatorname{gr} U \times \operatorname{gr} U \to \operatorname{gr} U$ to denote the multiplication in the graded ring,

$$\mu(\Delta(x_1 \cdots x_n)) = 2^n x_1 \cdots x_n.$$

Thus $\mu\Delta$ acts by 2^n on $\operatorname{gr}_n U$.

However if $u \in U$ is primitive then $\sigma(u) \in \operatorname{gr} U$ is also primitive, since

$$gr\Delta(\sigma(u)) = \sigma(\Delta(u)),$$

and so

$$\mu \operatorname{gr}\Delta(\sigma(u)) = \mu(\sigma(u) \otimes 1 + 1 \otimes \sigma(u)) = 2\sigma(u).$$

It follows that for primitive $u \in F_n U \backslash F_{n-1} U$ we have $(2^n - 2)\sigma(u) = 0$. By Theorem 8.7 and our assumption that $(k, +)$ is torsion-free it follows that all non-zero primitive u live in $F_1 U \backslash F_0 U$ i.e. $u = \lambda + y$ for some $\lambda \in k$ and $y \in \mathfrak{g}$. Since such y is primitive and $\mathcal{P}(U)$ is a k-submodule of U it follows that λ is primitive. Since $\lambda \in F_0 U$ it must be 0. □

8.2. **Free non-associative algebras and free Lie algebras.**

Definition 8.9. A *magma* is a set M with a binary operation. **Mag** is the category whose objects are magmas and whose morphisms $\operatorname{Hom}_{\mathbf{Mag}}(M, N)$ are functions $f\colon M \to N$ such that $f(ab) = f(a)f(b)$ for all $a, b \in M$.

Given a set X we can construct a magma as follows: $X(1) = X$. For $n \geqslant 2$, $X(n)$ is the disjoint union $\coprod_{p+q=n} X(p) \times X(q)$. Then $M(X)$ is the disjoint union $\coprod_{n \geqslant 1} X(n)$. The binary operation on $M(X)$ is defined by assembling the inclusion maps $\mu_{m,n}\colon X(m) \times X(n) \to X(m+n)$ together to give a (graded) map $\mu\colon M(X) \times M(X) \to M(X)$.

Example 8.10. If $X = X(1) = \{1\}$ we can write $X(2) = \{(1 \cdot 1)\}$ then

$$X(3) = \{(1 \cdot (1 \cdot 1)), ((1 \cdot 1) \cdot 1)\},$$

$$X(4) = \{(1 \cdot (1 \cdot (1 \cdot 1))), (1 \cdot ((1 \cdot 1) \cdot 1)), (1 \cdot 1) \cdot (1 \cdot 1), ((1 \cdot (1 \cdot 1)) \cdot 1), (((1 \cdot 1) \cdot 1) \cdot 1)\}$$

etc.

Exercise 8.11. $M(X)$ is the free magma on X with respect to the forgetful functor **Mag** $\to$ **Set**.

Definition 8.12. Given a commutative ring k, a (not necessarily associative not necessarily unital) k-algebra A is a k-module together with a k-linear multiplication map $\mu_A\colon A \times A \to A$. $\mathbf{Alg}_k$ is the category whose objects are such k-algebras and whose morphisms $\mathrm{Hom}_{\mathbf{Alg}_k}(A, B)$ are k-linear maps $f\colon A \to B$ such that $f(\mu_A(x, y)) = \mu_B(f(x), f(y))$ for all $x, y \in A$.

Exercise 8.13. The free k-algebra on a set X with respect to the forgetful functor $\mathbf{Alg}_k \to \mathbf{Set}$ is the free k-module on $M(X)$ with multiplication given by bilinear extension of the natural multiplication on the basis. Moreover the natural grading on $M(X)$ induces a grading on the free algebra $k[M(X)]$.

Exercise 8.14. The free k-Lie algebra L_X on a set X is the (graded) Lie algebra of k obtained from the free k-algebra on X by quotienting out by the (graded) ideal $(a \cdot a, a \cdot (b \cdot c) + b \cdot (c \cdot a) + c \cdot (a \cdot b) | a, b, c \in M(X))$.

Proposition 8.15. *Let X be a set. Then the free associative algebra $k\langle X\rangle$ on X is naturally isomorphic to the universal enveloping algebra $U(L_X)$ of the free Lie algebra on X.*

Proof. We identify X with its image in $L_X, U(L_X)$ and $k\langle X\rangle$ and identify L_X with its image in $U(L_X)$ under the maps given by the various universal properties.

Then the univeral property of $k\langle X\rangle$ gives a unique associative k-algebra map $\varphi\colon k\langle X\rangle \to U(L_X)$ sending $x \in X$ to itself. Similarly by the universal property of L_X there is a unique Lie algebra map $\alpha\colon L_X \to k\langle X\rangle$ sending $x \in X$ to itself.[16] By the universal property of $U(L_X)$ this extends uniquely to an associative k-algebra map $\psi\colon U(L_X) \to k\langle X\rangle$.

Now $\varphi\psi\colon k\langle X\rangle \to k\langle X\rangle$ is an associative k-algebra map such that $\varphi\psi(x) = x$ for all $x \in X$ so by the universal property for $k\langle X\rangle$ it is the identity map on $k\langle X\rangle$. Similarly $\psi\varphi\colon L_X \to U(L_X)$ is k-Lie algebra map such that $\psi\varphi(x) = x$ for all $x \in X$. Thus by the universal property for L_X, $\psi\varphi(y) = y$ for all $y \in L_X$ and so by the universal property for $U(L_X)$, $\varphi\psi = \mathrm{id}$. □

It follows that we may transport usual the coalgebra structure on $U(L_X)$ to $k\langle X\rangle$.

Exercise 8.16. Show that the isomorphism $\varphi\colon k\langle X\rangle \to U(L_X)$ is in fact an isomorphism of graded algebras where $k\langle X\rangle$ is given the grading

$$k\langle X\rangle = \bigoplus_{n \geqslant 0} T^n(k[X])$$

and $U(L_X)$ is given the grading induced from the grading on L_X as in Exercise 4.11.

Lecture 19

8.3. **The Campbell-Hausdorff formula.** Recall that given a set X we have constructed an $\mathbf{N}$-graded k-Lie-algebra L_X that is free on the set X. We will assume for the rest of this section that k is a field of characteristic 0.

Notation 8.17. We write $L_X^{(n)}$ for the nth-graded piece for $n \in \mathbf{N}$. Similarly we write $k\langle X\rangle^{(n)}$ to denote the nth graded piece of $k\langle X\rangle$ for $n \in \mathbf{N}_0$.

[16] As always the Lie structure on $k\langle X\rangle$ is the commutator one.

