

Noncommutative Rings

Konstantin Ardakov

January 2018

All rings in this course are associative and have an identity element 1, but are not necessarily commutative. Modules are *left* modules, unless stated otherwise.

1. SOME EXAMPLES OF NONCOMMUTATIVE RINGS

Definition 1.1. Let M be an abelian group, and let

$$\text{End}(M)$$

denote the set of homomorphisms $M \rightarrow M$. It is an additive group under pointwise addition, and a ring under composition. More generally, if M is an R -module for some ring R , then the set

$$\text{End}_R(M)$$

of R -module homomorphisms $M \rightarrow M$ is again an associative ring.

For example, if $M = \mathbb{Z}^n$ is the free abelian group of rank n then $\text{End}(M)$ is the ring $M_n(\mathbb{Z})$ of $n \times n$ -matrices with integer entries. Also, if k is a field and $V = k^n$ then $\text{End}_k(V)$ is the ring $M_n(k)$ of $n \times n$ -matrices with entries in k .

Definition 1.2. Let G be a group and let R be a ring. The *group algebra* RG consists of formal linear combinations

$$\sum_{g \in G} r_g g,$$

where $r_g \in R$ for all $g \in G$ and all but finitely many r_g are zero. Addition and multiplication is given by

$$\begin{aligned} \left(\sum_{g \in G} r_g g\right) + \left(\sum_{g \in G} s_g g\right) &= \sum_{g \in G} (r_g + s_g)g \\ \left(\sum_{h \in G} r_h h\right) \left(\sum_{k \in G} s_k k\right) &= \sum_{g \in G} \left(\sum_{\substack{h, k \in G \\ hk=g}} r_h s_k\right)g. \end{aligned}$$

Recall that a k -linear representation of G is a group homomorphism

$$\varphi : G \rightarrow \text{Aut}_k(V)$$

where V is some vector space over k .

Lemma 1.3. There is a natural bijection between k -linear representations of G and left kG -modules.

Proof. A group homomorphism $\varphi : G \rightarrow \text{Aut}_k(V)$ extends uniquely to a k -algebra homomorphism $\tilde{\varphi} : kG \rightarrow \text{End}_k(V)$, and V may then be regarded as a left kG -module, via $x.v = \tilde{\varphi}(x)(v)$ for all $x \in kG$.

Conversely, if V is a left kG -module, there is a representation $\varphi : G \rightarrow \text{Aut}_k(V)$ given by $\varphi(g)(v) = g.v$ for all $v \in V$. \square

Definition 1.4. A *Lie algebra* over k is a k -vector space \mathfrak{g} , equipped with bilinear map $[\cdot] : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$ satisfying

- (1) $[x, x] = 0$ for all $x \in \mathfrak{g}$ and hence $[y, z] = -[z, y]$ for all $y, z \in \mathfrak{g}$
- (2) $[x, [y, z]] + [y, [z, x]] + [z, [y, x]] = 0$ for all $x, y, z \in \mathfrak{g}$.

Note that this bracket is not associative.

Examples 1.5.

- (1) Any (associative) k -algebra R becomes a Lie algebra under the commutator bracket $[x, y] = xy - yx$.
- (2) $\mathfrak{gl}(V) := \text{End}_k(V)$ with the commutator bracket.
- (3) $\mathfrak{gl}_n(k) := \mathfrak{gl}(k^n) = M_n(k)$ with the commutator bracket.

Definition 1.6. A *representation* of the Lie algebra \mathfrak{g} is a homomorphism $\varphi : \mathfrak{g} \rightarrow \mathfrak{gl}(V)$ for some k -vector space V .

We now wish to find an analogue of the group algebra for representations of Lie algebras.

Definition 1.7. The *free associative algebra* on n generators $k\langle x_1, \dots, x_n \rangle$ is the k -vector space with basis given by all possible products $y_1 \cdots y_m$ where $y_1, \dots, y_m \in \{x_1, \dots, x_n\}$. Multiplication is given by concatenation on basis elements and is extended by k -linearity to the whole of $k\langle x_1, \dots, x_n \rangle$.

Note that $k\langle x_1, \dots, x_n \rangle$ is not finite dimensional over k . For example, if $n = 1$ then $k\langle x \rangle$ has $\{1, x, x^2, \dots\}$ as a basis. In fact $k\langle x \rangle \cong k[x]$, the polynomial algebra. Similarly, $k\langle x, y \rangle$ has as a k -basis the set $\{1, x, y, x^2, xy, yx, y^2, x^3, x^2y, \dots\}$. This algebra is not commutative!

Definition 1.8. The *universal enveloping algebra* $U(\mathfrak{g})$ of the Lie algebra \mathfrak{g} is

$$U(\mathfrak{g}) := k\langle x_1, \dots, x_n \rangle / I$$

where $\{x_1, x_2, \dots, x_n\}$ is a basis for \mathfrak{g} and I is the two-sided ideal of $k\langle x_1, \dots, x_n \rangle$ generated by the set $\{x_i x_j - x_j x_i - [x_i, x_j], 1 \leq i, j \leq n\}$.

For example, if \mathfrak{g} is abelian, then $U(\mathfrak{g})$ is just the polynomial algebra $k[x_1, \dots, x_n]$. This definition can be extended to arbitrary Lie algebras, and does not depend on the choice of basis.

Lemma 1.9. There is a natural bijection between representations of \mathfrak{g} and left $U(\mathfrak{g})$ -modules.

Proof. If $\varphi : \mathfrak{g} \rightarrow \mathfrak{gl}(V)$ is a representation, we make V into a left module over $k\langle x_1, \dots, x_d \rangle$ by setting $(x_{i_1} \cdots x_{i_d}) \cdot v := \varphi(x_{i_1})\varphi(x_{i_2}) \cdots \varphi(x_{i_d})(v)$. Because φ is a Lie algebra homomorphism, we see that $(x_i x_j - x_j x_i) \cdot v = [x_i, x_j] \cdot v$ for all i, j . So the ideal I kills V and therefore V is actually a left $U(\mathfrak{g})$ -module.

Conversely, if V is a $U(\mathfrak{g})$ -module, then there is a k -algebra homomorphism $U(\mathfrak{g}) \rightarrow \text{End}_k(V)$ given by $r \mapsto (v \mapsto r \cdot v)$. We can view it as a Lie homomorphism $U(\mathfrak{g}) \rightarrow \mathfrak{gl}(V)$. The map $\mathfrak{g} \rightarrow U(\mathfrak{g})$ is also a Lie homomorphism, so we get a representation $\varphi : \mathfrak{g} \rightarrow \mathfrak{gl}(V)$ by composing these. \square

We will now introduce a basic example of a *ring of differential operators*.

Definition 1.10. Let k be a field and let $A = k[x_1, \dots, x_n]$. Let $\Delta(A)$ be the k -subalgebra of $\text{End}_k(A)$ generated by the k -linear operators

$$\begin{aligned} \hat{x}_i : A &\rightarrow A & \text{and} & & \frac{\partial}{\partial x_i} : A &\rightarrow A \\ f &\mapsto x_i f & & & f &\mapsto \frac{\partial f}{\partial x_i}, \end{aligned}$$

for $1 \leq i \leq n$. When the characteristic of k is zero, we call $\Delta(A)$ the *ring of differential operators* on A , and also denote it by $\mathcal{D}(A)$.

Definition 1.11. Let k be a field. The n -th *Weyl algebra* $A_n(k)$ over k is

$$A_n(k) := k\langle x_1, \dots, x_n, y_1, \dots, y_n \rangle / I$$

where I is the ideal of the free algebra $k\langle x_1, \dots, x_n, y_1, \dots, y_n \rangle$ generated by

$$\begin{aligned} x_i x_j - x_j x_i & & 1 \leq i, j \leq n, \\ y_i y_j - y_j y_i & & 1 \leq i, j \leq n, \\ y_i x_i - x_i y_i - 1 & & 1 \leq i \leq n, \\ x_i y_j - y_j x_i & & i \neq j. \end{aligned}$$

For example, if $n = 1$ then $A_1(k) = k\langle x, y \rangle / \langle yx - xy - 1 \rangle$.

Lemma 1.12. There is a surjective k -algebra homomorphism from $A_n(k)$ onto $\Delta(A)$ which sends x_i to \hat{x}_i and y_i to $\frac{\partial}{\partial x_i}$.

Proof. All pairs of generators of $\Delta(A)$ commute, except possibly $\frac{\partial}{\partial x_i}$ and \hat{x}_i , and

$$\left[\frac{\partial}{\partial x_i}, \hat{x}_i \right] (f) = \frac{\partial}{\partial x_i}(x_i f) - x_i \frac{\partial f}{\partial x_i} = f$$

for all $f \in A$. So the surjective map $k\langle x_1, \dots, x_n, y_1, \dots, y_n \rangle \rightarrow \Delta(A)$ which sends x_i to \hat{x}_i and y_i to $\frac{\partial}{\partial x_i}$ factors through $A_n(k)$. You will see on Problem Sheet 1 that $A_n(k) \rightarrow \Delta(A)$ is an isomorphism if and only if $\text{char}(k)$ is zero. \square

We will now recall a key finiteness property of modules that is sufficiently restrictive to allow strong structure theorems to be proved, and yet sufficiently general to include large classes of interesting noncommutative rings: the *Noetherian condition*.

Definition 1.13. The left R -module M is said to be *cyclic* if it can be generated by a single element: $M = Rx$ for some $x \in M$. M is *finitely generated* if it can be written as a finite sum of cyclic submodules $M = Rx_1 + Rx_2 + \dots + Rx_n$.

Lemma 1.14. Let M be a left R -module. The following are equivalent:

- (a) Every submodule of M is finitely generated
- (b) **Ascending chain condition:** There does not exist an infinite strictly ascending chain of submodules of M
- (c) **Maximum condition:** Every non-empty subset of submodules of M contains at least one maximal element. (If \mathcal{S} is a set of submodules, then $N \in \mathcal{S}$ is a *maximal element* if and only if $N' \in \mathcal{S}$, $N \leq N'$ implies $N = N'$).

Proof. (a) \Rightarrow (b). Suppose $M_1 \subsetneq M_2 \subsetneq \dots$. Let $N = \cup M_n$. Then N is a submodule of M so N is finitely generated by m_1, \dots, m_r say. If $m_i \in M_{n_i}$, then it follows that $N = M_n$ where $n = \max n_i$, a contradiction.

(b) \Rightarrow (c) If \mathcal{S} is a nonempty subset with no maximal element, pick $M_1 \in \mathcal{S}$. Since \mathcal{S} has no maximal element, we can find $M_2 \in \mathcal{S}$ such that $M_1 \subsetneq M_2$. Continuing like this gives a strictly ascending infinite chain $M_1 \subsetneq M_2 \subsetneq \dots$, a contradiction.

(c) \Rightarrow (a) Let N be a submodule of M and let \mathcal{S} be the set of submodules of N which are finitely generated. Since $0 \in \mathcal{S}$, \mathcal{S} has a maximal element L , say. Let $x \in N$. Since $L + Rx$ is a finitely generated submodule of N and L is maximal in \mathcal{S} , $L + Rx = L$ so $x \in L$. Hence $N = L$ is itself finitely generated. \square

Dually, we have the *descending chain condition* and the *minimum condition*; these are equivalent to each other.

Definition 1.15. Let R be a ring.

- An R -module satisfying (a), (b), (c) of Lemma 1.14 is *Noetherian*.
- The ring R is *left Noetherian* if it is Noetherian as a left R -module.
- An R -module satisfying the descending chain condition, or equivalently, the minimum condition, is said to be *Artinian*.
- The ring R is *left Artinian* if it is Artinian as a left R -module.

We have similar definitions “on the right hand side”. Note that if the ring is commutative, there is no difference between “left” and “right”. If R is *both* left and right Noetherian, then we will simply say that R is *Noetherian*; similarly, R is *Artinian* if it is both left and right Artinian.

Here is the main engine for proving that certain rings are left Noetherian: it is a non-commutative version of *Hilbert’s Basis Theorem*.

Theorem 1.16 (McConnell, 1968). Let S be a ring, R a left Noetherian subring and suppose that for some $x \in S$ we have

- (1) $R + xR = R + Rx$, and

$$(2) S = \langle R, x \rangle.$$

Then S is also left Noetherian.

We postpone the proof of this result for a little while, and apply it immediately to obtain a large class of Noetherian group rings.

Definition 1.17. The group G is said to be *polycyclic* if there is a chain

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

of subgroups of G such that each G_i/G_{i-1} is cyclic for each $i = 1, \dots, n$.

Examples 1.18.

(a) Infinite cyclic $G = \langle x \rangle \cong \mathbb{Z}$.

(b) Free abelian $G = \langle x_1, \dots, x_n \rangle \cong \mathbb{Z}^n$.

(c) $G = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$. Here we have the chain $1 \triangleleft G_1 \triangleleft G_2 \triangleleft G_3 = G$ where

$$G_1 = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(d) $\{I + N \in M_n(\mathbb{Z}) : N \text{ is strictly upper triangular}\}$ is always polycyclic.

Proposition 1.19. Let R be a Noetherian ring and let G be a polycyclic group. Then RG is Noetherian.

Proof. Choosing a chain of subnormal subgroups with cyclic quotients

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

we see that it's sufficient to show that if RG_{i-1} is left Noetherian then so is RG_i for all $i = 1, \dots, n$. Choose a generator xG_{i-1} for the cyclic group G_i/G_{i-1} , let $S = RG_{i-1}$ and let $T = \langle S, x \rangle$, a subring of RG_i . Because $x^{-1}G_{i-1}x = G_{i-1}$, we see that $G_{i-1}x = xG_{i-1}$ so $Sx = xS$. Hence $S + Sx = S + xS$, and therefore T is left Noetherian by Theorem 1.16.

Let I be a left ideal of RG_i . Now, $I \cap T$ is a left ideal of T and is hence finitely generated: $I \cap T = \sum_{i=1}^n Ts_i$, say. If $s \in I$, then $x^m s \in I \cap T$ for some $m \geq 0$, so $s = \sum_{i=1}^n x^{-m} a_i s_i$ for some $a_i \in T$. Hence the s_i 's generate I as a left ideal of RG_i . Hence RG_i is left Noetherian. \square

Proof of Theorem 1.16. $R + Rx + \dots + Rx^n = R + xR + \dots + x^n R$: this follows from $R + xR = R + Rx$. To see this, use induction to show that $x^n R \subseteq R + Rx + \dots + Rx^n$ and $Rx^n \subseteq R + xR + \dots + x^n R$ for all $n \geq 1$.

Consequences:

(a) The set of polynomials of degree $\leq n$, namely $S_n := R + Rx + \dots + Rx^n$, is both a left and a right R -submodule of S .

(b) The set of all elements of S of the form

$$r_0 + xr_1 + \dots + x^n r_n, \quad n \geq 0 \quad (*)$$

forms a subring of S . Since it contains both R and x and $S = \langle R, x \rangle$, we see that S is the ring of all such 'polynomials'. Note that elements of S need *not* be uniquely expressible in the form $(*)$.

(c) For each $r \in R$ and $n \geq 0$ there exists $r' \in R$ such that $r'x^n = x^n r + s$ where $\deg s < n$.

Now, let I be a left ideal in S . We will show that I is finitely generated. Let

$$I_n := \{r_n \in R : \text{there exists } s \in I \text{ such that } s = r_0 + xr_1 + \dots + x^n r_n\}.$$

Then I_n is closed under addition. Let $r \in R$. By part (c) above, we can find $r' \in R$ such that $r'x^n - x^n r$ has degree $< n$. Since I is a left ideal, $r's \in I$, and

$$r's \equiv r'x^n r_n \equiv x^n (rr_n)$$

modulo terms of degree $< n$. Hence $rr_n \in I_n$ so I_n is a left ideal of R .

Next, if $s = \sum_{i=0}^n x^i r_i \in I$, then $xs = \sum_{i=1}^{n+1} x^i r_{i-1} \in I$ so $r_n \in I_{n+1}$. Hence $I_n \leq I_{n+1}$ for all $n \geq 0$. Since R is left Noetherian, the increasing chain

$$I_0 \leq I_1 \leq \dots \leq I_n \leq \dots$$

must terminate. Say $I_m = I_{m+1} = \dots$. For $i = 0, \dots, m$ let $\{r_{ij}\}$ be finitely many elements of R generating I_i as a left ideal of R . Choose $s_{ij} = x^i r_{ij} +$ lower degree terms $\in I$.

Claim: $X = \{s_{ij} : 0 \leq i \leq m, \text{ all } j\}$ generates I as a left ideal.

Let $s = r_0 + xr_1 + \dots + x^n r_n \in I$, so that $r_n \in I_n$; we'll show that $s \in SX$. Proceed by induction on n , the case $n = 0$ being trivial.

If $n \geq m$ then $r_n \in I_m$ so $r_n = \sum a_j r_{mj}$ for some $a_j \in R$. Choose $a'_j \in R$ such that $a'_j x^n = x^n a_j +$ lower degree terms. Then $s - \sum a'_j x^{n-m} s_{mj} \in I$ and modulo terms of degree $< n$,

$$s - \sum a'_j x^{n-m} s_{mj} \equiv x^n r_n - \sum a'_j x^n r_{mj} \equiv x^n r_n - \sum x^n a_j r_{mj} = 0.$$

So $s - \sum a'_j x^{n-m} s_{mj}$ has smaller degree than s and we can apply induction.

