# Amazingly important notes from commutative algebra

Fredrik Meyer

**Abstract**

These are notes based on "Introduction to commutative algebra" by Atiyah-MacDonald. Some proofs and concepts are omitted, others are extended. I have tried to use categorical language where possible. (written december 2010)

## Contents

**1 Chapter 1** **2**
- 1.1 Basic ideal theory . . . . . 2
- 1.2 Various small-facts . . . . . 6

**2 Modules** **6**
- 2.1 Various simple facts . . . . . 6
- 2.2 Exact sequences . . . . . 7
- 2.3 Tensor product of modules . . . . . 8
- 2.4 Exactness properties of the tensor product . . . . . 9
- 2.5 Various smallfacts . . . . . 11
- 2.6 Direct limits . . . . . 11

**3 Rings and modules of fractions** **13**
- 3.1 Local properties . . . . . 16
- 3.2 Extended and contracted ideals . . . . . 16
- 3.3 Various small-facts . . . . . 18

**4 Primary decomposition** **18**
- 4.1 Various small-facts and examples . . . . . 21

**5 Integral dependence** **21**
5.1 Going-up . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22
5.2 Going-down . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
5.3 Various . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 25

**6 Chain conditions** **27**

**7 Noetherian Rings** **29**
7.1 Primary decomposition in Noetherian rings . . . . . . . . . . . 30

**8 Artin rings** **32**

**9 Discrete Valuation Rings** **34**

**10 Completions** **34**
10.1 Topologies and completions . . . . . . . . . . . . . . . . . . . 34
10.2 Filtrations . . . . . . . . . . . . . . . . . . . . . . . . . . . . 37
10.3 Graded rings and modules . . . . . . . . . . . . . . . . . . . . 37
10.4 The associated graded ring . . . . . . . . . . . . . . . . . . . 40

**11 Dimension theory** **42**
11.1 The Poincaré series . . . . . . . . . . . . . . . . . . . . . . . 42
11.2 The characteristic polynomial . . . . . . . . . . . . . . . . . . 44
11.3 Dimension theory of Noetherian local rings . . . . . . . . . . . 45

# 1 Chapter 1

This chapter deals with the basics of ideal theory and prime ideals. Rings, ring homomorphisms, and quotiens of them are defined. "Must-knows": zero-divisor, integral domain, nilpotent, unit, principal ideal, field (in a field, $1 \neq 0$).

## 1.1 Basic ideal theory

We have the following useful result:

**Proposition 1.1.** *Let $A$ be a non-zero ring. TFAE:*
*1) $A$ is a field.*
*2) the only ideals in $A$ are $0$ and $(1)$*
*3) Every homomorphism of $A$ into a non-zero ring $B$ is injective.*

We have alternative definitions of prime and maximal ideals:

$$\mathfrak{p} \text{ is prime} \Leftrightarrow A/\mathfrak{p} \text{ is an integral domain}$$

$$\mathfrak{m} \text{ is maximal} \Leftrightarrow A/\mathfrak{m} \text{ is a field}$$

The contraction of a prime ideal is a prime ideal. The contraction of a maximal ideal is not necessarily a maximal ideal.

**Proposition 1.2.** *Every non-unit in $A$ is contained in some maximal ideal.*

**Definition 1.3.** *A ring with only one maximal ideal is a* ***local ring****. The field $A/\mathfrak{m}$ is called the* ***residue field****.*

**Proposition 1.4.** *1) Let $\mathfrak{m} \neq (1)$ such that all $x \in A - \mathfrak{m}$ is a unit. Then $A$ is a local ring and $\mathfrak{m}$ its maximal ideal.*
*2) Let $\mathfrak{m}$ be a maximal ideal of $A$. If every element of $1 + \mathfrak{m}$ is a unit, then $A$ is a local ring.*

The **nilradical** is the set of all nilpotent elements in the ring, and it is an ideal. Also:

**Proposition 1.5.** *The nilradical is the intersection of all prime ideals in $A$.*

$$\mathfrak{N}(A) = \bigcap_{\mathfrak{p} \subset A} \mathfrak{p}$$

*Proof.* We let $\mathfrak{N}$ denote the nilradical and $\mathfrak{N}'$ denote the intersection of all prime ideals in $A$.

