# Commutative Algebra

Harry Armitage

November 17, 2020

## Contents

# 0 Introduction

Commutative Algebra is the study of commutative rings and the spaces on which those rings act, namely modules. It was developed from two key sources: algebraic geometry, and algebraic number theory.

In algebraic geometry we are focused on polynomial rings over a field $k$, whilst in number theory we are focused on $\mathbb{Z}$, the ring of rational integers. Much of this work was done by Grothedieck, but the subject goes back much further, at least to Hilbert who wrote a series of papers on polynomial invariant theory in the late nineteenth century.

As an example, take $\Sigma_n$, the symmetric group on the set $\{1, 2, \ldots, n\}$. $\Sigma_n$ acts on $k[x_1, \ldots, x_n]$ by permuting the variables, so that $(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$. $\sigma_n$ acts here via ring automorphisms, and it is then natural to consider the ***ring of invariants***, given by $\{f \in k[\mathbf{x}] : \sigma f = f \quad \forall \sigma \in \Sigma_n] := S$. $S$ is a ring, ***the ring of symmetric polynomials***. We can consider the elementary symmetric functions, which are:

$$\begin{aligned}
e_1(x_1, \ldots, x_n) &= x_1 + \ldots + x_n \\
e_2(x_1, \ldots, x_n) &= \sum_{i<j} x_i x_j \\
&\vdots \\
e_n(x_1, \ldots, x_n) &= x_1 \ldots x_n
\end{aligned}$$

In fact, $S$ is generated as a ring by these $e_i$, and there are canonical maps $k[y_1, \ldots, y_n] \longrightarrow S$ such that $Y_i \mapsto e_i$, which is a ring isomorphism.

Hilbert showed that $S$ is finitely generated, and moreover for many other groups, not just symmetric groups.

Along the way, he proved four very deep theorems:

- Basis theorem
- Nullstellensatz
- The polynomial nature of the Hilbert function (leading to the beginnings of dimension theory)
- The syzygy theorem (leading to the beginnings of homological theory of polynomial rings)

In 1921 Emmy Noether extracted the key property that made the basis theorem, namely that a commutative ring is ***noetherian*** if every ideal is finitely generated (there are several equivalent definitions).

**Theorem 0.1** (Hilbert's Basis Theorem)**.** *If $R$ is a commutative noetherian ring, then $R[x]$ is also noetherian.*

**Corollary 0.2.** *If $k$ is a field, then $k[x_1, \ldots, x_n]$ is noetherian.*

Noether developed a theory of ideals for noetherian rings, for example the existence of primary decomposition, which generalises factorisation into primes in noetherian rings.

### Link between Commutative Algebra and Algebraic Geometry

The starting point for this link is the ***fundamental theorem of algebra***, which says that $f \in \mathbb{C}[x]$ is determined up to scalar multiples by its zeros up to multiplicity. Given $f \in \mathbb{C}[x_1, \ldots, x_n]$, there is a polynomial function $\mathbb{C}^n \to \mathbb{C}$ given by $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$.

Different polynomials will yield different functions, and so $\mathbb{C}[x_1, \ldots, x_n]$ can be viewed as a ring of polynomial functions on complex affine n-space.

More specifically, given $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$, we can define the ***set of common zeros***, $Z(I) = \{(a_1, \ldots, \_n) \in \mathbb{C}^n : f(a_1, \ldots, a_n) = 0 \ \ \forall f \in I\}$, called an ***(affine) algebraic set***.

Remarks:

- One can replace $I$ by the ideal generated by $I$, and you get the same algebraic set. Similarly, replacing an ideal by a generating set of the ideal leaves the algebraic set. The basis theorem asserts that any algebraic set is the set of common zeros of some ***finite*** set of polynomials.
- $\bigcap_j Z(I_j) = Z(\bigcup_j I_j), \bigcup_{j=1}^n Z(i_j) = Z(\prod_{j=1}^n I_j)$, for ideal $I_j$. If we define a topology on $\mathbb{C}^n$ by calling these algebraic sets the closed sets, we get the ***Zariski toplogy***, which is a rather coarser topology on $\mathbb{C}^n$ than the usual topology.
- For $S \subseteq \mathbb{C}^n$, we can define $I(S) = \{f \in \mathbb{C}[x_1, \ldots, x^n] : f(a_1, \ldots, a_n) = 0 \ \ \forall (a_1, \ldots, a_n) \in S\}$. This is an ***ideal*** of $\mathbb{C}[x_1, \ldots, x_n]$, and it is ***radical***, i.e. $f^r \in I(s) \implies f \in I(S)$. The Nullstellensatz is a family of results asserting that the correspondence

$$\begin{aligned} I &\mapsto Z(I) \\ I(S) &\leftarrow\!\shortmid S \end{aligned}$$

gives a bijection between the radical ideals in $\mathbb{C}[x_1, \ldots, x_n]$ and the algebraic subsets of $\mathbb{C}^n$. In particular, the maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ correspond to points in $\mathbb{C}^n$

### Dimension

A large portion of the course deals with the dimension of rings. We can define it in three main ways:

- The maximal length of a chain of prime ideals.
- In a geometric context in terms of growth rates.
- The transcendence degree of a field of fractions.

For commutative rings, all three give the same answer. There is in fact a fourth method, using homological algebra, which in the case of “nice" noetherian rings also gives the same answer.

Most of this theory dates back to 1920-1950. Rings of dimension 0 are called ***artinian*** rings, and in dimension 1 there are special properties which are important in number theory, particularly in the study of algebraic curves.

## 1 Noetherian Rings: Definitions and Examples

Throughout this section, $R$ is a commutative ring with a 1.

**Lemma 1.1.** *Let $M$ be a (left) $R$-module. The following are equivalent:*

1. *All submodules of $M$ (including $M$ itself) are finitely generated.*
2. *The ascending chain condition (ACC) holds: there are no strictly increasing infinite chains of submodules.*
3. *The maximum condition of submodules holds: any nonempty set $S$ of submodules of $M$ has a maximal element $L$, i.e. $L \subseteq L', L' \in S \implies L = L'$.*

*Proof.*
$\underline{1. \implies 2.}$ Suppose there is a strictly increasing chain $N_1 \subsetneq N_2 \subsetneq \ldots$, and let $N = \bigcup_{i=1}^{\infty} N_i$. By *1* $N$ is finitely generated, say by $m_1, \ldots, m_r$. Each $m_i$ lies in some $N_{n_i}$. Then let $n = \max_i n_i$, so that $m_i \in N_n$. Then $N_n = M$, contradicting strict ascent.

$\underline{2. \implies 3.}$ Assume ACC. Pick $M_1 \in S$. If it is the maximal member then we're done. If not, there is $M_2 \supsetneq M_1$. If $M_2$ is maximal, then we're done, otherwise there is some $M_3 \supsetneq M_2$, and so on. By ACC this process terminates, and we get a maximal element.

$\underline{3. \implies 1.}$ Let $N \triangleleft M$, and let $S$ be the collection of all finitely generated submodules of $N$. Then $S \neq \emptyset$ since it contains the 0 submodule. So $S$ contains a maximal member, say $L$. We then claim $N = L$. If $x \in N$ then $L + Rx \in S$, and by maximality of $L$, $x \in L$. □

**Definition 1.2.** *An $R$-module satisfying 1, 2, 3 is* **noetherian**.

**Lemma 1.3.** *Let $N \triangleleft M$. Then $M$ is noetherian if and only if $N$ and $M/N$ are noetherian.*

*Proof.*
$\underline{\implies}$ Let $M$ be noetherian, so that all its submodules are finitely generated. This property is inherited by $N$. Also, the submodules of $M/N$ are all of the form $Q/N$ with $Q \triangleleft M$ containing $N$. If $M$ is noetherian, then $Q$ is finitely generated, say by $x_1, \ldots, x_r$. Then $x_1 + N, \ldots, x_r + N$ generates $Q/N$.

$\underline{\impliedby}$ Let $N, M/N$ be noetherian, and let $L_1 \subset L_2 \subset L_3 \subset \ldots$ be a strictly increasing chain of submodules of $M$. Set $Q_i/N = (L_i + N)/N$, and $N_i = L_i \cap N$. These give ascending chains of submodules of $M/N$ and $N$ respectively. By ACC there are $r, s$ with $Q_i/N = Q_r/N$ for $i \geq r$, $N_i = N_s$ for $i \geq s$. Let $k = \max\{r, s\}$. Then we claim $L_i = L_k$ for $i \geq k$. Pick $\ell \in L_i$, $i \geq k$. Then $\ell + N \in Q_k/N$, and so there is some $\ell' \in L_k$ such that $\ell - \ell' \in N \cap L_i = N \cap L_k$. So $\ell \in L_k$, and the claim is proved. Hence our original ascending chain was not strictly increasing, $\lightning$. □

**Lemma 1.4.**
1. *If $M, N$ are $R$-modules, then $M \oplus N$ is noetherian iff $M$ and $N$ are noetherian.*
2. *If $M_1, \ldots, M_n$ are $R$-modules then $M_1 \oplus \ldots \oplus M_n$ is noetherian iff each $M_i$ is noetherian.*
3. *If $M$ is noetherian then every homomorphic image of $M$ is noetherian.*
4. *Suppose $M$ can be expressed as a sum of finitely many submodules (not necessarily as a direct sum) $M = M_1 + \ldots + M_n$. Then $M$ is noetherian iff each $M_i$ is.*

*Proof.*
1. $M \cong N/N$, so this follows by **1.3**.
2. Apply *1* and induction on $n$.
3. If $\theta : M \to N$ then $\operatorname{im}\theta \cong M/\ker\theta$, so apply **1.3**.

4. The forwards direction follows as $M_i \triangleleft M$. For the reverse, there is a map from $M_1 \oplus \ldots \oplus M_n \to M$, $(m_1, \ldots, m_n) \mapsto m_1 + \ldots + m_n$, and then apply *2* and *3*.

$\square$

**Definition 1.5.** *A ring $R$ is* **noetherian** *if it is noetherian as a (left) $R$-module*

Remark: Submodules of $R$ as an $R$-module are the same as ideals of $R$ as a ring, and so the ACC for modules gives us the ACC for ideals.

**Lemma 1.6.** *Let $R$ be a noetherian ring. Then any finitely generated $R$-module $M$ is noetherian.*

*Proof.* Suppose $M = Rm_1 + \ldots + Rm_n$. There exist $R$-module epimorphisms:

$$R \to Rm_i$$
$$r \mapsto rm_i$$

$R$ is noetherian, so $Rm_i$ is as the homomorphic image of $R$. Then, by **1.4** *(4)*, so is $M$. $\square$

**Theorem 1.7** (Hilbert Basis Theorem)**.** *Let $R$ be a noetherian ring. Then the polynomial ring $R[x]$ is noetherian.*

*Proof.* We show that every ideal of $R[x]$ is finitely generated. Let $I$ be an ideal. We define $I(n) = \{f \in I : \deg f \leq n\}$. Then $I(n) \neq \emptyset$ as $0 \in I(n)$, and $I(0) \subseteq I(1) \subseteq I(2) \subseteq \ldots$.

Let $R(n) = \{\text{Coefficient of } x^n \text{ in } f : f \in I(n)\} \subseteq R$. We claim $R(n) \triangleleft R$, and $R(n) \subseteq R(n+1)$.

To see this, suppose $a, b \in R(n)$. Then there are polynomials $f(x) = ax^n + \ldots, g(x) = bx^n + \ldots$ in $I$, where $\ldots$ indicates lower order terms. Since $I \triangleleft R$, $f \pm g \in I$, $rf \in I$ for all $r \in R$, and $xf \in I$.

Hence $a \pm b \in R(n), ra \in R(n)$, and $a \in R(n+1)$, and the claim is proved.

So then we have a chain $R(0) \subseteq R(1) \subseteq R(2) \subseteq \ldots$ terminates, so we may say $R(n) = R(N)\ \forall n \geq N$. Each of $R(0), \ldots, R(N)$ is a finitely generated ideal of $R$, say $R(j) = (a_{j,i}, \ldots, a_{j,k_j})$.

Then by definition of $R(j)$, we may take polynomials $f_{j,1}, \ldots, f_{j,k_j}$ in $I(j)$ which have the $a_{j,i}$ as their leading coefficients.

Clearly $I \supseteq (f_{j,k} : 0 \leq j \leq N, 1 \leq k \leq k_j) =: J$ - it remains to show that equality holds, then we will have found a finite generating set of $I$. So pick $f \in I$, then we claim $f \in J$, and prove this by induction on the degree of $f$.

If $\deg f = 0$, then $f(x) = a$, say. But then $a \in R(0)$, and so $a = \sum_i r_i a_{0,i}$ for some $r_i \in R$. Since $f_{0,i}$ has $a_{0,i}$ as its leading coefficient and has degree zero, $f_{0,i}(x) = a_{0,i}$, and $f = \sum_i r_i f_{0,i} \in J$.

If instead $\deg f = n$, with $0 < n \leq N$, and the claim holds for all $g$ with $\deg g < n$, then write $f(x) = ax^n + \ldots$. $a \in R(n)$ then by definition, so $a = \sum_i r_{n,i} a_{n,i}$ for some $r_{n,i} \in R$. Then define $g(x) = f(x) - \sum_i r_{n,i} f_{n,i}(x)$. $g(x)$ has degree $\leq n$, and the coefficient of $x^n$ is $a - a = 0$, hence $\deg g < n$. Since $f_{n,i} \in I$, we have $g \in I$, and hence by induction $g \in J$. But $f_{n,i} \in J$ as well, so $f \in J$.