If $n \leq m$ then $r_n = \sum a_j r_{nj}$ for some $a_j \in R$, so for suitable $a'_j \in R$, $s - \sum a'_j s_{nj} \in I$ also has smaller degree than s . By induction, these smaller degree elements of I lie SX , as required. \square

Definition 1.20. Let R be a ring. A $(\mathbb{Z}-)$ filtration on a R is a set of additive subgroups $(R_i)_{i \in \mathbb{Z}}$ such that

- $R_i \subseteq R_{i+1}$ for all $i \in \mathbb{Z}$,
- $R_i R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{Z}$,
- $1 \in R_0$, and
- $\cup_{i \in \mathbb{Z}} R_i = R$.

If R has a filtration, we say that R is a *filtered ring*. The filtration on R is *positive* if $R_i = 0$ for all $i < 0$.

Note that the axioms imply that R_0 is a subring of R and that each R_i is a left and right R_0 -module. Note also that $\bigcap_{i \in \mathbb{Z}} R_i$ is always an ideal in R .

Example 1.21. Suppose R is a finitely generated k -algebra with generating set $\{x_1, \dots, x_n\}$. Define $R_0 = k$ and let R_i be the k -subspace of R spanned by words in the x_j 's of length at most i for $i > 0$. Also define $R_i = 0$ whenever $i < 0$.

Definition 1.22. A $(\mathbb{Z}-)$ graded ring is a ring S which can be written as

$$S = \bigoplus_{i \in \mathbb{Z}} S_i$$

for some additive subgroups $S_i \subseteq S$, satisfying $S_i \cdot S_j \subseteq S_{i+j}$ for all $i, j \in \mathbb{Z}$ and $1 \in S_0$. S_i is called the i -th *homogeneous component* of S , and an element $s \in S$ is *homogeneous* iff it lies in some S_i .

Definition 1.23. Let R be a filtered ring with filtration $(R_i)_{i \in \mathbb{Z}}$. Define

$$\text{gr } R = \bigoplus_{i \in \mathbb{Z}} R_i / R_{i-1}.$$

Equip $\text{gr } R$ with multiplication, which is given on homogeneous components by

$$\begin{array}{ccc} R_i / R_{i-1} & \times & R_j / R_{j-1} & \longrightarrow & R_{i+j} / R_{i+j-1} \\ r + R_{i-1} & , & s + R_{j-1} & \mapsto & rs + R_{i+j-1} \end{array}$$

and on the whole of $\text{gr } R$ by bilinear extension. Then $\text{gr } R$ becomes a graded ring called the *associated graded ring* of R .

Note that the multiplication is well-defined because $R_i R_j \subseteq R_{i+j}$, $R_{i-1} R_j \subseteq R_{i+j-1}$ and $R_i R_{j-1} \subseteq R_{i+j-1}$. One should think of $\text{gr } R$ as an approximation to the ring R which is often easier to understand but nonetheless contains useful information about the ring R itself.

Proposition 1.24. Let \mathfrak{g} be a Lie algebra with basis $\{x_1, \dots, x_n\}$. Equip $U(\mathfrak{g})$ with the positive filtration as in Example 1.21. Then there is a surjective homomorphism of k -algebras

$$\varphi : k[X_1, \dots, X_n] \rightarrow \text{gr } U(\mathfrak{g})$$

given by $\varphi(X_i) = x_i + R_0$, $i = 1, \dots, n$.

Proof. Let $R = U(\mathfrak{g})$ and note that $x_i \in R_1$ for all i . Now because $x_i x_j - x_j x_i = [x_i, x_j] \in R_1$ for all i, j we have

$$(x_i + R_0)(x_j + R_0) = x_i x_j + R_1 = x_j x_i + R_1 = (x_j + R_0)(x_i + R_0),$$

meaning that $\varphi(X_i)$ and $\varphi(X_j)$ commute. Hence the k -algebra map φ exists. To show that φ is surjective, it's sufficient to show that $u + R_{t-1}$ lies in $\text{im } \varphi$ for any $u \in R_t \setminus R_{t-1}$. Now

$$x_{i_1}x_{i_2}\cdots x_{i_t} + R_{t-1} = \varphi(X_{i_1})\varphi(X_{i_2})\cdots\varphi(X_{i_t}) \in \text{im } \varphi$$

and u as a k -linear combination of words of length at most t in the generators $\{x_1, \dots, x_n\}$. \square

What about the Weyl algebra $A_n(k)$? Consider the standard monomials

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, y^\alpha = y_1^{\alpha_1} \cdots y_n^{\alpha_n} \in A_n(k) \quad \text{for all } \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n.$$

It follows from Exercise 1.3 that

$$\{x^\alpha y^\beta \in A_n(k) : \alpha, \beta \in \mathbb{N}^n\}$$

is a basis for $A_n(k)$ as a k -vector space. Write $|\alpha| = \sum_{i=1}^n \alpha_i$ for all $\alpha \in \mathbb{N}^n$.

Proposition 1.25. Let $R := A_n(k)$, set $R_0 := k[x_1, \dots, x_n]$, and define

$$R_i := \sum_{|\beta| \leq i} R_0 y^\beta \quad \text{for all } i \in \mathbb{N}.$$

- (a) (R_i) is a filtration on R .
- (b) $\text{gr } R \cong k[X_1, \dots, X_n, Y_1, \dots, Y_n]$ with respect to this filtration.

Proof. (a) By the defining relations in the Weyl algebra we have $y_i R_0 = R_0 y_i + R_0 \subseteq R_1$ for each i . It follows that $y^\beta R_0 \subseteq R_{|\beta|}$ for all $\beta \in \mathbb{N}^n$. Hence $R_0 y^\beta R_0 y^\gamma \subseteq R_{|\beta|+|\gamma|}$, so that $R_i R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{N}$.

(b) There is a natural map $\varphi : R_0[Y_1, \dots, Y_n] \rightarrow \text{gr } R$ of graded rings which sends Y_i to $\sigma(y_i) = y_i + R_0$. Because every element in R can be written as a finite sum $\sum_{\beta \in \mathbb{N}^n} r_\beta y^\beta$ for some $r_\beta \in R_0$, φ is surjective. Because φ respects the graded structure, to show that φ is injective it is enough to show that $\ker \varphi$ contains no non-zero homogeneous elements. So let $\sum_{|\beta|=m} r_\beta Y^\beta \in \ker \varphi$; then $\sum_{|\beta|=m} r_\beta y^\beta \in R_{m-1}$, so we can find $r_\beta \in R$ whenever $|\beta| < m$ such that

$$\sum_{|\beta|=m} r_\beta y^\beta = \sum_{|\beta|<m} r_\beta y^\beta.$$

Because $\{x^\alpha y^\beta \in A_n(k) : \alpha, \beta \in \mathbb{N}^n\}$ is a basis for R , $r_\beta = 0$ for all β . \square

Definition 1.26. The filtration on $A_n(k)$ constructed in Proposition 1.25 is called the *filtration by order of differential operator*.

Theorem 1.27. Suppose R is a positively filtered ring such that $\text{gr } R$ is left Noetherian. Then R is left Noetherian.

Proof. Let I be a left ideal in R , and consider the left ideal

$$\text{gr } I := \bigoplus_{n \geq 0} \frac{(I \cap R_n) + R_{n-1}}{R_{n-1}}.$$

in $\text{gr } R$. For each $n \in \mathbb{N}$, consider the projection operator $\pi_n : \text{gr } R \rightarrow \text{gr } R$ which sends $\sum x_i \in \text{gr } R$ to $x_n \in \text{gr } R$. Note that these operators preserve $\text{gr } I$. This means that $\text{gr } I$ contains the homogeneous components of each of its elements. Now because $\text{gr } R$ is Noetherian, $\text{gr } I$ has a finite generating set $\{X_1, \dots, X_m\}$, which we may without loss of generality assume to consist of homogeneous elements.

Choose some $x_i \in I \cap R_{n_i} \setminus R_{n_i-1}$ such that $x_i + R_{n_i-1}$ equals X_i . To finish the proof, we prove that

$$I = \sum_{i=1}^m R x_i.$$

The inclusion \supseteq is clear. For \subseteq , it is enough to prove that $I \cap R_n \subseteq \sum_{i=1}^m R x_i$ for all $n \geq -1$. Induct on n : $n = -1$ is clear because $R_{-1} = \{0\}$. If $x \in I \cap R_n$, then

$$x + R_{n-1} = \sum_{i=1}^m Y_i X_i$$

for some $Y_i \in \text{gr } R$. We can again assume that each Y_i is homogeneous of degree $n - n_i$, so choose $r_i \in R$ such that $Y_i = r_i + R_{n-n_i-1}$. Then $x \equiv \sum_{i=1}^m r_i x_i \pmod{R_{n-1}}$, so $x - \sum_{i=1}^m r_i x_i \in I \cap R_{n-1} \subseteq \sum_{i=1}^m R x_i$. So $x \in \sum_{i=1}^m R x_i$. \square

Corollary 1.28.

- (a) $U(\mathfrak{g})$ is Noetherian whenever $\dim_k \mathfrak{g} < \infty$.
- (b) $A_n(k)$ is Noetherian.

Proof. (a) By Proposition 1.24, $\text{gr } U(\mathfrak{g})$ is a quotient of a polynomial algebra $k[x_1, \dots, x_n]$ for some n , which is Noetherian by Theorem 1.16. Hence $U(\mathfrak{g})$ is Noetherian by Theorem 1.27.

- (b) Similar, using Proposition 1.25 instead. \square

Question 1.29. (a) Let \mathfrak{g} be a Lie algebra over a field k such that $U(\mathfrak{g})$ is Noetherian. Must $\dim_k \mathfrak{g} < \infty$?

- (b) Suppose that kG is left Noetherian. Must G contain a polycyclic subgroup of finite index?

2. SIMPLE MODULES AND ARTINIAN RINGS

Throughout this chapter, R denotes an arbitrary ring, unless stated otherwise.

Definition 2.1. An R -module M is *simple* or *irreducible* if $M \neq 0$ and the only submodules of M are 0 and M .

Suppose M is simple. Choose $0 \neq x \in M$; then $M = Rx$ so $M \cong R/I$ where $I = \text{ann}(x)$ is the point annihilator of x . Note that $\text{ann}(x)$ need *not* be equal to $\text{ann}(y)$ if x, y are distinct nonzero elements of M , unless R is commutative.

Note that $M = Rx$ is simple if and only if $\text{ann}(x)$ is a maximal left ideal of R .

Definition 2.2. A *poset* is a set equipped with a binary relation \leq which is reflexive, transitive and antisymmetric. A *chain* in a poset \mathcal{S} is totally ordered subset \mathcal{C} of \mathcal{S} : if $s, t \in \mathcal{C}$ then either $s \leq t$ or $t \leq s$. An *upper bound* for a subset \mathcal{C} of \mathcal{S} is an element $u \in \mathcal{S}$ such that $x \leq u$ for all $x \in \mathcal{C}$. We say that $x \in \mathcal{S}$ is a *maximal element* if $x \leq y$ with $y \in \mathcal{S}$ forces $x = y$.

Theorem 2.3 (Zorn's Lemma). Let \mathcal{S} be a nonempty poset. Suppose every chain in \mathcal{S} has an upper bound. Then \mathcal{S} has a maximal element.

This is equivalent to the Axiom of Choice, which we will always assume.

Lemma 2.4. Suppose L is a proper left ideal of R . Then L is contained in a maximal ideal I of R . Equivalently, every nonzero cyclic module has a simple quotient.

Proof. Since L is proper, $1 \notin L$. Let $\mathcal{S} = \{K \triangleleft_l R : L \subseteq K, 1 \notin K\}$. Since $L \in \mathcal{S}$, this set is nonempty. \mathcal{S} is partially ordered by inclusion. If \mathcal{C} is a chain in \mathcal{S} , then $\cup \mathcal{C}$ also contains L and doesn't contain 1, i.e. $\cup \mathcal{C} \in \mathcal{S}$. Hence every chain in \mathcal{S} has an upper bound in \mathcal{S} . By Zorn's Lemma, \mathcal{S} has a maximal element I . It's clear that I is now a maximal left ideal of R containing L . \square

By an *ideal* of R we mean a *two-sided* ideal.

Definition 2.5. Let I be a two-sided ideal of R . Then I is *left primitive* if I is the annihilator of a simple left R -module M :

$$I = \text{Ann}_R(M) = \{x \in R : xM = 0\} = \bigcap_{x \in M} \text{ann}(x).$$

The ring R itself is called *left primitive* if its zero ideal is left primitive, or equivalently, if R has at least one faithful simple left module.

There are examples due to George Bergman of rings which are left primitive, but not right primitive! Note that the annihilator I of any module M is always an ideal of R .

Lemma 2.6. Let $M = Rx$ be a cyclic left R -module. Then $I = \text{Ann}_R(M)$ is the largest two-sided ideal contained in $L = \text{ann}(x)$.

Proof. Note that this largest two-sided ideal K exists, since the sum of all two-sided ideals contained in L is itself a two-sided ideal contained in L . Certainly $I \subseteq L$, so $I \subseteq K$. Now $KM = KRx \subseteq Kx \subseteq Lx = 0$ since K is two-sided, so $K \subseteq I$. \square

Corollary 2.7. Every maximal ideal of R is left and right primitive. Moreover, if R is commutative, every primitive ideal is maximal.

Definition 2.8. The *Jacobson radical* $J(R)$ of R is defined to be the intersection of all left primitive ideals of R .

Note that $J(R)$ is the set of elements of R which annihilate every simple left R -module.

Lemma 2.9. $J(R)$ is equal to the intersection K of all maximal left ideals of R .

Proof. Let I be a maximal left ideal. Then $P = \text{Ann}_R(R/I)$ is primitive, so $J(R) \subseteq P \subseteq I$ by Definition 2.5. Hence $J(R) \subseteq K$.

Now let $P = \text{Ann}_R(M)$ be a primitive ideal, where M is a simple R -module. Note that $P = \bigcap_{0 \neq x \in M} \text{ann}(x)$ is an intersection of maximal left ideals, so $K \subseteq P$. It follows that $K \subseteq J(R)$ as required. \square

Lemma 2.10 (Nakayama). Let M be a finitely generated nonzero left R -module and let $J = J(R)$. Then JM is strictly contained in M .

Proof. Since M is finitely generated, by choosing a minimal finite generating set for M we see that M has a non-zero cyclic quotient module M/L , which in turn has a simple quotient M/K by Lemma 2.4. Then $J(M/K) = 0$ so $JM \subseteq K$ which is strictly contained in M . \square

Corollary 2.11. Let M be a finitely generated left R -module and let $J = J(R)$. If N is a submodule of M such that $M = N + JM$ then $M = N$.

Proof. Apply the Lemma to M/N . \square

Recall that an element $x \in R$ is a *unit* if there exists $y \in R$ such that $xy = yx = 1$.

Proposition 2.12.

$$J(R) = \{x \in R : 1 - axb \text{ is a unit for all } a, b \in R\} =: K.$$

Proof. Let $x \in J(R)$. Since $J(R)$ is a two-sided ideal, to show that $x \in K$ it's sufficient to show $1 - x$ is a unit. Now $R(1 - x) + Rx = R$, so Corollary 2.11 implies that $R(1 - x) = R$. Hence there exists $y \in R$ such that

$$y(1 - x) = 1.$$

Now, $1 - y = -yx \in J(R)$, so by the above argument applied to $1 - y$, we can find $z \in R$ such that

$$z(1 - (1 - y)) = zy = 1.$$

Hence $zy(1 - x) = 1 - x = z$ so $yz = 1$ and $zy = 1$. Hence $z = 1 - x \in R^\times$.

Now let $x \in K$, let I be a maximal left ideal of R and suppose that $x \notin I$. Since I is maximal, $I + Rx = R$, so $1 - ax \in I$ for some $a \in R$. Since $x \in K$, $1 - ax$

is a unit, a contradicting the fact that I is proper. Hence $x \in I$ so $K \subseteq I$ for all maximal left ideals I of R . By Lemma 2.9, $K \subseteq J(R)$. \square

This result shows that $J(R)$ is the largest ideal two-sided A of R such that $1 - A$ consists entirely of units of R .

Corollary 2.13. The Jacobson radical is left-right symmetric. It follows that the intersection of all maximal left ideals of R is equal to the intersection of all maximal right ideals.

We will now work towards understanding the structure of left primitive rings. Let V be a left R -module and let $D = \text{End}({}_R V)$. Let us write R -module endomorphisms of V on the *right*, and define composition of such endomorphisms by the rule

$$v(\alpha \cdot \beta) = (v\alpha)\beta \quad \text{for all } v \in V, \alpha, \beta \in D.$$

Thus $\alpha \cdot \beta$ is the product of α and β inside D in this new notation. Naturally, V is then a right D -module, and in fact, V becomes an *R - D -bimodule*: this means that V is simultaneously a left R -module and a right D -module via the rule $v \cdot \alpha = v\alpha$, and the two structures are compatible in the following sense:

$$r \cdot (v \cdot \alpha) = (r \cdot v) \cdot \alpha \quad \text{for all } r \in R, \alpha \in D.$$

Of course, this just says that every element of D is an endomorphism of the left R -module V .

Theorem 2.14 (Schur's Lemma). Let V be a simple left R -module. Then $D := \text{End}({}_R V)$ is a division ring.