In particular $L_X^{(1)}$ is the k-vector space with basis X and in general $L_X^{(n)}$ is spanned by n-fold commutators of elements of $X \subset L_X^{(1)}$. Similarly $k\langle X\rangle^{(n)}$ is spanned by all products of n elements of $X \subset k\langle X\rangle$.

By Exercise 8.16 we may identify L_X as a graded Lie-subalgebra of the graded Lie algebra $k\langle X\rangle$. Indeed after transporting the coalgebra structure on $U(L_X)$ along the graded k-algebra isomorphism $U(L_X) \to k\langle X\rangle$ we see, using Theorem 8.8, that under this identification $L_X^{(n)}$ consists of the primitive elements of $k\langle X\rangle$ of degree n.

We filter $k\langle X\rangle$ by

$$v\left(\sum_{n\geqslant 0} r_n\right) = \inf\{n \in \mathbf{N}_0 \mid r_n \neq 0\}$$

when each $r_n \in k\langle X\rangle^{(n)}$. Similarly we filter the free Lie algebra L_X by

$$v\left(\sum_{n>0} x_n\right) = \inf\{n \in \mathbf{N} \mid x_n \neq 0\}$$

when each $x_n \in L(X)_n$.[17]

Exercise 8.18. Show that $\widehat{k\langle X\rangle} \cong \prod_{n\geqslant 0} k\langle X\rangle^{(n)}$ can be viewed as a ring of formal (non-commutative) power series in the variables X and[18] $\widehat{L_X} \cong \prod_{n\geqslant 1}(L_X)^{(n)}$

Let $\widehat{\mathfrak{m}}_X = \widehat{\mathfrak{m}}$ denote the ideal $\widehat{k\langle X\rangle}_1$ given by filtration $\widehat{v}$ on $\widehat{k\langle X\rangle}$.

Lemma 8.19.
(a) $\widehat{k\langle X\rangle}^\times = k^\times + \widehat{\mathfrak{m}}$*;*
(b) $\widehat{\mathfrak{m}}$ *is the unique maximal ideal in* $\widehat{k\langle X\rangle}$ *and;*
(c) $1 + \widehat{\mathfrak{m}}$ *is a subgroup of* $\widehat{k\langle X\rangle}$*.*

Proof. The map $\epsilon\colon \widehat{k\langle X\rangle} \to k\langle X\rangle_0/k\langle X\rangle_1 = k$ is a homomorphism of unital k-algebras. Therefore any unit in $\widehat{k\langle X\rangle}$ must lie in the complement of the kernel of ϵ i.e. in $k^\times + \widehat{\mathfrak{m}}$. Conversely if $r \in \widehat{k\langle X\rangle}$ with $\epsilon(r) = r_0 \neq 0$ then $r - r_0 = r_1 \in \ker\epsilon = \widehat{\mathfrak{m}}$ i.e. $r = r_0(1-u)$ with $u = -r_0^{-1}r_1 \in \widehat{\mathfrak{m}}$ since r_0 is a unit in k. By Notation 3.14 and Exercise 3.15 $\sum_{i\geqslant 0} u^i \in \widehat{k\langle X\rangle}$ is an inverse for $1-u$. (a) & (b) follow immediately as does (c) by noting that $1 + \widehat{\mathfrak{m}} = \ker\epsilon\colon \widehat{k\langle X\rangle}^\times \to k^\times$. □

Remark 8.20. Note that if $X = \{T\}$ then $\widehat{k\langle X\rangle} = k[[T]]$ the usual commutative power series ring in one variable with its T-adic filtration. In general, given any $u \in \widehat{\mathfrak{m}}$ there is a unique filtered K-algebra homomorphism

$$ev_u\colon k[[T]] \to \widehat{k\langle X\rangle}$$

sending $T \to u$: since $\widehat{v}(\lambda_n u^n) \geqslant n$ for all $\lambda_n \in K$ and $n \in \mathbf{N}_0$, Exercise 3.15 shows that $ev_u\colon f(T) \mapsto f(u)$ is a well-defined filtered algebra homomorphism and uniqueness follows from Example Sheet 1 Q5.

[17] A filtration on a Lie algebra L is a function $v\colon L \to \mathbf{R}^{>0} \cup \{\infty\}$ such that $v(x+y) \geqslant \min(v(x), v(y))$, $v(\lambda x) \geqslant v(x)$ and $v([x,y]) \geqslant v(x) + v(y)$ for all $x, y \in L$ and $\lambda \in k$.

[18] writing $\widehat{L_X}$ to denote the completion of the filtered Lie algebra $\widehat{L_X} = \varprojlim_{\lambda>0} L_X/(L_X)_\lambda$ for $(L_X)_\lambda$ the Lie ideal $\{x \in L \mid v(x) \geqslant \lambda\}$.

Lemma 8.21. *The maps*

$$\exp\colon \widehat{\mathfrak{m}} \to 1+\widehat{\mathfrak{m}}; u \mapsto \sum_{n\geqslant 0} u^n/n!$$

and

$$\log\colon 1+\widehat{\mathfrak{m}} \to \widehat{\mathfrak{m}}; 1+u \mapsto \sum_{n\geqslant 1} (-1)^{n+1}u^n/n$$

are well defined mutual inverses.

Proof. $\exp(u) = ev_u(\exp(T))$ and $\log(1+u) = ev_u(\log(1+T)$ so the maps are well-defined by Remark 8.20. Moreover $\exp(\log(1+u)) = ev_u(\exp(\log(1+T))$ and $\log(\exp(u)) = ev_u(\log(\exp(T))$ so it suffices to solve the following exercise which is a special case of the Lemma. □

Exercise 8.22. Show that the pair of functions $\exp\colon T\mathbf{Q}[[T]] \to 1+T\mathbf{Q}[[T]]$ and $\log\colon 1+T\mathbf{Q}[[T] \to T\mathbf{Q}[[T]]$ are mutual inverses.

Hint: Prove a chain rule for formal differentiation of formal power series in one variable and apply it to $\exp(\log(1+T))$ and $\log(\exp(T))$.

Lemma 8.23. *If $a, b \in \widehat{\mathfrak{m}}$ commute then* $\exp(a+b) = \exp(a)\cdot\exp(b)$.