Finally if $\deg f = n$, with $n > N$, and the claim holds for all $g$ with $\deg g < n$, again write $f(x) = ax^n + \ldots$. Then $a \in R(n) = R(N)$, so $a = \sum r_{N,j} a_{N,j}$ for $r_{N,j} \in R$. We may then define $g(x) = f(x) - \sum_i x^{n-N} r_{N,j} f_{N,j}(x)$, and use the same argument as in the previous paragraph to deduce that $f \in J$.

Hence $I \subseteq J$, and so $I = J$ and $I$ is finitely generated. But $I$ was an arbitrary ideal of $R[x]$, so $R[x]$ is noetherian. $\square$

In practice, one uses ***Gröbner bases*** for ideals - these are generating sets with extra properties that make algorithms more efficient.

Examples:

- Fields are noetherian.
- Principle Ideal Domains (PIDs) are noetherian.
- $\{q \in Q : q = \frac{m}{n}, m, n \in \mathbb{Z}, p \nmid n$ for some fixed prime $p\}$, an example of a *localisation* of $\mathbb{Z}$. All localisations of noetherian rings are noetherian - we will see this later.
- $k[x_1, x_2, \ldots]$ is not noetherian: $(x_1) \subsetneq (x_1, x_2) \subsetneq$ is an infinite strictly increasing chain.
- $k[x_1, x_2, \ldots, x_n]$ is noetherian - this follows by induction using the Hilbert basis theorem.
- $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ is noetherian, so any finitely generated commutative ring is noetherian: if $R$ is generated by $r_1, \ldots, r_n$, then there is an epimorphism $\mathbb{Z}[x_1, \ldots, x_n] \to R$ given by $x_i \mapsto r_i$, and $R$ is the homomorphic image of a noetherian ring.
- If $A$ is a free abelian group, write $\mathbb{Z}A$ for its group algebra, which is the set of formal linear combinations of elements of $A$, i.e. terms of the form $\sum_{\alpha \in A} \lambda_\alpha \alpha$ where $\lambda_\alpha \in \mathbb{Z}$ and only finitely many of the $\lambda_\alpha$ are nonzero.

  If $A$ is generated as a group by $g_1, \ldots, g_n$, then its group algebra is generated as a ring by $g_1, g_1^{-1}, \ldots, g_n, g_n^{-1}$.
- $k[[x]]$, the ring of formal power series with coefficients in $k$, is noetherian.

There are also some non-commutative examples that are both left and right noetherian:

- Enveloping algebras of a finite dimensional Lie algebra.
- Iwasawa algebras of compact $p$-adic groups.

**Theorem 1.8.** *If $R$ is noetherian, then $R[[x]]$ is noetherian.*

*Proof 1.* As in **1.7**, consider $R(n)$ = the set of trailing coefficients $a_n$, for elements $a_n x^n$+ higher order terms, and mimic the proof. This is on example sheet 1. $\square$

We will give a second proof, which uses

**Theorem 1.9** (Cohen's Theorem)**.** *If every prime ideal in a ring $R$ is finitely generated, then $R$ is noetherian.*

*Proof.* If $R$ is not noetherian, then there is a family of non-finitely generated ideals. Call it $\mathcal{S}$. By assumption, $\mathcal{S} \neq \emptyset$. Partially order $\mathcal{S}$ by inclusion.

Suppose $I_1 \subseteq I_2 \subseteq \ldots$ is a chain of non-finitely generated ideals. Then we claim $\bigcup_i I_i$ is also non-finitely generated.

If it were, say by $(a_1, \ldots, a_k)$, then $a_i \in I_{n(i)}$ for some finite integer $n(i)$, and so, if $N = max\{n(i) : 1 \leq i \leq k\}$, $N$ is also finite and $a_i \in I_N$ for all $i$. But then $I_N = I_n$ for all $n \geq N$, and in particular $I_N$ is finitely generated $\lightning$.

So $\mathcal{S}$ has upper bounds to its chains, and so we may apply Zorn's lemma to get a maximal element of $\mathcal{S}$, say $I$, so that $I$ is not finitely generated but any ideal containing $I$ is finitely generated.

We now claim $I$ must be prime. Suppose $a \notin I, b \notin I$, but $ab \in I$. Then $I + (a) \supsetneq I$, so $I + (a)$ is finitely generated, say by $i_1 + r_1 a, \ldots, i_n + r_n a$. Define $J = \{s \in R : sa \in I\} \supseteq I + (b) \supsetneq I$. Again, $J$ is finitely generated.

Take $t \in I \subset I + (a)$, so $t = u_1(i_1 + r_1 a) + \ldots + u_n(i_n + r_n a)$ for some $u_i \in R$. So $t = u_1 i_1 + \ldots + u_n i_n + (u_1 r_1 + \ldots + u_n r_n)a \in (i_1) + (i_2) + \ldots + (i_n) + Ja$.

Hence $I \subseteq (i_1) + \ldots + (i_n) + Ja$, so $I = (i_1) + \ldots + (i_n) + Ja$, so $I$ is finitely generated $\lightning$.

So $I$ must be prime, but then by our hypothesis $I$ is still finitely generated $\lightning$. So $R$ must be noetherian. $\square$

We will also use the following lemma:

**Lemma 1.10.** *Let $P$ be a prime ideal of $R[[x]]$ and $\theta : R[[x]] \to R$, $x \mapsto 0$. Then $P$ is finitely generated if and only if $\theta(P)$ is a finitely generated ideal of $R$.*

*Proof.* Clearly if $P$ is finitely generated then $\theta(P)$ is.

Conversely, suppose $\theta(P) = Ra_1 + \ldots + Ra_n$.

If $x \in P$, then $P = (a_1, \ldots, a_n, x)$.

This is immediate - if $g \in P$, $g = a+$ higher order terms. Now $a \in (a_1, \ldots, a_n)$, so $g = \sum_i r_i a_i + xg'$ as required.

If $x \notin P$, then let $f_1, \ldots, f_n$ be power series with constant terms $a_1, \ldots, a_n$ respectively. Then $P = (f_1, \ldots, f_n)$.

Take $g \in p$, say $g = b+$ higher terms, with $b$ the constant term. Then $b = \sum b_i a_i$, so $g - \sum b_i f_i = g_1 x$ for some $g_1$. Note that $g_1 x \in P$, $P$ is prime, and $x \notin P$, so $g_1 \in P$. Similarly, $g_1 = \sum c_i f_i + g_2 x$, and $g_2 \in P$. Continuing, we get $h_1, \ldots, h_n \in R[[x]]$, where $h_i = b_i + c_i x + \ldots$ with $g = h_1 f_1 + \ldots + h_n f_n$. $\square$

We are now ready to give the second proof the $R$ noetherian implies $R[[x]]$ noetherian:

*Proof 2.* Suppose $P$ is a prime ideal of $R[[x]]$. Then $P$ is finitely generated iff $\theta(P)$ is. But $R$ is noetherian, so $\theta(P)$ is finitely generated, so $P$ was finitely generated. Then we apply Cohen's theorem to get $R[[x]]$ noetherian. $\square$

## 1.1 Ideal Structure

Here, we assume $R$ is a commutative ring with a 1, not necessarily noetherian.

**Lemma 1.11.** *The set $N(R)$ of all nilpotent[1] elements of $R$ is an ideal, and $R/N(R)$ has no nonzero nilpotent elements.*

*Proof.* If $x \in N(R)$, then $x^m = 0$ for some $m$. Hence $(rx)^m = 0$ for all $r \in R$, and so $rx \in N(R)$.

If $x, y \in N(R)$, then $x^n = 0$, $y^m = 0$ for some $n, m$. Then $(x+y)^{n+m-1}$ expands to give terms $\lambda x^s y^t$ where $s + t = m + n - 1$. So either $s \geq n$ or $y \geq m$, so all the terms are zero, and $x + y \in N(R)$.

[1] An element $x$ of a ring is called nilpotent if there is some integer $m$ such that $x^m = 0$.

So $N(R) \triangleleft R$.

Finally, if $s \in R/N(R)$ then $s = x + N(R)$. Note that $s^n = x^n + N(R)$ for all $n$. If $x + N(R)$ is nilpotent then $(x + N(R))^m = N(R)$ for some $m$, and hence $x^m \in N(R)$. So $x^m$ is nilpotent, and $(x^m)^n = x^{mn} = 0$ for some $n$. But then $x$ is nilpotent, so $x + N(R) = 0 + N(R)$. □

**Definition 1.12.** *$N(R)$ is called the* **nilradical** *of $R$.*

**Theorem 1.13** (Krull)**.** *$N(R)$ is the intersection of all prime ideals of $R$.*

*Proof.* Let $I = \bigcap_{P \text{ prime}} P$. If $x \in R$ is nilpotent then $x^n = 0 \in P\ \forall P$. So $x \in P\ \forall P \implies x \in I$, so $N(R) \subseteq I$.

Suppose $x$ is not nilpotent. Let $\mathcal{S}$ be the family of ideals $J$ such that for $n > 0$, $x^n \notin J$. Then $(0) \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$, and a union of a chain of ideals in $\mathcal{S}$ is also in $\mathcal{S}$. We apply Zorn's lemma to get a maximal element $J_1$.

We claim $J_1$ is prime - suppose $yz \in J_1$, but $y, z \notin J_1$. So the ideals $J_1 + Ry, J_1 + Rz$ strictly contain $J_1$, and so $x^m \in J_1 + Ry$ and $x^n \in J_1 + Rz$. But then $x^{m+n} \in J_1 + Ryz = J_1 \lightning$.

So $J_1$ is prime, so contains $I$, and hence $x \notin I$, so $I \supseteq N(R)$. Thus $I = N(R)$. □

**Definition 1.14.** *The* **radical** $\sqrt{I}$ *of an ideal $I$ is defined by $\{r \in R : \exists\ k \in \mathbb{N} \text{ s.t. } r^k \in I\}$.*

Note that $\sqrt{I}/I = N(R/I)$, and $\sqrt{I} = \bigcap_{\text{prime } P \supset I} P$. We say an ideal $I$ is radical if $I = \sqrt{I}$

**Definition 1.15.** *The* **Jacobson radical** *$J(R)$ of $R$ is the intersection of all the maximal ideals of $R$ (so $N(R) \subseteq J(R)$).*

**Theorem 1.16** (Nakayama's Lemma)**.** *If $M$ is a finitely generated $R$-module with $MJ = M$, where $J = J(R)$, then $M = 0$.*

*Proof.* [2] If $M \neq 0$ and is a finitely generated $R$-module, then by Zorn's lemma there are maximal proper submodules.

Take $M_1$ maximal in $M$. Then $M/M_1$ is irreducible (or simple), hence generated by $m + M_1$ say.

Then, considering the map $R \to M/M_1; r \mapsto rm + M_1$, which is an $R$-module homomorphism with kernel a maximal ideal, we see that $M/M_1 \cong R/I$, where $I$ is a maximal ideal of $R$, so $MI \leq M_1$

Finally, $J \leq I$, then $MJ \leq MI \leq M_1 \lneq M$, so if $M \neq 0, MJ \lneq M$. □

For a commutative ring $R$, $N(R) \leq J(R)$. These need not be equal - for example, take $R = \left\{\frac{m}{n} \in \mathbb{Q} : p \nmid n\right\} = \mathbb{Z}_{(p)}$. This has unique maximal ideal $P = \left\{\frac{m}{n} \in \mathbb{Q} : p | m, p \nmid n\right\}$. It is an integral domain, so has no nonzero nilpotent elements, so $N(R) = (0)$, and $J(R) = P$.

For rings $R = k[x_1, \ldots, x_n]/I$ with $k$ algebraically closed and $I$ any ideal, we do have $N(R) = J(R)$ - this is the Nullstellensatz - see later on.

<u>Example:</u> A commutative ring is ***artinian*** if it doesn't contain an infinite strictly descending chain of ideals (or equivalently if every nonempty set of ideals has a minimal member). An

[2]Note - this is not the usual Atiyah-Macdonald proof, but this one can be adapted to the case of non-commutative rings.

$R$-module is ***artinian*** if it satisfies the analogous properties for submodules. As an exercise (on the first example sheet), prove that artinian rings are noetherian.

For example, $\mathbb{Z}/p\mathbb{Z}$, $k[x]/(f)$. $k[x]$ is not artinian ($(x) > (x^2) > \ldots$)).

Recall that $I$ is prime if and only if one following three equivalent properties holds:

$$ab \in I \implies a \in I \text{ or } b \in I$$
$$R/I \text{ is an integral domain}$$
$$I_1 I_2 \subseteq I \implies I_1 \subseteq I \text{ or } I_2 \subseteq I$$

Claim: $J(R) = N(R)$ for artinian rings $R$
This follows if we can show that $R$ artinian $\implies$ every prime ideal is maximal.