Proof. Let $\varphi : V \rightarrow V$ be a nonzero R -module homomorphism. Then $\ker(\varphi) < V$ and $\text{im}(\varphi) > 0$. The simplicity of V forces $\ker(\varphi) = 0$ and $\text{im}(\varphi) = V$, so φ is an isomorphism. Thus every nonzero element of D is a unit. \square

So whenever V is a simple left R -module, V becomes a right vector space over the division ring $D = \text{End}_R(V)$.

Theorem 2.15 (Jacobson's Density). Let V be a simple left R -module, and let $X \subset V$ be a finite D -linearly independent subset of V where $D := \text{End}_R(V)$. Then for every $\alpha \in \text{End}(V_D)$ there exists $r \in R$ such that $\alpha(x) = r \cdot x$ for all $x \in X$.

Proof. Write $X = \{x_1, \dots, x_n\}$, fix $i \in \{1, \dots, n\}$ and write $X_i := X \setminus \{x_i\}$. Since $x_i \notin X_i \cdot D$, Lemma 2.16 below gives $\text{ann}(X_i) \cdot x_i \neq 0$. So there is some $r_i \in \text{ann}(X_i)$ such that $r_i \cdot x_i \neq 0$. Since V is simple, $R \cdot (r_i \cdot x_i) = V$, so we can find some $s_i \in R$ such that $s_i \cdot (r_i \cdot x_i) = \alpha(x_i)$. Now

$$\sum_{j=1}^n s_j r_j \cdot x_i = s_i \cdot r_i \cdot x_i = \alpha(x_i) \quad \text{for all } i = 1, \dots, n.$$

So we can take $r = \sum_{j=1}^n s_j r_j$. \square

Lemma 2.16. Let V be a simple left R -module, let $D = \text{End}_R(V)$, let X be a finite D -linearly independent subset of V , and let $I := \text{ann}(X)$. Suppose that $I \cdot y = \{0\}$ for some $y \in V$. Then $y \in X \cdot D$, the D -linear span of X .

Proof. We proceed by induction on $n = |X|$. When $n = 0$, we have $\text{ann}(\emptyset) = R$ and $\emptyset \cdot D = \{0\}$. So since $R \cdot y = \{0\}$ by assumption, we have $y = 0 \in \emptyset \cdot D$.

Assume now that $n \geq 1$ and let $J = \text{ann}(X \setminus \{x\})$ for some $x \in X$ so that $I = J \cap \text{ann}(x)$. If $J \subseteq \text{ann}(x)$ then $J = I$, so $J \cdot y = 0$ and we can apply the induction hypothesis. So we can assume that J is not contained in $\text{ann}(x)$. But then the R -submodule $J \cdot x$ of V is non-zero, so $J \cdot x = V$ by the simplicity of V .

Define $d : V \rightarrow V$ by the rule $(r \cdot x)d = r \cdot y$, whenever $r \in J$. This is well-defined, because if $r \cdot x = 0$ for some $r \in J$ then $r \in \text{ann}(x) \cap J = I$, so $r \cdot y = 0$ since $I \cdot y = 0$ by assumption. This function is left R -linear because $(s \cdot (r \cdot x))d = (sr \cdot x)d = sr \cdot y = s \cdot (r \cdot y) = s \cdot ((r \cdot x)d)$ for all $s \in R$. Thus we have found an element $d \in D$ such that $J \cdot (y - x \cdot d) = 0$. Hence $y - x \cdot d \in (X \setminus \{x\}) \cdot D$ by induction and therefore $y \in X \cdot D$. \square

This completes the proof of Theorem 2.15. Lemma 2.16 also has the following interesting consequence.

Lemma 2.17. Let R be a left Artinian ring, let V be a simple left R -module and let $D = \text{End}_R(V)$. Then V is finite dimensional as a right D -vector space.

Proof. Since R is left Artinian, by Exercise 2.4 the set $\{\text{ann}(X) : X \subset V, |X| < \infty\}$ has a minimal element $I = \text{ann}(X)$, say. We will show that $V = X \cdot D$. Let $y \in V$ and consider $\text{ann}(X \cup \{y\}) \subseteq \text{ann}(X)$. The minimality of $\text{ann}(X)$ forces these to be equal. Hence $I \cdot y = 0$, so $y \in X \cdot D$ for any $y \in V$ by Lemma 2.16. Hence $V = X \cdot D$. \square

Theorem 2.18 (Artin-Wedderburn). Let R be a left primitive, left Artinian ring. Then $R \cong M_n(D)$ for some division ring D and integer $n \geq 1$.

The proof requires the following

Lemma 2.19. Let S be a ring, let N be a right S -module and let $n \geq 1$ be an integer. Then the ring of right S -module endomorphisms of $(N_S)^n$ is isomorphic to the $n \times n$ matrix ring with coefficients in $T := \text{End}(N_S)$:

$$\text{End}((N_S)^n) \cong M_n(T).$$

Proof. This is best seen by writing elements of N^n as column vectors $x = (x_j)_{j=1}^n$ and thinking of S -module endomorphisms acting by matrix multiplication on the *left* of these column vectors.

Formally, let $\sigma_j : N \hookrightarrow N^n$ and $\pi_j : N^n \twoheadrightarrow N$ for $j = 1, \dots, n$ be given by

$$\sigma_j(x)_i = x\delta_{ij} \quad \text{and} \quad \pi_j(x) = x_j.$$

These are right S -module homomorphisms. We define $\alpha : \text{End}((N_S)^n) \rightarrow M_n(T)$ by setting the (i, j) element of $\alpha(f)$ to be the composition

$$N \xrightarrow{\sigma_j} N^n \xrightarrow{f} N^n \xrightarrow{\pi_i} N;$$

thus $\alpha(f)_{ij} = \pi_i f \sigma_j$. We can also define $\beta : M_n(T) \rightarrow \text{End}((N_S)^n)$ by

$$\beta(A) = \sum_{i,j=1}^n \sigma_j A_{ji} \pi_i.$$

It is a pleasant exercise to show that α and β are mutually inverse ring homomorphisms. \square

We say that a left R -module M is *faithful* if $\text{Ann}_R(M)$ is zero, or equivalently, if the representation $\rho_M : R \rightarrow \text{End}(M)$ afforded by M is injective.

Proof of Theorem 2.18. Let V be a faithful simple left R -module, and let $D = \text{End}({}_R V)$. Then D is a division ring by Theorem 2.14. Now $V_D \cong (D_D)^n$ for some positive integer n by Lemma 2.17 and $\text{End}(D_D) \cong D$ by Exercise 2.2(a). So

$$\text{End}((D_D)^n) \cong M_n(\text{End}(D_D)) \cong M_n(D)$$

by Lemma 2.19. Now we have a natural ring homomorphism

$$\psi : R \rightarrow \text{End}(V_D)$$

given by $\psi(r)(v) = r \cdot v$. It is injective because V is faithful, and it is surjective by Theorem 2.15. We conclude that $R \cong M_n(D)$. \square

Theorem 2.20 (Chinese Remainder). Let R be a ring, and let P_1, \dots, P_n be two-sided ideals in R such that $P_i + P_j = R$ whenever $i \neq j$. Then

$$R/(P_1 \cap P_2 \cap \dots \cap P_n) \cong (R/P_1) \oplus (R/P_2) \oplus \dots \oplus (R/P_n).$$

Proof. There is a natural ring homomorphism $\varphi : R \rightarrow \bigoplus_{i=1}^n R/P_i$ given by $\varphi(r) = (r + P_i)_{i=1}^n$. Its kernel is $P_1 \cap \dots \cap P_n$, so by the First Isomorphism Theorem for rings it will be sufficient to show that φ is surjective. We prove this by induction on n , the case $n = 1$ being clear.

Since $P_i + P_n = R$ for all $i < n$, we can find $a_i \in P_i$ and $b_i \in P_n$ such that $a_i + b_i = 1$ for all $i = 1, \dots, n-1$. Let $a := a_1 \cdots a_{n-1} \in P_1 \cap \dots \cap P_{n-1}$ and let $b := 1 - a$. Then

$$b = 1 - a = (a_1 + b_1) \cdots (a_{n-1} + b_{n-1}) - a_1 \cdots a_{n-1} \in P_n.$$

Now, given $(r_i + P_i) \in \bigoplus_{i=1}^n R/P_i$, we can find some $s \in R$ such that $s - r_i \in P_i$ for all $i < n$ by induction. Let $r := sb + r_n a$; then $r \equiv r_n \pmod{P_n}$ and $r \equiv sb \equiv r_i \pmod{P_i}$ for each $i < n$. So $\varphi(r) = (r_i + P_i)_{i=1}^n$ and φ is surjective. \square

Corollary 2.21. Let R be a left Artinian ring with $J(R) = 0$. Then there exist division rings D_1, \dots, D_n and integers $r_1, \dots, r_n \geq 1$ such that

$$R \cong M_{r_1}(D_1) \oplus \cdots \oplus M_{r_n}(D_n).$$

Proof. Let \mathcal{S} be the set of finite intersections of left primitive ideals of R ; it is non-empty by Lemma 2.4. Since R is left Artinian, this set has a minimal element $I := P_1 \cap \cdots \cap P_n$ say. If Q is another left primitive ideal of R then $I \cap Q = I$ by the minimality of I , so that $I \subseteq Q$. Hence $I \subseteq J(R) = \{0\}$ by assumption. Now $R/P_i \cong M_{r_i}(D_i)$ for some division ring D_i , and this ring is simple by Exercise 3.3(c). So each P_i is a maximal two-sided ideal, and therefore $P_i + P_j = R$ whenever $i \neq j$. Now apply Theorem 2.20. \square

Proposition 2.22. The Jacobson radical J of a left Artinian ring R is nilpotent.

Proof. The descending chain $J \supseteq J^2 \supseteq J^3 \supseteq \dots$ must terminate since R is left Artinian. Hence $J^n = J^{n+1} = \dots$ for some $n \geq 0$. Let $X = \text{rann}(J^n) = \{x \in R : J^n x = 0\}$, this is a two-sided ideal of R . Suppose for a contradiction that $X \neq R$. Then R/X has a minimal nonzero left submodule Y/X , being left Artinian. This module is simple. Now $J \cdot (Y/X) = 0$ so $JY \subseteq X$. It follows that $J^n Y = J^{n+1} Y \subseteq J^n X = 0$, so $Y \subseteq \text{rann}(J^n) = X$, contradicting $Y/X \neq 0$. Hence $X = R$ so $J^n = R J^n = X J^n = 0$. \square

Theorem 2.23 (Hopkins). Let R be a left Artinian ring. Then R is also left Noetherian.

Proof. Let $J = J(R)$. For any $i \in \mathbb{N}$, J^i/J^{i+1} is a left Artinian R/J -module, so it is also left Noetherian by Theorem 2.18 and Exercise 3.3(c). Since J is nilpotent by Proposition 2.22, R is a finite extension of left Noetherian modules, and is therefore itself left Noetherian by Exercise 1.4(a). \square

3. NONCOMMUTATIVE LOCALISATION

Let A be a ring and let S be a subset of A . We want to “invert S ”, meaning that we want to find a ring homomorphism

$$\varphi : A \rightarrow S^{-1}A \quad \text{such that} \quad \varphi(S) \subseteq (S^{-1}A)^\times,$$

and we want $S^{-1}A$ to be “minimal” in some sense.

Construction 3.1. Form the free algebra on a set which is in bijection with S

$$A\langle i_s : s \in S \rangle$$

and impose the relation that i_s is a two-sided inverse of $s \in S$ for each $s \in S$:

$$S^{-1}A := \frac{A\langle i_s : s \in S \rangle}{\langle s i_s - 1, i_s s - 1 : s \in S \rangle}.$$

Then define $\varphi : A \rightarrow S^{-1}A$ by letting $\varphi(s)$ be the image of s in $S^{-1}A$. By definition, $\varphi(S)$ consists of units in $S^{-1}A$.

This ring $S^{-1}A$ is minimal in the following precise sense.

Proposition 3.2 (Universal property of $S^{-1}A$). Suppose that $\theta : A \rightarrow B$ is a ring homomorphism such that $\theta(S) \subseteq B^\times$. Then there is a unique ring homomorphism $\bar{\theta} : S^{-1}A \rightarrow B$ such that $\theta = \bar{\theta} \circ \varphi$.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & S^{-1}A \\ & \searrow \theta & \downarrow \bar{\theta} \\ & & B \end{array}$$

Problems.

- (1) $S^{-1}A$ could be the zero ring!
- (2) *Non-examinable*: $S^{-1}A$ will not be a flat left A -module, in general.

Definition 3.3. The *left S -torsion* subset of A is

$$t_S(A) := \{a \in A : sa = 0 \text{ for some } s \in S\}.$$

Note that $\varphi(t_S(A)) = 0$, so that $t_S(A) \subseteq \ker \varphi$. Note also that if $\langle S \rangle$ is the sub-monoid of A generated by S , then $\langle S \rangle^{-1}A = S^{-1}A$. For this reason, we will focus on *multiplicatively closed* subsets of A : by definition, these are the subsets S of A such that $1 \in S$ and $s, t \in S \Rightarrow st \in S$.

Definition 3.4. Let S be a multiplicatively closed subset of A .

- (a) S is *left localisable* if
 - (i) $S^{-1}A = \{\varphi(s)^{-1}\varphi(a) \mid a \in A, s \in S\}$ and
 - (ii) $\ker \varphi = t_S(A)$.
- (b) S is a *left Ore set* if

$$Sa \cap As \neq \emptyset \text{ for all } a \in A, s \in S.$$

- (c) S is *left reversible* if whenever $as = 0$ for some $s \in S$ and $a \in A$, there is some $s' \in S$ such that $s'a = 0$. In other words, right S -torsion elements in A are also left S -torsion.
- (d) $s \in A$ is a *regular element* if $sa = 0$ or $as = 0$ imply that $a = 0$.
- (e) A is a *domain* if every non-zero element is regular.

Obviously if A is a commutative ring, or more generally, if S consists of central elements in A then S is a left Ore set. We will shortly see examples of multiplicatively closed sets which do not have this property.

Proposition 3.5. Every left localisable subset is a left reversible, left Ore set.

Proof. Let $a \in A$ and $s \in S$. Then by definition, the element $\varphi(a)\varphi(s)^{-1} \in S^{-1}A$ can be written as a right fraction

$$\varphi(a)\varphi(s)^{-1} = \varphi(u)^{-1}\varphi(c)$$

for some $c \in A$ and $u \in S$. Hence $ua - cs \in \ker \varphi$ so we can find $v \in S$ such that $v(ua - cs) = 0$. Hence $(vu)a = (vc)s$ so take $t = vu \in S$ and $b = vc \in A$, then

$$ta = bs$$

and hence S is a left Ore set. Next, if $as = 0$ for some $s \in S$ and $a \in A$, then

$$\varphi(a) = \varphi(as)\varphi(s)^{-1} = 0$$

so $s'a = 0$ for some $s' \in A$. Hence S is left reversible. \square

Examples 3.6.

- (a) Say that an element $s \in A$ is *normal* if $sA = As$. Then if every element $s \in S$ is regular and normal, then S is a left Ore set. This happens, for example, whenever every element of S is central in A .
- (b) Let $A = k\langle x, y \rangle$ be a free algebra in two variables over a field. This is a domain, so $S := A \setminus \{0\}$ is multiplicatively closed. But

$$Ax \cap Ay = \{0\}$$

so $Sx \cap Sy = \emptyset$. Hence S is not left localisable by Proposition 3.5.

Theorem 3.7 (Ore, 1930). Let S be a left Ore set in A consisting of regular elements. Then $\varphi : A \rightarrow S^{-1}A$ is injective.

Proof (non-examinable). Define a relation on $S \times A$ as follows:

$$(s, a) \sim (t, b) \Leftrightarrow \exists c, d \in A \quad \text{such that} \quad cs = dt \in S \quad \text{and} \quad ca = db.$$

This is an equivalence relation. Let Q be the set of equivalence classes on $S \times A$ under this equivalence relation:

$$Q := (S \times A) / \sim.$$

Then Q is a ring, and the map $\psi : A \rightarrow Q$ defined by $\psi(a) = [(1, a)]$ is an injective ring homomorphism which inverts S . So by the universal property of $S^{-1}A$, there is a map $\theta : S^{-1}A \rightarrow Q$ such that $\psi = \theta \circ \varphi$. Hence φ is injective because ψ is injective. More details can be found in the Appendix at the end of these notes. \square

Theorem 3.8 (Gabriel). Let S be a multiplicatively subset of A . Then S is left localisable if and only if it is a left reversible, left Ore set.

Proof. We need to prove the converse of Proposition 3.5. So suppose that S is a left reversible left Ore set, and consider the element

$$\varphi(s_1)^{-1}\varphi(a_1)\varphi(s_2)^{-1}\varphi(a_2) \cdots \varphi(s_n)^{-1}\varphi(a_n)$$

in $S^{-1}A$; notice that by the construction of $S^{-1}A$, since S is multiplicatively closed, every element of $S^{-1}A$ is a finite sum of such elements. Using the left Ore condition, we can rewrite it in the form $\varphi(s)^{-1}\varphi(a)$ for some $a \in A$ and $s \in S$.

Next, given $a, b \in A$ and $s, t \in S$, choose $u \in A$ and $v \in S$ such that

$$ut = vs.$$

Since $s, v \in S$ and S is multiplicatively closed, this element lies in S . So we can bring the sum of the two left fractions $\varphi(s)^{-1}\varphi(a)$ and $\varphi(t)^{-1}\varphi(b)$ to a common left denominator:

$$\varphi(s)^{-1}\varphi(a) + \varphi(t)^{-1}\varphi(b) = \varphi(vs)^{-1}\varphi(va + ub).$$

So every element of $S^{-1}A$ is of the form $\varphi(s)^{-1}\varphi(a)$ for some $a \in A$ and $s \in S$.