Proof. We compute

$$\begin{aligned}\exp(a+b) &= \sum_{n\geqslant 0}(a+b)^n/n! \\ &= \sum_{n\geqslant 0}\sum_{i+j=n} a^i/i!b^j/j! \\ &= \exp(a)\exp(b)\end{aligned}$$

as claimed. □

Lemma 8.24. *The comultiplication on $k\langle X\rangle$ extends uniquely to a k-algebra homomorphism*

$$\widehat{\Delta}\colon \widehat{k\langle X\rangle} \to \widehat{k\langle X\rangle \otimes_k k\langle X\rangle}.$$

Moreover

$$\mathcal{P}(\widehat{k\langle X\rangle}) = \{u \in \widehat{k\langle X\rangle} \mid \widehat{\Delta}(u) = u\otimes 1 + 1\otimes u\} = \widehat{L_X}.$$

Proof. If we give $k\langle X\rangle \otimes k\langle X\rangle$ the tensor product filtration then Δ is a morphism of filtered rings since

$$\Delta(k\langle X\rangle_0) = \Delta(k) = k = (k\langle X\rangle \otimes_k k\langle X\rangle)_0$$

and for $n \geqslant 1$

$$\begin{aligned}\Delta(k\langle X\rangle_n) &= \Delta(k\langle X\rangle_1)^n \\ &= (k.\{1\otimes 1, x\otimes 1 + 1\otimes x \mid x\in X)^n \\ &\subset (k\langle X\rangle \otimes_k k\langle X\rangle)_n.\end{aligned}$$

Thus by Example Sheeet 1 Q5 Δ extends as claimed. Moreover if $r = \sum_{n\geqslant 0} r_n \in \widehat{k\langle X\rangle}$ is primitive with each $r_n \in k\langle X\rangle^{(n)}$ then $\widehat{\Delta}(r) = \sum_{n\geqslant 0}\Delta(r_n)$. Since $\Delta(r_n)$ is in degree n in the graded ring $k\langle X\rangle \otimes_k k\langle X\rangle$, each r_n is primitive and so lives in $L_X^{(n)}$ by Theorem 8.8. Thus $r \in \widehat{L_X}$ as claimed. □

Lecture 20

Lemma 8.25. $\mathcal{G} = \mathcal{G}(\widehat{k\langle X\rangle}) = \{r \in \widehat{k\langle X\rangle}^\times \mid \widehat{\Delta}(r) = r \otimes r\}$ *is a subgroup of the multiplicative group* $1 + \widehat{\mathfrak{m}}$.

Proof. If $r = r_0 + x \in \mathcal{G}$ with $r_0 \in k^\times$ and $x \in \widehat{m}$ then

$$r_0 \otimes r_0 = \sigma(r \otimes r) = \sigma(\widehat{\Delta}(r)) = \sigma(\Delta(r_0) + \widehat{\Delta}(x)) = r_0 \otimes 1$$

so $r_0^2 = r_0$ and $r_0 = 1$.

Suppose that $r, s \in \mathcal{G}$ then

$$\widehat{\Delta}(rs) = \widehat{\Delta}(r)\widehat{\Delta}(s) = (r \otimes r)(s \otimes s) = rs \otimes rs$$

so $rs \in \mathcal{G}$. Moreover

$$\Delta(r^{-1}) = \Delta(r)^{-1} = (r \otimes r)^{-1} = r^{-1} \otimes r^{-1}$$

so $r^{-1} \in \mathcal{G}$. Finally $1 \in \mathcal{G}$ and we're done. □

Proposition 8.26. exp *restricts to a bijection*

$$\widehat{L_X} \to \mathcal{G}.$$

Proof. Suppose $u \in \widehat{L_X}$. Since $1 \otimes u$ and $u \otimes 1$ commute in $k\langle X\rangle \widehat{\otimes_k} k\langle X\rangle$,

$$\widehat{\Delta}(\exp(u)) = \exp(\widehat{\Delta}(u)) = (\exp(u) \otimes 1)(1 \otimes \exp(u)) = \exp(u) \otimes \exp(u)$$

i.e. $\exp(\widehat{L_X}) \subseteq \mathcal{G}$. Similarly if $v \in \mathcal{G}$ there is some $u \in \widehat{\mathfrak{m}}_X$ such that $\exp(u) = v$. Then

$$\begin{aligned} \widehat{\Delta}(u) &= \widehat{\Delta}(\log v) \\ &= \log(\widehat{\Delta}(v)) \\ &= \log(\exp(u) \otimes \exp(u)) \\ &= u \otimes 1 + 1 \otimes u. \end{aligned}$$

Thus $u \in \widehat{L_X}$ and $\exp(\widehat{L_X}) = \mathcal{G}$. □

Definition 8.27. The *Hausdorff series* in variables U, V is

$$\Phi(U, V) = \log(\exp(U)\exp(V)) \in \mathbf{Q}\widehat{\langle U, V\rangle}.$$

We will write $\Phi_n(U, V) \in \widehat{L_{\{U,V\}}}$ for the nth homogeneous component of $\Phi(U, V)$ for $n \geqslant 1$.

Exercise 8.28. Compute directly that $\Phi_1(U, V) = U + V$, $\Phi_2(U, V) = \frac{1}{2}[U, V]$ and

$$\Phi_3(U, V) = \frac{1}{12}([U, [U, V]] + [V, [V, U]]).$$

We will find an easier way to do these computations.

Corollary 8.29 (Campbell–Hausdorff)**.**

$$\Phi(U, V) \in \widehat{L_{\{U,V\}}} \subset \widehat{k\langle U, V\rangle}.$$

Proof. Let $X = \{U, V\}$. Then $U, V \in \widehat{L_X}$ so $\exp(U)$ and $\exp(V)$ are in $\mathcal{G}(\widehat{k\langle X\rangle})$ by Proposition 8.26 and so $\exp(U)\exp(V) \in \mathcal{G}(\widehat{k\langle X\rangle})$ by Lemma 8.25. Thus $\Phi(U, V) = \log(\exp(U)\exp(V)) \in \widehat{L_X}$ by Proposition 8.26 again. □

Lemma 8.30. *Let $\mathfrak{m} = k\langle X\rangle_1$ and define a k-linear map $\alpha\colon \mathfrak{m} \to L_X$ by linearly extending*

$$\alpha(x_1 \cdots x_n) = [x_1, [x_2, [\cdots, [x_{n-1}, x_n] \cdots]]] \in L_X^{(n)}$$

for $x_1, \ldots, x_n \in X$ and let $\theta\colon U(L_X) \to \mathrm{End}_k(L_X)$ be the extension to $U(L_X)$ of the adjoint representation $\mathrm{ad}\colon L_X \to \mathrm{End}_k(L_X)$. *Then*

$$\alpha(uv) = \theta(u)\alpha(v)$$

for all u in $U(L_X)$ and $v \in \mathfrak{m}$.

Proof. Since α and θ are k-linear we may assume that $u = x_1 \cdots x_n$ with $x_i \in X$. We proceed by induction on n. If $n = 0, 1$ the result is immediate.

