Notes

for MMA330 Commutative Algebra

Carl-Fredrik Lidgren

Contents

0 Chapter 0: Miscellany

Proposition 0.1. *Let A be a commutative ring. For a polynomial $f = a_0 + \cdots + a_n T^n \in A[T]$, define the* content *of f by*

$$c(f) := (a_0, \ldots, a_n).$$

Then

$$c(fg) \subseteq c(f)c(g) \subseteq \sqrt{c(fg)}.$$

Proof. Note that for any ideal I,

$$\sqrt{I} := \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}.$$

Therefore, we have to show that

$$c(fg) \subseteq \mathfrak{p} \implies c(f)c(g) \subseteq \mathfrak{p}.$$

It suffices to see that $c(f)c(g)$ is mapped to (0) in $A/\mathfrak{p}$, so we can assume that A is an integral domain and $\mathfrak{p} = (0)$. In that situation, we have

$$c(fg) = (0) \iff fg = 0 \iff f = 0 \text{ or } g = 0$$

and therefore

$$c(f)c(g) = (0)$$

as desired. ■

Definition 0.2. Let A be a commutative ring, and let $f \in A[T]$. We say f is *primitive* if $c(f) = (1)$.

Remark 0.3. Let A be a unique factorization domain, and let $K = \mathrm{Frac}(A)$. Let $f \in K[T]$ be any polynomial. Then one can write $f = af_0$ where $a \in K$, and $f_0 \in A[T]$ is primitive. This is called a *reduced expression* for f, and it is unique up to multiplication by a unit in A. To produce one such decomposition, simply factor each coefficient of f and clear any common factors, packing them into the coefficient a.

Corollary 0.4: Gauss's Lemma. *Let A be a commutative ring. Then, for all $f, g \in A[T]$,*

$$fg \text{ is primitive} \iff f \text{ and } g \text{ are primitive.}$$

Proof. If $c(fg) = (1)$, then

$$(1) = c(fg) \subseteq c(f)c(g) \subseteq (1).$$

Since $IJ \subseteq I$ and $IJ \subseteq J$ for all ideals I, J, we are done.

Conversely, if $c(f) = c(g) = 1$, then

$$(1) = c(f)c(g) \subseteq \sqrt{c(fg)}$$

so $\sqrt{c(fg)} = (1)$. Therefore, there is some $x \in c(fg)$ such that $x^n = 1$, so x is invertible and $c(fg) = (1)$ as desired. ■

Remark 0.5. Consider the situation from Remark 0.3, and let $f, g \in K[T]$ have reduced expressions $f = af_0$ and $g = bg_0$. Then abf_0g_0 is a reduced expression for fg by Corollary 0.4.

1 Chapter 1: Ideals

Definition 1.1. Let R be a commutative ring. An *ideal* of R is a subset $I \subseteq R$ for which $af + bg \in I$ for all $f, g \in I$, $a, b \in R$. That is, it is an R-submodule of R. An ideal $\mathfrak{m}$ is maximal if it is proper and maximal with respect to containment. An ideal $\mathfrak{p}$ is *prime* if it is proper and whenever $fg \in \mathfrak{p}$, either $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$.

Example 1.2. For any morphism $R \longrightarrow S$ of rings, the kernel is an ideal of R.

Example 1.3. Any maximal ideal is prime. An ideal I is prime (resp. maximal) if and only if R/I is an integral domain (resp. a field).

Proposition 1.4. *Let R be a commutative ring, $I \subseteq R$ an ideal. Let $\pi\colon R \longrightarrow R/I$ be the canonical projection. Then π^{-1} induces a bijection*

$$\{\text{ideals of } R/I\} \cong \{\text{ideals of } R \text{ containing } I\}.$$

Furthermore, this preserves prime ideals, hence induces a bijection

$$\pi^{-1}\colon \operatorname{Spec} R/I \xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\} = V(I).$$

1.1 Existence of maximal and prime ideals

Proposition 1.5. *Let R be a commutative ring, $I \subseteq R$ a proper ideal. Then I is contained in a maximal ideal. In particular, an element $f \in R$ is invertible if and only if it is not contained in a maximal ideal.*

Proof. Consider the non-empty poset Σ of ideals in R containing I. Taking the union, each totally ordered subset of Σ has an upper bound, so by Zorn's lemma, there is a maximal element $\mathfrak{m}$ as desired. The last assertion follows by considering the ideal (f). ■

Proposition 1.6. *Let R be a commutative ring, let S be a multiplicative subset of R, and let $I \subseteq R$ be an ideal such that $I \cap S = \varnothing$. Then there is a prime ideal $\mathfrak{p}$ containing I such that $\mathfrak{p} \cap S = \varnothing$.*

Proof. By Zorn's lemma, there is an ideal $\mathfrak{p}$ maximal with respect to the condition that $\mathfrak{p} \supseteq I$ and $\mathfrak{p} \cap S = \varnothing$. It is prime: if $f, g \notin \mathfrak{p}$, then by maximality $(\mathfrak{p}, f) \cap S \neq \varnothing$ and similarly for g, so there are elements $p, q \in \mathfrak{p}$ and $a, b \in R$ such that $p + af$, $q + bg \in S$. Since S is multiplicative, their product is in S, so

$$(p + af)(q + bg) = pq + bgp + afq + abfg = p' + abfg \in S, \quad \text{where } p' \in \mathfrak{p}.$$

Since $\mathfrak{p} \cap S = \varnothing$, it follows that $fg \notin \mathfrak{p}$. ■

1.2 Radicals of ideals

Definition 1.7. Let R be a commutative ring. The *radical* of an ideal I in R is

$$\sqrt{I} := \{f \in R \mid \exists n > 0 \text{ such that } f^n \in I\}.$$

The radical $\sqrt{(0)}$ of (0) is called the *nilradical* of R, and consists of all nilpotent elements of R. An ideal I is called *radical* if $\sqrt{I} = I$.

Proposition 1.8. *Let R be a commutative ring, $I \subseteq R$ an ideal. Then*

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}.$$

In particular, en element of R is nilpotent if and only if it is contained in every prime ideal of R.

Proof. By taking the quotient by I, one reduces to the case where $I = 0$, so we need only show the statement about nilpotents. If $f \in R$ is nilpotent, then clearly it is contained in every prime ideal $\mathfrak{p}$ since $0 \in \mathfrak{p}$. For the converse, we show the contrapositive: if an element f is not nilpotent, then there is some prime $\mathfrak{p}$ such that $f \notin \mathfrak{p}$. If f is not nilpotent, then $\{1, f, f^2, \ldots\}$ is a multiplicative subset of R not containing 0. Applying Proposition 1.6, we find a prime ideal $\mathfrak{p}$ such that $f \notin \mathfrak{p}$. ■

1.3 Prime ideals in the reduction of a commutative ring

Definition 1.9. A commutative ring R is *reduced* if it has no non-zero nilpotents. Given any commutative ring R, the quotient $R_{\text{red}} := R/\sqrt{(0)}$ is called the *reduction* of R.