It remains to prove that $\ker \varphi = t_S(A)$. Now, the left S -torsion subset $t_S(A)$ of A satisfies $t_S(A) \cdot A \subset t_S(A)$. It is also a left ideal in A by Exercise 4.1. So it is a two-sided ideal. Next, let $s \in S$ and $a \in A$ and suppose that $as \in t_S(A)$. Then $tas = 0$ for some $t \in S$, but S is left reversible so $s'ta = 0$ for some $s' \in S$. So $a \in t_S(A)$ because $s't \in S$. If on the other hand $sa \in t_S(A)$ then $tsa = 0$ for some $t \in S$ so $a \in t_S(A)$ because $ts \in S$.

Thus the image \bar{S} of S in the factor ring $\bar{A} := A/t_S(A)$ consists of non-zero divisors, and \bar{S} is a left Ore set in \bar{A} by Exercise 4.2. Now, the universal \bar{S} -inverting ring homomorphism $\bar{\varphi} : \bar{A} \rightarrow \bar{S}^{-1}\bar{A}$ is injective by Theorem 3.7. If $\pi : A \rightarrow \bar{A}$ is the natural surjection, then $\bar{\varphi}\pi : A \rightarrow \bar{S}^{-1}\bar{A}$ inverts S , so by the universal property of $S^{-1}A$ there is a ring homomorphism $\theta : S^{-1}A \rightarrow \bar{S}^{-1}\bar{A}$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\pi} & \bar{A} \\ \varphi \downarrow & & \downarrow \bar{\varphi} \\ S^{-1}A & \xrightarrow{\theta} & \bar{S}^{-1}\bar{A}. \end{array}$$

Now if $a \in \ker \varphi$ then $\bar{\varphi}(\pi(a)) = \theta(\varphi(a)) = 0$, but $\bar{\varphi}$ is injective so $\pi(a) = 0$, and therefore $a \in t_S(A) = \ker \pi$. \square

A similar procedure is involved in the construction of the derived category of an abelian category.

Theorem 3.9. [Goldie, 1957] Let A be a left Noetherian domain. Then $S = A \setminus \{0\}$ is a left Ore set.

Proof. Let $x \in A$, $y \in S$. We want to show that $Ay \cap Sx \neq \emptyset$. Let $k \in \mathbb{N}$ and consider the left ideal

$$I_k := Ax + Axy + \cdots + Axy^k$$

of A . These form an ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ which has to terminate. Choose $k \in \mathbb{N}$ *minimal* such that $I_k = I_{k+1}$. Then $xy^{k+1} \in I_k$, so

$$xy^{k+1} = a_0x + a_1xy + \cdots + a_kxy^k$$

for some $a_0, \dots, a_k \in A$. If $k = 0$ then $xy = a_0x$; since A is a domain, $xy \neq 0$ so $a_0 \neq 0$. Thus $a_0 \in S$ so that

$$xy = a_0x \in Ay \cap Sx.$$

If $k \geq 1$ then $(xy^k - a_1x - \cdots - a_kxy^{k-1})y = a_0x$ and the minimality of k forces $a_0 \neq 0$. So $a_0 \in S$ and $a_0x \in Sx \cap Ay$. \square

Corollary 3.10. Every Noetherian domain has a division ring of fractions.

Proof. Let $S = A \setminus \{0\}$. This is a left Ore set by Theorem 3.9, and it consists of regular elements because A is a domain. So A embeds into $S^{-1}A$ by Theorem 3.7 and $S^{-1}A = \{s^{-1}a : s \in S, a \in A\}$. Now if $s^{-1}x \in S^{-1}A$ is a non-zero element then $x, s \in S$ and $x^{-1}s$ is the inverse of $s^{-1}x$. Hence every non-zero element of $S^{-1}A$ is a unit, so $S^{-1}A$ is a division ring. \square

It turns out that in left Noetherian rings, we don't have to worry about the left-reversibility condition on left Ore sets.

Proposition 3.11. Let A be a left Noetherian ring, and let $S \subset A$ be a left Ore set. Then S is left reversible.

Proof. Suppose that $as = 0$ for some $s \in S$ and $a \in A$, and consider the ascending chain of left annihilators

$$\text{lann}(s) \leq \text{lann}(s^2) \leq \cdots$$

Since A is left Noetherian this chain stops, so that $\text{lann}(s^{k+1}) = \text{lann}(s^k)$ for some integer $k \geq 1$. Now because S is a left Ore set, we can find $b \in A$ and $t \in S$ such that $ta = bs^k$. Then $bs^{k+1} = tas = 0$ so $b \in \text{lann}(s^{k+1}) = \text{lann}(s^k)$. Hence $ta = bs^k = 0$ with $t \in S$. \square

We say that A is a *prime ring* if whenever I, J are non-zero two-sided ideals of A , their product IJ is again non-zero. We say that A is a *left Goldie ring* if A doesn't have an infinite direct sum of non-zero left ideals, and every ascending chain of left annihilators in A is stationary.

Theorem 3.12. [Goldie, 1958] Let A be a ring, and let S be the set of regular elements of A . The following are equivalent:

- (a) S is a left Ore set in A and $S^{-1}A$ is a left Artinian, left primitive ring
- (b) A is a prime, *left Goldie ring*.

Proof. Omitted. \square

Clearly, every left Noetherian ring is a left Goldie ring. It follows from Corollary 2.21 that if A is a prime, left Goldie ring, then S is left localisable and $S^{-1}A$ is a matrix ring over a division ring. In this way, Theorem 3.12 is a generalisation of Theorem 3.9.

Definition 3.13. Let S be a left localisable subset of A and let M be a left A -module.

(a) The *localisation of M at S* is defined to be the set of equivalence classes

$$S^{-1}M = \{s \setminus m : m \in M, s \in S\}$$

in $S \times M$ under the equivalence relation \sim given by

$$(s, m) \sim (t, n) \quad \text{if and only if} \quad ut'm = us'n \quad \text{for some} \quad u \in S,$$

where $t' \in A, s' \in S$ are such that $t's = s't \in S$.

(b) The *S -torsion submodule* of M is defined to be

$$t_S(M) = \{m \in M : sm = 0 \quad \text{for some} \quad s \in S\}.$$

A long calculation shows that $S^{-1}M$ has the structure of an $S^{-1}A$ -module. To do this, it is sufficient to check that $S^{-1}M$ is an A -module; then S clearly acts invertibly on $S^{-1}M$ so by the universal property of $S^{-1}A$ the ring homomorphism $A \rightarrow \text{End}_{\mathbb{Z}}(S^{-1}M)$ extends to $S^{-1}A$.

4. DIMENSION THEORY FOR NOETHERIAN MODULES

We will develop some dimension theory for finitely generated modules over Noetherian rings, with an emphasis on minimal primes.

Definition 4.1. Let R be a ring.

- (a) A proper ideal P of R is said to be *prime* if, whenever I, J are ideals in R such that $IJ \subseteq P$, either $I \subseteq P$ or $J \subseteq P$.
- (b) The set of prime ideals in R is denoted by $\text{Spec}(R)$.
- (c) Let I be an ideal in R . A prime ideal P of R is a *minimal prime over I* if $P \supseteq I$ and $I \subseteq Q \subseteq P$ with Q prime forces $Q = P$.
- (d) P is a *minimal prime of R* if it is a minimal prime over the zero ideal.
- (e) $\min(I) := \{\text{minimal primes over } I\}$.

Be warned that if R is not commutative and P is a prime ideal, then the factor ring R/P may well have zero-divisors. For example, the zero ideal in every simple ring is prime, and plenty of simple rings have zero-divisors: take, for example, any matrix algebra $M_n(k)$ over a field k with $n \geq 2$.

Proposition 4.2. Let R be a left (or right) Noetherian ring and let I be a proper ideal. Then

- (1) There exist primes P_1, \dots, P_n containing I such that $P_1 \cdots P_n \subseteq I$.

(2) The set of minimal primes over I is finite and non-empty.

Proof. Suppose that (1) is false. Since R is Noetherian, we can choose a maximal counterexample I . Thus I contains no finite product of prime ideals containing I , and I is maximal with respect to this property. We will show that I is prime.

If I is not prime, we can find $A, B \triangleleft R$ are such that $AB \subseteq I$ but $A \not\subseteq I$ and $B \not\subseteq I$. By the maximality of I , $I + A$ contains the product of primes P_1, \dots, P_n containing $I + A$, and similarly $Q_1 \cdots Q_m \subseteq I + B$ for some primes Q_1, \dots, Q_m containing $I + B$. Hence

$$P_1 \cdots P_n Q_1 \cdots Q_m \subseteq (I + A)(I + B) \subseteq I^2 + AI + IB + AB \subseteq I,$$

so I itself contains a finite product of primes containing it. This contradicts the definition of I , so in fact I is prime. Thus we have a contradiction, and (1) follows.

Hence we have a finite set of primes P_1, \dots, P_n containing I such that $P_1 \cdots P_n \subseteq I$. After relabelling, we may assume that $\{P_1, \dots, P_m\}$ are the distinct minimal primes of $\{P_1, \dots, P_n\}$. Thus I contains a product of primes from $\{P_1, \dots, P_m\}$, possibly with repetition:

$$P_{i_1} \cdots P_{i_n} \subseteq I$$

for some $i_1, \dots, i_n \in \{1, \dots, m\}$. Now, suppose Q is any prime containing I . Then $P_{i_1} P_{i_2} \cdots P_{i_n} \subseteq I \subseteq Q$ which forces $P_{i_j} \subseteq Q$ for some j . If Q is a minimal prime over I , Q must equal P_{i_j} .

Finally, we show that each P_k is a minimal prime over I for $k = 1, \dots, m$. If $I \subseteq Q \subseteq P_k$ then $P_j \subseteq Q \subseteq P_k$ for some $j \leq m$ by the above. But P_1, \dots, P_m are the minimal primes in $\{P_1, \dots, P_n\}$, so $P_j = Q = P_k$ and (2) follows. \square

Definition 4.3. Let I be an ideal in a left (or right) Noetherian ring R .

- (a) The *prime radical* $N(R)$ of R is the intersection of all prime ideals of R .
- (b) The *prime radical* \sqrt{I} of I is the intersection of all prime ideals of R that contain I .
- (c) R is *semiprime* if $N(R) = 0$.
- (d) I is said to be *semiprime* if $I = \sqrt{I}$.

Thus I is semiprime if and only if it is the intersection of some collection of prime ideals of R . Note that $\min(I)$ is completely determined by \sqrt{I} because $\min(I) = \min(\sqrt{I})$.

Corollary 4.4. Let R be a left (or right) Noetherian ring. Then

$$N(R) = \bigcap_{P \in \min(0)} P$$

is the largest nilpotent ideal in R .

Proof. Every nilpotent ideal is contained in every prime ideal. Thus $N(R)$ contains every nilpotent ideal. On the other hand, it follows from Proposition 4.2, that a finite product of the minimal primes of R is zero. If there are k terms in this product, then $N(R)^k = 0$, so $N(R)$ is nilpotent. \square

Definition 4.5. Let R be a left or right Noetherian ring. A *dimension function* for R is a rule which assigns to every finitely generated R -module M a number $d(M) \in \mathbb{N}$, such that

$$d(M) = \max\{d(N), d(M/N)\}$$

whenever N is a submodule of M .

Theorem 4.6. Let R be a left or right Noetherian ring. Then every function

$$d : \{R/P : P \in \text{Spec}(R)\} \rightarrow \mathbb{N}$$

such that $d(R/P) \leq d(R/Q)$ whenever $Q \subset P$ extends to a dimension function d for R , given by

$$d(M) = \max\{d(R/P) : P \in \min(\text{Ann}(M))\}$$

for every finitely generated R -module M .

Proof. Let N be a submodule of a finitely generated R -module M , and write $\min(\text{Ann}(M)) = \{P_\alpha\}$, $\min(\text{Ann}(N)) = \{I_\beta\}$ and $\min(\text{Ann}(M/N)) = \{J_\gamma\}$. Now some finite product of the P_α 's kills M by Proposition 4.2, so it kills both N and M/N . It follows that

- every I_β contains some P_α , and
- every J_γ contains some P_α .

Now $d(N) = d(R/I_\beta)$ for some β and I_β contains some P_α , so

$$d(N) = d(R/I_\beta) \leq d(R/P_\alpha) \leq d(M).$$

Similarly, $d(M/N) \leq d(M)$, and we have shown that $d(M) \geq \max\{d(N), d(M/N)\}$. On the other hand, some product, A say, of the I_β 's kills N and some product, B say, of the J_γ 's kills M/N , again by Proposition 4.2. So $BM \subseteq N$ and $AN = 0$, whence $ABM = 0$ and $AB \subseteq \text{Ann}(M)$. It follows that

- every P_α contains either an I_β or a J_γ .

So if $d(M) = d(R/P_\alpha)$ for some α then either P_α contains some I_β , in which case

$$d(M) = d(R/P_\alpha) \leq d(R/I_\beta) \leq d(N),$$

or P_α contains some J_γ , in which case

$$d(M) = d(R/P_\alpha) \leq d(R/J_\gamma) \leq d(M/N).$$

In either case, we see that $d(M) \leq \max\{d(N), d(M/N)\}$. \square

It can be shown that if in addition R is *commutative*, then this extension is unique. More precisely, any dimension function d' for R such that $d(R/P) = d'(R/P)$ for all $P \in \text{Spec}(R)$ must actually be equal to d , and is therefore completely determined by the values that it takes on modules of the form R/P , $P \in \text{Spec}(R)$ — see Exercise 5.3.

Definition 4.7. Let R be a commutative ring.

(a) The *Krull dimension* of R is $\text{Kdim}(R)$ is the supremum of the lengths of chains of prime ideals in R :

$$\text{Kdim}(R) = \max\{n \in \mathbb{N} : \text{there exist } P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n, \quad P_i \in \text{Spec}(R)\}.$$

(b) Let M be a finitely generated R -module. Then

$$\text{Kdim}(M) := \max\{\text{Kdim}(R/P) : P \in \min(\text{Ann}(M))\}$$

is the *Krull dimension* of M .

In general, $\text{Kdim}(R)$ may well be infinite, even if R is Noetherian. However it is always finite if R is a finitely generated commutative algebra over a field k . This follows from the following Theorem, whose proof we omit.

Theorem 4.8. Let R be a finitely generated commutative k -algebra which is a domain. Then

$$\text{Kdim}(R) := \min\{\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) : \mathfrak{m} \text{ is a maximal ideal of } R\}.$$

The proof uses the *Noether Normalisation Lemma* and the fact that every affine variety has a smooth, dense, open subset. Unfortunately we don't have time in this course to give all details of the proof.

Corollary 4.9. Let R be a finitely generated commutative k -algebra. Then Kdim is a dimension function for R .

Proof. In order to apply Theorem 4.6, we just need to check that

$$\text{Kdim}(R/P) \leq \text{Kdim}(R/Q) \quad \text{whenever } Q \subseteq P.$$

Suppose that $P = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ is the longest chain of prime ideals in R starting with P so that $n = \text{Kdim}(R/P)$ by Theorem 4.8. Then this chain induces a chain of prime ideals of R/Q of length n . Thus $n \leq \text{Kdim}(R/Q)$. \square

The vector space $(\mathfrak{m}/\mathfrak{m}^2)^*$ is the *Zariski tangent space* to the affine algebraic variety $X := \text{Spec}(R)$ at the point \mathfrak{m} , so $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ is (roughly speaking) the number of linearly independent tangent vectors to X at the point x .

We also need to borrow the following consequence of the *Weak Nullstellensatz* from C2.6 Commutative Algebra:

Lemma 4.10. If k is an algebraically closed field, then every maximal ideal of the polynomial algebra $k[x_1, \dots, x_n]$ is of the form $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ for some $\alpha \in k^n$.

Proof. Omitted. □

Example 4.11. Let $R = k[x, y]/(xy)$ with k algebraically closed. This is the coordinate ring of a pair of lines $X = \{(a, b) \in k^2 : ab = 0\}$ in the affine plane k^2 . By Lemma 4.10, its maximal ideals are

$$\text{MaxSpec}(R) = \{\langle x - a, y \rangle : 0 \neq a \in k\} \cup \{\langle x, y - b \rangle : 0 \neq b \in k\} \cup \{\langle x, y \rangle\}.$$

If $\mathfrak{m} = \langle x - a, y \rangle$ with $a \neq 0$ then $\mathfrak{m}^2 = \langle (x - a)^2, (x - a)y, y^2 \rangle = \langle (x - a)^2, y \rangle$ and $\mathfrak{m}/\mathfrak{m}^2$ is a one-dimensional vector space spanned by the image of $x - a$. Similarly, if $\mathfrak{m} = \langle x, y - b \rangle$ then $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$. However

$$\langle x, y \rangle^2 = \langle x^2, xy, y^2 \rangle = \langle x^2, y^2 \rangle$$

so $\dim_k \langle x, y \rangle / \langle x^2, y^2 \rangle = 2$: there are two linearly independent tangent directions at the origin. Thus, as might be expected geometrically, $\text{Kdim}(R) = 1$ since it is intuitively clear that X is a one-dimensional space.