Suppose that $n > 1$. Then

$$\alpha(x_1 \cdots x_n v) = \theta(x_1)\alpha(x_2 \cdots x_n v) = \theta(x_1)\theta(x_2 \cdots x_n)\alpha(v) = \theta(u)\alpha(v)$$

by the induction hypothesis and because θ is a ring homomorphism. □

Proposition 8.31. *$\alpha(u) = nu$ for all $u \in L_X^{(n)}$ and $n \geqslant 1$.*

Proof. Again by induction on n. When $n = 1$ the result is clear as $L_X^{(1)}$ is spanned by X. If $u \in L_X^{(n)}$ for some $n > 1$ then u is a sum of terms $\sum[a_i, b_i]$ with $a_i, b_i \in L_X$, $\deg a_i + \deg b_i = n$ and $\deg a_i, \deg b_i < n$. By linearity we can reduce to the case $u = [a, b]$.

Now

$$\alpha([a,b]) = \alpha(ab) - \alpha(ba) = \theta(a)\alpha(b) - \theta(b)\alpha(a) = \deg(b)\theta(a)(b) - \deg(a)\theta(b)a$$

by the induction hypothesis. But

$$\deg(b)\theta(a)(b) - \deg(a)\theta(b)a = \deg(b)[a,b] - \deg(a)[b,a] = n[a,b]$$

as required. □

Corollary 8.32. *The map $\phi\colon \mathfrak{m} \to L_X$ given by $\phi(\sum_{n\geqslant 1} x_n) = \sum_{n\geqslant 1} \frac{1}{n}\alpha(x_n)$ for $x_n \in k\langle X\rangle^{(n)}$ is a projection onto L_X.*

Proof. If $\sum x_n \in L_X$ then $x_n \in L_X^{(n)}$ so $\alpha(x_n) = nx_n$ and the result follows easily. □

Notation 8.33. Given $p, q \in \mathbf{N}_0$ and $m \in \mathbf{N}$ let $S_{p,q}^m$ denote the set of $2m$-tuples $(i_1, \ldots, i_m, j_1, \ldots, j_m) \in \mathbf{N}_0^{2m}$ such that $i_1 + \cdots + i_m = p$, $j_1 + \cdots + j_m = q$ and $i_k + j_k \geqslant 1$ for $k = 1, \ldots, m$.

Theorem 8.34 (Dynkin)**.** *For $p, q \in \mathbf{N}_0$. Write*

$$\Phi_{p,q}^{m,1}(U,V) = \sum_{\substack{(\mathbf{i},\mathbf{j})\in S_{p,q}^m \\ j_m = 1}} \frac{\mathrm{ad}(U)^{i_1}\,\mathrm{ad}(V)^{j_1}\cdots\mathrm{ad}(U)^{i_m}(V)}{i_1!j_1!\cdots i_m!j_m!}$$

and

$$\Phi_{p,q}^{m,2}(U,V) = \sum_{\substack{(\mathbf{i},\mathbf{j})\in S_{p,q}^m \\ i_m = 1, j_m = 0}} \frac{\mathrm{ad}(U)^{i_1}\,\mathrm{ad}(V)^{j_1}\cdots\mathrm{ad}(V)^{j_{m-1}}(U)}{i_1!j_1!\cdots i_m!j_m!}.$$

Then

$$\Phi_n(U,V) = \frac{1}{n}\sum_{m=1}^{n} \frac{(-1)^{m+1}}{m}\left(\sum_{p+q=n} \Phi_{p,q}^{m,1}(U,V) + \Phi_{p,q}^{m,2}(U,V)\right).$$

Proof. By definition

$$\Phi(U,V) = \log(\exp(U)\exp(V)) = \sum_{m\geqslant 1} \frac{(-1)^{m+1}}{m} \left(\sum_{i+j\geqslant 1} \frac{U^i}{i!}\frac{V^j}{j!} \right)^m$$

so

$$\Phi_n(U,V) = \sum_{m\geqslant 1} \frac{(-1)^{m+1}}{m} \sum_{p+q=n} \left(\sum_{(\mathbf{i},\mathbf{j})\in S^m_{p,q}} \frac{U^{i_1}}{i_1!}\frac{V^{j_1}}{j_1!}\cdots\frac{U^{i_m}}{i_m!}\frac{V^{j_m}}{j_m!} \right)$$

Now

$$\alpha(U^{i_1}V^{j_1}\cdots U^{i_m}V^{j_m}) = \begin{cases} \operatorname{ad}(U)^{i_1}\operatorname{ad}(V)^{j_1}\cdots\operatorname{ad}(V)^{j_m-1}(V) & \text{if } j_m \geqslant 1 \\ \operatorname{ad}(U)^{i_1}\operatorname{ad}(V)^{j_1}\cdots\operatorname{ad}(U)^{i_m-1}(U) & \text{if } j_m = 0. \end{cases}$$

These values are zero unless $j_m = 1$ or $j_m = 0$ and $i_m = 1$ since

$$\operatorname{ad}(U)(U) = \operatorname{ad}(V)(V) = 0.$$

Thus as $\Phi_n(U,V) \in L^{(n)}_{\{U,V\}}$ and $S^m_{p,q} = \emptyset$ if $m > p+q$, $\Phi_n(U,V) = \frac{1}{n}\alpha(\Phi_n(U,V))$ is given by the required formula. □

Lecture 21

9. p-adic Lie Theory

Definition 9.1. A (descending) **R**-filtration on a ring R is a function

$$v\colon R \to \mathbf{R}^{\geqslant 0} \cup \{\infty\}$$

that satisfies the usual defining properties[19] of a filtration as in Definiton 2.1. In particular $(R_0 = \{r \in R \mid v(r) \geqslant 0\}, v|_{R_0})$ is a filtered ring in the sense of Definition 2.1. Such a filtration is a *valuation* if $v(ab) = v(a)v(b)$ for all $a, b \in R$.

As in section 5 here we suppose that $\mathcal{O}$ is a complete discrete valuation ring with uniformiser p and K will denote its field of fractions[20] equipped with the valuation v_p such that $K_0 = \mathcal{O}$ and $v_p(p) = 1$.