Remark 1.10. The reduction of R is the universal reduced ring with a morphism from R.

Proposition 1.11. *Let R be a commutative ring. Then the canonical projection $\pi : R \longrightarrow R_{\text{red}}$ induces a bijection*

$$\pi^{-1} : \operatorname{Spec} R_{\text{red}} \xrightarrow{\sim} \operatorname{Spec} R.$$

Proof. Follows by the ideal correspondence theorem and Proposition 1.8. ■

Example 1.12. Let k be a field and consider the quotient $A = k[X, Y]/(Y^2)$. Then the prime ideals of A are in bijection with prime ideals of $k[X]$. Indeed, $A = k[X][Y]/(Y^2)$ has reduction $k[X]$.

1.4 Local rings

Definition 1.13. A commutative ring is *local* if it has a unique maximal ideal. Equivalently, if the non-invertible elements form an ideal.

Example 1.14. Localizations by prime ideal, or power series rings.

Remark 1.15. By the existence of maximal ideals, an element of a local ring R is invertible if and only if it is not contained in the unique maximal ideal. In particular, for every $f \in \mathfrak{m}$, $1 + f$ is invertible, i.e. $1 + \mathfrak{m} \subseteq R^\times$.

1.5 Prime ideals in a one-variable polynomial ring over a PID

Definition 1.16. A commutative ring R is a unique factorization domain if it is an integral domain and every non-zero non-invertible element can be written as a product of finitely many irreducible elements in R, in a way unique up to rearrangement and multiplication by units.

Definition 1.17. A ring is a principal ideal domain if it is an integral domain and each ideal is generated by one element.

Proposition 1.18. *Principal ideal domains are unique factorization domains. Any prime ideal of a principal ideal is maximal.*

Proof. Repeatedly decompose, which must terminate as divisibility chains must stabilize (since PIDs are Noetherian). ∎

Proposition 1.19. *Let B be a principal ideal domain. Then the prime ideals of $B[Y]$ are*

(1) the zero ideal (0),

(2) the principal ideals (f), where $f \in B[Y]$ is irreducible, and

(3) the ideals (p, g) where $p \in B$ is prime, and $g \in B[Y]$ is a polynomial whose image in $B[Y]/(p)$ is irreducible.

In particular, for any maximal ideal $\mathfrak{m} = (p, g)$ of B, the quotient $B[Y]/\mathfrak{m}$ is a finite algebraic extension of $B/(p)$.

Proof. It is clear that the ideals in (1) and (2) are prime. Therefore, let $\mathfrak{p} \subseteq B[Y]$ be a prime ideal, and assume that this contains two elements f_1, f_2 who have no common factor.

Denote by K the field of fractions of B. Then f_1 and f_2 also share no common factor in $K[B]$. Indeed, suppose that they do, and write $f_1 = hg_1$, $f_2 = hg_2$ where $\deg h \geq 1$. Then we may write $h = ah_0$, $g_i = b_i g_{i,0}$ in reduced form, i.e. where $a, b_i \in K$ and $h_0, g_{i,0} \in B[Y]$ are primitive, since PIDs are unique factorization domains. Then the polynomials $h_0 g_{i,0}$ are primitive by Corollary 0.4, so $f_i = hg_i = ab_i h_0 g_{i,0} \in B[Y]$ is a reduced expression for f_i, which then means that $ab_i \in B$. However, then f_1 and f_2 share a common factor, namely h_0.

Now, consider the ideal $(f_1, f_2) \subseteq K[Y]$. Since $K[Y]$ is a PID (hence a UFD) and f_1, f_2 share no common factor, we have that $(f_1, f_2) = K[Y]$, so there are $a, b \in K[Y]$ such that $af_1 + bf_2 = 1$. Clearing denominators, we find some $c \in B$ such that $caf_1 + cbf_2 = c \in B$, so in particular, $B \cap (f_1, f_2) \neq (0)$. Since B is a PID and $B \cap (f_1, f_2)$ is prime, it is also a maximal ideal of B. However, it is contained in $B \cap \mathfrak{p}$, hence $B \cap \mathfrak{p} = B \cap (f_1, f_2) = (p) \subseteq B$. The result follows. ∎

2 Chapter 2: Modules

Definition 2.1. Let R be a commutative ring. A left R-module is an Abelian group M together with an action of R, i.e. a map $R \times M \to M$ such that

(1) $1m = m$,

(2) $(rs)m = r(sm)$,

(3) $r(m+m') = rm + rm'$, and

(4) $(r+s)m = rm + sm$.

A morphism of R-modules is an R-linear morphism of Abelian groups. This organizes into a category $\mathbf{Mod}_R$.

An R-algebra is a commutative ring A together with a map $R \to A$. A morphism of R-algebras $A \to B$ is a morphism of rings compatible with the structure maps. This organizes into a category $\mathbf{Alg}_R$.

Example 2.2. R itself is an R-module, with the obvious multiplication. The R-submodules of R are exactly the ideals of R. Any R-algebra A has the structure of an R-module induced by the structure map. Furthermore, if $A \to B$ is a ring homomorphism, one obtains functors

$$\mathbf{Mod}_A \to \mathbf{Mod}_B, \quad \mathbf{Mod}_B \to \mathbf{Mod}_A$$

given by $(-) \otimes_A B$ on one hand, and restricting scalars on the other.

Example 2.3. For any R-module M, the endomorphism ring $\mathrm{End}(M)$ has the structure of an R-module, given by

$$r\varphi : m \mapsto r\varphi(m).$$

In fact, the map $R \to \mathrm{End}(M)$, $r \mapsto (r\cdot)$ makes $\mathrm{End}(M)$ into an R-algebra.

Example 2.4. For any A-algebra B and element $b \in B$, one may consider the A-module $A[b]$ generated by b.

Remark 2.5. The category $\mathbf{Mod}_A$ has all small limits and all small colimits.

Example 2.6. For a commutative ring A, the modules $\coprod_S A$ given by coproducts of copies of A are called *free modules.*

2.1 Finitely generated modules & Nakayama's lemma

Let A be a commutative ring, and M an A-module. Any such M has a *free resolution*, presenting M in terms of generators, relations, relations between those relations, and so on. In particular, one can define a map

$$\coprod_{x \in M} A \cdot x \twoheadrightarrow M, \quad x \mapsto x$$

and take the kernel. Doing the same procedure over and over again yields a *resolution* of M by free modules. In general, one cannot choose any of these to be finite.