*Proof.* Let $P$ be prime, $x \notin P$. By the descending chain condition, $(x) \supseteq (x^2) \subseteq \ldots$ is not strict, so $(x^n) = (x^{n+1}) = \ldots$ for some $n$. Hence $x^n = yx^{n+1}$ for some $y$. Then $x^n(1 - xy) = 0 \in P$. But $x^n \notin P$, and $P$ is prime, so $1 - xy \in P$. Thus $y + P$ is the inverse of $x + P$ in $R/P$, and so $R/P$ is a field, and $P$ is maximal. □

**Lemma 1.17** (Artin-Tate)**.** *Suppose we have commutative rings $R \leq S \leq T$. Suppose $R$ is noetherian and $T$ is generated as a ring by $R$ and finitely many elements $t_1, \ldots, t_n$. Suppose that $T$ is a finitely generated $S$-module. Then $S$ is generated by $R$ and finitely many elements as an $R$-algebra.*

*Proof.* $T$ is generated by $x_1 \ldots, x_m \in T$ as an $S$-module, so $T = Sx_1 + \ldots + Sx_m$. Then:

$$t_i = \sum_j s_{ij} x_j, \quad s_{ij} \in S \tag{1}$$

$$x_i x_j = \sum_k s_{ijk} x_k, \quad s_{ijk} \in S \tag{2}$$

Let $S_0$ be the ring generated by $R$, the $s_{ij}$ and the $s_{ijk}$, so that $R \leq s_0 \leq S$.

Any element of $T$ is polynomial in the $t_i$ with coefficients in $R$. In (1), (2), each element is a linear combination of the $x_j$ with coefficients in $S_0$. Thus $T$ is a finitely generated $S_0$-module. But $S_0$ is noetherian, being generated as a ring by $R$ and finitely many elements. $T$ is noetherian as an $S_0$-module, and $S$ is an $S_0$-submodule of $T$, hence is finitely generated as an $S_0$-module.

But $S_0$ is generated by $R$ and finitely many elements, so $S$ is generated by $R$ and finitely many elements. □

**Lemma 1.18** (Zariski)**.** *Let $k$ be a field, and $R$ a finitely generated $k$-algebra. If $R$ itself is a field, then it is a finite algebraic extension of $k$, i.e. a finitely generated $k$-space.*

*Proof.* Suppose $R$ is generated by $k$ and $x_1, \ldots, x_n$, and is a field. If $R$ is not a finite algebraic extension over $k$, then we can reorder the $x_1, \ldots, x_n$ so that $x_1, \ldots, x_m$ are algebraically independent, i.e. the ring generated by $k$ and $x_1, \ldots, x_m$ is a polynomial algebra $k[x_1, \ldots, x_m]$, and $x_{m+1}, \ldots, x_n$ are algebraic over the field of fractions $F = k(x_1, \ldots, x_m)$. Because $R$ is not finite algebraic over $k$, $m \geq 1$.

Hence $R$ is a finite algebraic extension over $F$, and $R$ is a finitely generated $F$-module, (i.e. vector space). Apply Artin-Tate (**1.17**) for $k \leq F \leq R$, it follows that $F$ is a finitely generated $k$-algebra by $k$ and $q_1 \ldots, q_t$ say, with each $q_i = f_i/g_i$, where $f_i, g_i \in k[x_1, \ldots, x_m]$, $g_i \neq 0$.

Now there is a polynomial $h$ which is prime to each of the $g_i$s, e.g. $g_1 \dots g_m + 1$, and the element $1/h$ cannot be in the ring generated by $k$ and $q_1, \dots, q_t$. This a contradiction, and hence $m = 0$, and $R$ was indeed algebraic over $k$. ◻

**Theorem 1.19** (Weak Nullstellensatz)**.** *Let $k$ be a field, $T$ a finitely generated $k$-algebra. Let $P$ be a maximal ideal of $T$. Then $T/P$ is a finite algebraic extension of $k$. In particular, if $k$ is algebraically closed and $T$ is the polynomial algebra, then the maximal ideals are of the form $(x_1 - a_1, \dots, x_n - a_n)$.*

*Proof.* See later. ◻

**Theorem 1.20** (Strong Nullstellensatz)**.** *Let $k$ be an algebraically closed field, and $R$ a finitely generated $k$-algebra. Then $N(R) = J(R)$. Thus, if $I$ is a radical ideal of $k[x_1, \dots, x_n]$ and $R = k[x_1, \dots, x_n]/I$, then the intersection of the maximal ideals of $R$ is 0.*

*Furthermore, any radical ideal is the intersection of the maximal ideals containing it.*

*Proof.* Deferred until chapter 2. ◻

*Proof of **1.19**.* Let $P$ be the maximal ideal of the finitely generated $k$-algebra $T$. Put $R = T/P$. By Zariski's lemma, $T/P$ over $k$ is a finite algebraic extension. If $k$ is closed, then $k = T/P$. Set $\pi : T \to k$ with kernel $P$.

We then claim that $\ker \pi = (x_1 - \pi(x_1), \dots, x_n - \pi(x_n))$.

Now $\pi$ fixes elements of $k$, so the RHS is in the kernel. Conversely, $T/(x_1 - \pi(x_1), \dots, x_n - \pi(x_n))$ is a 1-dimensional $k$-space, so the kernel is contained in the RHS, and so they are equal.

Recall the bijection proposed earlier between radical ideals in $\mathbb{C}[\mathbf{x}]$ and affine algebraic sets in $\mathbb{C}^n$.

Rephrase this by defining $Q_{(a_1,\dots,a_n)} = (x_1 - a_1, \dots, x_n - a_n)$. We claim there is a bijection:

$$\begin{aligned} \{\text{radical ideals}\} &\leftrightarrow \{\text{algebraic subsets}\} \\ I &\mapsto \{(a_1, \dots, a_n) : I \subseteq Q_{(a_1,\dots,a_n)}\} \\ \bigcap_{(a_1,\dots,a_n)\in S} Q_{(a_1,\dots,a_n)} &\leftarrow\!\shortmid S \end{aligned}$$

◻

## 1.2 Minimal and Associated Primes

**Lemma 1.21.** *If $R$ is noetherian, then any ideal $I$ contains a power of its radical $\sqrt{I}$. In particular, $N(R)$ is nilpotent, i.e. $N(R)^m = (0)$ for some $m$, as $N(R) = \sqrt{(0)}$.*

*Proof.* Suppose $x_1, \dots, x_m \in \sqrt{I}$ generate $\sqrt{I}$ as an ideal. Then $x_i^{n_i} \in I$ for some $n_i$. Then, if $n$ is sufficiently sufficiently large (e.g. $n \geq \sum(n_i - 1) + 1$). Then $\sqrt{I}^n$ is generated by $x_1^{r_1}, \dots, x_m^{r_m}$ with $\sum r_i = n$. We must thus have some $r_i \geq n_i$, and so $\sqrt{I}^n \subseteq I$. ◻

**Lemma 1.22.** *If $R$ is noetherian, then a radical ideal is the intersection of finitely many prime ideals.*

*Proof.* Suppose not for contradiction, and take a maximal element $I$ from the set of radical ideals not of this form (using Zorn's lemma). We then claim that $I$ is prime, yielding a contradiction.

If not, there is $J_1, J_1 \nsubseteq I$ with $J_1 J_2 \subseteq I$. If necessary, replace $J_i$ by $J_i + I$, we can assume $I \subsetneq J_1, J_2$.

Then by the maximality of $I$, $\sqrt{J_1} = Q_1 \cap \ldots Q_m$; $\sqrt{J_2} = Q'_1 \cap \ldots \cap Q'_n$ as prime intersections.

Set $J = \sqrt{J_1} \cap \sqrt{J_2} = Q_1 \cap \ldots \cap Q_m \cap Q'_1 \cap \ldots \cap Q'_n$. So $J^{n_1} \leq J_1, J^{n_2} \leq J_2$ for some $n_1, n_2$. Hence $J^{n_1+n_2} \leq J_1 J_2 \leq I$. But $I$ is radical, so $J \leq I$. Now all $Q_i, Q'_j$ contain $I$, so $J \geq I$. Thus $J = I$ ↯. □

Now suppose by the previous lemma that any radical ideal $\sqrt{I} = P_1 \cap \ldots \cap P_m$ is an intersection of finitely many primes. We can remove $P_i$ from the list if it contains any of the others, so WLOG we may assume that $P_i \nleq P_j$ for any $i \neq j$. If $P$ is prime with $\sqrt{I} \leq P$, then $P_1 \ldots P_m \leq \bigcap_i P_i = \sqrt{I} \leq P$, and so some $P_i \leq P$.

**Definition 1.23.** *The* **minimal primes P over an ideal I** *of a noetherian ring are those such that, if $P'$ is prime with $I \leq P' \leq P$, then $P' = P$.*

Clearly the $P_i$ mentioned above are minimal primes over $I$. In fact:

**Lemma 1.24.** *Let $I$ be an ideal in a noetherian ring. Then $\sqrt{I}$ is the intersection of the minimal primes over $I$, and $I$ contains a finite product of the minimal primes over $I$.*

*Proof.* Each minimal prime over $I$ contains $\sqrt{I}$. So the primes minimal over $I$ are precisely the minimal ones over $\sqrt{I}$. We know $\sqrt{I}$ is the intersection of these, and thus their product lies in $\sqrt{I}$, and **1.21** gives the last part. □

Example: The Nullstellensatz bijection between radical ideals of $\mathbb{C}[x_1, \ldots, x_n]$ and algebraic subsets of $\mathbb{C}^n$.

Suppose $(a_1, \ldots, a_n)$ is a common zero of all $f \in I$, a radical ideal. Then $I \leq (x_1 - a_1, \ldots, x_n - a_n)$. This latter ideal is maximal as it is the kernel of $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}; x_i \mapsto a_i$.

Now consider

$$\bigcap_{\substack{(a_1,\ldots,a_n) \\ \text{common zeros} \\ \text{of all } f \in I}} (x_1 - a_1, \ldots, x_n - a_n)$$

This ideal is radical, and the bijection in the Nullstellensatz implies that this radical ideal is the same as $I$. Thus $I$ is an intersection of maximal ideals, and moreover all maximal ideals are of the form $(x_1 - a_1, \ldots, x_n - a_n)$. Also, for any ideal $J_1$ of $\mathbb{C}[x_1, \ldots, x_n]$, we have $N(\mathbb{C}[x_1, \ldots, x_n]/J_1) = J(\mathbb{C}[x_1, \ldots, x_n]/J_1)$.

## 1.3 Annihilators and Associated Primes

**Definition 1.25.** *Let $M$ be a finitely generated $R$-module, where $R$ is noetherian. The* **annihilator** *of $m$,* $\text{ann}(m) = \{r \in R : rm = 0\}$. *A prime ideal $P$ is an* **associated prime** *of $M$ if it is the annihilator of an element of $M$*

*We call the set of associated primes* $\text{Ass}(M)$.

For example, $\text{Ass}(R/P) = \{P\}$ for $P$ prime.

**Definition 1.26.** *A submodule $N$ of $M$ is* **p-primary** *(or just* **primary***) if* $\operatorname{Ass}(M/N) = \{p\}$ *for a prime ideal $p$. An ideal is* **p-primary** *if $I$ is $p$-primary as a submodule of $R$.*

**Lemma 1.27.** *If* $\operatorname{ann}(M) = P$ *for a prime ideal $P$, then* $P \in \operatorname{Ass}(M)$.

*Proof.* Suppose that $M$ is generated by $m_1, \dots, m_k$. Let $I_j = \operatorname{ann}(m_j)$. Then the product $\prod I_j$ annihilates each $m_j$, so $\Pi I_j \leq \operatorname{ann}(M) = P$. So $I_j = P$ for some $j$ as $P$ prime, and so $P \in \operatorname{Ass}(M)$. □

**Lemma 1.28.** *Let $Q$ be maximal amongst all annihilators of nonzero elements. Then $Q$ is a prime ideal and so* $Q \in \operatorname{Ass}(M)$.

*Proof.* Let $Q = \operatorname{ann}(m)$ and $r_1 r_2 \in \mathbb{Q}$, $r_2 \notin \mathbb{Q}$. We show that $r_1 \in Q$.

Now $r_1 r_2 \in Q \implies r_1 r_2 m = 0$, so $r_1 \in \operatorname{ann}(r_2 m)$.

And $r_2 \notin Q \implies r_2 m \neq 0$. But $Q \leq \operatorname{ann}(r_2 m)$, and hence $Q$ and $r_2$ lie in $\operatorname{ann}(r_2 m)$. By maximality, $Q = \operatorname{ann}(r_2 m)$, and so $r_1 \in Q$. □

**Lemma 1.29.** *For finitely generated nonzero $R$-module $M$, where $R$ is noetherian, there is a chain*

$$0 \lneq M_1 \lneq M_2 \lneq \ldots \lneq M_t = M$$

*of submodules with $M_i/M_{i-1} \cong R/P_i$ for some prime ideal $P_i$.*

*Proof.* By **1.28**, there is $0 \neq m_1 \in M$ with $\operatorname{ann}(m_1)$ prime, say $P_1$. Set $M_1 = Rm_1$. Hence $M_1 \cong R/P_1$. Repeat for $M/M_1$ to find $M_2/M_1 \cong R/P_2$ for some prime $P_2$. Continue - the noetherian property forces the process to terminate. □

**Lemma 1.30.** $N \subseteq M \implies \operatorname{Ass}(M) \subseteq \operatorname{Ass}(N) \cup \operatorname{Ass}(M/N)$.

*Proof.* Take $P \in \operatorname{Ass}(M)$, so that $P = \operatorname{ann}(m)$ for some $m \in M$, and $P$ is prime.