Now, let's return to the non-commutative setting and seek a well-behaved dimension function in the case where the ring in question doesn't necessarily have many two-sided ideals.

Definition 4.12. Let R be a filtered ring with filtration $(R_i)_{i \in \mathbb{Z}}$ and let M be a left R -module. A *filtration* on M is a set $(M_i)_{i \in \mathbb{Z}}$ of additive subgroups of M satisfying

- $M_i \subseteq M_{i+1}$ for all $i \in \mathbb{Z}$,
- $R_i \cdot M_j \subseteq M_{i+j}$ for all $i, j \in \mathbb{Z}$,
- $\cup_{i \in \mathbb{Z}} M_i = M$.

Filtered right modules are defined similarly.

Example 4.13. Let M be a left R -module with generating set X . Then $M_i := R_i \cdot X$ for all $i \in \mathbb{Z}$ gives a filtration of M , known as a *standard filtration*.

Definition 4.14. (a) Let $S = \oplus_{i \in \mathbb{Z}} S_i$ be a graded ring. A *graded left S -module* is a left S -module V of the form

$$V = \bigoplus_{i \in \mathbb{Z}} V_i$$

such that $S_i V_j \subseteq V_{i+j}$ for all $i, j \in \mathbb{Z}$.

(b) A *graded left ideal* of S is a left ideal of the form $J = \oplus_{i \in \mathbb{Z}} J_i$, where $J_i \subseteq S_i$ for each $i \in \mathbb{Z}$.

Definition 4.15. Let R be a filtered ring and let M be a filtered left R -module with filtration $(M_i)_{i \in \mathbb{Z}}$. Define the abelian group

$$\text{gr } M = \bigoplus_{i \in \mathbb{Z}} M_i / M_{i-1}.$$

Equip $\text{gr } M$ with a $\text{gr } R$ -action, which is given on homogeneous components by

$$\begin{aligned} R_i / R_{i-1} \times M_j / M_{j-1} &\longrightarrow M_{i+j} / M_{i+j-1} \\ r + R_{i-1} \quad , \quad m + M_{j-1} &\mapsto \quad rm + M_{i+j-1} \end{aligned}$$

and on the whole of $\text{gr } M$ by bilinear extension. Then $\text{gr } M$ becomes a graded left $\text{gr } R$ -module, called the *associated graded module* of M .

Our next goal will be to define a well-behaved dimension function for certain filtered non-commutative rings. For this, we first need to make a digression to study Rees rings and good filtrations.

Definition 4.16. Let R be a filtered ring with filtration $(R_i)_{i \in \mathbb{Z}}$, and let M be a filtered left R -module with filtration $(M_i)_{i \in \mathbb{Z}}$. The *Rees ring* is the following subring \tilde{R} of the ring of Laurent polynomials $R[t, t^{-1}]$:

$$\tilde{R} = \bigoplus_{i \in \mathbb{Z}} R_i t^i \subseteq \bigoplus_{i \in \mathbb{Z}} R t^i = R[t, t^{-1}].$$

The *Rees module* \tilde{M} of M is the abelian group

$$\tilde{M} = \bigoplus_{i \in \mathbb{Z}} M_i t^i$$

where the action of \tilde{R} is given by on homogeneous components by

$$\begin{aligned} R_i t^i \times M_j t^j &\rightarrow M_{i+j} t^{i+j} \\ r_i t^i \quad , \quad m_j t^j &\mapsto \quad r_i m_j t^{i+j}. \end{aligned}$$

Definition 4.17. Let R be a filtered ring and let M be a left R -module. A filtration (M_i) on M is said to be *good* if the Rees module \tilde{M} is finitely generated over \tilde{R} .

Proposition 4.18. Let R be a filtered ring and let M be a left R -module. A filtration (M_i) on M is good if and only if there exist $k_1, k_2, \dots, k_s \in \mathbb{Z}$ and $m_1 \in M_{k_1}, m_2 \in M_{k_2}, \dots, m_s \in M_{k_s}$ such that

$$M_i = R_{i-k_1} m_1 + R_{i-k_2} m_2 + \dots + R_{i-k_s} m_s \quad \text{for all } i \in \mathbb{Z}.$$

Proof. If the graded module \tilde{M} is finitely generated, it has a finite homogeneous generating set $\{t^{k_1} m_1, \dots, t^{k_s} m_s\}$ say, with $m_j \in M_{k_j}$. Then the i -th homogeneous component of \tilde{M} is

$$\begin{aligned} t^i M_i &= R_{i-k_1} t^{i-k_1} (t^{k_1} m_1) + \dots + R_{i-k_s} t^{i-k_s} (t^{k_s} m_s), \quad \text{so} \\ M_i &= R_{i-k_1} m_1 + R_{i-k_2} m_2 + \dots + R_{i-k_s} m_s. \end{aligned}$$

Conversely, any filtration of this form is good, since $\{t^{k_1}m_1, \dots, t^{k_s}m_s\}$ is then a generating set for \widetilde{M} . \square

Corollary 4.19. Every finitely generated module over a filtered ring has at least one good filtration.

Proof. Let $X = \{x_1, \dots, x_s\}$ be a finite generating set for M , and let

$$M_i := R_i x_1 + \dots + R_i x_s = R_i X$$

be the standard filtration on M . It is good by Proposition 4.18. \square

Note that $t \in \widetilde{R}$ is a central regular element, since $1 \in R_1$ always. There is a certain amount of interplay between the Rees ring of R and the associated graded ring $\text{gr } R$.

Lemma 4.20. Let R and M be as above. Then

- (1) $\widetilde{R}/t\widetilde{R} \cong \text{gr } R$ as rings,
- (2) $\widetilde{R}/(t-1)\widetilde{R} \cong R$ as rings,
- (3) $\widetilde{M}/t\widetilde{M} \cong \text{gr } M$ as left $\text{gr } R$ -modules,
- (4) $\widetilde{M}/(t-1)\widetilde{M} \cong M$ as left R -modules.

Proof. We will only prove the result for the rings, leaving the modules as an exercise.

(1). We have an isomorphism of abelian groups

$$\widetilde{R}/t\widetilde{R} = \frac{\bigoplus_{i \in \mathbb{Z}} R_i t^i}{\bigoplus_{i \in \mathbb{Z}} R_{i-1} t^i} \cong \bigoplus_{i \in \mathbb{Z}} R_i / R_{i-1} \cong \text{gr } R.$$

It can be checked that this is also a ring isomorphism.

(2). Define a ring homomorphism $\pi : R[t, t^{-1}] \rightarrow R$ by $\pi(\sum r_i t^i) = \sum r_i$. First we show that $\ker \pi = R[t, t^{-1}](t-1)$. To see this, let $a = \sum a_i t^i \in \ker \pi$ so that $\sum a_i t^i = 0$. Hence $a = a - \sum a_i = \sum a_i (t^i - 1) \in R[t, t^{-1}](t-1)$ because $t^i - 1$ is a multiple of $t-1$ for any $i \in \mathbb{Z}$. Next, we will show that

$$\ker(\pi|_{\widetilde{R}}) = \widetilde{R}(t-1),$$

the inclusion \supseteq being clear. Now

$$\ker(\pi|_{\widetilde{R}}) = \ker \pi \cap \widetilde{R} = R[t, t^{-1}](t-1) \cap \widetilde{R}$$

from above, so suppose that $b(t-1) \in \widetilde{R}$ for some $b = \sum_{i=m}^n b_i t^i \in R[t, t^{-1}]$. Then

$$-b_m t^m + \sum_{i=m+1}^n (b_{i-1} - b_i) t^i + b_n t^{n+1} \in \widetilde{R}$$

and we deduce that $-b_m \in R_m$ and $b_i - b_{i-1} \in R_i$ for all $m < i \leq n$. An induction starting with $i = m$ now shows that $b_i \in R_i$ for all $m \leq i \leq n$ and hence $b \in \widetilde{R}$. Hence $\ker(\pi|_{\widetilde{R}}) = \widetilde{R}(t-1)$ as claimed.

Finally, if $a \in R$ then $a \in R_i$ for some $i \in \mathbb{Z}$ and hence $\pi(at^i) = a$ with $at^i \in \widetilde{R}$; this shows that $\pi|_{\widetilde{R}}$ is surjective. Hence

$$R = \text{im } \pi|_{\widetilde{R}} \cong \widetilde{R} / \ker \pi|_{\widetilde{R}} = \widetilde{R} / \widetilde{R}(t-1)$$

by the First Isomorphism Theorem for rings. \square

So \widetilde{R} is a ring which has both R and $\text{gr } R$ as epimorphic images. It follows that if \widetilde{R} is right (or left) Noetherian, then so are both R and $\text{gr } R$.

Note that if (M_i) is a good filtration, then $\text{gr } M \cong \widetilde{M}/t\widetilde{M}$ is finitely generated over $\text{gr } R$ and $M \cong \widetilde{M}/(t-1)\widetilde{M}$ is finitely generated over R , by Lemma 4.20.

Definition 4.21. Let R be a filtered ring and let M be a left R -module. Two filtrations (M_i) and (M'_i) on M are *algebraically equivalent* (or just *equivalent*) if there exist $c, d \in \mathbb{Z}$ such that

$$M'_i \subseteq M_{i+c} \quad \text{and} \quad M_j \subseteq M'_{j+d} \quad \text{for all } i, j \in \mathbb{Z}.$$

Lemma 4.22. All good filtrations on M are equivalent.

Proof. Take two good filtrations (M_i) and (M'_i) . Then by Proposition 4.18,

$$\begin{aligned} M_i &= R_{i-k_1}m_1 + \cdots + R_{i-k_u}m_u \quad \text{for all } i \\ M'_j &= R_{j-l_1}m'_1 + \cdots + R_{j-l_v}m'_v \quad \text{for all } j. \end{aligned}$$

We can find $c \in \mathbb{Z}$ such that $m'_s \in M_{i_s+c}$ for all $s = 1, \dots, v$. Then $M'_i \subseteq M_{i+c}$ for all i , and similarly there exists $d \in \mathbb{Z}$ such that $M_i \subseteq M'_{i+d}$ for all i . \square

Theorem 4.23. Let R be a filtered ring such that $\text{gr } R$ is commutative and Noetherian, and let M be a finitely generated R -module. Let (M_i) and (M'_i) be two good filtrations on M , and let $\text{gr } M, \text{gr}' M$ be the respective associated graded modules. Then

$$\min(\text{Ann}(\text{gr } M)) = \min(\text{Ann}(\text{gr}' M)).$$

Proof. By Lemma 4.22, we can find an integer $c > 0$ such that

$$M_{i-c} \subseteq M'_i \subseteq M_{i+c} \quad \text{for all } i \in \mathbb{Z}.$$

Let $I = \sqrt{\text{Ann}(\text{gr } M)}$ and $I' = \sqrt{\text{Ann}(\text{gr}' M)}$. Since $\min(\text{Ann}(\text{gr } M)) = \min(I)$, by symmetry it will be sufficient to show that $I \subseteq I'$. Because these ideals are graded and $\text{gr } R$ is commutative, it will be enough to show that every homogeneous element $X \in I$ lies in I' . We can assume that $X = x + R_{n-1}$ for some $x \in R_n$.

Since $I/\text{Ann}(\text{gr } M)$ is a nilpotent ideal by Corollary 4.4, $X^m \in \text{Ann}(\text{gr } M)$ for some $m \in \mathbb{N}$. Thus $x^m + R_{mn-1}$ kills $\text{gr } M$:

$$x^m M_i \subseteq M_{i+mn-1} \quad \text{for all } i \in \mathbb{Z}.$$

Apply this relation repeatedly to deduce that

$$x^{am} M_i \subseteq M_{i+amn-a} \quad \text{for all } i \in \mathbb{Z}, a \in \mathbb{N}.$$

Now, take $a = 3c$ and use $M_{i-c} \subseteq M'_i \subseteq M_{i+c}$ to obtain

$$x^{3cm} M'_i \subseteq x^{3cm} M_{i+c} \subseteq M_{i+3cmn-2c} \subseteq M'_{i+3cmn-c} \quad \text{for all } i \in \mathbb{Z}.$$

Since $X = x + R_{n-1}$ and $c \geq 1$, we see that X^{3cm} kills $\text{gr}' M$:

$$X^{3cm} \in \text{Ann}(\text{gr}' M).$$

Because $\text{gr } R$ is commutative, the image of $X \text{ gr } R$ in $\text{gr } R / \text{Ann}(\text{gr}' M)$ is a nilpotent ideal, so $X \in \sqrt{\text{Ann}(\text{gr}' M)}$. \square

Definition 4.24. Let R be a filtered ring such that $\text{gr } R$ is a finitely generated commutative algebra over a field k , and let M be a finitely generated R -module. Choose a good filtration on M using Corollary 4.19.

- (a) The *set of characteristic primes* of M is $\text{Ch}(M) := \min(\text{Ann}(\text{gr } M))$.
- (b) The *dimension* of M is $d(M) := \text{Kdim}(\text{gr } M)$.

The *characteristic variety* of M is the affine subvariety of $\text{Spec}(\text{gr } R)$ defined by $\text{Ann}(\text{gr } M)$. Its irreducible components are the affine varieties defined by the members of $\text{Ch}(M)$. Theorem 4.23 ensures that $\text{Ch}(M)$ does not depend on the choice of good filtration on M . Since by Definition 4.7 $\text{Kdim}(\text{gr } M)$ only depends on $\text{Ch}(M)$, it also does not depend on this choice.

To ensure that d really is a dimension function for R in the setting of Definition 4.24, we need to do a little more work.

Definition 4.25. Let N be a submodule of a filtered left R -module M .

- The *subspace filtration* $(N_i)_{i \in \mathbb{Z}}$ on N is given by

$$N_i := N \cap M_i.$$

- The *quotient filtration* $((M/N)_i)_{i \in \mathbb{Z}}$ on M/N is given by

$$(M/N)_i := (M_i + N)/N.$$

Proposition 4.26. Let R be a positively filtered ring such that $\text{gr } R$ is a finitely generated commutative algebra over a field k . Then

$$M \mapsto d(M) = \text{Kdim}(\text{gr } M)$$

is a dimension function for R .

Proof. We have to show that $d(M) = \max\{d(N), d(M/N)\}$ whenever N is a submodule of a finitely generated R -module M . Equip M with a good filtration using Corollary 4.19, and endow N and M/N with the subspace and quotient filtrations, respectively. Then by definition, the associated sequence of Rees modules

$$0 \rightarrow \widetilde{N} \rightarrow \widetilde{M} \rightarrow \widetilde{M/N} \rightarrow 0$$

is exact. Now $\text{gr } R$ is Noetherian by Theorem 1.16, so \widetilde{R} is left Noetherian by Exercise 6.7. Thus \widetilde{N} and $\widetilde{M/N}$ are finitely generated over \widetilde{R} , so that the filtrations on N and M are *good*. Now,

$$0 \rightarrow \text{gr } N \rightarrow \text{gr } M \rightarrow \text{gr } M/N \rightarrow 0$$

is an exact sequence of finitely generated $\text{gr } R$ -modules by Exercise 6.5, so

$$\text{Kdim}(\text{gr } M) = \max\{\text{Kdim}(\text{gr } N), \text{Kdim}(\text{gr}(M/N))\}$$

by Corollary 4.9. □

We can now state one of the main results in this course: the proof occupies most of Chapter 5.

Theorem 4.27 (Bernstein's Inequality). Let k be an algebraically closed field of characteristic zero, and let M be a finitely generated, non-zero module over the Weyl algebra $A_n(k)$. Then

$$d(M) \geq n.$$

The Weyl algebra $A_n(k)$ can be thought of as a non-commutative polynomial ring in $2n$ variables because $\text{gr } A_n(k) \cong k[X_1, \dots, X_{2n}]$ by Proposition 1.25. So even though $\text{gr } A_n(k)$ has finitely generated modules of all possible dimensions between 0 and $2n$, non-zero finitely generated $A_n(k)$ -modules M are "large": $n \leq d(M) \leq 2n$.

Remarks 4.28. Even though Theorem 4.23 ensures that $d(M)$ does not depend on the particular choice of good filtration on M , the definition still depends on the choice of filtration on the ring R . It is quite possible that the same non-commutative ring R has two "different" filtrations, in the sense that the respective associated graded rings are not isomorphic. However, using more advanced techniques from homological algebra such as the *bidualising complex*, it can be shown that in fact $d(M)$ does *not* depend on the choice of filtration on the ring R , and is therefore an intrinsic invariant of the R -module M .

5. THE INTEGRABILITY OF THE CHARACTERISTIC VARIETY

Definition 5.1. Let R be a ring. A *Poisson bracket* on R is a function

$$\{, \} : R \times R \rightarrow R$$

such that

- (a) $\{, \}$ is bi-additive,
- (b) $\{x, x\} = 0$ for all $x \in R$,
- (c) $\{x, \{y, z\}\} + \{y, \{z, x\}\} + \{z, \{x, y\}\} = 0$ for all $x, y, z \in R$,
- (d) $\{x, yz\} = \{x, y\}z + y\{x, z\}$ for all $x, y, z \in R$.