Definition 2.7. An A-module M is *finitely generated* if there is a surjective map

$$\bigoplus_{i=1}^{n} A \twoheadrightarrow M.$$

One says M is of *finite presentation* if there is a map as above for which the kernel is finitely generated.

Remark 2.8. Equivalently, we have a finite subset $\{x_1, \ldots, x_n\} \subseteq M$ for which the map canonical map

$$\bigoplus_{i=1}^{n} A \cdot x_i \twoheadrightarrow M$$

is surjective, i.e. every element of M can be written as a linear combination of the x_i.

Theorem 2.9. *Let A be a commutative ring, and M a f.g. A-module with generators $\{x_1, \ldots, x_n\}$. Let $\varphi \in \mathrm{End}(M)$, and suppose that $I \subseteq A$ is an ideal for which $\varphi(M) \subseteq IM$. Then there is a relation in $\mathrm{End}(M)$ of the form*

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0,$$

where $a_n \in I^n$.

Proof. Note that

$$\varphi(x_i) = \sum_{j=1}^{n} a_{ij}x_j, \quad a_{ij} \in I$$

since $\{x_1, \ldots, x_n\}$ is a generating set and $\varphi(x_i) \in IM$ by assumption. In $\mathrm{End}(M)$, identifying a_{ij} with $\mu_{a_{ij}}$, we can rewrite this as

$$\sum_j (\delta_{ij}\varphi - a_{ij})x_j = 0$$

and thus, considering the matrix $(\delta_{ij}\varphi - a_{ij})$ and its adjugate, we get that $\det(\delta_{ij}\varphi - a_{ij}) = 0$. Expanding this out yields the result. ∎

Corollary 2.10. *Let A be a commutative ring, let I be an ideal of A, and let M a finitely generated A-module such that $IM = M$. Then there is an element $a \in A$ such that $aM = 0$ and $a \in 1 + I$.*

Proof. Consider the identity map $\mathrm{id}_M \in \mathrm{End}(M)$, and apply Theorem 2.9. Then we get that $x + a_1x + \cdots + a_nx = 0$ where $a_i \in I$, and in particular,

$$(1 + b)x = 0$$

where $b \in I$, so that $a = 1 + b \in 1 + I$. ∎

Corollary 2.11: Nakayama's Lemma. *Let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated A-module such that $\mathfrak{m}M = M$. Then $M = 0$.*

Proof. Apply Corollary 2.10 to get an element $a \in 1 + \mathfrak{m} \subseteq A^\times$ such that $aM = 0$. Since a is invertible, it follows that $M = 0$. ∎

Corollary 2.12. *Let A be a local ring with maximal ideal $\mathfrak{m}$, let M be an A-module, and let $N \subseteq M$ be a submodule. Suppose that M/N is finitely generated, and that $M = N + \mathfrak{m}M$. Then $N = M$.*

In particular, letting $k = A/\mathfrak{m}$, if M is finitely generated over A and some elements $x_1, \ldots, x_n \in M$ generate $M/\mathfrak{m}M$ as a k-module, then $x_1, \ldots, x_n$ generate M.

Proof. Since $M = N + \mathfrak{m}M$, we see that $M/N = \mathfrak{m}(M/N)$. Applying Nakayama's lemma, we see that $M/N = 0$, so $M = N$. To see the last statement, let $N = \sum_i Ax_i$. Then

$\mathfrak{m}M + \sum_i Ax_i = M$ since for any $x \in M$ we can write $[x] = \sum_i a_i[x_i]$, so $M = N$. ∎

Remark 2.13. This means that a generating set for $\mathfrak{m}/\mathfrak{m}^2$ lifts to a generating set for $\mathfrak{m}$.

Corollary 2.14. *If A is a commutative ring and I a finitely generated ideal satisfying $I^2 = I$, then I is generated by a single idempotent element.*

Proof. By Corollary 2.10, there is an element $x \in 1 + I$ such that $xI = 0$. Write $x = 1 - e$, where $e \in I$. Since $e(1-e) = 0$, we have that

$$(1-e)^2 = 1 - 2e + e^2 = (1-e) - e(1-e) = 1 - e$$

so that $1 - e$ is idempotent, and thus e is idempotent. Now, let $f \in I$. Then $(1-e)f = 0$, so $f = ef$ and we see that $I = (e)$. ∎

2.2 Exact sequences

Definition 2.15. A sequence of morphisms of A-modules

$$\cdots M^{i-1} \xrightarrow{\varphi^{i-1}} M^i \xrightarrow{\varphi^i} M^i \to \cdots$$

is exact at i if $\operatorname{im}(\varphi^{i-1}) = \ker(\varphi^i)$. The sequence is exact if it is exact for all $i \in \mathbb{Z}$. A *short exact sequence* is an exact sequence of the form

$$0 \to M' \to M \to M'' \to 0.$$

Theorem 2.16. *Consider a short exact sequence*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0.$$

Then the following are equivalent.

(1) There is an isomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \longrightarrow & 0 \\ \| & & \| & & \downarrow{\cong} & & \| & & \| \\ 0 & \longrightarrow & L & \xrightarrow{\iota_L} & L \oplus N & \xrightarrow{\pi_N} & N & \longrightarrow & 0 \end{array}$$

(2) The map β has a section.

(3) The map α has a retraction.

Proof. It is clear that (1) implies (2) and (3). We show that (2) implies (1), as (3) implies (1) is similar. Let $s : N \to M$ be a section of β. It is automatically injective; we want to show that $M = \alpha(L) \oplus s(N) \cong L \oplus N$. First, we have $M = \alpha(L) + s(N)$ since

$$\forall x \in M, \quad x = (x - s(\beta(x))) + s(\beta(x))$$

where we note that $\beta(x - s(\beta(x))) = \beta(x) - \beta(x) = 0$, so that by exactness the first term is in $\alpha(L)$. Additionally, if $s(y) \in \alpha(L) \cap s(N)$, then $s(y) \in \ker \beta$ so that $0 = \beta(s(y)) = y$, so

$s(y) = 0$. Therefore, this sum is direct. ■

3 Chapter 3: The Noetherian Hypothesis

3.1 Noetherian rings and modules

Definition 3.1. Let R be a commutative ring, and let M be an R-module. We say that M is *Noetherian* if any ascending chain

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq M$$

of submodules of M stabilizes at some finite point. We say R is a *Noetherian ring* if it is Noetherian as an R-module.

Remark 3.2. Clearly, any submodule of a Noetherian module is Noetherian. On the other hand, a subring of a Noetherian ring need not be Noetherian.

Proposition 3.3. *Let M be an R-module. The following are equivalent.*

(1) M is Noetherian.

(2) Every submodule of M is finitely generated.

In particular, R is Noetherian if and only if every ideal is finitely generated.