Let $M_1 = Rm = R/P$. For any $0 \neq m_1 \in M_1$, we have $\operatorname{ann}(m_1) = P$, since $P$ is prime. If $M_1 \cap N \neq 0$, then there is $x \in M_1 \cap N$ with $\operatorname{ann}(x) = P$, and so $P \in \operatorname{Ass}(N)$. Otherwise, $M_1 \cap N = 0$, and the image of $M_1$ in $M/N$ is isomorphic to $R/P$, and hence $P \in \operatorname{Ass}(M/N)$. □

**Lemma 1.31.** $\operatorname{Ass}(M)$ *is finite for any finitely generated $R$-module, where $R$ is noetherian.*

*Proof.* Apply **1.30** inductively to the chain in **1.29** recalling that $\operatorname{Ass}(R/P_i) = \{P_i\}$. We thus conclude $\operatorname{Ass}(M) \subset \{P_1, \dots, P_t\}$ is finite. □

**Proposition 1.32.** *Each minimal prime over an ideal $I$ is an associated prime, i.e.:*

$$\{\textit{minimal primes over } I\} \subseteq \operatorname{Ass}(R/I)$$

*Proof.* By **1.24**, there is a product of minimal primes over $I$, possibly with repetitions, contained in $I$, say $p_1^{s_1} \dots p_n^{s_n} \leq I$ with $p_i \neq p_j$ for $i \neq j$.

Let $J = \operatorname{ann}(\underbrace{(p_2^{s_2} \dots p_n^{s_n} + I)/I}_{M})$. Now $J \geq p_1^{s_1}$, and also $J p_2^{s_2} \dots J p_n^{s_n} \leq I \leq p_1$. Since $p_1$ prime, we have $J \leq p_1$, and so $J \neq R \implies M \neq 0$.

By **1.29**, there is a chain of submodules in $M$, say $0 \lneq M_1 \lneq \ldots \lneq M_t = M$ such that each factor is isomorphic to $R/q_j$ for some primes $q_j$.

But $p_1^{s_1}$ annihilates $M$, and hence each $M_j/M_{j-1}$, and the primeness of $q_j$ ensures that $p_1 \leq q_j$ for each $j$. Not all of the $q_j \gneq p_1$ since $\prod q_j \leq J \leq p_1$, and hence some $q_j \leq p_1$, so $q_j = p_1$.

Now pick $j$ minimal such that $q_j = p_1$. Then $\prod_{k<j} q_k \nleq p_1$. We show that $p_1 \in \text{Ass}(M)$.

Take $x \in M_j \setminus M_{j-1}$. If $j = 1$, then $\text{ann}(x) = p_1$, and so $p_1 \in \text{Ass}(R/I)$. If $j > 1$, take $r \in (\prod_{k<j} q_k) \setminus p_1$. Note that $r(sx) = 0$ for any $s \in p_1 = q_j$. So $s(rx) = 0$, so $p_1 \leq \text{ann}(rx)$. However, $rx \notin M_{j-1}$ since $M_j/M_{j-1} = R/q_j = R/p_1$.

So $\text{ann}(rx) \subseteq p_1$, and hence is equal to, and we've shown that $p_1 \in \text{Ass}(M) \subseteq \text{Ass}(R/I)$. □

**Example 1.33.** The converse is false. An example where $p \in \text{Ass}(R/I)$ with $p$ is not minimal over $I$ is as follows:

Take $R = k[x, y], p = (x, y) > q = (x)$, and $I = pq = (x^2, xy)$, so that $\sqrt{I} = (x) = q$.

Then $\text{Ass}(R/I) = \{p, q\}$. The only minimal prime over $I$ is $q$, since $\sqrt{I} = q$. Now $I$ is not primary as there are two primes in $\text{Ass}(R/I)$. However, we can write $I = (x^2, xy, y^2) \cap (x)$, with $(x^2, xy, y^2) = (x, y)^2$, is $p$-primary, and $(x)$ is $q$-primary. This is an example of ***primary decomposition***:

**Definition 1.34.** *Let $M$ be a finitely generated $R$-module with $R$ noetherian, and $N \subset M$ a submodule. Then there are submodules $N_1, \ldots, N_s$ of $M$ containing $N$ such that $N_i$ is $p_i$-primary with $p_i$ distinct, and $N = \bigcap_{i=1}^{s} N_I$, so that $M/N \hookrightarrow \bigoplus_i M/N_i$.*

The primary decomposition is not necessarily unique, although in §4 of Atiyah-MacDonald proves two uniqueness theorems for finitely generated modules over noetherian rings:

- The $p_i$ occurring in the primary decomposition are unique, and are precisely $\text{Ass}(M/N)$.
- If the $p_j$ are minimal among all occurring $p_i$s, then the corresponding $N_j$ are unique. If $p_j$ are not minimal (which we call ***embedded***), then the $N_j$ can vary.

In **1.33**, $q$ is minimal and $p$ is embedded. Hence the ideal $(x)$ is unique and $\text{Ass}(R/I) = \{p, q\}$.

# 2 Localisation

As always, all rings are commutative with a 1.

Let $S$ be a ***multiplicatively closed*** subset of $R$ - i.e. $S$ is closed under multiplication and $1 \in S$. Define a relation on $R \times S$ via

$$(r_1, s_1) \equiv (r_2, s_2) \iff (r_1 s_2 - r_2 s_1)x = 0 \text{ for some } x \in S$$

This is reflexive, symmetric, and transitive. Reflexivity and symmetry are easy - for transitivity, if $(r_1, s_1) \equiv (r_2, s_2) \equiv (r_3, s_3)$, then we have $(r_1 s_2 - r_2 s_1)x = 0 = (r_2 s_3 - r_3 s_2)y$.

Then $s_3 y \cdot \text{LHS} - s_1 x \cdot \text{RHS} = 0$, and so $(r_1 s_3 - r_3 s_1) s_2 x y = 0$, and $s_2 x y \in S$ since $S$ is multiplicatively closed.

Denote the equivalence class of $(r_1, s_1)$ as $\frac{r_1}{s_1}$, and denote the set of equivalence classes by $S^{-1}R$. Then $S^{-1}R$ is a ring, and there is a ring homomorphism $\theta : R \to S^{-1}R$ via $r \mapsto \frac{r}{1}$.

We also have the following universal property:

**Lemma 2.1.** *Let $\varphi : R \to T$ be a ring homomorphism with $\varphi(s)$ a unit in $T$ for all $s \in S$. Then there is a unique ring homomorphism $\alpha : S^{-1}R \to T$ such that following diagram commutes:*

$$\begin{tikzcd} R \arrow[rr, "\theta"] \arrow[dr, "\varphi"'] & & S^{-1}R \arrow[dl, "\alpha"] \\ & T & \end{tikzcd}$$

*Proof.* For uniqueness, suppose that $\alpha$ exists, then $\alpha : S^{-1}R \to T$ such that $\alpha\theta = \varphi$.

Then

$$\alpha(r/1) = \alpha(\theta(r)) = \varphi(r)\ \forall r \in R$$
$$\alpha(1/s) = \alpha((s/1)^{-1}) = (\alpha(s/1))^{-1} = \varphi(s)^{-1}\ \forall s \in S$$

Thus $\alpha(r/s) = \varphi(r)\varphi(s)^{-1}$, and $\alpha$ is uniquely determined.

For existence, let $\alpha(r/s) = \varphi(r)\varphi(s)^{-1}$. We need to show this is well defined.

Suppose $(r_1/s_1) = (r_2/s_2)$. Then there is $x \in S$ with $(r_1s_2 - r_2s_1)x = 0$.

So $(\varphi(r_1)\varphi(s_2) - \varphi(r_2)\varphi(s_1))\varphi(x) = 0$.

Since $\varphi(x)$ is a unit, we must have $\varphi(r_1)\varphi(s_2) = \varphi(r_2)\varphi(s_1)$, and thus $\alpha(r_1/s_1) = \alpha(r_2/s_2)$. □

<u>Examples:</u>

- The field of fractions of an integral domain $R$. Put $S = R \setminus \{0\}$.
- $S^{-1}R = (0) \iff 0 \in S$.
- If $I \triangleleft R$, then take $S = 1 + I$ is multiplicatively closed.
- If $p$ is a prime ideal, then let $S = R \setminus p$, and this is multiplicatively closed since $p$ is prime. In this case, we write $R_p$ for $S^{-1}R$ in this case.

This process of passing from $R$ to $R_p$ is called ***localisation at p***. The elements $\frac{r}{s}$ with $r \in p$ form an ideal of $R_p$, and in fact is the unique maximal ideal in $R_p$ - if $\frac{r}{s}$ is such that $r \notin p$, then $r \in S$, and hence $\frac{s}{r} \in R_p$ is its inverse.

**Definition 2.2.** *A ring with a unique maximal ideal is called* **local**.[3]

<u>Examples:</u>

- $\mathbb{R} = \mathbb{Z}, p = (p)$ for $p$ prime. Then $R_p = \{\frac{m}{n} : p \nmid n\} < \mathbb{Q}$, with unique maximal ideal $\{\frac{m}{n} : p | m, p \nmid n\}$
- $R = k[x_1, \ldots, x_n], p = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. Then $R_p \leq k(x_1, \ldots, x_n)$, and is those functions that are defined at $(\alpha_1, \ldots, \alpha_n) \in k^n$. The unique maximal ideal consists of those rational functions which are zero at $(\alpha, \ldots, \alpha_n)$.

[3]Some authors require local rings to be noetherian - we will be explicit here when we need this.

## 2.1 Modules

Given a (left) $R$-module $M$, for a multiplicatively closed set $S \subseteq R$, define a relation on $M \times S$ by $(m_1, s_1) \equiv (m_2, s_2) \iff x(m_1 s_2 - m_2 s_1) = 0$ for some $x \in S$. Again, this is an equivalence relation, with $\frac{m}{s}$ denoting an equivalence class, and we write for the set of equivalence classes $S^{-1}M$. Now $S^{-1}M$ is an $S^{-1}R$-module.

Write $M_p$ in the case where $S = R \setminus p$ for some prime ideal $p$. If $\theta : M_1 \longrightarrow M_2$ is an $R$-homomorphism, then $S^{-1}\theta : S^{-1}M_1 \longrightarrow S^{-1}M_2$ is an $S^{-1}R$-homomorphism, defined by $S^{-1}\theta : \frac{m_1}{s} \mapsto \frac{\theta(m_1)}{s}$.

If $\varphi : M_2 \longrightarrow M_3$, then $S^{-1}(\varphi \circ \theta) = S^{-1}\varphi \circ S^{-1}\theta$.

A sequence of $R$-modules

$$M_0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \ldots \xrightarrow{\theta} M_i \xrightarrow{\varphi} \ldots \longrightarrow M_t$$

is ***exact*** at $M_i$ if $\operatorname{im}\theta = \ker\varphi$. A ***short exact sequence*** is one of the form

$$0 \longrightarrow M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \longrightarrow 0$$

with exactness at $M_1, M, M_2$. Then $\theta$ is injective, $\varphi$ is surjective, and $\operatorname{im}\theta = \ker\varphi$.

**Lemma 2.3.** *If $M_1, M, M_2$ are $R$-modules and $M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2$ is exact at $M$, then*

$$S^{-1}M_1 \xrightarrow{S^{-1}\theta} S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}M_2$$

*is exact at $S^{-1}M$.*

*Proof.* Since $\ker\varphi = \operatorname{im}\theta$, we have $\varphi \circ \theta = 0$. So $(S^{-1}\varphi) \circ (S^{-1}\theta) = S^{-1}(\varphi \circ \theta) = S^{-1}(0) = 0$, and hence $\operatorname{im} S^{-1}\theta \leq \ker S^{-1}\varphi$.

Now suppose that $\frac{m}{s} \in \ker S^{-1}\varphi \subseteq S^{-1}M$. Then $\frac{\varphi(m)}{s} = 0$ in $S^{-1}M_2$ and there is some $t \in S$ with $t\varphi(m) = 0$ in $M_2$. But $t\varphi(m) = \varphi(tm)$, since $\varphi$ is a $R$-module homomorphism. Thus $tm \in \ker\varphi = \operatorname{im}\theta$, and so $tm = \theta(m_1)$ for some $m_1 \in M_1$.

Hence in $S^{-1}M$, $\frac{m}{s} = \frac{\theta(m_1)}{ts} = (S^{-1}\theta)\left(\frac{m_1}{ts}\right) \in \operatorname{im} S^{-1}\theta$, and so $\ker S^{-1}\varphi \leq \operatorname{im} S^{-1}\theta$.

Thus $\ker S^{-1}\varphi = \operatorname{im} S^{-1}\theta$, and the sequence is exact. □

**Lemma 2.4.** *Let $N \trianglelefteq M$. Then $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.*

*Proof.* Apply **2.3** to the short exact sequence $0 \longrightarrow N \overset{\iota}{\hookrightarrow} M \overset{\varepsilon}{\twoheadrightarrow} M/N \longrightarrow 0$ to get that

$$0 \longrightarrow S^{-1}N \overset{S^{-1}\iota}{\hookrightarrow} S^{-1}M \overset{S^{-1}\varepsilon}{\twoheadrightarrow} M/N \longrightarrow 0$$

is a short exact sequence. Hence $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$. □

If $R$ is a ring with a multiplicatively closed subset $S$, and $I \trianglelefteq R$, then $S^{-1}I$ is an ideal of $S^{-1}R$. If $N \subset M$, then $S^{-1}N$ can be regarded as a submodule of $S^{-1}M$.