First, assume $f$ is nilpotent and let $\mathfrak{p}$ be a prime ideal. Then $f^n = 0 \in \mathfrak{p}$ for some $n$. Since $\mathfrak{p}$ is prime, $f \in \mathfrak{p}$, so $f \in \mathfrak{N}'$ (since $\mathfrak{p}$ was arbitrary).

Now, assume $f$ is not nilpotent and let $\Sigma$ be the set of ideals $\mathfrak{a}$ such that

$$n > 0 \Rightarrow f^n \notin \mathfrak{a}$$

$\Sigma$ is non-empty since $0 \in \Sigma$. By Zorn's lemma, $\Sigma$ has a maximal element $\mathfrak{p}$. Let $x, y \notin \mathfrak{p}$. Then $\mathfrak{p}$ is strictly contained in $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$, so by maximality they don't belong to $\Sigma$. By the definition of $\Sigma$, we have $f^m \in \mathfrak{p} + (x)$ and $f^n \in \mathfrak{p} + (y)$ for some $m, n$. It follows that $f^{m+n} \in \mathfrak{p} + (xy)$, so $\mathfrak{p} + (xy) \notin \Sigma$, so $xy \notin \mathfrak{p}$. Hence $\mathfrak{p}$ is a prime ideal not containing $f$, so $f \notin \mathfrak{N}'$.[1] $\square$

[1] Note that if $A$ is Noetherian, then we need not use Zorn's lemma. Every set of ideals in a Noetherian ring has a maximal element.

The **Jacobson radical** of $A$ is the intersection of all the maximal ideals of $A$.

**Proposition 1.6.** *Let the Jacobson radical be denoted by* $\mathfrak{J}$. *Then*

$$x \in \mathfrak{J} \Leftrightarrow 1 - xy \text{ is a unit in } A \text{ for all } y \in A$$

One can form the sum of any family of ideals, the product of any finite set of ideals. The intersection of any family of ideals is an ideal.

**Definition 1.7.** *Two ideals* $\mathfrak{a}, \mathfrak{b}$ *are* ***coprime*** *if* $\mathfrak{a} + \mathfrak{b} = (1)$.

**Proposition 1.8.** *Let* $A$ *be a ring and let* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *be ideals of* $A$. *Define*

$$\phi : A \to \prod_{i=1}^{n} (A/\mathfrak{a}_i)$$

*by* $x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$. *Then*
*1) If the* $\mathfrak{a}_j$ *are pairwise coprime, then* $\Pi \mathfrak{a}_i = \cap \mathfrak{a}_i$.
*2)* $\phi$ *is surjective* $\Leftrightarrow$ *the* $\mathfrak{a}_j$ *are pairwise coprime.*
*3)* $\phi$ *is injective* $\Leftrightarrow \cap \mathfrak{a}_i = (0)$.

For prime ideals we have the following important result:

**Proposition 1.9.** *1) Let* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *be prime ideals and let* $\mathfrak{a} \subseteq \cup_{i=1}^{n} \mathfrak{p}_i$. *Then* $\mathfrak{a} \subseteq \mathfrak{p}_i$ *for some* $i$.
*2) Let* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *be ideals and let* $\mathfrak{p}$ *be a prime ideal such that* $\cap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p}$. *Then* $\mathfrak{a}_i \subseteq \mathfrak{p}$ *for some* $i$. *If* $\mathfrak{p} = \cap \mathfrak{a}_i$, *then* $\mathfrak{p} = \mathfrak{a}_i$.

We can "divide" ideals.

**Definition 1.10.** *If* $\mathfrak{a}, \mathfrak{b}$ *are ideals in* $A$, *their* ***ideal quotient*** *is*

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A | x\mathfrak{b} \subseteq \mathfrak{a}\}$$

**Example:** $(6 : 2) = (3)$. The **annihilator** of $\mathfrak{b}$ is $(0 : \mathfrak{b}) = \mathrm{Ann}(\mathfrak{b})$. Thus the set of zero-divisors is

$$D = \bigcup_{x \neq 0} \mathrm{Ann}(x)$$

We have

**Proposition 1.11.**

$$\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b}) \qquad (\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$$
$$(\cap_i \mathfrak{a}_i : \mathfrak{b}) = \cap_i (\mathfrak{a}_i : \mathfrak{b}) \quad (\mathfrak{a} : \sum_i \mathfrak{b}_i) = \cap_i (\mathfrak{a} : \mathfrak{b}_i)$$

*and* $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.