Proof. Assuming (1), if $N \subseteq M$ is a submodule, we can pick elements $x_1, x_2, \ldots, \in N$ to get an ascending chain

$$Ax_1 \subseteq Ax_1 + Ax_2 \subseteq \cdots \subseteq N$$

and so the Noetherian hypothesis implies that there is some n for which $N = \sum_{i=1}^{n} Ax_n$.

Conversely, if (2) holds, and we have some chain of submodules

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq M$$

then the union $\cup_i N_i$ is a submodule of M, which is generated by some finite number of elements. Therefore, the chain must stabilize as soon as all those elements have been covered. ■

3.2 Noetherian hypothesis in exact sequences

Proposition 3.4. *Let A be a commutatve ring, and consider a short exact sequence*

$$0 \to L \overset{\alpha}{\hookrightarrow} M \overset{\beta}{\twoheadrightarrow} N \to 0$$

of A-modules. Then M is Noetherian if and only if L and N are Noetherian.

Proof. If M is Noetherian, then because we can identify L with a submodule of M it will be Noetherian. Furthermore, if we are given an ascending chain in N then taking the preimage we get an ascending chain in M which must stabilize, hence the original chain stabilizes.

Conversely, suppose L and N are Noetherian, and consider an ascending chain

$$M_1 \subseteq M_2 \subseteq \cdots$$

in M. Then we get two ascending chains

$$\alpha^{-1}(M_1) \subseteq \alpha^{-1}(M_2) \subseteq \cdots, \quad \text{in } L,$$

and

$$\beta(M_1) \subseteq \beta(M_2) \subseteq \cdots, \quad \text{in } N$$

which must stabilize at some points k, ℓ, since L and N are Noetherian. Let $m = \max\{\ell, k\}$, so that both chains are stable after m, and consider an element $x \in M_{m+1}$. By assumption, $\beta(M_{m+1}) = \beta(M_m)$, so $\beta(x) \in \beta(M_m)$ and there is some $y \in M_m$ such that $\beta(x) = \beta(y)$. In particular, $x - y \in \ker \beta = \operatorname{im} \alpha$, so $x - y = \alpha(z)$. Now, $\alpha(z) = x - y \in M_{m+1}$, so $z \in \alpha^{-1}(M_{m+1}) = \alpha^{-1}(M_m)$, and therefore $\alpha(z) \in M_m$. Finally, $x = z + y \in M_m$, so $M_m = M_{m+1}$. ■

Corollary 3.5. *Let A be a commutative ring, and M_1, M_2 two Noetherian A-modules. Then $M_1 \oplus M_2$ is Noetherian.*

Proof. Consider the short exact sequence

$$0 \longrightarrow M_1 \hookrightarrow M_1 \oplus M_2 \twoheadrightarrow M_2 \longrightarrow 0$$

and conclude using the above proposition. ■

Corollary 3.6. *Let A be a commutative ring.*

(1) If $\{M_i\}_{i=1}^n$ are Noetherian A-modules, then $\bigoplus_i M_i$ is Noetherian.

(2) If A is Noetherian, then an A-module M is Noetherian if and only if it is finitely generated.

(3) If A is Noetherian and M is an A-module, then any submodule $N \subseteq M$ is finitely generated.

(4) If A is Noetherian and $A \longrightarrow B$ is a finite A-algebra, then B is Noetherian.

3.3 The Hilbert basis theorem

Theorem 3.7. *Let A be a Noetherian ring. Then $A[X]$ is Noetherian.*

Proof. Let $I \subseteq A[X]$ be an ideal; we will show it is finitely generated. Consider the auxiliary sets

$$J_i := \{a \in A \mid \exists f \in I,\ f = aX^i + \text{lower order terms}\}.$$

Then each J_i is an ideal in A, and since $Xf \in I$ for all $f \in I$, we have an ascending chain

$$J_1 \subseteq J_2 \subseteq \cdots \subseteq A.$$

Since A is Noetherian, this terminates at some point

$$J_n = J_{n+1} = \cdots.$$

In addition, since A is Noetherian, each J_i is finitely generated; for $m \leq n$, let

$$\{f_{m,1}, \ldots, f_{m,r_m}\} \subseteq I$$

be polynomials corresponding to the generating elements of J_m. We may then consider the finite set

$$J = \{f_{m,j}\}_{1\le m\le n, 1\le j\le r_m}.$$

This generates I. To see this, let $f = aX^N + g \in I$, $\deg(g) < f$. If $N \ge n$, then there is some $h \in (J)$ such that $f - X^{N-n}h \in I$ kills the top order term. If $N < n$, then there are some $b \in A$, $h \in (J)$ such that $f - h$ kills the top order term. Thus, by induction, we see that any element of I can be written in terms of elements of J. ■

Corollary 3.8. *Let A be a Noetherian ring. Then $A[X_1, \dots, X_n]$ is Noetherian. In particular, any finitely generated A-algebra $B = A[X_1, \dots, X_n]/I$ is Noetherian.*

4 Chapter 4: Integrality & Normality

Definition 4.1. Let A be a commutative ring, and let B be an A-algebra. An element $b \in B$ is *integral* over A if there is a monic polynomial $f \in A[X]$ such that $f(b) = 0$. We say B is integral over A if every $b \in B$ is integral over A.

4.1 Integrality as finiteness, and tower laws

Theorem 4.2. *Let A be a commutative ring, $A \longrightarrow B$ a ring homomorphism making B an A-algebra. Then the followinig are equivalent.*

(1) $b \in B$ is integral over A.

(2) $A[b] \subseteq B$ is a finitely generated A-module.

(3) b is contained in a finitely generated A-submodule $B' \subseteq B$.

Proof. That (1) implies (2) is clear. If (2) holds, so that $A[b]$ is finitely generated, then clearly $B' = A[b]$ provides (3). Finally, assume (3), and let $B' \ni b$ be some finitely-generated A-submodule with generators $x_1, \dots, x_n$. Then

$$bx_i = \sum_{j=1}^{n} \beta_{ij} x_j, \quad \beta_{ij} \in A.$$

In particular, leting $\beta = (\beta_{ij})$ and $x = (x_i)$, we have

$$(b \cdot \mathrm{id} - \beta)x = 0.$$

Letting γ be the adjugate matrix of $b \cdot \mathrm{id} - \beta$, we have

$$\gamma \cdot (b \cdot \mathrm{id} - \beta)x = \det(b \cdot \mathrm{id} - \beta)x = 0$$

so that $\det(b \cdot \mathrm{id} - \beta) = 0$ since the components of x generate B'. Writing out this determinant now gives an integral expression for b. ■

Corollary 4.3. *Let B be an A-algebra.*

(1) If $b_1, \dots, b_n \in B$ are integral over A, then $A[b_1, \dots, b_n] \subseteq B$ is an integral A-algebra.