In other words, a Poisson bracket is a \mathbb{Z} -Lie bracket on R which is a *bi-derivation* in the sense that the functions $\{x, -\} : R \rightarrow R$ and $\{-, y\} : R \rightarrow R$ are derivations of R for all $x, y \in R$. For example, the commutator bracket on every ring is an example of a Poisson bracket. However, it can happen that a commutative ring has an interesting and non-trivial additional Poisson structure. One of the main mechanisms for constructing Poisson brackets comes from *deformation theory* as follows:

Proposition 5.2. Let \mathcal{R} be a ring and suppose that $\tau \in \mathcal{R}$ is a central element such that $R := \mathcal{R}/\tau\mathcal{R}$ is commutative, and

$$\text{ann}(\tau) = \tau\mathcal{R}.$$

Define $\{, \} : R \times R \rightarrow R$ by the rule

$$\{x + \tau R, y + \tau R\} = z + \tau\mathcal{R}$$

where $[x, y] = \tau z$. Then $\{, \}$ is a well-defined Poisson bracket on R .

Proof. We will check that $\{, \}$ is well-defined. Note that every commutator $[x, y]$ in \mathcal{R} lies in $\tau\mathcal{R}$ because $\mathcal{R}/\tau\mathcal{R}$ is commutative by assumption: this ensures the existence of $z \in \mathcal{R}$ such that $[x, y] = \tau z$. Now suppose that

$$x' = x + \tau a \quad \text{and} \quad y' = y + \tau b \quad \text{for some} \quad a, b \in \mathcal{R}.$$

Then because $\tau^2 = 0$ we have

$$[x', y'] = [x, y] + \tau[x, b] + \tau[a, y].$$

But $[\mathcal{R}, \mathcal{R}] \subseteq \tau\mathcal{R}$ and $\tau^2 = 0$, so in fact $[x', y'] = [x, y]$.

Finally, if $[x, y] = \tau z = \tau z'$ for some $z' \in \mathcal{R}$ then by assumption,

$$z - z' \in \text{ann}(\tau) = \tau\mathcal{R}$$

so $z + \tau\mathcal{R} = z' + \tau\mathcal{R}$. The rest is straightforward. \square

The following elementary Lemma will be useful many times in what follows. It transforms questions about filtered modules into a problem in deformation theory.

Lemma 5.3. Let R be a filtered ring and let M be a filtered left R -module. Let $\mathcal{R} := \widetilde{R}/t^2\widetilde{R}$, $\tau := t + t^2\widetilde{R} \in \mathcal{R}$ and let $\mathcal{N} := \widetilde{M}/t^2\widetilde{M}$. Then $\tau \in \mathcal{R}$ is a central element such that $\tau^2 = 0$, and $\{m \in \mathcal{N} : \tau m = 0\} = \tau\mathcal{N}$.

Proof. Only the last part requires proof. Suppose that $\tau m = 0$ for some $m \in \mathcal{N}$. To show that $m \in \tau\mathcal{N}$ we may assume that m is homogeneous, and thus of the form $m = at^i + t^2\widetilde{M}$ for some $a \in M_i$. Now

$$0 = \tau m = (t + t^2\widetilde{R})(at^i + t^2\widetilde{M}) = at^{i+1} + t^2\widetilde{M}$$

implies that $at^{i+1} \in t^2\widetilde{M}$. But the homogeneous component of $t^2\widetilde{M}$ of degree $i+1$ is $M_{i-1}t^{i+1}$, so $a \in M_{i-1}$. Hence $at^i = t(at^{i-1}) \in t\widetilde{M}$ and thus $m \in \tau\mathcal{N}$. \square

Corollary 5.4. Let R be a filtered ring such that $\text{gr } R$ is commutative. Then there is a Poisson bracket

$$\{, \} : \text{gr } R \times \text{gr } R \rightarrow \text{gr } R$$

such that

$$\{x + R_{i-1}, y + R_{j-1}\} = [x, y] + R_{i+j-2}$$

whenever $x \in R_i$ and $y \in R_j$.

Proof. We form the Rees ring \tilde{R} and set $\mathcal{R} := \tilde{R}/t^2\tilde{R}$. Let $\tau \in \mathcal{R}$ be the image of $t \in \tilde{R}$ in \mathcal{R} ; then $\tau^2 = 0$ and τ is central in \mathcal{R} by Lemma 5.3. Also, $\mathcal{R}/\tau\mathcal{R} \cong \tilde{R}/t\tilde{R} \cong \text{gr } R$ by Lemma 4.20(1), and because R is itself a filtered left R -module,

$$\text{ann}(\tau) = \tau\mathcal{R}$$

by Lemma 5.3. Proposition 5.2 now gives a Poisson bracket $\{, \}$ on $\text{gr } R \cong \mathcal{R}/\tau\mathcal{R}$. If $x \in R_i$ and $y \in R_j$ then $x + R_{i-1}$ and $y + R_{j-1}$ are the images of $xt^i + t^2\tilde{R}$ and $yt^j + t^2\tilde{R}$ respectively under the map $\mathcal{R} \rightarrow \text{gr } R$. Now since $\text{gr } R$ is commutative, $[x, y] \in R_{i+j-1}$ so $[x, y]t^{i+j-1} \in R[t, t^{-1}]$ lies in \tilde{R} . Hence

$$[xt^i + t^2\tilde{R}, yt^j + t^2\tilde{R}] = [x, y]t^{i+j} + t^2\tilde{R} = t([x, y]t^{i+j-1} + t^2\tilde{R})$$

so that

$$\left\{ (xt^i + t^2\tilde{R}) + \tau\mathcal{R}, (yt^j + t^2\tilde{R}) + \tau\mathcal{R} \right\} = ([x, y]t^{i+j-1} + t^2\tilde{R}) + \tau\mathcal{R}.$$

Therefore $\{x + R_{i-1}, y + R_{j-1}\} = [x, y] + R_{i+j-2}$ by the definition of $\{, \}$. \square

We will next calculate the Poisson bracket induced by the Weyl algebra $A_n(k)$. Equip $A_n(k)$ with the filtration by order of differential operator, and recall that

$$\text{gr } A_n(k) \cong k[X_1, \dots, X_n, Y_1, \dots, Y_n]$$

by Proposition 1.25 with X_i in degree zero and Y_j in degree one.

Example 5.5. The Poisson bracket on $\text{gr } A_n(k)$ is given by

$$\{Y_i, X_j\} = \delta_{ij}, \quad \text{and} \quad \{X_i, X_j\} = \{Y_i, Y_j\} = 0 \quad \text{for all } i, j = 1, \dots, n.$$

The goal of this Chapter is to prove the following Theorem.

Theorem 5.6 (Gabber). Let R be a filtered ring such that $\text{gr } R$ is a commutative Noetherian \mathbb{Q} -algebra and let M be a finitely generated R -module. Then

$$\{P, P\} \subset P$$

for every $P \in \text{Ch}(M) = \min(\text{Ann}(\text{gr } M))$.

To see how powerful this Theorem is, we will use it to prove Bernstein's Inequality (Theorem 4.27) after the next Lemma.

Lemma 5.7. Let $(,)$ be a non-degenerate bilinear form on a finite dimensional k -vector space V , and let W be a subspace of V such that $(W, W) = 0$. Then

$$\dim W \leq \frac{1}{2} \dim V.$$

Proof. Since $(,)$ is non-degenerate, the map $\Phi : V \rightarrow V^*$ given by $\Phi(v)(w) = (v, w)$ is injective. Pick a basis $\{f_1, \dots, f_r\}$ for $\Phi(W)$, extend it to a basis $\{f_1, \dots, f_m\}$ for V^* and let $\{v_1, \dots, v_m\}$ be the dual basis for V . Then $\{v_{r+1}, \dots, v_m\}$ is a basis for $W^\perp := \{v \in V : (W, v) = 0\}$ by construction, so $\dim W + \dim W^\perp = \dim V$. But $(W, W) = 0$, so $W \leq W^\perp$ and hence $2 \dim W \leq \dim V$. \square

Proof of Theorem 4.27. Recall from Proposition 1.25(b) that the associated graded ring of $A_n(k)$ with respect to the filtration by order of differential operators is a polynomial algebra over k in $2n$ -variables:

$$R := \text{gr } A_n(k) \cong k[X_1, \dots, X_{2n}].$$

Choose a good filtration on M and let $P \in \text{Ch}(M)$. Every maximal ideal of R/P is of the form \mathfrak{m}/P for some maximal ideal \mathfrak{m} of R containing P , and

$$(\mathfrak{m}/P)/(\mathfrak{m}/P)^2 \cong \mathfrak{m}/(\mathfrak{m}^2 + P)$$

as vector spaces over $F := R/\mathfrak{m}$. By Definition 4.24 and Theorem 4.7, it is enough to prove that

$$\dim_F \frac{\mathfrak{m}}{\mathfrak{m}^2 + P} \geq n$$

for every maximal ideal \mathfrak{m} of R containing P . The Poisson bracket $\{, \}$ on R given in Example 5.5 induces a well-defined alternating F -bilinear form

$$(\cdot, \cdot)_{\mathfrak{m}} : \mathfrak{m}/\mathfrak{m}^2 \times \mathfrak{m}/\mathfrak{m}^2 \rightarrow F$$

given by $(v + \mathfrak{m}^2, w + \mathfrak{m}^2)_{\mathfrak{m}} = \{v, w\} + \mathfrak{m}$. Now because k is algebraically closed, we can write $\mathfrak{m} = (X_1 - \alpha_1, \dots, X_{2n} - \alpha_{2n})$ for some $\alpha \in k^{2n}$ by Lemma 4.10. So the natural map $k \rightarrow F$ is an isomorphism, and if $v_i := X_i - \alpha + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$ then the form $(\cdot, \cdot)_{\mathfrak{m}}$ is given by

$$(v_i, v_j)_{\mathfrak{m}} = \begin{cases} 1 & \text{if } j = i + n \\ -1 & \text{if } i = j + n \\ 0 & \text{otherwise.} \end{cases}$$

by Example 5.5. It follows that $(\cdot, \cdot)_{\mathfrak{m}}$ is non-degenerate. Now $\{P, P\} \subseteq P \subseteq \mathfrak{m}$ by Theorem 5.6, so $(\cdot, \cdot)_{\mathfrak{m}}$ vanishes on the subspace $(P + \mathfrak{m}^2)/\mathfrak{m}^2$ of $\mathfrak{m}/\mathfrak{m}^2$. Hence

$$\dim_k \frac{\mathfrak{m}}{\mathfrak{m}^2 + P} = \dim_k \frac{\mathfrak{m}}{\mathfrak{m}^2} - \dim_k \frac{P + \mathfrak{m}^2}{\mathfrak{m}^2} \geq 2n - n = n$$

by Lemma 5.7. \square

We will use the techniques of *Rees rings* and *noncommutative localisation* to prove Theorem 5.6. First, three preliminary Lemmas.

Lemma 5.8. Let R be a commutative Noetherian ring and let M be a finitely generated, non-zero, R -module. Let $P \in \min(\text{Ann}(M))$ and let $S = R \setminus P$. Then

$$(S^{-1}P)^w \cdot S^{-1}M = 0$$

for some $w \in \mathbb{N}$.

Proof. Since $M \neq 0$, $I := \text{Ann}(M)$ is a proper ideal, so $\min(I)$ is non-empty by Proposition 4.2(1). Write $\min(I) = \{P_1, \dots, P_n\}$ with $P = P_1$. Then

$$P_1^{w_1} P_2^{w_2} \dots P_n^{w_n} \subseteq I$$

for some $w_i \in \mathbb{N}$ by Proposition 4.2(2). Now pass to the localisation $S^{-1}R$:

$$(S^{-1}P_1)^{w_1} (S^{-1}P_2)^{w_2} \dots (S^{-1}P_n)^{w_n} \subseteq S^{-1}I.$$

Now $P_i \not\subseteq P_1$ whenever $i \geq 2$, so $P_i \cap S \neq \emptyset$ and hence $S^{-1}P_i = S^{-1}R$ for all $i \geq 2$. Hence

$$(S^{-1}P)^{w_1} \cdot (S^{-1}M) = 0$$

because $S^{-1}I \cdot S^{-1}M = 0$. \square

Our next result gives a very general mechanism for creating Ore sets. It can be viewed as the start of the theory of *algebraic microlocalisation*.

Lemma 5.9. Let \mathcal{R} be a ring containing a central element $\tau \in \mathcal{R}$ such that $\tau^2 = 0$. Let $\xi : \mathcal{R} \rightarrow R := \mathcal{R}/\tau\mathcal{R}$ be the canonical surjection. If $S \subseteq R$ is a left Ore set in R , then $\xi^{-1}S \subseteq \mathcal{R}$ is a left Ore set in \mathcal{R} .

Proof. Let $a \in \mathcal{R}$, $s \in \xi^{-1}(S)$. Then $ta \equiv bs \pmod{\tau\mathcal{R}}$ for some $t \in \xi^{-1}(S)$, $b \in \mathcal{R}$. So $ta = bs + \tau u$, and also $t'u = b's + \tau u'$ for some $t' \in \xi^{-1}(S)$. But then,

$$(t't)a = t'bs + \tau t'u = t'bs + \tau(b's + \tau u') = (t'b + \tau b')s$$

because $\tau^2 = 0$, and $t't \in \xi^{-1}(S)$. \square

We need one more preliminary result on non-commutative localisation before we can start our proof of Theorem 5.6.

Lemma 5.10. Let S be a left localisable subset of A and let N be a submodule of an A -module M . Then there is an $S^{-1}A$ -linear isomorphism

$$S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N).$$

Proof. There is a map $\alpha : S^{-1}N \rightarrow S^{-1}M$ which sends $s \setminus n \in S^{-1}N$ to $s \setminus n \in S^{-1}M$. It is left $S^{-1}A$ -linear, so its image is an $S^{-1}A$ -submodule. If $s \setminus n$ maps to zero, then there is $t \in S$ such that $tn = 0$. So $s \setminus n = ts \setminus tn = 0$. So α is injective. Now define $\beta : S^{-1}M \rightarrow S^{-1}(M/N)$ by $\beta(s \setminus m) = s \setminus (m + N)$. It is a well-defined, surjective, $S^{-1}A$ -linear map. If $s \setminus m \in \ker \beta$ then $t(m + N) = 0$ for some $t \in S$ so that $tm \in N$. But then

$$s \setminus m = (ts) \setminus (tm) \in S^{-1}N$$

so that $\ker \beta = S^{-1}N$. □

Remarks 5.11. Here is an alternative way of constructing $S^{-1}M$:

$$S^{-1}M \cong S^{-1}A \otimes_A M.$$

So, it follows from Lemma 5.10 that $S^{-1}A$ is a flat right A -module, whenever S is a left localisable subset of A .

Proof of Theorem 5.6. As in the proof of Corollary 5.4, form the Rees ring \tilde{R} and set $\mathcal{R} := \tilde{R}/t^2\tilde{R}$. Let $\xi : \mathcal{R} \rightarrow \text{gr } R$ be the map defined by $\xi(xt^i + t^2\tilde{R}) = x + R_{i-1}$ for $x \in R_i$, and let $\tau = t + t^2\tilde{R} \in \mathcal{R}$. Then τ is central in \mathcal{R} , $\tau^2 = 0$ and

$$\ker \xi = \tau\mathcal{R} = \text{ann}(\tau)$$

by Lemma 5.3. Let $S = \text{gr } R \setminus P$ and set $\mathcal{S} := \xi^{-1}(S)$. Then \mathcal{S} is a left Ore set in \mathcal{R} by Lemma 5.9, and \mathcal{R} is a left Noetherian ring by Exercise 1.4(a) because $\text{gr } R$ is Noetherian, so \mathcal{S} is left localisable by Proposition 3.11. Form the localised ring

$$\mathcal{B} := S^{-1}\mathcal{R}$$

and note that $\mathcal{B}/\tau\mathcal{B} \cong S^{-1}(\mathcal{R}/\tau\mathcal{R}) \cong S^{-1}(\text{gr } R)$ by Proposition 5.10. Note that $\mathcal{P} := S^{-1}\xi^{-1}(P)$ is a two-sided ideal in \mathcal{B} , and

$$\mathcal{B}/\mathcal{P} \cong S^{-1}(\mathcal{R}/\xi^{-1}(P)) \cong S^{-1}(R/P)$$

is the field of fractions of R/P . Thus \mathcal{P} is a maximal ideal in \mathcal{B} .