**Lemma 2.5.**

1. *Every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some $I \trianglelefteq R$.*
2. *The prime ideals of $S^{-1}R$ are in one-to-one correspondence with the prime ideals of $R$ that don't intersect $S$.*

*Proof.*

1. Let $J \trianglelefteq S^{-1}R$, and $I = \{r \in R : \frac{r}{1} \in J\} \subseteq R$. Then if $\frac{r}{s} \in J$, we have $\frac{r}{1} \in J$, and hence $r \in I$, so $J \subseteq S^{-1}I$

   Conversely, if $r \in I$ then $\frac{r}{1} \in J$, and so $\frac{r}{s} \in J$ for all $S$, so $S^{-1}I \subseteq J$.
2. Let $q$ be a prime ideal in $S^{-1}R$. Set $p := \{r \in R : \frac{r}{1} \in q\}$.

   $p$ is prime: if $xy \in p$, then $\frac{xy}{1} \in q$, and so either $\frac{x}{1}$ or $\frac{y}{1}$ is in $q$, so $x \in p$ or $y \in p$.

   $p \cap S = \emptyset$: Suppose $r \in S \cap p$. Then $\frac{r}{1} \in q$ and $\frac{1}{r} \in q$, and so $\frac{1}{r} \cdot \frac{r}{1} = \frac{1}{1} \in q$ ↯.

   Conversely, if $\frac{r}{s}, \frac{x}{y} \in S^{-1}p$, then $\frac{rx}{sy} \in S^{-1}p$. So $z(rx) \in p$ for some $z \in S$. Hence $rx \in p$ since $p$ is prime and $z \notin p$. Thus $r \in p$ or $x \in p$, and so $\frac{r}{s} \in S^{-1}p$ or $\frac{x}{y} \in S^{-1}p$.

□

**Lemma 2.6.** *If $R$ is noetherian, then so is $S^{-1}R$.*

*Proof.* Any chain of ideals in $S^{-1}R$ is of the form $J_1 \leq J_2 \leq \ldots = S^{-1}I_1 \leq S^{-1}I_2 \leq \ldots$.

Note that, by the construction given in the proof above, if $S^{-1}I_1 \leq S^{-1}I_2$, then we must have $I_1 \leq I_2$, as $r \in I_1 \implies \frac{r}{1} \in S^{-1}I_1 \implies \frac{r}{1} \in S^{-1}I_2 \implies r \in I_2$.

Then we have a chain of ideals in $R$ given by $I_1 \leq I_2 \leq \ldots$, which must terminate as $R$ is noetherian. Then $I_t = I_{t+k}$ for some $t$ and all $k \in \mathbb{N}$, and thus $J_t = J_{t+k}$ for some $t$ and all $k \in \mathbb{N}$, and so our original sequence terminated. □

**Definition 2.7.** *A property $\mathscr{P}$ of a ring $R$ (or $R$-module $M$) is* **local** *if $R$ (or $M$) has $\mathscr{P}$ if and only if $R_p$ (or $M_p$) has $\mathscr{P}$ for every prime ideal $p \subseteq R$.*

We have just shown that "being noetherian" is a local property. We will now go on to prove that another property is local:

**Lemma 2.8.** *The following are all equivalent:*

1. $M = 0$
2. $M_p = 0$ *for all prime $p$*
3. $M_q = 0$ *for all maximal $q$*

*Proof.* *1.* $\implies$ *2.* $\implies$ *3.* is immediate. Now we show *3.* $\implies$ *1.*

Suppose $M_q = 0$ for all maximal $q$, but $M \neq=$. Then take $0 \neq m \in M$. The annihilator of $m$ is a proper ideal of $R$, and so it is contained in a maximal ideal $q$ by Zorn. Consider $\frac{m}{1} \in M_q$. By assumption, $M_q = 0$, and hence $\frac{m}{1} = 0$. So $sm = 0$ for some $s \in S := R \setminus q$. But we already had $q$ containing the annihilator of $m$, and so we have a contradiction. □

So "being 0" is a local property!

**Lemma 2.9.** *Let $\varphi : M \to N$ be a R-module homomorphism. Then the following are equivalent:*

1. *$\varphi$ is injective.*
2. *$\varphi_p : M_p \to N_p$ is injective for all primes $p$ of $R$.*
3. *$\varphi_q : M_q \to N_q$ is injective for all maximal $q$ of $R$.*

*Proof.* *1.* $\implies$ *2.* by exactness of localisation, and *2.* $\implies$ *3.* is clear.

For *3.* $\implies$ *1.*, let $M_1 = \ker \varphi$. Then $0 \to M_1 \to M \xrightarrow{\varphi} N \to 0$ is exact at $M_1$ and $M$. So **2.3** gives us $0 \to (M_1)_q \to M_q \xrightarrow{\varphi_q} N_q \to 0$ is exact at $(M_1)_q$ and $M_q$ for maximal $q$, and hence $(M_1)_q = \ker \varphi_q = 0$, and so $(M_1)_q = 0$. Hence $M_1 = 0$ by **2.8**. □

**Lemma 2.10.** *Let $p$ be a prime of $R$ and $S$ be a multiplicatively closed subset of $R$, with $S \cap p = 0$. By* **2.5***, we know $S^{-1}p$ is a prime of $S^{-1}R$. In fact, we have:*

$$(S^{-1}R)_{S^{-1}p} \cong R_p$$

*In particular, if $q$ is prime with $p \leq q$, then $(R_q)_{p_q} \cong R_p$, by taking $S = R \setminus q$.*

*Proof.* On example sheet 2. □

# 3 Tensor Products

Let $R$ be a commutative ring with a 1, and $L, M, N, T$ all $R$-modules.

**Definition 3.1.** *A function $\varphi : M \times N \to L$ is* **R-bilinear** *if*

- $\varphi(r_1 m_1 + r_2 m_2, n) = r_1 \varphi(m_1, n) + r_2 \varphi(m_2, n)$
- $\varphi(m, r_1 n_1 + r_2 n_2) = r_1 \varphi(m, n_1) + r_2 \varphi(m, n_2)$

The idea of this section is reduce the study of bilinear maps to the study of linear maps.

If $\varphi : M \times N \to T$ is bilinear and $\theta : T \to L$ is linear, then the composition $\theta \circ \varphi$ is bilinear. So composition with $\varphi$ gives a well-defined function $\varphi^*$ from

$$\{R - \text{module maps } T \to L\} \to \{\text{bilinear maps } M \times N \to L\}$$

We say $\varphi$ is ***universal*** if $\varphi^*$ is a 1-1 correspondence for all $L$. If this happens, the study of bilinear maps $M \times N \to L$ is reduced to the study of linear maps $T \to L$.

**Lemma 3.2.**

1. *Given $R$-modules $M, N$, there is an $R$-module $T$ and a universal map $\varphi : M \times N \to T$*
2. *Given two such maps $\varphi_1 : M \times N \to T_1, \varphi_2 : M \times N \to T_2$, there is a unique isomorphism $\beta : T_1 \to T_2$ with $\varphi_2 = \beta \circ \varphi_1$.*

*Proof.*

1. Let $F$ be the free $R$-module on generators $e_{(m,n)}$, indexed by pairs $m, n \in M \times N$. Then let $X$ be the $R$-submodule generated by all elements of the forms:

$$e_{(r_1 m_1 + r_2 m_2, n)} - r_1 e_{(m_1,n)} - r_2 e_{(m_2,n)}$$
$$e_{(m, r_1 n_1 + r_2 n_2)} - r_1 e_{(m,n_1)} - r_2 e_{(m,n_2)}$$

   Now set $T = F/X$, and write $m \otimes n$ for the image of the basis element $e_{(m,n)}$ in $T$. Then $T$ is generated as an $R$-module by elements of the form $m \otimes n$, and

$$(r_1 m_1 + r_2 m_2) \otimes n = r_1(m_1 \otimes n) + r_2(m_2 \otimes n)$$
$$m \otimes (r_1 n_1 + r_2 n_2) = r_1(m \otimes n_1) + r_2(m \otimes n_2)$$

   Define $\varphi : M \times N \to T; (m, n) \mapsto m \otimes n$.

   Then any map $\alpha : M \times N \to L$ extends to an $R$-module map $\bar{\alpha} : F \to L; e_{(m,n)} \mapsto \alpha(m, n)$. If $\alpha$ is bilinear, then $\bar{\alpha}$ is zero on all the generators of $X$, hence on all of $X$. So $\bar{\alpha}$ induces an $R$-module map $\alpha' : T \to L$ with $\alpha'(m \otimes n) = \alpha(m, n)$, and $\alpha'$ is uniquely defined by this.

2. Suppose there are universal maps $\varphi_i : M \times N \to T_i$ for $i = 1, 2$. Since $\varphi_1$ is universal, there is a unique $R$-module map $\beta_1 : T_1 \to T_2$ with $\varphi_2 = \beta_1 \circ \varphi_1$. Similarly, there is unique $\beta_2 : T_2 \to T_1; \varphi_1 = \beta_2 \circ \varphi_2$.

   Then $(\beta_2 \circ \beta_1) \circ \varphi_1 = \beta_2 \circ \varphi_2 = \varphi_1 = \mathrm{id} \circ \varphi_1$. But $\varphi^*$ is a bijection, and hence $\beta_2 \circ \beta_1 = \mathrm{id}_{T_1}$, and similarly $\beta_1 \circ \beta_2 = \mathrm{id}_{T_2}$. Hence $\beta_1$ is the required isomorphism.

□

**Definition 3.3.** *$T$ in the above proof is written $M \otimes_R N$, the* **tensor product** *of $M$ and $N$ over $R$. We often drop the subscript $R$ if it's clear what ring we're working over.*

Note: not all elements of $M \otimes_R N$ are of the form $m \otimes n$. A generated element is a finite sum of $\sum_{i=1}^{r} m_1 \otimes n_i$.

If $R = k$ is a field, and $M, N$ are finite dimensional $k$-vector spaces, of dimension $s, t$ respectively, then $((a_1, \dots, a_s), (b_1, \dots, b_t)) \mapsto (a_i b_j)_{\substack{1 \le i \le s \\ 1 \le j \le t}}$ is a universal map, and $M \otimes_k N = k^{st}$.

We may also define the tensor product over non-commutative rings, where $M$ is a right $R$-module and $N$ is a left $R$-module. Then $M \otimes N$ is only an abelian group, and not necessarily an $R$-module. If $M$ is an $(R, S)$-bimodule, and $N$ an $(S, T)$-bimodule, then $M \otimes N$ is an $(R, T)$-bimodule.

As an simple example, you can check that $\mathbb{Z}/r\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/s\mathbb{Z} \cong \mathbb{Z}/\gcd(r, s)\mathbb{Z}$.

It's also worth noting that we can do the same with trilinear maps $L \times M \times N \to T$, giving us $L \otimes M \otimes N$.

**Lemma 3.4.** *There are unique isomorphisms:*

1. $M \otimes N \to N \otimes M; m \otimes n \mapsto n \otimes m$.
2. $(M \otimes N) \otimes L \to M \otimes (N \otimes L) \to M \otimes N \otimes L; (m \otimes n) \otimes \ell \mapsto m \otimes (n \otimes \ell) \mapsto m \otimes n \otimes \ell$
3. $(M \oplus N) \otimes L \to (M \otimes L) \oplus (N \otimes L); (m, n) \otimes \ell \mapsto ((m \otimes \ell), (n \otimes \ell))$
4. $R \otimes_R M \to M; r \otimes m \to rm$

*Proof.*

1. The map $M \times N \to N \otimes M; (m,n) \to n \otimes m$ is bilinear. So by universality there is a map $M \otimes N \to N \otimes M; m \otimes n \mapsto n \otimes m$, which clearly has an inverse.

2. Exercise on sheet 2.

3. There is a bilinear map $\phi : (M \oplus N) \times L \to (M \otimes L) \oplus (N \otimes L); ((m,n),\ell) \mapsto (m \otimes \ell, n \otimes \ell)$.

   Using the universal property, we have a unique linear map as described in the statement, so we need to produce an inverse, and then it is an isomorphism. We have the following diagram:

   $$\begin{tikzcd} & (M \otimes L) \oplus (N \otimes L) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ M \otimes L \arrow[dr, "\psi_1"'] & & N \otimes L \arrow[dl, "\psi_2"] \\ & (M \oplus N) \otimes L & \end{tikzcd}$$

   Where $\pi_1, \pi_2$ are the projections, and $\psi_1, \psi_2$ are the obvious linear inclusions.

   Set $\psi = \psi_1\pi_1 + \psi_2\pi_2$ to give the linear map:

   $$\begin{aligned} \psi : (M \otimes L) \oplus (N \otimes L) &\to (M \oplus N) \otimes L \\ ((m \otimes \ell_1), (n \otimes \ell_2)) &\mapsto (m, 0) \otimes \ell_1 + (0, n) \otimes \ell_2 \end{aligned}$$

   Then $\psi$ is the required inverse of $\phi$.

4. Left as an exercise. See Atiyah-Macdonald 2.14.

$\square$

Example: $\mathrm{Hom}(M \otimes N, L) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, L))$. Given a bilinear map $\varphi : M \times N \to L$, we get $\theta : M \to \mathrm{Hom}(N, L)$ where $m \mapsto (\theta_m : N \to L, n \mapsto \varphi(m,n))$.