(2) *If C is an integral B-algebra, and B is an integral A-algebra, then C is an integral A-algebra.*

(3) *The subset $\tilde{A} = \{b \in B \mid b \text{ is integral over } A\}$ is a subring of B such that $\tilde{\tilde{A}} = \tilde{A}$.*

Proof. (1) is clear by induction. For (2), if $c \in C$ is integral over B then there is some monic $f = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in B[X]$ such that $f(c) = 0$. In particular, c is integral over $A[b_1, \ldots, b_{n-1}]$. However, since each b_i is integral over A, we have that

$$A \longrightarrow A[b_1, \ldots, b_{n-1}, c]$$

is a finitely generated A-module, so c is integral over A. (3) follows by (1) and (2). ∎

4.2 Interal closures and normalizations

Definition 4.4. Let $A \subseteq B$ be a ring extension. The *integral closure* of A in B is $\tilde{A}$ from above. If $A = \tilde{A}$, then we say that A is *integrally closed* in B. The integral closure A_{nor} of an integral domain A in its field of fractions is called the *normalization* of A, and A is *normal* if $A = A_{\text{nor}}$.

Proposition 4.5. *Let A be a unique factorization domain. Then A is normal.*

Proof. Let K be the field of fractions of A, and let $f \in A[T]$ be a monic polynomial with a root $\alpha \in K$. Write

$$f = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \quad \text{and} \quad \alpha = \frac{p}{q}$$

where $p, q \in A$ have no common non-invertible factors. Then

$$0 = f(\alpha) = \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0.$$

Multiplying by q^n, we get

$$0 = q^n f(\alpha) = p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n,$$

and therefore

$$-p^n = a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n.$$

We conclude that q divides p^n, which is a contradiction since, by assumption, they share no factors. ∎

Example 4.6. Let k be a field, and consider $A = k[X, Y]/(Y^2 - X^3)$. Let $x = [X]$, $y = [Y]$, so that $A = k[x, y]$. Then $A_{\text{nor}} = k[t]$ where $t = y/x$. To see this, first note that $\text{Frac}(A) = k(t)$. Since $t^2 = y^2/x^2 = x^3/x^2 = x$, and $t^3 = xt = y$, we clearly have $t \in A_{\text{nor}}$. On the other hand, $k[t] \cong k[T]$ is a unique factorization domain, hence normal, so $A_{\text{nor}} = k[t]$.

Example 4.7. Let k be a field, and consider $A = k[X, Y]/(Y^2 - X^3 - X^2)$. As above, let $x = [X]$ and $y = [Y]$. Then we again have $A_{\text{nor}} = k[t]$ where $t = y/x$. To see this, note that

$$t^2 = y^2/x^2 = (x^3 + x^2)/x^2 = x + 1, \quad y = xt = t(t^2 - 1)$$

give monic integral relations for t in $\text{Frac}(A) \cong k(t)$. Therefore, $t \in A_{\text{nor}}$, so $k[t] \subseteq A_{\text{nor}}$. On the other hand, $k[t] \cong k[T]$ is normal and $A \subseteq k[t]$.

4.3 Integral extensions of fields are fields

Proposition 4.8. *Let $A \subseteq B$ be an integral extension of integral domains. Then A is a field if and only if B is a field.*

Proof. Assume A is a field, and let $b \in B$. Since b is integral, we have a monic polynomial

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Since B is an integral domain, we may assume that $a_0 \neq 0$ (by otherwise cancelling b's until this is true). Rearranging, this gives an inverse for b.

Conversely, if B is a field and $a \in A$, then $a^{-1} \in B$ has an integral dependency relation with coefficients in A, which provides an expression for a^{-1} in terms of elements of A. ■

Corollary 4.9. *Let $A \subseteq B$ be an integral ring extension of integral domains. If $\mathfrak{p}$ is a prime of B, then $\mathfrak{p}$ is maximal if and only if $A \cap \mathfrak{p}$ is maximal in A.*

Proof. Suppose that $\mathfrak{p}$ is a prime ideal of B. Then, taking the quotient, we have

$$A/(A \cap \mathfrak{p}) \subseteq B/\mathfrak{p}.$$

This is an integral extension. By Proposition 4.8, the latter is a field if and only if the former is a field. ■

4.4 Noether normalization

No.

4.5 Primes in integral extensions

Proposition 4.10: Lying over and going down. *Let $A \subseteq B$ be an integral ring extension, and let $\mathfrak{p}$ be a prime of A. Then there is a prime $\mathfrak{q}$ of B such that $A \cap \mathfrak{q} = \mathfrak{p}$. Furthermore, for any ideal $I \subseteq B$ for which $A \cap I \subseteq \mathfrak{p}$, one may choose $\mathfrak{q}$ such that $I \subseteq \mathfrak{q}$.*

Proof. We reduce to the case $I = 0$ by considering the integral extension

$$A/(A \cap I) \subseteq B/I.$$

Therefore, we may assume $I = 0$. On the other hand, we can assume that A is local with maximal ideal $\mathfrak{p}$ is maximal by considering the multiplicative subset $U = A \backslash \mathfrak{p}$ and the integral extension

$$A_{\mathfrak{p}} = A[U^{-1}] \subseteq B[U^{-1}].$$

Now, under these hypotheses, a maximal ideal $\mathfrak{m} \subseteq B$ containing $\mathfrak{p}B$ will satisfy $\mathfrak{m} \cap A \supseteq \mathfrak{p}$, hence $\mathfrak{m} \cap A = \mathfrak{p}$. In particular, such a maximal ideal will exist if and only if $\mathfrak{p}B$ is a proper ideal. It is: if it were not, then $1 \in \mathfrak{p}B$ so

$$1 = p_1 b_1 + \cdots + p_n b_n, \quad p_i \in \mathfrak{p}, \quad b_i \in B.$$

Let $B' = A[b_1, \ldots, b_n]$. We have $1 \in \mathfrak{p}B'$, so that $\mathfrak{p}B' = B'$. By the integrality of $B \supseteq A$, we see that B' is integral over A, so B' is a finitely generated A-module. Applying Nakayama's lemma, we see that $B' = 0$, which would mean that $1 = 0$, a contradiction. ■

Lemma 4.11. *Let $A \subseteq B$ be a ring extension of integral domains. If the induced field extension* $\mathrm{Frac}(A) \subseteq \mathrm{Frac}(B)$ *is algebraic, then any non-zero ideal of B intersects A non-trivially.*