**Definition 1.12.** *The* ***radical*** *of* $\mathfrak{a}$ *is*

$$r(\mathfrak{a}) = \{x \in A | x^n \in \mathfrak{a} \textit{ for some } n > 0\}$$

*Or equivalently, the contraction of the nilradical in* $A/\mathfrak{a}$*.*

**Example:** $r(x^2, y^3) = (x, y)$. We have

**Proposition 1.13.**

$$r(\mathfrak{a}) \supseteq \mathfrak{a} \qquad r(r(\mathfrak{a})) = r(\mathfrak{a})$$
$$r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b}) \qquad r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$$
$$r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) \quad r(\mathfrak{p}^n) = \mathfrak{p} \textit{ for all prime } \mathfrak{p}$$

*Proof.* We prove only $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$. Since $\mathfrak{a} + \mathfrak{b} \subseteq r(\mathfrak{a}) + r(\mathfrak{b})$, the inclusion $r(\mathfrak{a} + \mathfrak{b}) \subseteq r(r(\mathfrak{a}) + r(\mathfrak{b}))$ is obvious. Conversely, let $x \in r(r(\mathfrak{a}) + r(\mathfrak{b}))$. Then $x$ is on the form $x = r + q$ with $r \in r(\mathfrak{a})$ and $q \in r(\mathfrak{b})$. That is, $r^k \in \mathfrak{a}$ and $q^l \in \mathfrak{b}$ for some $k, l > 0$. Then $x^{k+l+1} \in \mathfrak{a} + \mathfrak{b}$. $\square$

**Proposition 1.14.** *The radical of* $\mathfrak{a}$ *is the intersection of the prime ideals containing* $\mathfrak{a}$*.*

**Example 1:** We want to find the radical of the ideal $I = (x^2y, y^2x)$ in the polynomial ring $k[x, y]$, where $k$ is a field. We have $I = (x^2y) + (y^2x)$, and so $r(x^2y, y^2x) = r((x^2y) + (y^2x)) = r(r(x^2y) + r(y^2x)) = r((x, y) + (x, y)) = r(x, y) = r(x, y)$, since $(x, y)$ is prime.

**Example 2:** Continouing the previous example, we want to find the ideal quotient $(I : xy)$. That is, all $f \in k[x, y]$ such that $fxy \in I$. The natural guess is $(x, y)$. Obviously, $(x, y) \subseteq (I : xy)$ (since every element of $(x, y)$ is of the form $fx + gy$). But $(x, y)$ is maximal, so $(x, y) = (I : xy)$.

**Example 3:** We will find the radical of $J = (x^3, x^2y) \subseteq k[x, y]$. But this is easy, using the same technique as in Example 1: $r(x^3, x^2y) = r((x^3) + (x^2y)) = r(r(x^3) + r(x^2y)) = r(r(x) + r(x^2) \cap r(y)) = r((x) + (xy)) = r(x) = (x)$ since $(x)$ is prime.

**Example 4:** We will find the annihilator of $(xy)$ in $k[x, y]/J$. This is the same as finding the ideal quotient $(J : xy)$ in $k[x, y]$. That is, all $f \in k[x, y]$

such that $fxy \in (x^3, x^2y)$. What must such an $f$ satisfy? First of all, it need not divide $y$, because for any $f$, we have $fxy \in (y)$. But $f$ must divide $x$, so $f$ is of the form $f = gx$, so $fxy = fx^2y \in (x^2, y) \subseteq J$. So $(x) \subseteq (J : xy)$. Since $(x)$ is maximal, we have an equality.

### 1.2 Various small-facts

If $x$ is nilpotent, then $1 + x$ is a unit. In the ring $A[x]$ the Jacobson radical equals the the nilradical. The set of prime ideals in $A$ has minimal elements with respect to inclusion[2].

## 2 Modules

Modules, finitely-generatedness, tensor products, exact sequences, flatness.

An $A$-**module** is an abelian group $M$ on which $A$ acts linearly. More precisely, it is a pair $(M, \mu)$, with $\mu : A \times M \to M$ a linear mapping in the obvious sense. It is crucial to remember that different $A$-modules may consist of the same abelian group $M$ but with different mappings $\mu$.