Conversely, given a linear map $\theta : M \to \mathrm{Hom}(N, L)$, we get a bilinear map $M \times N \to L, (m,n) \mapsto \theta(m)(n)$. Hence we have a 1-1 correspondence

$$\{\text{bilinear maps } M \times N \to L\} \leftrightarrow \{\text{linear maps } M \to \mathrm{Hom}(N, L)\}$$

But the LHS corresponds to the linear maps $M \otimes N \to L$.

## 3.1 Restriction and Extension of Scalars

**Definition 3.5.**
**Restriction:** *If $\varphi : R \to T$ is a ring homomorphism, and $N$ is a $T$-module, then $N$ may be regarded as an $R$-module via $r \cdot m = \varphi(r)m$. In particular, $T$ itself is an $R$-module.*

**Extension:** *If $M$ is an $R$-module, we can form another $R$-module $T \otimes_R M$. This can also be viewed as a $T$-module via $t_1(t_2 \otimes m) = (t_1t_2) \otimes m$.*

Example: Localisation is an extension of scalars $R \to S^{-1}R$. Given an $R$-module $M$ and the multiplicatively closed set $S$, there is a unique isomorphism $f : S^{-1}R \otimes_R M \to S^{-1}M$, via $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$.

The map $S^{-1}R \times M \to S^{-1}M; (\frac{r}{s}, m) \mapsto \frac{rm}{s}$, so by the universal property there is some $f : S^{-1}R \otimes M \to S^{-1}M$. Then $f$ is clearly surjective - is it injective?

A general element of the LHS is of the form $\sum_{i=1}^{n} \left(\frac{r_i}{s_i}\right) \otimes m_i$. Then set $s = s_1 \dots s_n$, $t_i = \prod_{j \neq i} s_j$. Then $\sum \left(\frac{r_i}{s_i}\right) \otimes m_i = \frac{1}{s} \otimes m$ for some $m \in M$.

Now if $f(\frac{1}{s} \otimes m) = 0$, then $\frac{m}{s}$ is zero in $S^{-1}M$, and so $xm = 0$ for some $x \in S$. But then $\frac{1}{s} \otimes m = \frac{x}{xs} \otimes m = \frac{1}{sx} \otimes xm = \frac{1}{sx} \otimes 0 = 0$, and $f$ is indeed injective.

## 3.2 Tensor Products of Maps

**Definition 3.6.** *Given R-module maps $\theta : M_1 \to M_2; \varphi : N_1 \to N_2$, the* **tensor product** *of $\theta$ and $\varphi$ is the R-module map*

$$\begin{aligned} \theta \otimes \varphi : M_1 \otimes N_1 &\to M_2 \otimes N_2 \\ m_1 \otimes n_1 &\mapsto \theta(m_1) \otimes \varphi(n_1) \end{aligned}$$

Note that $\theta \otimes \varphi$ is bilinear, and so universality tells us it is well-defined.

## 3.3 Tensor Product of Algebras

**Definition 3.7.** *Given $\varphi_1 : R \to T_1$ a ring homomorphism (so that $T_1$ is an R-module), then we say that $T_1$ together with the map $\varphi_1$ is an* **R-algebra**. *Given another ring homomorphism $\varphi_2 : R \to T_2$, we can take the tensor product of the R-modules $T_1, T_2$, to give $T_1 \otimes_R T_2$. We then define a product on $T_1 \otimes T_2$ by*

$$\begin{aligned} (T_1 \otimes T_2) \times (T_1 \otimes T_2) &\to T_1 \otimes T_2 \\ ((t_1 \otimes t_2), (t_1' \otimes t_2')) &\mapsto (t_1 t_1') \otimes (t_2 t_2') \end{aligned}$$

To check this multiplication is actually well-defined, note that multiplication $T_i \times T_i \to T_i; (t_i, t_i') \mapsto t_i t_i'$ is bilinear, and hence there is a corresponding $R$-module map $T_i \otimes T_i \to T_i$.

The composition $(T_1 \otimes T_1) \times (T_2 \otimes T_2) \to T_1 \otimes T_2 \to T_2 \otimes T_2$ is bilinear, and so we have a corresponding $R$-module map

$$\begin{aligned} (T_1 \otimes T_1) \otimes (T_2 \otimes T_2) &\to T_1 \otimes T_2 \\ (t_1 \otimes t_1') \otimes (t_2 \otimes t_2') &\mapsto t_1 t_1' \otimes t_2 t_2' \end{aligned}$$

Then by **3.4** there are isomorphisms:

$$\begin{aligned} (T_1 \otimes T_2) \otimes (T_1 \otimes T_2) &\to T_1 \otimes (T_2 \otimes (T_1 \otimes T_2)) \\ &\to T_1 \otimes ((T_2 \otimes T_1) \otimes T_2) \\ &\to T_1 \otimes ((T_1 \otimes T_2) \otimes T_2) \\ &\to T_1 \otimes (T_1 \otimes (T_2 \otimes T_2)) \\ &\to (T_1 \otimes T_1) \otimes (T_2 \otimes T_2) \end{aligned}$$

with $(t_1 \otimes t_1') \otimes (t_2 \otimes t_2') \mapsto (t_1 \otimes t_1') \otimes (t_2 \otimes t_2')$.

Composing gives our product as a well defined map. $1 \otimes 1$ is the multiplicative identity. $T_1 \otimes T_2$ is a ring with $R \to T_1 \otimes T_2; r \mapsto \varphi_1(r) \otimes 1 = 1 \otimes \varphi_2(r)$ a ring homomorphism. Hence $T_1 \otimes T_2$ is an $R$-algebra.

Examples:

1. If $k$ is a field, then $k[x]$ is a $k$-algebra. Note that $k[x_1] \otimes_k k[x_2] \cong k[x_1, x_2]$.
2. $\mathbb{Q}[x]/(x^2+1) \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}[x]/(x^1+1)$.
3. $k[x_1]/(f(x_1))) \otimes_k k[x_2]/(g(x_2)) \cong k[x_1, x_2]/((f(x_1), g(x_2)))$.

**Definition 3.8.** *If $R$ is a $k$-algebra, $M, N$ are $R$-modules, we regard $M \otimes_R N$ as an $R$-module via the* **diagonal action**

$$r(m \otimes n) = rm \otimes rn$$

*Note that if $M, N$ are finitely generated, so is $M \otimes N$.*

**Lemma 3.9.** *If $M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \to 0$ is a sequence of $R$-modules, then it is exact if and only if, for all $R$-modules $N$,*

$$0 \to \operatorname{Hom}(M_2, N) \xrightarrow{\alpha} \operatorname{Hom}(M, N) \xrightarrow{\beta} \operatorname{Hom} M_1, N$$

*is exact.*

*Proof.* ( $\Longrightarrow$ ) Let $N$ be an $R$-module. If $f \in \operatorname{Hom}(M_2, N)$, then $f \circ \varphi \in \operatorname{Hom}(M, N)$. This gives an injective map $\alpha : \operatorname{Hom}(M_2, N) \to \operatorname{Hom}(M, N)$, since if $f \neq 0$, there is some $m_2 \in M_2$ with $f(m_2) \neq 0$. But $m_2 = \varphi(m)$ for some $m$ since $\varphi$ is surjective, and hence $f\varphi(m) \neq 0$, and we have exactness at $\operatorname{Hom}(M_2, N)$.

If $g \in \operatorname{Hom}(M, N)$, then $g \circ \theta \in \operatorname{Hom}(M_1, N)$. Suppose $g \circ \theta \equiv 0$. Then $\theta(M_1) \subseteq \ker g$. By exactness, $\theta(M_1) = \ker \varphi$, and hence $\ker \varphi \subseteq \ker g$. So there is $f \in \operatorname{Hom}(M_2, N)$ with $f\varphi = g$, and we have exactness at $\operatorname{Hom}(M, N)$.

( $\Longleftarrow$ ) $\alpha$ is injective for all $N$, and hence $\varphi$ is surjective. Also $\beta\alpha \equiv 0$, and so $f \circ \varphi \circ \theta \equiv 0$ for any $f : M_2 \to N$. Take $N$ to be $M_2$ and $f$ to be $\mathrm{id}_{M_2}$. Then $\varphi \circ \theta = 0$, and so $\mathrm{i}\theta \subseteq \ker \varphi$. Now take $N = M/\mathrm{i}\theta$ and let $p : M \to N$ be projection. Then $p \in \ker \beta$, and hence there is some $g : M_2 \to N$ with $p = g \circ \varphi$. Thus $\mathrm{i}\theta = \ker p \supseteq \ker \varphi$. $\square$

Note that it is not true in general that a short exact sequence yields another one by applying $\operatorname{Hom}(\cdot, N)$ - this is the start of cohomology theory. However, the analogous statement that $0 \to M_1 \to M \to M_2$ is exact if and only if $0 \to \operatorname{Hom}(N, M_1) \to \operatorname{Hom}(N, M) \to \operatorname{Hom}(N, M_2)$ is exact for all $N$ (note that the 0 is at the other end, and the $N$ is in the other position in the Hom).

**Lemma 3.10.** *If $M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \to 0$ is an exact sequence and $N$ is an $R$-module, then:*

$$M_1 \otimes N \xrightarrow{\theta \otimes \mathrm{id}} M \otimes N \xrightarrow{\varphi \otimes \mathrm{id}} M_2 \otimes N \to 0$$
$$N \otimes M_1 \xrightarrow{\mathrm{id} \otimes \theta} N \otimes M \xrightarrow{\mathrm{id} \otimes \varphi} N \otimes M_2 \to 0$$

*are exact. The second statement follows from the first by commutativity of tensor products.*

*Proof.* Let $N'$ be any $R$-module. Since $\otimes$ is exact:

$$0 \to \operatorname{Hom}(M_2, \operatorname{Hom}(N, N')) \to \operatorname{Hom}(M, \operatorname{Hom}(N, N')) \to \operatorname{Hom}(M_1, \operatorname{Hom}(N, N'))$$

is exact by **3.9**. By the example after **3.4**, we have $\mathrm{Hom}(M, \mathrm{Hom}(N, N')) \cong \mathrm{Hom}(M \otimes N, N')$. So:

$$0 \to \mathrm{Hom}(M_2 \otimes, N') \to \mathrm{Hom}(M \otimes N', N') \to \mathrm{Hom}(M \otimes N, N')$$

is exact. Then use the converse part of **3.9** to get the result. $\square$

These are *not* short exact sequences: given a short exact sequence, applying $\cdot \otimes N$ does not necessarily preserve injectivity of the left hand map. For example:

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\pi}\!\!\to \mathbb{Z}/(2) \to 0$$

Take $N = \mathbb{Z}/(2)$. Then $\mathbb{Z} \otimes N \cong \mathbb{Z}/(2)$, so we get $\mathbb{Z}/(2) \xrightarrow{0} \mathbb{Z}/(2) \to \mathbb{Z}/(2) \to 0$. The left hand map here is not injective.

**Definition 3.11.** *We say an $R$-module $N$ is* **flat** *if, given any short exact sequence*

$$0 \to M_1 \to M \to M_2 \to 0$$

*the sequence*

$$0 \to M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$$

*is exact.*

For example:

- $R$ itself is a flat $R$-module.
- $R^n$ is a flat $R$-module, the free $R$-module on $n$ generators.
- If $R = \mathbb{Z}$, then $\mathbb{Q}$ is a flat $\mathbb{Z}$-module. In fact, any torsion-free abelian group is a flat $\mathbb{Z}$-module.

The subject of homology deals with measuring the failure of modules to be flat.

# 4 Integrality and Dimension

In this section, $R$ is a commutative ring with a 1.

**Definition 4.1.** *The* **spectrum** *of $R$, denoted* $\mathrm{Spec}(R)$ *is the set of prime ideals of $R$.*

**Definition 4.2.** *The* **length** *of a chain of prime ideals*

$$\mathfrak{p}_0 \lneq \mathfrak{p}_1 \lneq \mathfrak{p}_2 \lneq \ldots \lneq \mathfrak{p}_n$$

*is $n$ - note the numbering starts at 0.*

**Definition 4.3.** *The* **(Krull) dimension** *of a $R$, denoted* $\dim R$*, or Kr* $\dim R$*, is:*

$$\dim R = \begin{cases} \sup\{n : \exists \text{ a chain of prime ideals of length } n\} & \text{if this exists, and} \\ \infty & \text{otherwise} \end{cases}$$

**Definition 4.4.** *The* **height** *of $\mathfrak{p} \in \mathrm{Spec}(R)$, denoted* $\mathrm{ht}(\mathfrak{p})$ *(or sometimes* $\mathrm{ht}_R(\mathfrak{p})$ *to emphasise the ring), is*

$$\mathrm{ht}(\mathfrak{p}) = \sup\{n : \exists \text{ a chain of prime ideals of length } n \text{ with } \mathfrak{p}_n = \mathfrak{p}\}$$

Note that the 1-1 correspondence between primes that don't intersect $R \setminus \mathfrak{p}$ and the primes of $R_{\mathfrak{p}}$ shows that $\operatorname{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$.