Choose a good filtration on M and let $\mathcal{N} := \tilde{M}/t^2\tilde{M}$. This is a finitely generated \mathcal{R} -module, and

$$\tau\mathcal{N} \cong \mathcal{N}/\tau\mathcal{N} \cong \text{gr } M$$

as $\text{gr } R \cong \mathcal{R}/\tau\mathcal{R}$ -modules by Lemma 5.3 and Lemma 4.20(2). The localised module

$$\mathcal{M} := S^{-1}\mathcal{N}$$

is finitely generated over \mathcal{B} , and

$$\tau\mathcal{M} \cong \mathcal{M}/\tau\mathcal{M} \cong S^{-1}(\text{gr } M)$$

by Proposition 5.10. By Lemma 5.8, $S^{-1}(\text{gr } M)$ is killed by $(S^{-1}P)^w$ for some $w \in \mathbb{N}$, so $\mathcal{P}^w \cdot \mathcal{M} \subseteq \tau\mathcal{M}$. Hence $\mathcal{P}^{2w} \cdot \mathcal{M} = 0$, so \mathcal{M} is a finitely generated module over

$$\mathcal{A} := \mathcal{B}/\mathcal{P}^{2w}.$$

Let \mathcal{J} be the image of \mathcal{P} in \mathcal{A} ; then \mathcal{J} is a maximal ideal of \mathcal{A} such that $\mathcal{A}/\mathcal{J} \cong \mathcal{B}/\mathcal{P} \cong S^{-1}(R/P)$. Since \mathcal{J} is finitely generated as a one-sided ideal and $\mathcal{J}^{2w} = 0$, the ring \mathcal{A} is left Artinian. So by Theorem 5.12 below,

$$[\mathcal{J}, \mathcal{J}] \subseteq \tau\mathcal{J}.$$

Pulling back to \mathcal{B} , we deduce that $[\mathcal{P}, \mathcal{P}] \subseteq \tau\mathcal{P} + \mathcal{P}^{2w}$. But $\mathcal{B}/\tau\mathcal{B}$ is commutative by construction, so $[\mathcal{P}, \mathcal{P}] \subseteq \tau\mathcal{B}$ and

$$[\mathcal{P}, \mathcal{P}] \subseteq (\tau\mathcal{P} + \mathcal{P}^{2w}) \cap \tau\mathcal{B} \subseteq \tau\mathcal{P} + (\mathcal{P}^{2w} \cap \tau\mathcal{B})$$

by the modular law. But if $x \in \mathcal{B}$ and $\tau x \in \mathcal{P}^{2w}$ then τx kills \mathcal{M} , so $x\mathcal{M} \subseteq \tau\mathcal{M}$ and $x^2\mathcal{M} = 0$. If $x \notin \mathcal{P}$ then x is a unit in \mathcal{B} which would force $\mathcal{M} = 0$. But then $S^{-1}(\text{gr } M) = 0$, and since $\text{gr } M$ is finitely generated, it is killed by some $s \in S$. But then $s \in \text{Ann}(\text{gr } M) \subseteq P$, which contradicts $s \in S$. Hence $x \in \mathcal{P}$, so $[\mathcal{P}, \mathcal{P}] \subseteq \tau\mathcal{P}$.

Finally, let $x, y \in P$ and choose $a, b \in \xi^{-1}(P)$ such that $x = \xi(a)$ and $y = \xi(b)$. Then $[a, b] \in \tau\mathcal{P}$ and $\mathcal{P} = S^{-1}\xi^{-1}(P)$, so there is some $s \in S$ such that $s[a, b] \in \tau\xi^{-1}(P)$. Hence $\xi(s)\{x, y\} \in P$ and $\xi(s) \in S$. But $S = \text{gr } R \setminus P$ and P is prime, so $\{x, y\} \in P$. \square

Thus it remains to prove

Theorem 5.12 (Gabber's Local Theorem). Let \mathcal{A} be a left Artinian \mathbb{Q} -algebra with unique maximal ideal \mathcal{J} and a central element $\tau \in \mathcal{J}$ such that $\tau^2 = 0$ and $\mathcal{A}/\tau\mathcal{A}$ is commutative. Suppose that \mathcal{M} is a finitely generated non-zero \mathcal{A} -module such that

$$\{m \in \mathcal{M} : \tau m = 0\} = \tau\mathcal{M}.$$

Then $[\mathcal{J}, \mathcal{J}] \subseteq \tau\mathcal{J}$.

Only the following easy case of Gabber's Local Theorem is examinable. The full proof can be found in Appendix B.

Theorem 5.13. Theorem 5.12 holds whenever \mathcal{A} contains a central subfield K such that $K \oplus \mathcal{J} = \mathcal{A}$.

Proof. Note that $V := \mathcal{M}/\tau\mathcal{M}$ is a finite dimensional K -vector space, because it is a module of finite length over the commutative Artinian local ring $\mathcal{A}/\tau\mathcal{A}$, and because the subfield K of \mathcal{A} maps isomorphically onto the unique simple \mathcal{A} -module \mathcal{A}/\mathcal{J} . Let $\{v_1 + \tau\mathcal{M}, \dots, v_n + \tau\mathcal{M}\}$ be a basis for V as a K -vector space, and let $\mathcal{N} := \sum_{i=1}^n K[\tau]v_i$. Then $\mathcal{N} + \tau\mathcal{M} = \mathcal{M}$, so $\tau\mathcal{N} = \tau\mathcal{M}$ and hence $\mathcal{M} = \mathcal{N} + \tau\mathcal{N} = \mathcal{N}$. Thus $\{v_1, \dots, v_n\}$ generates \mathcal{M} as a $K[\tau]$ -module. On the other hand, if $\sum_{i=1}^n (\lambda_i + \tau\mu_i)v_i = 0$ for some $\lambda_i, \mu_i \in K$, then looking in $\mathcal{M}/\tau\mathcal{M}$ we see that $\lambda_i = 0$ for each i , and hence $\tau \sum_{i=1}^n \mu_i v_i = 0$. By our assumption on \mathcal{M} , this implies that $\sum_{i=1}^n \mu_i v_i \in \tau\mathcal{M}$. Looking in $\mathcal{M}/\tau\mathcal{M}$ again, we conclude that $\mu_i = 0$ for all i . So, in fact $\{v_1, \dots, v_n\}$ forms a *basis* for \mathcal{M} as a $K[\tau]$ -module.

Since $K[\tau]$ is central in \mathcal{A} , the \mathcal{A} -action on \mathcal{M} gives a representation

$$\rho : \mathcal{A} \longrightarrow \text{End}_{K[\tau]}(\mathcal{M}) \cong M_n(K[\tau]).$$

Now, let $x, y \in \mathcal{J}$ and write $[x, y] = \tau z$ where $z = \lambda + u$ for some $\lambda \in K$ and $u \in \mathcal{J}$. Since \mathcal{J} is the unique maximal ideal of \mathcal{A} , it is nilpotent by Proposition

2.22. Hence u is also nilpotent. Now, apply $\text{tr} \circ \rho$ to this equation:

$$\text{tr} \rho([x, y]) = \text{tr}(\lambda \tau \rho(1)) + \text{tr} \tau \rho(u).$$

Now $\rho([x, y]) = [\rho(x), \rho(y)]$ has trace zero, and $\rho(u)$ is nilpotent, hence it also has trace zero. Since $\text{tr} \rho(1) = n$, we conclude that

$$n\lambda\tau = 0$$

must hold inside the ground ring $K[\tau] = K \oplus K\tau$. But K is a \mathbb{Q} -algebra and $n \geq 1$ since \mathcal{M} is non-zero, so in fact $\lambda = 0$. Hence $[x, y] = \tau u \in \tau\mathcal{J}$ as claimed. \square

Definition 5.14. Let A be a commutative ring.

- (a) A is *local* if it has a unique maximal ideal.
- (b) Let A be a local ring with unique maximal ideal J . A *coefficient field* is a subfield K of A such that $K + J = A$.

Every coefficient field K is isomorphic to A/J : $(K + J)/J \cong K/J \cap K \cong K$ because every proper ideal of a field is zero. Unfortunately coefficient fields do not exist in general, as the example $A = \mathbb{Z}/4\mathbb{Z}$ shows: this ring does not contain any subfield whatsoever. In fact coefficient fields exist in *any* commutative complete Noetherian local ring that contains a field: this is the key ingredient of the proof of Cohen's famous *Structure Theorem for complete commutative Noetherian local rings*. The proof of Theorem 5.12 needs the following statement.

Theorem 5.15. Every commutative local Artinian \mathbb{Q} -algebra has a coefficient field.

Proof. Let \mathcal{S} be the set of subfields of the Artinian \mathbb{Q} -algebra A . It is not empty because A contains a copy of the rational numbers \mathbb{Q} by assumption. If \mathcal{C} is a chain in \mathcal{S} then $\cup \mathcal{C}$ is again a subfield of A , so $\cup \mathcal{C} \in \mathcal{S}$. Hence by Zorn's Lemma 2.3, \mathcal{S} has a maximal element K . We will show that K is the required coefficient field.

Let J be the unique maximal ideal of A , fix $x \in A$ and consider the subring $K[x]$ of A generated by x . Suppose for a contradiction that x is transcendental over K . Then $g(x) \notin J$ for any non-zero $g(X) \in K[X]$, because J is nilpotent by Proposition 2.22. Hence $g(x)$ is a unit in A for all non-zero $g(X) \in K[X]$, which means that the K -algebra homomorphism $K[X] \rightarrow A$ which sends X to x factors through the field of fractions $K(X)$ of $K[X]$. Then the image $K(x)$ of $K(X)$ in A is a subfield of A which properly contains K , contradicting the maximality of K .

Hence x is algebraic over K . Let $I := K[x] \cap J$; then $K[x]/I$ is isomorphic to a K -subalgebra of the field A/J , and it is generated by the algebraic element $x + I$. So $K[x]/I$ is itself a field and hence I is a maximal ideal in $K[x]$. It is also nilpotent because J is nilpotent, so by Lemma 5.16 below we can find $y \in K[x]$ such that $y \equiv x \pmod{I}$ and such that $K[y]$ is a field. The maximality of K now forces $y \in K$, and we conclude that $x \in I + K \subseteq J + K$. Hence $A = J + K$. \square

To complete the proof of Theorem 5.15 it remains to prove the following version of Hensel's Lemma.

Lemma 5.16. Let K be a field of characteristic zero and let A be a K -algebra such that $A = K[x]$ for some $x \in A$. Suppose that I is a maximal, nilpotent ideal in A . Then there exists $y \in A$ such that $y \equiv x \pmod{I}$ and such that $K[y]$ is a field.

Proof. Let $f(X) \in K[X]$ be the monic minimal polynomial of $x+I \in A/I$. We will find a sequence of elements $x_1 := x, x_2, x_3, \dots$ such that $f(x_m) \in I^m$ and $x_m \equiv x \pmod{I}$ for all $m \geq 0$. Assume inductively that $f(x_m) \in I^m$ and consider

$$f(x_m + h) = f(x_m) + hf'(x_m) + \frac{h^2}{2!}f''(x_m) + \dots$$

for some $h \in I^m$; this formal Taylor series makes sense because $h \in I^m$ is nilpotent by assumption and because K has characteristic zero. Now if $f'(x_m) \in I$ then $f'(x) \in I$ since $x_m \equiv x \pmod{I}$. So $f(X)$ divides $f'(X)$ in $K[X]$. This is impossible over a field of characteristic zero, so $f'(x_m) \notin I$. Hence $f'(x_m)$ is a unit in A . Since

$$f(x_m + h) \equiv f(x_m) + hf'(x_m) \pmod{I^{m+1}}$$

we can take $h := -f(x_m)f'(x_m)^{-1}$ and $x_{m+1} := x_m + h$. This completes the induction. Now since I is nilpotent, $I^n = 0$ for some $n \geq 1$ and hence $f(x_n) = 0$. But then $K[x_n]$ is a homomorphic image of the field $K[X]/\langle f(X) \rangle$, so $K[x_n]$ is the required subfield of A with $x_n \equiv x \pmod{I}$. \square

APPENDIX A. ORE'S THEOREM

Let R be a ring, and let S be a left Ore set in R consisting of regular elements. We will define an equivalence relation on $S \times R$, and define the structure of a ring on the set of equivalence classes.

Definition A.1. Define a relation \sim on $S \times R$ by setting

$$(s, a) \sim (t, b)$$

if and only if there exist $c, d \in R$ such that $ca = db$ and $cs = dt \in S$.

Lemma A.2.

(a) Suppose $s_1, s_2, \dots, s_n \in S$. There exist $c_1, c_2, \dots, c_n \in R$ and $s \in S$ such that

$$c_1 s_1 = c_2 s_2 = \dots = c_n s_n = s.$$

(b) Suppose $(s, a) \sim (t, b)$ and $c', d' \in R$ are such that $c's = d't \in S$. Then

$$c'a = d'b.$$

Proof. (a) Proceed by induction on n . When $n = 1$ we can take $c_1 = 1$, so assume $n > 1$. By induction, we can find $b_1, b_2, \dots, b_{n-1} \in R$ such that

$$b_1 s_1 = b_2 s_2 = \dots = b_{n-1} s_{n-1} = u \in S,$$

say. By the left Ore condition, we can find $v \in S$ and $c_n \in R$ such that $vu = c_n s_n$. Since $u, v \in S$ and S multiplicatively closed, $s := vu \in S$. So if $c_i := vb_i \in R$, then

$$c_1 s_1 = \dots = c_{n-1} s_{n-1} = vu = c_n s_n = s.$$

(b) We have $ca = db$ and $cs = dt \in S$ for some $c, d \in R$. The left Ore condition gives $x' \in S$ and $x \in R$ such that $x'(c's) = x(cs)$. Hence $x(dt) = x(d't)$. Since $s, t \in S$ are regular, $xc = x'c'$ and $xd = x'd'$. Hence

$$x'c'a = xca = xdb = xd'b$$

but $x' \in S$ is regular so $c'a = d'b$. \square

The first part of this Lemma shows that “any finite collection of denominators have a common left multiple which is a denominator”, and consequently that any finite set of fractions of the form $s_i \backslash a_i$ “has a common denominator”, that is, each one can be written in the form $s \backslash c_i a_i$ for some $c_i \in R$. It will also be useful to us in the technical verifications below.

Lemma A.3. \sim is an equivalence relation on $S \times R$.

Proof. Since $1 \in S$, we can take $c = d = 1$ and obtain $(s, a) \sim (s, a)$ for any $a \in R, s \in S$. Hence \sim is reflexive. Also, \sim is clearly symmetric.

Suppose $(s, a) \sim (t, b) \sim (u, c)$. By Lemma A.2(a), we can find $d, e, f \in R$ such that $ds = et = fu \in S$. By Lemma A.2(b), $da = eb = fc$, so $(s, a) \sim (u, c)$. \square

Denote the equivalence class of $(r, s) \in R \times S$ by $s \setminus r$ and let Q be the set of equivalence classes.

Definition A.4. We define the *sum* of the elements $s \setminus a$ and $t \setminus b$ of Q to be

$$s \setminus a + t \setminus b := z \setminus (xa + yb)$$

where $x, y \in R$ are any elements given by Lemma A.2(a) such that $xs = yt = z \in S$.

Lemma A.5. Addition is well-defined.

Proof. Suppose $a', b', x', y' \in R$ and $s', t', z' \in S$ are such that

$$s \setminus a = s' \setminus a', \quad t \setminus b = t' \setminus b' \quad \text{and} \quad x's' = y't' = z' \in S.$$

By the left Ore condition, we can find $u, u' \in R$ such that $uz = u'z' \in S$. Hence

$$uxs = u'x's' \in S \quad \text{and} \quad uyt = u'y't' \in S.$$

By Lemma A.2(b), since $s \setminus a = s' \setminus a'$, we have $uxa = u'x'a'$ and similarly $uyb = u'y'b'$. Hence

$$u(xa + yb) = u'(x'a' + y'b') \quad \text{and} \quad uz = u'z' \in S$$

and hence

$$z \setminus (xa + yb) = z' \setminus (x'a' + y'b')$$

So addition is independent of the choices of a, b, s, t, x and y . \square

Since any two fractions can be brought to a common left denominator by Lemma A.2(a), it is easy to verify that addition is commutative and associative, that $1 \setminus 0$ is the zero element and that the additive inverse of $s \setminus a$ is $s \setminus (-a)$.

Definition A.6. The *product* of two elements $s \setminus a$ and $t \setminus b$ in Q is

$$(s \setminus a) \cdot (t \setminus b) := (us) \setminus (cb)$$

for any $c \in R$ and $u \in S$ such that $ua = ct$ given by the left Ore condition.

Lemma A.7. Multiplication is well-defined.

Proof. First we show that this is independent of the choice of $c \in R$ and $u \in S$. Suppose that $c' \in R$ and $u' \in S$ are such that $u'a = c't$. By the left Ore condition, there exist $x, x' \in R$ with $xu = x'u' \in S$. Hence $xct = xua = x'u'a = x'c't$ so $xc = x'c'$ as $t \in S$ is regular. Hence $xcb = x'c'b$ and $xus = x'u's \in S$, so $us \setminus cb = u's \setminus c'b$.

Now, suppose that $s \setminus a = s' \setminus a'$ and $t \setminus b = t' \setminus b'$; we will find $u, u' \in S$ and $c, c' \in R$ such that $us \setminus cb = u's' \setminus c'b'$. First, we bring $t \setminus b$ and $t' \setminus b'$ to a common denominator: there exist $w, w' \in R$ such that $wt = w't' \in S$, whence $wb = w'b'$ by Lemma A.2(b). By the left Ore condition, there exist $u, u' \in S$ and $d, d' \in R$ such that $ua = dwt$ and $u'a' = d'w't'$. Then

$$(s \setminus a)(t \setminus b) = (s \setminus a)(wt \setminus wb) = us \setminus dwb \quad \text{and similarly} \quad (s' \setminus a')(t' \setminus b') = u's' \setminus d'w'b'.$$

By Lemma A.2(a) there exist $x, x' \in R$ such that $xus = x'u's' \in S$. Since $s \setminus a = s' \setminus a'$, we obtain from Lemma A.2(b) that $xua = x'u'a'$. Hence

$$xdwt = xua = x'u'a' = x'd'w't',$$

but $wt = w't' \in S$ is regular so $xd = x'd'$. Finally, as $wb = w'b'$,

$$xdwb = x'd'w'b' \quad \text{and} \quad xus = x'u's' \in S, \quad \text{so} \quad us \setminus dwb = u's' \setminus d'w'b'.$$

Set $c := dw$ and $c' := d'w'$; then $us \setminus cb = u's' \setminus c'b'$. \square

Lemma A.8. Multiplication in Q is associative.