9.1. Some p-adic estimates.

Lemma 9.2. *Let* $n = \sum_{i=0}^k a_i p^i \in \mathbf{N}$ *with* $a_0, \ldots, a_k \in \{0, 1, \ldots, p-1\}$ *and let* $s(n) = \sum a_i$. *Then*

$$v_p(n!) = \frac{n - s(n)}{p-1} \leqslant \frac{n}{p-1}$$

Proof.

$$\begin{aligned} v_p(n!) &= \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots \lfloor n/p^k \rfloor \\ &= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots a_k(p^{k-1} + p^{k-2} + \cdots + 1) \\ &= \sum_{i=0}^k a_i \frac{(p^i - 1)}{p-1} \\ &= \frac{n - s(n)}{p-1} \end{aligned}$$

[19] conditions (a)-(d) of Definition 2.1

[20] which can be viewed as $\mathcal{O}$ localised at $\{p^n \mid n \in \mathbf{N}_0\}$

as required. □

Lemma 9.3. *$v_p(n) < \log_p(n) + 1$ for all $n \in \mathbf{N}$.*

Proof. Let $k \in \mathbf{N}$ such that $p^k \leqslant n < p^{k+1}$. Then $v_p(n) < k+1$ and $k \leqslant \log_p(n)$. □

Definition 9.4. A *Banach K-algebra* is an associative K-algebra A equipped with a filtration $w\colon A \to \mathbf{R} \cup \{\infty\}$ such that

(1) $w(\lambda a) = v_p(\lambda) + w(a)$ for all $\lambda \in K$ amd $a \in A$.
(2) A_0 is complete with respect to $w|_{A^0}$ i.e. $A_0 \cong \varprojlim_{\lambda>0} A_0/A_\lambda$. A *morphism* $(A, w) \to (B, w')$ *of Banach K-algebras* is a filtered K-algebra homomorphism $A \to B$.

Proposition 9.5. *Suppose A is a Banach K-algebra and let $I = A_{(1/p-1)^+}$ and $\mathfrak{m} = A_{0^+}$.*

(a) $\exp\colon I \to 1 + \mathfrak{m}$ *converges.*
(b) $\log\colon 1 + \mathfrak{m} \to A$ *converges.*
(c) $\Phi\colon I^2 \to A$ *converges.*

Proof. (a) Let $x \in I$. Then $w(x^n/n!) = w(x^n) - v_p(n!) \geqslant nw(x) - \frac{n}{p-1} \to \infty$ as $n \to \infty$ since $w(x) > 1/p - 1$. Moreover $w(x^n/n!) > 0$ for all $n \geqslant 1$ for the same reason. Thus $\sum x^n/n! \in A_0$ by Notation 3.14.

(b) Let $x \in \mathfrak{m}$. Then $w(x^n/n) = w(x^n) - v(n) \geqslant nw(x) - \log_p(n) - 1 \to \infty$ as $n \to \infty$ since $w(x) > 0$. Thus $\log(1 + x)$ converges.

(c) Let $x, y \in I$. Let $t = \min(w(x), w(y)) > 1/(p-1)$. Then

$$\Phi_n(x,y) = \sum_{m=1}^{n} \frac{(-1)^{m+1}}{m} \sum_{a+b=n} \left(\sum_{(\mathbf{i},\mathbf{j}) \in S^m_{a,b}} \frac{x^{i_1}}{i_1!}\frac{y^{j_1}}{j_1!} \cdots \frac{x^{i_m}}{i_m!}\frac{y^{j_m}}{j_m!} \right).$$

Now

$$\begin{aligned} w(x^{i_1}y^{j_1}\cdots x^{i_m}y^{j_m}) &\geqslant nt, \\ v_p(1/m) &\geqslant -\log_p(m) - 1 \text{ and} \\ v_p\left(\frac{1}{i_1!j_1!\cdots i_m!j_m!}\right) &= v_p\left(\binom{n}{i_1, \cdots, j_m}\right) - v_p(n!) \\ &\geqslant -\frac{n}{p-1} \end{aligned}$$

since $\binom{n}{i_1, j_1, \cdots, j_m} \in \mathbf{N}$. Thus $w(\Phi_n(x,y)) \geqslant n(t - \frac{1}{p-1}) - \log_p(n) - 1 \to \infty$ as $n \to \infty$ and so $\sum_{n \geqslant 1} \Phi_n(x,y)$ converges. □

Exercise 9.6. With the notation of Proposition 9.5 show that

(a) $\exp(\log(1 + x)) = 1 + x$ for all $x \in I$;
(b) $\log(\exp(x)) = x$ for all $x \in I$ and
(c) $\Phi(x, y) = \log(\exp(x)\exp(y))$ for all $x, y \in I$.

9.2. **The Banach algebra associated to $\mathcal{O}G$.** Now we consider a complete p-valued group (G,ω) of finite rank with ordered basis $(g_1,\dots,g_d)$. We recall, Remark 6.24, that

$$\mathcal{O}G = \left\{ \sum_{\alpha\in\mathbf{N}_0^d} \lambda_\alpha \mathbf{b}^\alpha \mid \lambda_\alpha \in \mathcal{O} \right\}$$ [21]

has valuation v given by

$$v\left(\sum \lambda_\alpha \mathbf{b}^\alpha\right) = \min_{\alpha\in\mathbf{N}_0^d} \left\{ v_p(\lambda_\alpha) + \sum_{i=1}^d \alpha_i \omega(g_i) \right\}$$

Notation 9.7. We write KG to denote the K-algebra $K\otimes_{\mathcal{O}} \mathcal{O}G = \mathcal{O}G[1/p]$. [22]

Since $\mathcal{O}G$ has no p-torsion we may view it as a subring of KG. Moreover the elements of KG can be viewed as sums $\sum_{\alpha\in\mathbf{N}_0^d}\lambda_\alpha\mathbf{b}^\alpha$ with each $\lambda_\alpha\in K$ and $\{v_p(\lambda_\alpha)\mid \alpha\in\mathbf{N}_0^d\}\subset\mathbf{R}$ bounded below.

Lemma 9.8. *The valuation v on $\mathcal{O}G$ extends uniquely to a valuation*

$$w\colon KG\to \mathbf{R}\cup\{\infty\}$$

such that $w(\lambda r) = v_p(\lambda) + w(r)$ for all $\lambda\in K$ and $r\in KG$.

Proof. Suppose that w is such an extension of v to KG. For $r\in KG$ there is $n\in\mathbf{N}$ such that $p^n r\in\mathcal{O}G$. Then

$$w(r) = v_p(p^{-n}) + v(p^n r) = v(p^n r) - n$$

so such a w is necessarily unique. It is straightforward to verify that if we define $w(r)$ to be $v_p(p^{-n})+v(p^n r)$ for $n\in\mathbf{N}$ such that $p^n r\in\mathcal{O}G$, the definition does not depend on the choice of n and does define a valuation on KG extending v. □

Remark 9.9. $\mathcal{O}G$ is a subring of KG_0 but these are not equal unless G is trivial. For example $p^{-1}b_1^n\in KG_0\backslash\mathcal{O}G$ if $n\omega(g_1)\geqslant 1$.