**Examples.**

- An artinian ring has dimension 0, as all prime ideals are maximal. Conversely, any noetherian ring of dimension 0 is artinian.
- $\dim \mathbb{Z} = 1$. This holds for any PID, as primes are maximal, so any chain of prime ideals must be of the form $0 \subsetneq \mathfrak{p}$. In particular if $k$ is a field, $\dim k[x] = 1$. In general, we call any integral domain of Krull dimension 1 a ***Dedekind domain*** (so all PIDs are Dedekind domains).
- $\dim k[x_1, \ldots, x_n] \geq n$ since we have a chain of ideals

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \ldots \subsetneq (x_1, \ldots, x_n)$$

  Actually, if $k$ is a field, then $\dim k[x_1, \ldots, x_n] = n$. To prove this, we will need some results about the relationship between chains of prime ideals in subrings and chains in the whole ring under some condition relating the subring to the larger ring.

**Lemma 4.5.** *The height 1 primes of $k[x_1, \ldots, x_n]$ are precisely those of the form $(f)$ where $f$ is irreducible.*

*Proof.* Certainly, such an ideal is prime in a UFD. Any nonzero $\mathfrak{p}$ contains such an $(f)$, since if $g \in \mathfrak{p}$ then one of its irreducible factors is, by primality of $\mathfrak{p}$.

If $0 \subsetneq \mathfrak{p} \subsetneq (f)$, then there is an irreducible $h$ with $(h) \subsetneq \mathfrak{p}$ - take $h \in \mathfrak{p} \setminus (f)$. This would imply that $f$ divides $h$. But $h$ is irreducible $\lightning$. So $\mathfrak{p} = (f)$, and $\operatorname{ht}(f) = 1$.

For the converse, see example sheet 3. $\square$

**Definition 4.6.** *Let $R \leq S$ be rings. Then $x \in S$ is* **integral over R** *if it satisfies some monic polynomial with coefficients in $R$, i.e. if there is $n \in \mathbb{N}$ and $r_i \in R$ such that*

$$x^n = r_0 + r_1 x^n + \ldots + r_{n-1} x^{n-1}$$

For example, the elements of $\mathbb{Q}$ which are integral over $\mathbb{Z}$ are precisely $\mathbb{Z}$.

**Lemma 4.7.** *The following are equivalent:*

1. *$x \in S$ is integral over $R$.*
2. *$R[x]$ is a finitely generated $R$-module.*
3. *$R[x]$ is contained in $T$, a subring of $S$ that is also a finitely generated $R$-module.*

Some authors say ***S is finite over R*** if $S$ is a finitely generated $R$-module, and $k$-algebra $R$ is ***of finite type*** if it is finitely generated as a $k$-algebra.

*Proof.*

1. $\implies$ 2. For $j \geq 0$, we have

$$x^{n+j} = r_0 x^j + \ldots + r_{n-1} x^{n+j-1}$$

So by induction all positive powers of $x$ lie in $R + xR + \ldots + x^{n-1}R$. Clearly this is a submodule of $R[x]$, so we have equality, and $R[x] = R + xR + \ldots + x^{n-1}R$ is finitely generated.

2. $\implies$ 3. Take $T = R[x]$.

3. $\implies$ 1. Consider multiplication by $x$ in the ring $T = y_1R + \ldots + y_nR$, by finiteness.

Then $xy_i = \sum_j r_{ij}y_j$ for $r_{ij} \in R$, so we have

$$\sum_j \underbrace{(x\delta_{ij} - r_{ij})}_{A_{ij}} y_j = 0$$

where $\delta_{ij}$ is the Kronecker delta.

Multiplying on the left by $\operatorname{adj}(A)$ gives us $(\det A)y = 0$ for all $y$. Taking $y$ to be 1, we get $\det A = 0$. But $\det A$ is also a monic polynomial in $x$, and hence $x$ is integral over $R$.

□

The proof is reminiscent of the proof in Atiyah-Macdonald for Nakayama's lemma. Some authors say $S$ is ***of finite type*** over $R$ is $S$ is generated as a ring by $R$ and some finite set.

**Lemma 4.8.** *If $x_1, \ldots, x_m \in S$ are integral over $R$, then $R[x_1, \ldots, x_m]$ is a finitely-generated $R$-module.*

*Proof.* This is an easy induction on $m$. The case of $m = 1$ is **4.7**. Now assume $m > 1$.

Suppose that $R[x_1, \ldots, x_k]$ is finite over $R$, generated by $y_1, \ldots, y_\ell$ say. Now $x_{k+1}$ is integral over $R$, and hence over $R[x_1, \ldots, x_k]$. Thus $R[x_1, \ldots, x_{k+1}]$ is a finitely generated $R[x_1, \ldots, x_k]$-module, with generators $z_1, \ldots, z_t$. Then

$$\{z_iy_j : 12 \leq i \leq t, 1 \leq j \leq \ell\}$$

generate $R[x_1, \ldots, x_{k+1}]$ as an $R$-module. □

**Lemma 4.9.** *The set $T \subseteq S$ of elements integral over $R$ form a subring of $S$.*

*Proof.* Every element of $R$ is integral over $R$. If $x, y \in T$, then by **4.8**, $R[x, y]$ is finitely generated $R$-module. So by **4.7.3** $x \pm y$ and $xy$ are integral over $R$. □

**Definition 4.10.**

- *$T$ in **4.9** is the* **integral closure** *of $R$ in $S$.*
- *If $T = R$ then $R$ is* **integrally closed** *in $S$.*
- *If $T = S$ then $S$ is* **integral** *over $R$.*
- *If $R$ is an integral domain then $R$ is* **integrally closed** *if it is integrally closed in its field of fractions.*

**Examples.**

- $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.
- $k[x_1, \ldots, x_n]$ is integrally closed in $k(x_1, \ldots, x_n)$.
- In an algebraic number field $K$ with $[K : \mathbb{Q}] < \infty$, the integral closure of $\mathbb{Z}$ in $K$ is the ring of integers in $K$, denoted $\mathcal{O}_K$.
- Being integrally closed is a local property.

**Lemma 4.11.** *Let $R \leq T \leq S$ be rings, with $T$ integral over $R$ and $S$ integral over $T$. Then $S$ is integral over $R$.*

*Proof.* Take some $x \in S$. It satisfies $x^n + t_{n-1}x^{n-1} + \ldots + t_0 = 0$ for $t_i \in T$. The subring $R[t_0, \ldots, t_{n-1}]$ is a finitely generated $R$-module by **4.8**, and $x$ is integral over it, so $R[t_0, \ldots, t_{n-1}, x]$ is a finitely generated $R[t_0, \ldots, t_{n-1}]$-module.

So, as in **4.8** $R[t_0, \ldots, t_{n-1}, x]$ is a finitely generated $R$-module. Now apply **4.7.3**. □

**Lemma 4.12.** *Let $R \leq T$ be rings, and $T$ integral over $R$.*

1. *If $J \triangleleft T$, then $T/J$ is integral over $R/(J \cap R)$, identifying $R/(J \cap R)$ with $(R + J)/J$ as a subring of $T/J$.*
2. *If $S$ is a multiplicatively closed subset of $R$, then $S^{-1}T$ is integral over $S^{-1}R$.*

*Proof.*

1. If $x \in T$, then $x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0$ for some $r_i \in R$. Modulo $J$, putting bars on for images in $T/J$, we have the monic equation:

$$\bar{x}^n + \bar{r}_{n-1}\bar{x}^{n-1} + \ldots + \bar{r}_0 = \bar{0}$$

   in $T/J$ with $r_i \in (R + J)/J$.

2. Suppose $\frac{x}{s} \in S^{-1}T$. Then $x$ satisfies a monic polynomial equation as in *1.*. So

$$\left(\frac{x}{s}\right)^n + \frac{r_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \ldots + \frac{r_0}{s^n} = 0$$

   in $S^{-1}T$. Hence $\frac{x}{s}$ is integral over $S^{-1}R$.

□

**Lemma 4.13.** *Let $R \leq T$ be both integral domains with $T$ integral over $R$. Then $T$ is a field if and only if $R$ is a field.*

*Proof.* If $R$ is a field, let $t \in T$ be nonzero, and choose a monic equation of least degree of the form

$$t^n + r_{n-1}t^{n-1} + \ldots + r_0 = 0$$

with $r_i \in R$. Since $T$ is a domain, $r_0 \neq 0$, as otherwise this polynomial factors, contradicting minimality. Hence $t$ has an inverse, namely $-r_0^{-1}(t^{n-1} + \ldots + r_0) \in T$, and so $T$ is a field.

Conversely, suppose that $T$ is a field. Let $0 \neq x \in R$. Then $x$ has an inverse $x^{-1} \in T$. So $x^{-1}$ satisfies a monic equation $x^{-m} + r'_m x^{-m+1} + \ldots + r'_0 = 0$. Rearrange for a formula for $x^{-1} = -(r'_m + r'_{m-1}x + \ldots + r'_0 x^{m-1}) \in R$. Thus $R$ is a field. □

**Lemma 4.14.** *Let $R \leq T$ be rings, with $T$ integral over $R$. Let $\mathfrak{q}$ be a prime ideal in $T$ and set $\mathfrak{p} = R \cap \mathfrak{q}$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

*Proof.* By **4.2.1**, $T/\mathfrak{q}$ is integral over $R/\mathfrak{p}$, and since $\mathfrak{p}, \mathfrak{q}$ are prime, we have $T/\mathfrak{q}$ and $R/\mathfrak{p}$ are domains.

So **4.13** gives $T/\mathfrak{q}$ a field if and only if $R/\mathfrak{p}$ a field, i.e. $\mathfrak{q}$ maximal if and only if $\mathfrak{p}$ maximal. □

**Theorem 4.15** (Incomparability Theorem)**.** *Let $R \subset T$ be rings with $T$ integral over $R$. Let $\mathfrak{q} \subseteq \mathfrak{q}_1$ be prime ideals of $T$. Suppose $\mathfrak{q} \cap R = \mathfrak{p} = \mathfrak{q}_1 \cap R$. Then $\mathfrak{q} = \mathfrak{q}_1$.*

This theorem tells us that strict chains of primes in $T$ induce strict chains of primes in $R$, and in particular, that $\dim R \geq \dim T$.

*Proof.* Apply **4.12.2** with $S = R \setminus \mathfrak{p}$. Now $T_\mathfrak{p}$ is integral over $R_\mathfrak{p}$, (writing $T_\mathfrak{p} = S^{-1}T$, even though $\mathfrak{p}$ might not be prime in $T$). By chapter 2, there is a prime $S^{-1}\mathfrak{p}$ in $R_\mathfrak{p}$, the unique maximal ideal. Also, there is $S^{-1}\mathfrak{q}, S^{-1}\mathfrak{q}_1$ in $T_\mathfrak{p}$ which are also prime. And $S^{-1}\mathfrak{q} \cap S^{-1}R = S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}_1 \cap S^{-1}R$, since $\mathfrak{q} \cap R = \mathfrak{p} = \mathfrak{q}_1 \cap R$.

Now by **14.4**, $S^{-1}\mathfrak{q}$ and $S^{-1}\mathfrak{q}_1$ are maximal. But $S^{-1}\mathfrak{q} \leq S^{-1}\mathfrak{q}_1$, and hence $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{q}_1$. Using the one-to-one correspondence between primes of $S^{-1}T$ and of $T$ not intersecting $S$, we must have $\mathfrak{q} = \mathfrak{q}_1$. □

**Theorem 4.16** (Lying over Theorem)**.** *Let $R \leq T$ be rings, and $T$ integral over $R$. Let $\mathfrak{p}$ be a prime ideal of $R$. Then there is a prime ideal $\mathfrak{q}$ of $T$ with $\mathfrak{q} \cap R = \mathfrak{p}$ - we say $\mathfrak{q}$ "lies over" $\mathfrak{p}$.*

*In other words, the map* $\mathrm{Spec}(T) \longrightarrow \mathrm{Spec}(R)$ *is surjective.*

*Proof.* By **4.12**, $T_\mathfrak{p}$ is integral over $R_\mathfrak{p}$. Consider a maximal ideal of $T_\mathfrak{p}$. It is of the form $S^{-1}\mathfrak{q}$ for some ideal $\mathfrak{q}$ of $T$ which is necessarily prime, as primality is preserved in the one-to-one correspondence.