### 2.1 Various simple facts

An $A$-**module homomorphism** must satisfy $f(x + y) = f(x) + f(y)$ and $f(ax) = af(x)$. The set of $A$-module homomorphisms $M \to N$ has an obvious $A$-module structure. We denote it by $\mathrm{Hom}_A(M, N)$.

There is a natural isomorphism $\mathrm{Hom}(A, M) \cong M$. (by $f \mapsto f(1)$)

**Proposition 2.1.** *1) If $L \supseteq M \supseteq N$ are $A$-modules, then*

$$(L/N)/(M/N) \cong L/M$$

*2) If $M_1, M_2$ are submodules of $M$, then*

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$$

**Definition 2.2.** *An $A$-module is* ***faithful*** *if $Ann(M) = 0$. If $Ann(M) = \mathfrak{a}$, then $M$ is faithful as an $A/\mathfrak{a}$-module.*

**Definition 2.3.** *If $M = \sum_{i \in J} Ax_i$, the $x_i$ are said to be a* ***set of generators of*** *$M$. If $J$ is finite, then $M$ is* ***finitely-generated****.*

[2] The proof of this fact requires the choice axiom, but for Artinian rings, it follows by d.c.c.

**Definition 2.4.** *If $(M_i)_{i \in J}$ is any family of $A$-modules, their* ***direct sum*** *$\oplus_{i \in J} M_i$ consists of families $(x_i)_{i \in J}$ with almost all $x_i = 0$ (thus addition is well-defined within the direct sum). Dropping the restriction on the number of nonzero elements, we get the* ***direct product****.*

**Proposition 2.5.** *$M$ is a finitely-generated $A$-module $\Leftrightarrow$ $M$ is isomorphic to a quotient of $A^n$ for some integer $n > 0$. (or equivalently, there exists a surjection $\phi : A^n \to M$)*

**Proposition 2.6** (Nakayama's lemma)**.** *Let $M$ be a finitely generated $A$-module and $\mathfrak{a}$ an ideal of $A$ contained in the Jacobson radical of $A$. Then $\mathfrak{a}M = M$ implies $M = 0$.*

*Proof.* Suppose $M \neq 0$. And let $u_1, \dots, u_n$ be a set of generators of $M$. We may assume it is a minimal generating set. Then $u_n \in \mathfrak{a}M$, so $u_n = \sum_{i=1}^{n} a_i u_i$ for some $a_i \in \mathfrak{a}$. Hence

$$(1 - a_n)u_n = \sum_{i=1}^{n-1} a_i u_i$$

Since $a_n$ is contained in the Jacobson radical, $1 - a_n$ is a unit, and multiplying by its inverse on both sides of the equation tells us that $u_n$ may be expressed entirely in terms of the $u_i$ $(1 \leq i \leq n-1)$, contradicting our assumption that the $u_i$ $(1 \leq i \leq n)$ was a minimal generating set. $\square$

## 2.2 Exact sequences

Exact sequences allows to draw diagrams, assisting us in our constant struggle to understand morphisms between modules. But seriously:

**Definition 2.7.** *A sequence of $A$-modules and $A$-module homomorphisms*

$$\dots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \dots$$

*is* ***exact*** *if $Im(f_i) = Ker(f_{i+1})$ for each $i$.*

In particular

$$0 \longrightarrow M' \xrightarrow{f} M \text{ is exact} \Leftrightarrow \text{f is injective}$$

$$M \xrightarrow{g} M'' \longrightarrow 0 \text{ is exact} \Leftrightarrow \text{f is surjective}$$

.

**Proposition 2.8.** *The sequence*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

*is exact if and only if the sequence*

$$0 \longrightarrow Hom(M'', N) \xrightarrow{\bar{v}} Hom(M, N) \xrightarrow{\bar{u}} Hom(M', N)$$

*is exact for all A-modules N.*

**Proposition 2.9.** *The sequence*

$$0 \longrightarrow N' \xrightarrow{u} N \xrightarrow{v} N''$$

*is exact if and only if the sequence*

$$0 \longrightarrow Hom(M, N') \xrightarrow{\bar{u}} Hom(M, N) \xrightarrow{\bar{v}} Hom(M, N'')$$

*is exact for all A-modules M.*

We also have the famous *"Snake Lemma"*:

**Proposition 2.10.** *Given the commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'"] & N \arrow[r, "v'"] & N'' \arrow[r] & 0
\end{tikzcd}$$