Notation 9.10. We will write $\widehat{KG}$ to denote the completion of KG with respect to w. That is

$$\widehat{KG} = \left(\varprojlim_{\lambda>0} KG_0/KG_\lambda\right)[1/p].$$

Thus $\widehat{KG}$ is a Banach K-algebra whose elements may be viewed as convergent sums

$$\sum_{\alpha\in\mathbf{N}_0^d}\lambda_\alpha\mathbf{b}^\alpha \text{ with each } \lambda_\alpha\in K \text{ and } v_p(\lambda_\alpha)+\sum\alpha_i\omega(g_i)\to\infty \text{ as } |\alpha|\to\infty$$

and

$$\widehat{w}\left(\sum_{\alpha\in\mathbf{N}_0^d}\lambda_\alpha\mathbf{b}^\alpha\right) = \min_{\alpha\in\mathbf{N}_0^d}\left\{v_p(\lambda_\alpha)+\sum\alpha_i\omega(g_i)\right\}.$$

[21] For $b_i = g_i - 1$

[22] This is inconsistent with Definition 6.13 and so replaces it in this case.

Lecture 22

Definition 9.11. We say that G is *p-saturated* if for all $g \in G$ with $\omega(g) > \frac{p}{p-1}$ there is $h \in G$ with $h^p = g$.

Note that there is a sequence of natural inclusion maps

$$G \to \mathcal{O}[G] \to \mathcal{O}G \to KG \to \widehat{KG}$$

and that for $g \in G$,

$$\widehat{w}(g-1) = w(g-1) = v(g-1) \geqslant \omega(g) > \frac{1}{p-1}.$$

Thus by Proposition 9.5 and Exercise 9.6, $\log(g)$ converges in $\widehat{KG}$ and

$$\exp\log(g) = g.$$

Proposition 9.12. *If G is p-saturated then $\log G$ is a $\mathbf{Z}_p$-Lie subalgebra of $\widehat{KG}$.*

Proof. Suppose that $u = \log g$ and $v = \log h$ are in $\log G$. By Lemma 3.6(b) for each $n \in \mathbf{N}$, $\omega(g^{p^n}h^{p^n}) = \omega(gh)+n$. So since G is p-saturated there is some $x_n \in G$ such that $g^{p^n}h^{p^n} = x_n^{p^n}$.

Then

$$p^n \log x_n = \log(g^{p^n}h^{p^n}) = \log(\exp(p^n u)\exp(p^n v)) = \Phi(p^n u, p^n v)$$

by Exercise 9.6(c). So

$$\begin{aligned} \log(x_n) &= u + v + \sum_{k\geqslant 2} p^{-n}\Phi_k(p^n u, p^n v) \\ &= u + v + \sum_{k\geqslant 2} p^{(k-1)n}\Phi_k(u,v) \\ &\to u + v \qquad \text{as } n \to \infty \end{aligned}$$

Since G is compact and $\log|_G$ is continuous, $\log G$ is compact and so closed in $\widehat{KG}$. Thus $u + v = \lim_{n\to\infty} x_n \in \log G$ and $\log G$ is closed under $+$.

If $\lambda \in \mathbf{Z}_p$ then by continuity of log, $\log(g^\lambda) = \lambda u$ so $\log G$ is a $\mathbf{Z}_p$-submodule of $\widehat{KG}$.

Writing

$$\begin{aligned} \Psi(X,Y) &= \log(\exp(-X)\exp(-Y)\exp(X)\exp(Y)) \\ &= \Phi(-X, \Phi(-Y, \Phi(X,Y))) \end{aligned}$$

for the *commutator Campbell-Baker-Hausdorff series* we see that

$$\Psi(X,Y) = XY - YX + \sum_{k\geqslant 3} \Psi_k(X,Y);$$

where Ψ_k denotes the homogeneous degree k part of Ψ. Thus by a similar argument to the above

$$\log(g^{-p^n}h^{-p^n}g^{p^n}h^{p^n}) = \Psi(p^n u, p^n v) \in p^{2n}[u,v] + \widehat{KG}_{3n+w(u)+w(v)}.$$

In particular $\omega\left((g^{p^n}, h^{p^n})\right) > 2n + \frac{1}{p-1}$ so there exists $y_n \in G$ such that

$$y_n^{p^{2n}} = (g^{p^n}, h^{p^n})$$

By a similar argument to the above $\lim_{n\to\infty} \log y_n = [u,v]$ and so $[u,v] \in \log G$. $\square$

Exercise 9.13. Show that there is a canonical functor from the category of complete p-valued groups of finite rank to the category of K-Banach algebras that sends G to $\widehat{KG}$ and such that each natural diagram

$$\begin{array}{ccc} H & \longrightarrow & G \\ \downarrow & & \downarrow \\ \widehat{KH} & \longrightarrow & \widehat{KG} \end{array}$$

commutes.

Exercise 9.14. Show that if we equip $G \times G$ with the filtration

$$\omega_{G\times G}((g,h)) = \min(\omega(g), \omega(h))$$

then $(G \times G, \omega)$ is a complete p-valued group with $\operatorname{gr}(G \times G) \cong \operatorname{gr} G \times \operatorname{gr} G$.

It follows from these two exercises that there are natural morphisms

$$\iota_1, \iota_2, \Delta\colon \widehat{KG} \to K\widehat{(G \times G)}$$

associated to the morphisms of filtered groups $\iota_1, \iota_2, \Delta\colon G \to G \times G$ such that $\iota_1(g) = (g, e_G)$, $\iota_2(g) = (e_G, g)$ and $\Delta(g) = (g, g)$ and a natural morphism

$$\epsilon\colon \widehat{KG} \to K$$

associated to the morphism of filtered groups $G \to \{e\}$.

Definition 9.15. Let

$$\mathcal{G}(\widehat{KG}) = \{x \in \widehat{KG} \mid \Delta(x) = \iota_1(x)\iota_2(x)\}$$

and

$$\mathcal{P}(\widehat{KG}) = \{x \in \widehat{KG} \mid \Delta(x) = \iota_1(x) + \iota_2(x)\}.$$

Exercise 9.16. Show that $\mathcal{G}(\widehat{KG})$ is a subgroup of $\widehat{KG}^\times$ containing the image of G in $\widehat{KG}$ and that $\mathcal{P}(\widehat{KG})$ is a Lie K-subalgebra of $\widehat{KG}$ equipped with its commutator bracket. Finally show that exp restricts to a bijection

$$\mathcal{P}(\widehat{KG}) \cap \widehat{KG}_{\frac{1}{p-1}+} \to \mathcal{G}(\widehat{KG}) \cap \left(1 + \widehat{KG}_{\frac{1}{p-1}+}\right)$$

with inverse log.

Definition 9.17. The *Lie algebra of* G is $\mathcal{L}(G) = \mathcal{P}(\widehat{\mathbf{Q}_p G})$ with its natural Lie structure.