Proof. Let $s \setminus a, t \setminus b, u \setminus c \in Q$. Choose $d \in R$ and $v \in S$ such that $vb = ds$ using the left Ore condition; then $(t \setminus b)(s \setminus a) = vt \setminus da$. Now choose $e \in R$ and $w \in S$ such that $wc = evt$. Now

$$\begin{aligned} (u \setminus c)((t \setminus b)(s \setminus a)) &= (u \setminus c)(vt \setminus da) = wu \setminus eda, \quad \text{and} \\ ((u \setminus c)(t \setminus b))(s \setminus a) &= (wu \setminus evb)(s \setminus a) = wu \setminus eda \end{aligned}$$

because $t \setminus b = (vt) \setminus (vb)$ and $evb = eds$. \square

Theorem A.9. Q is a ring.

Proof. It is easy to check that $1 \setminus 1$ is the identity element in Q , so by Lemmas A.5, A.7 and A.8, it remains to check that the distributive laws hold in Q . Note first that it follows from Definition A.6 that

$$(s \setminus a).(1 \setminus b) = s \setminus ab \quad \text{and} \quad (s \setminus 1).(t \setminus b) = ts \setminus b \quad \text{for any } s, t \in S \quad \text{and} \quad a, b \in R.$$

Given $\alpha = s \setminus a$ and $\beta = t \setminus b \in Q$, choose $x, y \in R$ so that $xs = yt = z \in S$. Let $c \in R$; then

$$(s \setminus a + t \setminus b)(1 \setminus c) = (z \setminus (xa + yb))(1 \setminus c) = z \setminus (xac + ybc) = s \setminus ac + t \setminus bc.$$

We have shown that for any $c \in R$ and $\alpha, \beta \in Q$ we have

$$(\alpha + \beta)(1 \setminus c) = \alpha(1 \setminus c) + \beta(1 \setminus c).$$

Now if $u \in S$, we can apply this to obtain

$$(\alpha(u \setminus 1) + \beta(u \setminus 1))(1 \setminus u) = \alpha + \beta$$

and right multiplying this equation by $u \setminus 1$ gives

$$(\alpha + \beta)(u \setminus 1) = \alpha(u \setminus 1) + \beta(u \setminus 1).$$

Hence we obtain the right distributive law

$$(\alpha + \beta)(u \setminus c) = (\alpha + \beta)(u \setminus 1)(1 \setminus c) = (\alpha(u \setminus 1) + \beta(u \setminus 1))(1 \setminus c) = \alpha(u \setminus c) + \beta(u \setminus c).$$

The left distributive law

$$(s \setminus a)(\beta + \gamma) = (s \setminus a)(\beta + \gamma)$$

is obtained in a similar manner, by writing $s \setminus a$ as the product $(s \setminus 1)(1 \setminus a)$ first. \square

APPENDIX B. PROOF OF GABBER'S LOCAL THEOREM

The proof of Theorem 5.12 is an elaboration on the proof of Theorem 5.13: the assumption that J admits a central subfield complement in A can in fact fail in many examples, but Gabber gets around this in a very clever way.

Throughout this Appendix, we assume that:

- \mathcal{A} is a left Artinian ring with unique maximal ideal \mathcal{J} ,
- $\tau \in \mathcal{A}$ is a central element,
- $\tau^2 = 0$ and $A := \mathcal{A}/\tau\mathcal{A}$ is commutative.
- \mathcal{M} is a finitely generated non-zero \mathcal{A} -module.

Write $J := \mathcal{J}/\tau\mathcal{A}$ and $M := \mathcal{M}/\tau\mathcal{M}$. Choose a coefficient field $K \subset A$ using Theorem 5.15: $K + J = A$. Since J is nilpotent, $J^{t+1}M = 0$ and $J^tM \neq 0$ for some $t \geq 0$. Consider the following chain of K -subspaces of M :

$$0 < J^tM < J^{t-1}M < \dots < JM < M.$$

Because M and J are finitely generated, each $J^nM/J^{n+1}M$ is finite dimensional over K , so we can find a K -basis $\{e_1, \dots, e_s\}$ for M such that the action of every element $x \in A$ on M has upper triangular matrix with respect to this basis:

$$xe_j = \sum_{i=1}^s \chi(x)_{ij} e_i \quad \text{for all } j = 1, \dots, s.$$

In this way we obtain a K -algebra homomorphism $\chi : A \rightarrow M_s(K)$ such $\chi(x)$ is *strictly* upper triangular whenever $x \in J$: $\chi(J) \subseteq \mathfrak{n}_s^+(K)$.

Let \mathcal{K} be the inverse image of K in \mathcal{A} , so that \mathcal{K} contains $\tau\mathcal{A}$ as an ideal and $\mathcal{K}/\tau\mathcal{A} = K$. Choose $\epsilon_1, \dots, \epsilon_s \in \mathcal{M}$ such that $e_i = \bar{\epsilon}_i := \epsilon_i + \tau\mathcal{M}$ for each i ; then $\sum_{i=1}^s \mathcal{K}\epsilon_i + \tau\mathcal{M} = \mathcal{M}$ and hence

$$\mathcal{M} = \sum_{i=1}^s \mathcal{K}\epsilon_i + \tau \left(\sum_{i=1}^s \mathcal{K}\epsilon_i + \tau\mathcal{M} \right) = \sum_{i=1}^s \mathcal{K}\epsilon_i.$$

Lemma B.1.

(a) For all $x \in \mathcal{J}$, there exist $\tilde{\chi}(x) \in \mathfrak{n}_s^+(\mathcal{K})$ and $\mathcal{F}(x) \in M_s(\mathcal{K})$ such that if

$$\Phi(x) := \tilde{\chi}(x) + \tau\mathcal{F}(x) \in M_s(\mathcal{K})$$

then

$$x\epsilon_j = \sum_{i=1}^s \Phi(x)_{ij} \epsilon_i \quad \text{for all } j.$$

(b) For all $x, y \in \mathcal{J}$ there exists $\Gamma(x, y) \in \mathfrak{n}_s^+(\mathcal{K})$ such that

$$xy\epsilon_j = \sum_{i=1}^s (\Phi(x)\Phi(y) + \tau\Gamma(x, y))_{ij} \epsilon_i \quad \text{for all } j.$$

(c) For all $W \in \mathfrak{n}_s^+(A)$ there exists $W' \in \mathfrak{n}_s^+(K)$ such that

$$\sum_{i=1}^s W_{ij} e_i = \sum_{i=1}^s W'_{ij} e_i \quad \text{for all } j.$$

Proof. (a) Since $x e_j \in \sum_{i < j} K e_i$, we can find $\tilde{\chi}(x)_{ij} \in \mathcal{K}$ such that

$$x e_j - \sum_{i < j} \tilde{\chi}(x)_{ij} e_i \in \tau \mathcal{M} = \sum_{i=1}^s \tau \mathcal{K} e_i.$$

So there is a matrix $\mathcal{F}(x) \in M_s(\mathcal{K})$ such that

$$x e_j = \sum_{i < j} \tilde{\chi}(x)_{ij} e_i + \tau \sum_{i=1}^s \mathcal{F}(x)_{ij} e_i.$$

Now set $\tilde{\chi}(x)_{ij} := 0$ whenever $i \leq j$. Note that $\chi(x) = \overline{\tilde{\chi}(x)}$.

(b) By (a), we have $x y e_j = \sum_{i=1}^s x \Phi(y)_{ij} e_i = \sum_{i=1}^s ([x, \Phi(y)_{ij}] + \Phi(y)_{ij} x) e_i$. Now

$$\begin{aligned} \sum_{i=1}^s \Phi(y)_{ij} x e_i &= \sum_{i=1}^s \Phi(y)_{ij} \sum_{k=1}^s \Phi(x)_{ki} e_k = \\ &= \sum_{k=1}^s \left(\sum_{i=1}^s \Phi(y)_{ij} \Phi(x)_{ki} \right) e_k = \\ &= \sum_{i=1}^s \left(\sum_{k=1}^s \Phi(y)_{kj} \Phi(x)_{ik} \right) e_i. \end{aligned}$$

Therefore

$$x y e_j = \sum_{i=1}^s (\Phi(x) \Phi(y) + \mathcal{E}(x, y))_{ij} e_i \quad \text{for all } j$$

where

$$\mathcal{E}(x, y)_{ij} := [x, \Phi(y)_{ij}] + \sum_{k=1}^s [\Phi(y)_{kj}, \Phi(x)_{ik}] \in \mathcal{K}.$$

Since $\Phi(x) = \tilde{\chi}(x) + \tau \mathcal{F}(x)$ and $[\tau \mathcal{A}, \mathcal{A}] \subseteq \tau [\mathcal{A}, \mathcal{A}] \subseteq \tau^2 \mathcal{A} = 0$, we have

$$\mathcal{E}(x, y)_{ij} = [x, \tilde{\chi}(y)_{ij}] + \sum_{k=1}^s [\tilde{\chi}(y)_{kj}, \tilde{\chi}(x)_{ik}].$$

Since $\tilde{\chi}(x), \tilde{\chi}(y) \in \mathfrak{n}_s^+(\mathcal{K})$, $\tilde{\chi}(y)_{kj} \neq 0$ and $\tilde{\chi}(x)_{ik} \neq 0$ imply that $k < j$ and $i < k$. But then $i < j$, so $\mathcal{E}(x, y)_{ij} = 0$ whenever $i \geq j$. Being a sum of commutators in \mathcal{A} , $\mathcal{E}(x, y)_{ij}$ is also an element of $\tau \mathcal{A}$.

Hence $\mathcal{E}(x, y) \in \mathfrak{n}_s^+(\mathcal{K}) \cap M_s(\tau \mathcal{A}) = \tau \mathfrak{n}_s^+(\mathcal{A})$. Choose $W(x, y) \in \mathfrak{n}_s^+(\mathcal{A})$ such that $\mathcal{E}(x, y) = \tau W(x, y)$; then by part (c) below there is some $\Gamma(x, y) \in \mathfrak{n}_s^+(\mathcal{K})$ such that

$$\sum_{i=1}^s W(x, y)_{ij} e_i - \sum_{i=1}^s \Gamma(x, y)_{ij} e_i \in \tau \mathcal{M}.$$

Hence $\sum_{i=1}^s \mathcal{E}(x, y)_{ij} e_i = \tau \sum_{i=1}^s \Gamma(x, y)_{ij} e_i$ and therefore $x y e_j = \sum_{i=1}^s (\Phi(x) \Phi(y) + \tau \Gamma(x, y))_{ij} e_i$ for all j .

(c) Since $A = K + J$, we may assume that $W \in \mathfrak{n}_s^+(J)$. Now for any i, j, b ,

$$W_{ij}e_b = \sum_{a=1}^s \chi(W_{ij})_{ab}e_a$$

and $\chi(W_{ij})_{ab} = 0$ whenever $i \geq j$ or $a \geq b$. Hence

$$\sum_{i=1}^s W_{ij}e_i = \sum_{i=1}^s \sum_{a=1}^s \chi(W_{ij})_{ai}e_a = \sum_{a=1}^s \left(\sum_{i=1}^s \chi(W_{ij})_{ai} \right) e_a = \sum_{i=1}^s \left(\sum_{a=1}^s \chi(W_{aj})_{ia} \right) e_i.$$

Set $W'_{ij} := \sum_{a=1}^s \chi(W_{aj})_{ia} \in K$. Now if $\chi(W_{aj})_{ia} \neq 0$ then $i < a$ and $a < j$. Hence $\chi(W_{aj})_{ia} = 0$ whenever $i \geq j$, so $W' \in \mathfrak{n}_s^+(K)$. \square

Proposition B.2. For all $x, y \in \mathcal{J}$, there exists $\mathcal{G}(x, y) \in \mathfrak{n}_s^+(\mathcal{K})$ such that

$$[x, y]\epsilon_j = \tau \sum_{i=1}^s ([\tilde{\chi}(x), \mathcal{F}(y)] - [\tilde{\chi}(y), \mathcal{F}(x)] + \mathcal{G}(x, y))_{ij} \epsilon_i$$

for all j .

Proof. By parts (a) and (b) of Lemma B.1 we have

$$(xy - yx)\epsilon_j = \sum_{i=1}^s ([\Phi(x), \Phi(y)] + \tau\Gamma(x, y) - \tau\Gamma(y, x))_{ij} \epsilon_i \quad \text{for all } j$$

where $\Phi(x) = \tilde{\chi}(x) + \tau\mathcal{F}(x)$ and $\Gamma(x, y), \Gamma(y, x) \in \mathfrak{n}_s^+(\mathcal{K})$. Because $\tau^2 = 0$, we have

$$\begin{aligned} [\Phi(x), \Phi(y)] &= [\tilde{\chi}(x) + \tau\mathcal{F}(x), \tilde{\chi}(y) + \tau\mathcal{F}(y)] = \\ &= [\tilde{\chi}(x), \tilde{\chi}(y)] + \tau[\tilde{\chi}(x), \mathcal{F}(y)] - \tau[\tilde{\chi}(y), \mathcal{F}(x)]. \end{aligned}$$

Now $[\tilde{\chi}(x), \tilde{\chi}(y)] \in \mathfrak{n}_s^+(\mathcal{K})$ since both $\tilde{\chi}(x)$ and $\tilde{\chi}(y)$ lie in $\mathfrak{n}_s^+(\mathcal{K})$. On the other hand, the images of these matrices under $M_s(\mathcal{K}) \twoheadrightarrow M_s(K)$ equal $\chi(x)$ and $\chi(y)$, which commute because $\chi : A \rightarrow M_s(K)$ is a ring homomorphism and A is commutative. This implies that $[\tilde{\chi}(x), \tilde{\chi}(y)] \in \ker(M_s(\mathcal{K}) \rightarrow M_s(K)) = M_s(\tau\mathcal{A})$. Thus $[\tilde{\chi}(x), \tilde{\chi}(y)] \in \mathfrak{n}_s^+(\mathcal{K}) \cap M_s(\tau\mathcal{A}) = \tau\mathfrak{n}_s^+(\mathcal{A})$. So there is $W(x, y) \in \mathfrak{n}_s^+(\mathcal{A})$ such that

$$[\tilde{\chi}(x), \tilde{\chi}(y)] = \tau W(x, y).$$

By Lemma B.1(c), we can further find some $W'(x, y) \in \mathfrak{n}_s^+(\mathcal{K})$ such that

$$\sum_{i=1}^s W(x, y)_{ij} \epsilon_i - \sum_{i=1}^s W'(x, y)_{ij} \epsilon_i \in \tau\mathcal{M}.$$

Therefore

$$[x, y]\epsilon_j = \tau \sum_{i=1}^s ([\tilde{\chi}(x), \mathcal{F}(y)] - [\tilde{\chi}(y), \mathcal{F}(x)] + W'(x, y) + \Gamma(x, y) - \Gamma(y, x))_{ij} \epsilon_i$$

for all j , and we may take $\mathcal{G}(x, y) := \Gamma(x, y) - \Gamma(y, x) + W'(x, y) \in \mathfrak{n}_s^+(\mathcal{K})$. \square

Finally, we can prove Theorem 5.12.

Theorem B.3. Let \mathcal{A} be a left Artinian \mathbb{Q} -algebra with unique maximal ideal \mathcal{J} and a central element $\tau \in \mathcal{J}$ such that $\tau^2 = 0$ and $\mathcal{A}/\tau\mathcal{A}$ is commutative. Suppose that \mathcal{M} is a finitely generated non-zero \mathcal{A} -module such that

$$\{m \in \mathcal{M} : \tau m = 0\} = \tau\mathcal{M}.$$

Then $[\mathcal{J}, \mathcal{J}] \subseteq \tau\mathcal{J}$.

Proof. Let $x, y \in \mathcal{J}$ and write $[x, y] = \tau z$ for some $z \in \mathcal{A}$. Write $\bar{z} = \lambda + u$ with $\lambda \in K$ and $u \in \mathcal{J}$; we have to show that $\lambda = 0$. Now by Proposition B.2, we have

$$\tau z e_j = \tau \sum_{i=1}^s \mathcal{Z}_{ij} e_i \quad \text{for all } j$$

where $\mathcal{Z} := [\tilde{\chi}(x), \mathcal{F}(y)] - [\tilde{\chi}(y), \mathcal{F}(x)] + \mathcal{G}(x, y)$. By the assumption on our module \mathcal{M} , we can deduce that

$$\bar{z} e_j = \sum_{i=1}^s \overline{\mathcal{Z}_{ij}} e_i.$$

Note that $\chi(x) = \overline{\tilde{\chi}(x)}$ for all $x \in \mathcal{J}$, and write $F(x) := \overline{\mathcal{F}(x)}$, $G(x, y) := \overline{\mathcal{G}(x, y)}$. Because $\{e_1, \dots, e_s\}$ is a K -basis for M and $\chi(1)$ is the identity matrix,

$$\lambda I_s + \chi(u) = [\chi(x), F(y)] - [\chi(y), F(x)] + G(x, y)$$

inside $M_s(K)$. Now $\chi(u)$ and $G(x, y)$ are strictly upper triangular, so they have trace zero. The trace of every commutator is also zero. Therefore

$$s\lambda = \text{tr}([\chi(x), F(y)] - [\chi(y), F(x)] + G(x, y) - \chi(u)) = 0.$$

Because A is a \mathbb{Q} -algebra, we can cancel the positive integer s and obtain $\lambda = 0$. \square