Proof. All ideals contain principal ideals, so it suffices to consider the latter. Let $b \in B$. Then, by the hypothesis, we have a polynomial relationship

$$a_n b^n + \cdots + a_1 b + a_0 = 0, \quad a_i \in \mathrm{Frac}(A).$$

We can assume that $a_0 \neq 0$ by cancellativity, and by cancelling denominators, we can assume that $a_i \in A$ for all $0 \leq i \leq n$. Then $a_0 \in (b) \cap A$ is a non-trivial element of intersection. ∎

Corollary 4.12. *Let $A \subseteq B$ be an integral ring extension, and let $\mathfrak{q}_1, \mathfrak{q}_2 \subseteq B$ be distinct prime ideals such that $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$. Then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are incomparable with respect to inclusion.*

Proof. Suppose that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and that $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \mathfrak{p}$. Taking the quotient, we have an integral extension

$$A/\mathfrak{p} \subseteq B/\mathfrak{q}_1$$

so we may assume that A is an integral domain, $\mathfrak{q}_1 = (0)$, and $\mathfrak{q}_2 \cap A = (0)$. Applying Lemma 4.11, we see that $\mathfrak{q}_2 = (0)$. ∎

5 Chapter 5: The Nullstellensatz

5.1 Jacobson rings

Definition 5.1. A commutative ring R is *Jacobson* if every prime ideal is the intersection of maximal ideals.

Example 5.2. Every field is Jacobson, since (0) is their only prime ideal.

Example 5.3. Quotients of Jacobson rings are Jacobson, by the ideal correspondence theorem.

Lemma 5.4. *Let R be a commutative ring. The following are equivalent.*

(1) R is Jacobson.

(2) If $\mathfrak{p} \subseteq R$ is prime and $R/\mathfrak{p}$ has an element b such that $(R/\mathfrak{p})[b^{-1}]$ is a field, then $R/\mathfrak{p}$ is a field.

(3) For every prime ideal $\mathfrak{p} \subseteq R$, the quotient $R/\mathfrak{p}$ is Jacobson.

Proof. Assume (1) holds. Since $\mathfrak{p}$ is prime, $S := R/\mathfrak{p}$ is an integral domain, so the intersection of the maximal ideals of S is (0). Let $b \in S$ be such that $S[b^{-1}]$ is a field. The prime ideals of $S[b^{-1}]$ correspond to prime ideals in S not containing b, but since $S[b^{-1}]$ is a field, this means b is contained in any non-zero prime ideal of S. It follows that (0) is maximal, since otherwise $b = 0$. Hence S is a field

Now suppose (2) holds, and let $\mathfrak{q} \subseteq R$ be a prime ideal. Let I be the intersection of all maximal ideals containing $\mathfrak{q}$. We want to see that $\mathfrak{q} = I$. If this does not hold, let $f \in I \backslash \mathfrak{q}$; by Proposition 1.6, we find a prime ideal $\mathfrak{p}$ maximal with respect to including $\mathfrak{q}$ but not including f. The ideal $\mathfrak{p}$ cannot be a maximal ideal, so that $R/\mathfrak{p}$ is not a field. On the other hand, inverting f, we see that $\mathfrak{p}R[f^{-1}]$ is maximal, so $(R/\mathfrak{p})[f^{-1}]$ is a field, a contradiction.

That (1) and (3) are equivalent is clear by the ideal correspondence theorem. In particular, if R is Jacobson then (3) follows easily; conversely, if (3) holds, then we consider the reduction of R since they have the same poset of prime ideals. Then $R = R/(0)$ is Jacobson. ∎

5.2 The Nullstellensatz for Jacobson rings

Theorem 5.5. *Let R be a Jacobson ring, and S a finitely generated R-algebra. Then:*

(1) S is Jacobson.

(2) If $\mathfrak{n} \subseteq S$ is maximal, then $\mathfrak{m} := \mathfrak{n} \cap R$ is a maximal ideal of R and $S/\mathfrak{n}$ is a finite extension of $R/\mathfrak{m}$.

Proof. **Step one:** the special case when R is a field and $S = R[X]$. The ring S is of dimension one, i.e. every prime ideal is maximal. Let $\mathfrak{n} = (f) \subseteq S$ be maximal. Since R is a field and $\mathfrak{n}$ is proper, we must have $R \cap \mathfrak{n} = (0)$. By standard field theory, $\dim_R(S/\mathfrak{n}) = \deg f < \infty$, so we see that (2) holds. To see that (1) holds, since every non-zero prime is maximal, we must show that $(0) \subseteq S$ is the intersection of prime ideals in S. To see that this holds, note that S has infinitely many irreducible polynomials, and no non-zero polynomial can be divisible by all of them. This establishes (1) and (2) when R is a field and $S = R[X]$.

Step two: the case when R is Jacobson and S is generated by one element over R. We want to apply Lemma 5.4 to prove (1), so let $\mathfrak{p} \subseteq S$ be a prime ideal such that $\exists b \in S' := S/\mathfrak{p}$ such that $S'[b^{-1}]$ is a field. Write $R' = R/(R \cap \mathfrak{p})$, so we have integral domains R' and S' with S' finitely generated over R' by one element, and we have $b \in S'$ such that $S'[b^{-1}]$ is a field. We will show that R' and S' are fields, which proves both (1) and (2).

Since S' is generated by one element t, there is an isomorphism $R'[x]/\mathfrak{q} \cong S'$ sending x to t, where $\mathfrak{q} \subseteq R'[x]$ is a prime ideal (since S' is an integral domain). We have $\mathfrak{q} \neq (0)$: indeed, otherwise $R'[x] \cong S'$ and we obtain a polynomial $b \in R'[x]$ such that $R'[x][b^{-1}]$ is a field. Letting $K' = \mathrm{Frac}(R')$, we see that $K'[x][b^{-1}]$ is also a field, but by step one (which proves $K'[x]$ is Jacobson) this would imply $K'[x]$ is a field (by Lemma 5.4), which is false. So, $\mathfrak{q} \neq (0)$, and $S'[b^{-1}] \cong K'[x]/\mathfrak{q}K'[x]$.[a]

Pick a non-zero polynomial $p(x) \in \mathfrak{q}$ for which

$$p(t) = p_n t^n + \cdots + p_1 t + p_0 = 0 \quad \text{in } S.$$

Inverting p_n, we see that $S'[p_n^{-1}]$ is integral over $R'[p_n^{-1}]$. Our selected element $b \in S'$ from earlier also satisfies an algebraic equation

$$q(b) = q_m b^m + \cdots + q_1 b + q_0 = 0.$$

Since S' is an integral domains, we may assume that $q_0 \neq 0$ (by dividing out otherwise). Inverting q_0, we see that the field $S'[b^{-1}]$ is integral over $R'[(p_n q_0)^{-1}]$, which implies that $R'[(p_n q_0)^{-1}]$ is a field. Since R' is Jacobson, this means R' is a field, and since S' is then integral over R',[b] it is a field. This completes the proof when R is Jacobson and S is generated by one element.