Theorem 9.18. *Let* $u_i = \log(g_i) \in \widehat{\mathbf{Q}_p G} \subset \widehat{KG}$. *Then* $\{u_1, \dots, u_d\}$ *is a* K*-basis for* $\mathcal{P}(\widehat{KG})$ *and*

$$w\left(\sum_{i=1}^{d} \lambda_i u_i\right) = \min_{1 \leqslant i \leqslant d} \{v_p(\lambda_i) + \omega(g_i)\}$$

for $\lambda_1, \dots, \lambda_d \in K$.

Corollary 9.19. *If* G *is* p*-saturated then*

$$\log G = \mathcal{L}(G)_{\frac{1}{p-1}+} = \bigoplus_{i=1}^{d} \mathbf{Z}_p u_i$$

Proof. The g_i cannot be pth powers by Exercise 3.34 and so each $\omega(g_i) \leqslant \frac{p}{p-1}$ since G is p-saturated. Thus by Theorem 9.18 for $\lambda_1, \dots, \lambda_d \in \mathbf{Q}_p$, $w\left(\sum \lambda_i u_i\right) > \frac{1}{p-1}$ if and only if each $v_p(\lambda_i) \geqslant 0$; i.e. precisely if each $\lambda_i \in \mathbf{Z}_p$. This establishes the second equality.

Now each $u_i \in \log G$ so Proposition 9.12 gives that $\sum \mathbf{Z}_p u_i \subseteq \log G$.

Suppose that

$$g \in G \subset \mathcal{G}(\widehat{\mathbf{Q}_p G}) \cap (1 + \widehat{\mathbf{Q}_p G}_{\frac{1}{p-1}^+}).$$

Then $\log g \in \mathcal{L}(G)_{\frac{1}{p-1}^+}$ by Exercise 9.16. Thus $\log G \subseteq \mathcal{L}(G)_{\frac{1}{p-1}^+}$. □

Corollary 9.20. *If G is p-saturated then there is a natural isomorphism of $\mathbf{Q}_p$ Lie algebras*

$$\mathcal{L}(G) \cong \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \log G.$$

Corollary 9.21. *If G is p-saturated then the group operation on G is given by the Campbell–Hausdorff formula:*

$$gh = \exp(\Phi(\log g, \log h)) \in \widehat{\mathbf{Q}_p G}.$$

Proof. For $g, h \in G$, $\log g, \log h \in \mathcal{L}(G)_{\frac{1}{p-1}^+}$ so

$$\Phi(\log g, \log h) = \log\left(\exp(\log g)\exp(\log h)\right) = \log(gh)$$

by Exercise 9.6. But $\log(gh) \in \log G = \mathcal{L}(G)_{\frac{1}{p-1}^+}$ so $\exp \Phi(\log g, \log h)$ converges to gh by Exercise 9.6 again. □

Lecture 23

Proof of Theorem 9.18. Suppose $z = \sum_{i=1}^{d} \lambda_i u_i$. Then as $u_i = \log(g_i) = \log(1 + b_i)$ we see that

$$z = \sum_{i=1}^{d} \sum_{n \geqslant 1} \lambda_i \frac{(-1)^{n+1}}{n} b_i^n.$$

Thus

$$\begin{aligned} w(z) &= \min_{\substack{1 \leqslant i \leqslant d \\ n \geqslant 1}} \{v_p(\lambda_i/n) + n\omega(g_i)\} \\ &= \min_{1 \leqslant i \leqslant d} \left\{ v_p(\lambda_i) + \min_{n \geqslant 1} \{n\omega(g_i) - v_p(n)\} \right\} \\ &= \min_{1 \leqslant i \leqslant d} \{v_p(\lambda_i) + \omega(g_i)\} \end{aligned}$$

Thus $u_1, \dots, u_d$ are linearly independent over K.

It remains to show that every element of $\mathcal{P}(\widehat{KG})$ is in the span of $u_1, \dots, u_n$. So suppose that $z = \sum \lambda_\alpha \mathbf{b}^\alpha \in \mathcal{P}(\widehat{KG})$. We compute that

$$\begin{aligned} \Delta(b_i^n) &= \Delta(g_i - 1)^n = (\iota_1(1 + b_i)\iota_2(1 + b_i) - 1)^n \\ &= (\iota_1(b_i) + \iota_2(b_i) + \iota_1(b_i)\iota_2(b_i))^n \\ &= \sum_{j+k+l=n} \binom{n}{j,k,l} \iota_1(b_i)^{j+l} \iota_2(b_i)^{k+l} \\ &= \sum_{\substack{a,b \leqslant n \\ a+b \geqslant n}} \binom{n}{n-b, n-a, a+b-n} \iota_1(b_i)^a \iota_2(b_i)^b; \end{aligned}$$

where $a = j + l$ and $b = k + l$ so $a + b = n + l$. Thus

$$\begin{aligned}\Delta(z) &= \sum_{\alpha\in\mathbf{N}_0^d} \lambda_\alpha \sum_{\substack{\beta,\gamma\leqslant\alpha\\ \beta+\gamma\geqslant\alpha}} \binom{\alpha}{\alpha-\beta,\alpha-\gamma,\beta+\gamma-\alpha} \iota_1(\mathbf{b}^\beta)\iota_2(\mathbf{b}^\gamma)\\ &= \iota_1(z) + \iota_2(z)\\ &= \sum_{\beta\in\mathbf{N}_0^d} \lambda_\beta \iota_1(\mathbf{b}^\beta) + \sum_{\gamma\in\mathbf{N}_0^d} \lambda_\gamma \iota_2(\mathbf{b}^\gamma).\end{aligned}$$

Equating constant coefficients we get $\lambda_0 = \lambda_0 + \lambda_0 = 0$. Equating $\iota_1(\mathbf{b}^\beta)\iota_2(\mathbf{b}^\gamma)$ coefficients when $\beta = e_i$ and $\gamma \neq 0$ arbitrary we see that the pairs of conditions $\beta, \gamma \leqslant \alpha$ and $\beta + \gamma \geqslant \alpha$ is equivalent to $\alpha_i \geqslant 1$ and $\alpha = \gamma$ or $\gamma + e_i$. Thus

$$\lambda_\gamma \binom{\gamma}{\gamma - e_i} + \lambda_{\gamma+e_i} \binom{\gamma + e_i}{\gamma} = 0$$

i.e. $\lambda_{\gamma+e_i} = -\frac{\gamma_i}{\gamma_i+1}\lambda_\gamma$ for each $1 \leqslant i \leqslant d$ and $\gamma \in \mathbf{N}_0^d$ with $\gamma_i \geqslant 1$; and $\lambda_{\gamma+e_i} = 0$ if $\gamma \neq 0$ but $\gamma_i = 0$.

In particular $\lambda_{ne_i} = \frac{(-1)^{n+1}}{n}\lambda_{e_i}$ and $\lambda_\gamma = 0$ if there are $i \neq j$ with $\gamma_i, \gamma_j \geqslant 1$.