Then $S^{-1}\mathfrak{q} \cap S^{-1}R$ is maximal by **4.14** and hence is the unique maximal ideal $S^{-1}\mathfrak{p}$ of $S^{-1}R = R_\mathfrak{p}$. So $S^{-1}\mathfrak{q} \cap S^{-1}R = S^{-1}\mathfrak{p}$. Hence $\mathfrak{q} \cap R = \mathfrak{p}$. □

Now we will have two theorems of Cohen and Seidelberg (1946) - the "going up" and "going down" theorems, that will allow us to move from chains of prime ideals in $R$ to such chains in $T$, where $R \leq T$ are rings and $T$ is integral over $R$. The second theorem will need stronger conditions:

**Theorem 4.17** ("Going-up Theorem")**.** *Let $R \subset T$ be rings with $T$ integral over $R$. Let $\mathfrak{p}_1 \leq \ldots \leq \mathfrak{p}_n$ be a chain of prime ideals of $R$, and $\mathfrak{q}_1 \leq \ldots \leq \mathfrak{q}_m$ ($m < n$) a chain of prime ideals in $T$, with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$.*

*Then we can extend the chain of $\mathfrak{q}$s to a chain of length $n$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq n$.*

*Proof.* By induction, it's enough to consider the case $n = 2, m = 1$. Write $\bar{R}$ for $R/\mathfrak{p}_1$, $\bar{T}$ for $T/\mathfrak{q}_1$. Then $\bar{R} \hookrightarrow \bar{T}$ with $\bar{T}$ integral over $\bar{R}$, using the fact that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$ and **4.12.2**. By the lying over theorem, there is a prime $\mathfrak{q}_2$ of $\bar{T}$ such that $\bar{q}_2 \cap \bar{R} = \bar{\mathfrak{p}}_2$. Lifting back gives a prime ideal $\mathfrak{q}_2$ of $T$ with $\mathfrak{q}_2 \geq \mathfrak{q}_1$, and $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$. □

**Theorem 4.18** ("Going-down Theorem")**.** *Let $R \subset T$ be integral domains, with $R$ integrally closed in $T$ and $T$ integral over $R$. Let $\mathfrak{p}_1 \geq \ldots \geq \mathfrak{p}_n$ be a chain of prime ideals of $R$, and $\mathfrak{q}_1 \geq \ldots \geq \mathfrak{q}_m$ ($m < n$) be a chain of prime ideals in $T$, with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$.*

*Then we can extend the chain of $\mathfrak{q}$s to a chain of length $n$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq n$.*

Later we will apply these to finitely generated $k$-algebras $T$ and prove "Noether normalisations" - if $T$ is a domain the $T$ is integral over a subalgebra isomorphic to a polynomial algebra.

**Corollary 4.19** (of going up)**.** *Let $R \leq T$, with $T$ integral over $R$. Then* $\dim R = \dim T$.

*Proof.* Take a chain $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_n$ of primes in $T$. Intersecting with $R$ gives a strict chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ of primes in $R$, with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. Thus $\dim R \geq \dim T$.

Conversely, suppose $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ is a chain of primes in $R$. Then there is a prime $\mathfrak{q}_0$ lying over $\mathfrak{p}_0$ by **4.16**, and the going-up theorem gives a strict chain $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. So $\dim R \leq \dim T$. □

**Corollary 4.20** (of going down)**.** *Let $R \leq T$, with $T$ an integral domain, $R$ integrally closed, and $T$ integral over $R$. Let $\mathfrak{q}$ be a prime of $T$. Then*

$$\operatorname{ht}(\mathfrak{q} \cap R) = \operatorname{ht} \mathfrak{q}$$

*Proof.* Take the chain $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n = \mathfrak{q}$ in $\operatorname{Spec}(T)$. As above, there is a chain $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{q} \cap R$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, so $\operatorname{ht}(\mathfrak{q} \cap R) \geq \operatorname{ht}(\mathfrak{q})$.

Conversely, if $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{q} \cap R$, then the going-down theorem gives $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n = \mathfrak{q}$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. So $\operatorname{ht}(\mathfrak{q} \cap R) \leq \operatorname{ht} q$. □

To prove the going down theorem, we'll need two lemmas and a bit of Galois theory.

**Definition 4.21.** *If $I \lhd R$ and $R \leq T$, then $x \in T$ is* **integral over I** *if $x$ satisfies a monic equation $x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0$ with $r_i \in I$. The* **integral closure** *of $I$ in $T$ is the set of such $x$.*

**Lemma 4.22.** *Let $R \leq T$ be rings with $T$ integral over $R$. Let $I \lhd R$. Then the integral closure of $I$ in $T$ is the radical $\sqrt{TI}$ (note that $TI \lhd I$), and this is closed under addition and multiplication. In particular, if $R = T$, then the integral closure of $I$ in $R$ is $\sqrt{I}$.*

*Proof.* If $x$ is integral over $I$, then **4.21** implies $x^n \in TI$, and hence $x \in \sqrt{TI}$.

Conversely, if $x \in \sqrt{TI}$, then $x^n = \sum_i t_i r_i$ say, for some $n \in \mathbb{N}, r_i \in I, t_i \in T$.

But each $t_i$ is integral over $R$, so **4.8** implies that $M = R[t_1, \ldots, t_n]$ is a finitely generated $R$-module. Also, $x^n R[t_1, \ldots, t_n] \subseteq IM$. Let $y_1, \ldots, y_s$ be a generating set for $M$. Then $x^n y_j = \sum_\ell r_{j\ell} y_\ell$ for some $r_{j\ell} \in I$. As in the proof of **4.7**, we then get

$$\sum_\ell (x^n \delta_{j\ell} - r_{j\ell}) y_\ell = 0$$

and we thus deduce that $x^n$ satisfies an equation of the form $(x^n)^s + \ldots + r_0' = 0$. Note that the coefficients are $I$. Thus $x^n$, and so $x$, is integral over $I$. □

**Lemma 4.23.** *Let $R \subseteq T$ be integral domains, with $R$ integrally closed, and let $x \in T$ be integral over an ideal $I$ of $R$. Then $x$ is algebraic over $K$, the field of fractions $R$, and the minimal polynomial over $K$, say $m_x(t) = t^n + r_{n-1}t^{n-1} + \ldots + r_0$ has its coefficients in $\sqrt{I}$.*

*Proof.* Certainly $x$ is algebraic over $K$ as it is integral over $I$. We claim the coefficients $r_i$ of the minimal polynomial of $x$ over $K$ are all integral over $I$.

This will then imply that $r_i \in R$, as $R$ integrally closed, and by **4.22**, with $T = R$, we have $r_i \in \sqrt{I}$ since they lie in the integral closure of $I$ in $R$.

To see the claim, take an extension field $L$ of $K$ containing all of the conjugates $x_1, \ldots, x_n$ of $x$, for instance a splitting field of $m_x(t)$. If $y = x_i$ is a root of $m_x(t)$, the applying there is a $K$-automorphism of $L$ with $x \mapsto \alpha$.

Now $y$ is integral over $I$: if $x$ satisfies the monic equation $x^m + r'_{m-1}x^{m-1} + \ldots + r'_0 = 0$ with $r'_i \in I$, then applying the automorphism gives $y^m + r'_{m-1}y^{m-1} + \ldots + r'_0 = 0$, as $r'_i \in I \subseteq R \subseteq K$. So $y$ lies in the integral closure of $R$ in $L$.

The coefficients $m_x(t)$ are obtained from its roots in $L$ by taking sums and products, and hence these coefficients are integral over $I$. $\square$

Finally, we move on to a proof of the going-down theorem:

*Proof of Going-down.* By induction, it's enough to consider the case $m = 1, n = 2$.

So $\mathfrak{p}_1 \gneq \mathfrak{p}_2$, and $\mathfrak{q}_1$ is such that $\mathfrak{q} \cap R = \mathfrak{p}_1$. We seek $\mathfrak{q}_2 \leq \mathfrak{q}_2$ with $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$.

Let $S_1 = T \setminus \mathfrak{q}_1, S_2 = R \setminus \mathfrak{p}_2$, and set $S = S_1S_2 = \{rt : r \in S_1, t \in S_2\}$. Then $S$ is multiplicatively closed and contains both $S_1, S_2$.

Assume first that $T\mathfrak{p}_2 \cap S = \emptyset$. Now $T\mathfrak{p}_2$ is an ideal of $T$, so $S^{-1}(T\mathfrak{p}_2) \lneq S^{-1}T$ and is proper by assumption.

Hence $S^{-1}T\mathfrak{p}_2$ lies in a maximal ideal of $S^{-1}T$, which is necessarily of the form $S^{-1}\mathfrak{q}_2$ for some prime ideal $\mathfrak{q}_2$ of $T$ such that $\mathfrak{q}_2 \cap S = \emptyset$ and $T\mathfrak{p}_2 \leq \mathfrak{q}_2$ (as $S^{-1}(T\mathfrak{p}_2) \leq S^{-1}\mathfrak{q}_2$). Hence $\mathfrak{p}_2 \leq T\mathfrak{p}_2 \cap R \leq \mathfrak{q}_2 \cap R$.

Moreover, since $\mathfrak{q}_2 \cap S = \emptyset$ and $S_2 = R \setminus \mathfrak{p}_2 \subset S$, we get that $\mathfrak{p}_2 \geq \mathfrak{q}_2 \cap R$, and hence we have equality.

Similarly, $S_1 = T \setminus fq_1 \subseteq S$, and $\mathfrak{q}_2 \leq \mathfrak{q}_1$.

It remains to prove that assumption that $T\mathfrak{p}_2 \cap S = \emptyset$.

Suppose not, and take some $0 \neq x \in T\mathfrak{p}_2 \cap S$. By **4.22** with $I = \mathfrak{p}_2$, $x$ lies in the integral closure of $\mathfrak{p}_2$ in $T$. Hence, by **4.23** it must be algebraic over the field of fractions $K$ of $R$, and its minimal polynomial over $K$ has coefficients in $\mathfrak{p}_2$ (as $\sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$ by primality).

But $x \in S$, and hence is of the form $rt$ for some $r \in S_1, t \in S_2$. Now if $x$ has minimal polynomial $X^n + r_{n-1}X^{n-1} + \ldots + r_0$ over $K$, then $t = \frac{x}{r}$ has minimal polynomial

$$X^n + \frac{r_{n-1}}{r}x^{n-1} + \ldots + \frac{r_0}{r^n}$$

again over $K$, and these coefficients are in $R$ since $t_1 \in T$ is integral over $R$.

Calling these coefficients $r'_i$, we have $r_i \in \mathfrak{p}_2$ and $r \notin \mathfrak{p}_2$, so $r'_i \in \mathfrak{p}_2$. By definition, $t$ is integral over $\mathfrak{p}_2$, and so by **4.22** we see $t \in \sqrt{T\mathfrak{p}_2}$. However $t \in S_1 = T \setminus \mathfrak{q}_1$, but $T\mathfrak{p}_2 \leq \mathfrak{q}_1$, and hence we have a contradiction. $\square$

Now we focus on ***affine k-algebras*** where $k$ is a field, i.e. the $k$-algebras of finite type over $k$, i.e. the algebras generated as rings by $k$ and a finite set $x_1, \ldots, x_n$, and thus homomorphic images of the polynomial rings $k[x_1, \ldots, x_n]$. We will work away towards the following theorem:

**Theorem 4.24.** *Let $R$ be an affine algebra which is an integral domain with fraction field $K$. Then*

$$\dim R = \operatorname{tr}\deg_k K$$

*where* $\operatorname{tr}\deg_k K$ *is the* **transcendence degree** *of $K$ over $k$.*

## 4.1 Transcendence Degree

We say that $x_1, \dots, x_n$ are ***algebraically independent*** over $k$ if the ring map $k[X_1, \dots, X_n] \to k[x_1, \dots, x_n]$, $X_i \mapsto x_i$ is an isomorphism, and so $k[x_1, \dots, x_n]$ may be regarded as a polynomial algebra. As in linear algebra, we consider maximal algebraically independent sets - they all have the same size. Such a set is a ***transcendence basis*** over $k$, the ***transcendence degree*** is the cardinality of the set. We have a translation from the terminology of linear algebra:

| | | |
|---|---|---|
| Linearly independent set | $\longleftrightarrow$ | Algebraically independent set |
| Span $\langle S \rangle$ | $\longleftrightarrow$ | The algebraic closure of $S$: the maximal algebraic extension of $k[x_1, \dots, x_n]$ |
| Dimension | $\longleftrightarrow$ | Transcendence degree |

For example, let $L = k(X_1, \dots, X_n)$ be the fraction field of $k[X_1, \dots, X_n]$, and $f$ irreducible in $k[X_1, \dots, X_n]$. Put $K = \operatorname{Frac} k[X_1, \dots, X_n]/(f)$. Then:

$\operatorname{tr}\deg_k L = n$ $X_1, \dots, X_n$ is a maximal algebraically independent set

$\operatorname{tr}\deg_k K = n - 1$ $K$ is an algebraic extension of $k(X_1, \dots, \widehat{X}_i, \dots, X_n)$ where $X_i$ appears in $f$

The key result for proving **4.24** is:

**Theorem 4.25** (Noether's Normalisation Lemma (AM p.69))**.** *Let $T$ be an affine algebra. Then $T$ is integral over a subalgebra of the form $R = k[x_1, \dots, x_n]$ with the $x_i$ algebraically independent.*

*Proof.* Let $T = k[a_1, \dots, a_n]$. The proof will be by induction on $n$.

Let $r$ be the maximal number of algebraically independent elements. Without loss of generality, we take $r \geq 1$, otherwise $T$ is a finite dimensional vector space over $k$ and we can take $R = k$.

There is nothing to do if $a_1, \dots, a_n$ are algebraically independent. So renumber the $a_i$ so that the first $r$ of them are algebraically independent, and $a_{r+1}, \dots, a_n$ are algebraically dependent on $a_1, \dots, a_r$ over $k$.

Then take $0 \neq f \in k[x_1, \dots, x_r, x_n]$ with $f(a_1, \dots, a_r, a_n) = 0$. Then $f(x_1, \dots, x_r, x_n)$ is a sum of terms $\lambda_{\tilde{\ell}} x_1^{\ell_1} \dots x_r^{\ell_r} x_n^{\ell_n}$, where the $(r+1)$-tuple $\widetilde{\ell}$ is of the form $(\ell_1, \dots, \ell_r, \ell_n)$ for $\ell_i \in \mathbb{R}_{\geq 0}$. □