Step three: R is Jacobson and S is generated by $r > 1$ elements. We proceed by induction. Consider the R-algebra S' generated by $r - 1$ of the generators of S. Then, by assumption, S' is Jacobson, and S is an S'-algebra generated by one element, hence Jacobson. If $\mathfrak{n} \subseteq S$ is a maximal ideal, then $S' \cap \mathfrak{n}$ is a maximal ideal by the case $r = 1$, and

$R \cap \mathfrak{n} = R \cap (S' \cap \mathfrak{n})$ is hence maximal by the induction assumption. The extensions

$$R/(R \cap \mathfrak{n}) \hookrightarrow S'/(S' \cap \mathfrak{n}) \quad \text{and} \quad S'/(S' \cap \mathfrak{n}) \hookrightarrow S/\mathfrak{n}$$

are finite by the induction step and by the case $r = 1$, so that $S/\mathfrak{n}$ is a finite extension of $R/(R \cap \mathfrak{n})$ by the tower law. ■

[a] Why?
[b] Also why?

5.3 The Nullstellensatz for fields

Definition 5.6. Let k be a field. *Affine n-space* over k is defined to be $\mathbb{A}^n(k) := k^n$. For any ideal $I \subseteq k[x_1, \ldots, x_n]$, we associate a set

$$V(I) := \{p \in \mathbb{A}^n(k) \mid \forall f \in I,\ f(p) = 0\}.$$

A subset $X \subseteq \mathbb{A}^n(k)$ is called an *algebraic set* if it is of the form $V(I)$ for some ideal I. To any ideal subset $X \subseteq \mathbb{A}^n(k)$, we associate an ideal

$$I(X) := \{f \in k[x_1, \ldots, x_n] \mid \forall x \in X,\ f(x) = 0\}.$$

Corollary 5.7. *Let k be a field.*

(1) For each $p = (a_1, \ldots, a_n) \in k^n$, the ideal

$$\mathfrak{m}_p := (x_1 - a_1, \ldots, x_r - a_n) \subseteq k[x_1, \ldots, x_n]$$

is maximal.

(2) If k is algebraically closed and $X \subseteq \mathbb{A}^n(k)$ is an algebraic set, then every maximal ideal in $k[x_1, \ldots, x_n]/I(X)$ is of the form $\mathfrak{m}_p/I(X)$ for some $p \in X$.

Proof. (1) is easy, since $k[x_1, \ldots, x_n]/\mathfrak{m}_p \cong k$ is a field. Furthermore, $\mathfrak{m}_p \supseteq I(X)$ if and only if $p \in X$. To prove (2), note that ideals in $k[x_1, \ldots, x_n]/I(X)$ are in bijection with ideals in $k[x_1, \ldots, x_n]$ containing $I(X)$, and this bijection preserves maximal ideals. Thus, we need only check that every maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $\mathfrak{m}_p$ for some $p \in \mathbb{A}^n(k)$. If $\mathfrak{n} \subseteq k[x_1, \ldots, x_n]$ is a maximal ideal, then by the Nullstellensatz for Jacobson rings we see that

$$k = k/(k \cap \mathfrak{n}) \to k[x_1, \ldots, x_n]/\mathfrak{n}$$

is a finite degree field extension. Since k is algebraically closed, it must then be an isomorphism. Let a_i be the preimage of x_i under this isomorphism, and set $p = (a_1, \ldots, a_n)$. Then $\mathfrak{m}_p \subseteq \mathfrak{n}$, so they are equal. ■

Corollary 5.8. *Let k be an algebraically closed field, and let I be an ideal in $k[x_1, \ldots, x_n]$.*

(1) If $I \neq 0$, then $V(I) \neq \varnothing$.

(2) Generically, $I(V(I)) = \sqrt{I}$.

In particular, we have a bijection between algebraic sets and radical ideals.

Proof. For (1), note that I is contained in a maximal ideal $\mathfrak{m}_p$ which will determine a point $p \in V(I)$. For (2), note that points of $V(I)$ correspond to maximal ideals $\mathfrak{m}_p$ containing I. In particular, $I(V(I))$ is the intersection of all maximal ideals containing I, but since $k[x_1, \dots, x_n]$ is Jacobson, this means that $I(V(I))$ is the intersection of all prime ideals containing I. ■

6 Chapter 6: Localizations of Rings & Modules

8 Chapter 8: Discrete Valuation Rings

8.1 Discrete valuations and their corresponding rings of integers

Definition 8.1. Let K be a field. A *discrete valuation* of K is a surjective function

$$v: K^\times \to \mathbb{Z}$$

such that

(DV1) $v(xy) = v(x) + v(y)$, and

(DV2) $v(x \pm y) \geq \min\{v(x), v(y)\}$.

We extend this to a function $v: K \to \mathbb{Z}$ by setting $v(0) := -\infty$.

Proposition 8.2. *Let K be a field with a valuation v. Then*

(1) $v(1) = 0$,

(2) for all $x \in K^\times$, $v(x^{-1}) = -v(x)$, and

(3) for all $x \in K^\times$ and $m \in \mathbb{Z}$, $v(x^m) = mv(x)$.

Proof. For (1), apply (DV1) to see that

$$v(1) = v(1 \cdot 1) = v(1) + v(1) \implies v(1) = 0.$$

For (2), we use (1) and (DV1) to see that

$$0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) \implies v(x^{-1}) = -v(x)$$

as desired. For (3), apply (1), (2) of the proposition, as well as (DV1) in the definition. ■

Proposition 8.3. *Let K be a field and v a discrete valuation on K. Define*

$$\mathcal{O}_K := \{x \in K \mid v(x) \geq 0\}, \quad \mathfrak{m} := \{x \in K \mid v(x) > 0\}.$$

Then the following statements hold.

(1) $\mathcal{O}_K$ is a local ring with maximal ideal $\mathfrak{m}$, and $\mathcal{O}_K^\times = \{x \in K \mid v(x) = 0\}$.

(2) Let $t \in \mathcal{O}_K$ be such that $v(t) = 1$. Then every element $x \in \mathcal{O}_K$ can be written uniquely in the form $x = t^n u$, where $u \in \mathcal{O}_K^\times$.

(3) Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Then $I = (t^n)$ for some $n \geq 0$. In particular, $\mathfrak{m} = (t)$ and $\mathcal{O}_K$ is Noetherian.