Thus $z = \sum_{i=1}^d \lambda_{e_i} \sum_{n\geqslant 1} \frac{(-1)^{n+1}}{n} b_i^n$ as required. □

Definition 9.22. Suppose that $\mathfrak{g}$ is a Lie algebra over $\mathcal{O}$ that is free of finite rank. We can filter $U(\mathfrak{g})$ p-adically so that

$$v(\alpha) = \sup\{n \in \mathbf{N}_0 \mid \alpha \in p^n U(\mathfrak{g})\}$$

The *affinoid enveloping algebra* of $\mathfrak{g}$ is

$$\widehat{U(\mathfrak{g}_K)} = K \otimes_{\mathcal{O}} \widehat{U(\mathfrak{g})}.$$

There is a unique way to define a filtration $\widehat{v_K}$ extending $\widehat{v}$ on $\widehat{U(\mathfrak{g})}$ that will make $\widehat{U(\mathfrak{g}_K)}$ is a K-Banach algebra

Example 9.23. If $\mathfrak{g} = \mathfrak{sl}_2(\mathcal{O}) = \mathcal{O}e \oplus \mathcal{O}h \oplus \mathcal{O}f$ then elements of $\widehat{U(\mathfrak{g}_K)}$ can be written uniquely as convergent sums $\sum_{i,j,k\in\mathbf{N}_0} \lambda_{ijk} f^i h^j e^k$ with each $\lambda_{ijk} \in K$ and $v_p(\lambda_{ijk}) \to \infty$ as $i + j + k \to 0$.

Theorem 9.24. *Suppose that p is odd, G is p-saturated, and that $\omega(g_i) = 1$ for $i = 1, \dots, d$. Let*

$$\mathfrak{g} = \{x \in \mathcal{P}(\widehat{KG}) \mid w(x) \geqslant 0\}.$$

Then $\mathfrak{g}$ is an $\mathcal{O}$-Lie algebra free of finite rank over $\mathcal{O}$ and there is an isomorphism of Banach algebras

$$\widehat{U(\mathfrak{g}_K)} \xrightarrow{\sim} \widehat{KG}.$$

Proof. By Theorem 9.18, $\mathcal{P}(\widehat{KG}) = \bigoplus_{i=1}^d Ku_i$ and, writing $x = \sum_{i=1}^d \lambda_i u_i$ with $\lambda_i \in K$,

$$w(x) = \min_{1\leqslant i\leqslant d}\{v(\lambda_i) + \omega(g_i)\}.$$

Thus, as $\omega(g_i) = 1$ for all i, $w(x) \geqslant 0$ if and only if $v(\lambda_i) \geqslant -1$ for each $i = 1, \dots, d$.

Then $w(x) \geqslant 0$ if and only if $\lambda_i \in p^{-1}\mathcal{O}$ for $1 \leqslant i \leqslant d$ i.e. $(u_1/p, \dots, u_d/p)$ is an $\mathcal{O}$-module basis for $\mathfrak{g}$.

Since for $x, y \in \mathfrak{g}$, $w([x, y]) \geqslant w(x) + w(y) \geqslant 0$ we see that $\mathfrak{g}$ is an $\mathcal{O}$-Lie-subalgebra of $\mathcal{P}(\widehat{KG})$. Thus the universal property of the universal enveloping

algebra induces an $\mathcal{O}$-algebra map $U(\mathfrak{g}) \to (\widehat{KG})_0$. Since this is a filtered $\mathcal{O}$-algebra map and $(\widehat{KG})_0$ is complete, this in turn extends to a filtered $\mathcal{O}$-algebra map

$$\widehat{U(\mathfrak{g})} \to (\widehat{KG})_0$$

and thence to a morphism of K-Banach algebras

$$\varphi\colon \widehat{U(\mathfrak{g})_K} \to \widehat{KG}.$$

We must show that this is an isomorphism of Banach algebras.

Since for $g \in G$,

$$\widehat{w}(g-1)^m/m) \geqslant m\omega(g) - v_p(m)$$

we see that

$$\log g = \sum_{m \geqslant 1} \frac{(-1)^{m+1}}{m}(g-1)^m \in \mathcal{P}(\widehat{KG}) \cap (\widehat{KG})_{\omega(g)}.$$

Thus $\log g \in p^{\omega(g)}\mathfrak{g} \subseteq p\mathfrak{g}$ and

$$G \to \widehat{U(\mathfrak{g})}^\times; \qquad g \mapsto \exp(\log g)$$

converges by Proposition 9.5 with $\widehat{v}(\exp\log(g)) \geqslant \omega(g)$.

Since

$$\exp(\log g)\exp(\log h) = \exp\log(gh) \in \widehat{U(\mathfrak{g})}^\times,$$

the universal property of $\mathcal{O}[G]$, i.e. Example Sheet 2 Q10, shows that this extends to a filtered ring map $\mathcal{O}[G]$ to $\widehat{U(\mathfrak{g})}$. Since the latter is complete, this extends a filtered ring map $\mathcal{O}G \to \widehat{U(\mathfrak{g})}$ and thence to a filtered ring map $KG \to \widehat{U(\mathfrak{g})_K}$, and finally to a morphism of K-Banach algebras

$$\psi\colon \widehat{KG} \to \widehat{U(\mathfrak{g})_K}$$

Since

$$\varphi\psi(g_i) = \varphi(\exp(\log(g_i)) = \exp(\varphi(\log g_i)) = \exp(\varphi(u_i)) = g_i$$

for $i = 1, \ldots, d$. By various universal properties $\varphi\psi = \mathrm{id}_{\widehat{KG}}$. Similarly

$$\psi\varphi(u_i) = \psi(u_i) = \psi(\log(g_i)) = \log(\psi(g_i)) = \log(\exp(\log(g_i))) = \log(g_i) = u_i$$

and by various other universal properties $\psi\varphi = \mathrm{id}_{\widehat{U(\mathfrak{g})_K}}$

□

Exercise 9.25. Repeat this argument in the case $p = 2$, G is p-saturated and $\omega(g_i) = 2$ for each $i = 1, \ldots, d$.

Exercise 9.26. Show that the conditions of Theorem 9.24 (resp. Exercise 9.25) are satisfied when $G = GL_n^1(\mathbf{Z}_p)$ (resp $G = GL_n^2(\mathbf{Z}_2)$) with respect to its usual p-valuation.

Exercise 9.27 (Harder)**.** Show that $\mathcal{G}(\widehat{KG}) \cap (1+\widehat{KG})_{\frac{1}{p-1}^+}$ is always a p-saturated complete p-valued group of the same rank of G and that G is isomorphic to an open subgroup of it.