Proof. (1) By the definition of a valuation, we have that

$$\forall x, y \in \mathcal{O}_K, \quad xy \in \mathcal{O}_K, \quad x \pm y \in \mathcal{O}_K.$$

In addition, the set $\mathfrak{m}$ clearly forms an ideal. Indeed, if $x \in \mathfrak{m}$ and $r \in \mathcal{O}_K$, then

$$v(rx) = v(r) + v(x) > v(r) \geq 0$$

so that $rx \in \mathfrak{m}$. If $x, y \in \mathfrak{m}$, then

$$v(x + y) \geq \min\{v(x), v(y)\} > 0$$

so that $x + y \in \mathfrak{m}$. Now, if $f \in \mathcal{O}_K$ satisfies $v(f) = 0$, then $f^{-1} \in K$ satisfies

$$v(f^{-1}) = -v(f) = 0 \implies f^{-1} \in \mathcal{O}_K,$$

so $f \in \mathcal{O}_K^\times$. Conversely, if $f \in \mathcal{O}_K^\times$ then $v(f) \geq 0$ and $-v(f) \geq 0$, so $v(f) = 0$. Notably, every non-invertible element is contained in the ideal $\mathfrak{m}$, so that $\mathfrak{m}$ is maximal.

(2) Let $v(t) = 1$, and let $x \in \mathcal{O}_K$. If x is a unit, then $x = t^0 x$ provides the result. Otherwise, $v(x) = n_0 \geq 1$. In particular,

$$v(xt^{-n_0}) = v(x) - n_0 v(t) = n_0 - n_0 = 0 \implies xt^{-n_0} \in \mathcal{O}_K^\times.$$

We then have $x = t^{n_0} \cdot xt^{-n_0}$. If $t^n u = t^m u'$, then

$$v(t^n u) = v(t^m u') \implies n = m,$$

and therefore, dividing out, we have $u = u'$.

(3) Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. If $I = (1)$, then $I = (t^0)$. If I is a proper ideal, by (2) any element of I is of the form $t^\nu u$. Let n be the smallest natural number appearing in the exponent of t. It is clear that $I = (t^n)$. In the case when $I = \mathfrak{m}$, since $t \in \mathfrak{m}$ we easily see that $\mathfrak{m} = (t)$. ■

Definition 8.4. A commutative ring A is a *discrete valuation ring* if there is a field K with a valuation v such that $A \cong \mathcal{O}_K$. The induced element $t \in \mathfrak{m}$ is called a *parameter*, or *uniformizer.*

Lemma 8.5. *Let A be a Noetherian integral domain, and let $t \in A$ be non-invertible. Then*

$$\bigcap_{n=1}^{\infty} (t^n) = 0.$$

Proof. Let $x \in A$. We aim to show that $x \notin \cap_n (t^n)$. Certainly, either $x \notin (t)$ or $x \in (t)$. In the former case, we are done. In the latter, write $x = x^{(1)} t$. If $x^{(1)} \notin (t)$, then $x \notin (t^2)$, and we are done. Repeating the argument, we find a sequence of elements $x^{(n)}$ with inclusions

$$(x) \subseteq (x^{(1)}) \subseteq \cdots (x^{(n)}) \subseteq \cdots A.$$

These inclusions must be strict: in general, if $(y) = (ty)$, then $y = aty$ and $(1 - at)y = 0$ implies that t is a unit, since A is an integral domain. Notably, since A is Noetherian, this implies that the chain must stop at some point n (as otherwise, it would have to stabilize, which is impossible since the inclusions are strict). One then sees that $x \in (t^n) \backslash (t^{n+1})$. ■

8.2 A criterion for being a discrete valuation ring

Proposition 8.6. *Let A be a local integral domain with a principal maximal ideal $\mathfrak{m} = (t)$, and let K be the field of fractions of A. Suppose that $\cap_n (t^n) = 0$. Then A is a discrete valuation ring. More precisely, the following statements hold.*

(1) Let $x \in A \backslash \{0\}$. Then there is a unique representation $x = t^n u$, where $n \geq 0$ and $u \in A^\times$. Moreover, if $x \in K$ then there is a unique representation $x = t^n u$ where $n \in \mathbb{Z}$ and $u \in A^\times$.

(2) Define a map $v \colon A \to \mathbb{Z}_{\geq 0}$ by $v(x) = n$ where $x = t^n u$. This extends to a map $v \colon K \to \mathbb{Z}$ given by

$$v(x/y) := v(x) - v(y), \quad x/y \in K.$$

The map v defines a discrete valuation on K for which $A = \mathcal{O}_K$.

(3) Every non-zero ideal I of A is of the form $I = (t^n)$.

Proof. (1) Let $x \in A \backslash \{0\}$. Find n such that $x \in (t^n) \backslash (t^{n+1})$, so that $x = t^n u$ with $u \notin (t) = \mathfrak{m}$. Since A is a local ring, this means $u \in A^\times$. Clearly, n is uniquely chosen, and if $x = t^n u = t^n u'$, cancelling the t^n's shows $u = u'$ (this is allowed since A is an integral domain). If $x \in K$, write $x = a/b$ where $a = t^n u$ and $b = t^m u'$. Then

$$x = \frac{t^n u}{t^m u'} = t^{n-m} u u'^{-1}.$$

This is clearly unique.

(2) Since $z \in K^\times$ has a unique representation of the form $z = t^n u$, it follows that v is well-defined and that v is surjective. It is clear that $z \in A$ if and only if $v(z) \geq 0$. Thus, it remains to see that v is a valuation. That $v(xy) = v(x) + v(y)$ is trivial, so (DV1) is satisfied. For (DV2), write $x = t^n u$, $y = t^m u'$. Suppose without loss of generality that $n \geq m$. Then

$$v(x \pm y) = v(t^n u \pm t^m u') = m + v(t^{n-m} u + u') \geq m = v(y).$$

Therefore, v is a discrete valuation on K and A is a discrete valuation ring. (3) follows since (1) and (2) prove that A is a discrete valuation ring. ■

Corollary 8.7. *Let A be a commutative ring. Then the following are equivalent.*

(1) A is a discrete valuation ring.

(2) A is a Noetherian local ring such that $\dim_{\Bbbk}(\mathfrak{m}/\mathfrak{m}^2) = 1$ and $\operatorname{Spec} A = \{(0), \mathfrak{m}\}$. Here, $\mathfrak{m}$ is the unique maximal ideal of A and $\Bbbk := A/\mathfrak{m}$.

Proof. If (1) holds, then A is automatically a local Noetherian integral domain and every ideal is of the form (t^n), where t is the uniformizer. It follows that the only prime ideals in A are (0) and (t). Since $\mathfrak{m}$ is generated by one element, so is $\mathfrak{m}/\mathfrak{m}^2$.

Supposing (2) holds, we apply Nakayama's lemma (noting that A is an integral domain since (0) is prime) to see that the generator $[t]$ of $\mathfrak{m}/\mathfrak{m}^2$ lifts to a generator t of $\mathfrak{m}$. Applying the above proposition, we see that A is a discrete valuation ring. ■