*with the rows exact, there is an exact snake:*

$$0 \longrightarrow Ker(f') \longrightarrow Ker(f) \longrightarrow Ker(f'') \longrightarrow$$

$$Coker(f') \longrightarrow Coker(f) \longrightarrow Coker(f'') \longrightarrow 0$$

## 2.3 Tensor product of modules

Let $M, N, P$ be three $A$-modules. A mapping $f : M \times N \to P$ is $A$-bilinear if for each $x \in M$, the mapping $y \mapsto f(x, y)$ of $N$ into $P$ is $A$-linear, and similarly for each $y \in M$. The **tensor product** $M \otimes_A N$ of $M$ and $N$ has the following universal property:

**Definition 2.11.** *Let $M, N$ be $A$-modules. Let $g : M \times N \to M \otimes N$ be given by $(m, n) \mapsto m \otimes n$. (it is bilinear by a construction of the tensor product)*

*Given any $A$-module $P$ and any $A$-bilinear mapping $f : M \times N \to P$, there exists a unique $A$-bilinear mapping $f' : M \otimes N \to P$ such that $f = f' \circ g$.*

*Moreover, for any other $A$-module $T$ and homomorphism $g' : M \times N \to T$ satisfying these properties, there is a unique isomorphism $j : M \otimes N \to T$ such that $j \circ g = g'$.*

Graphically:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "g"] & P \\ M \otimes N \arrow[ur, "\exists! f'"'] & \end{tikzcd}$$

The tensor product may be constructed in various ways, but all its relevant properties follow from its universal property. For example, the bilinearity of $g$ follows from the construction of the tensor product in Atitah-MacDonald - however, because of the uniqueness property, every other construction will have this property.

We have

$$(x+x')\otimes y = x\otimes y + x'\otimes y, x\otimes(y+y') = x\otimes y + x\otimes y', (ax)\otimes y = x\otimes(ay) = a(x\otimes y)$$

We have canonical isomorphisms:

**Proposition 2.12.** *Let $M, N, P$ be $A$-modules. There exists unique isomorphisms*
*1) $M \otimes N \to N \otimes M$*
*2) $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$*
*3) $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$*
*4) $A \otimes M \to M$*

## 2.4 Exactness properties of the tensor product

**Proposition 2.13.** *We have a canonical isomorphism*

$$Hom(M \otimes N, P) \cong Hom(M, Hom(N, P))$$

*Proof.* Let $f : M \times N \to P$ be any $A$-bilinear mapping. For each $x \in M$, the mapping $y \mapsto f(x, y)$ is $A$-linear, hence we have a homomorphism $M \to \mathrm{Hom}(N, P)$ (sending $x$ to the mapping defined by $y \mapsto f(x, y)$). Conversely, any $A$-homomorphism $\phi : M \to \mathrm{Hom}(N, P)$ defines a $A$-bilinear map $M \times N \to P$, namely $(x, y) \mapsto \phi(x)(y)$. Hence the set $S$ of all bilinear mappings $M \times N \to P$ is in one-to-one correspondence with $\mathrm{Hom}(M, \mathrm{Hom}(N, P))$. On the other hand, $S$ is in one-to-one correspondence with $\mathrm{Hom}(M \otimes N, P)$ by the defining property of the tensor product. Hence the result. □

If we let $T(M) = M \otimes N$ and $U(P) = \mathrm{Hom}(N, P)$, the proposition takes the form $\mathrm{Hom}(T(M), P) = \mathrm{Hom}(M, U(P))$. In a language of abstract nonsense[3] this proposition tells us that the functor $T$ is a left adjoint of the functor $U$, and likewise $U$ is a right adjoint for $T$. (we leave it to the reader to check that $T, U$ really are functors)

This gives us the important result concerning exactness and tensor products:

**Proposition 2.14.** *Let*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

*be an exact sequence of $A$-modules, and let $N$ be any $A$-module. Then the sequence*

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \longrightarrow 0$$

*is exact.*

*Proof.* Repeated use of (2.9) and the bijection of the previous proposition. □

The functor $T_N : M \mapsto M \otimes_A N$ on the category of $A$-modules and homomorphisms is not in general exact, that is, tensoring with $N$ does not always take an exact sequence to an exact sequence. The previous proposition is surely nice to have, but it restricts to the case when $g$ is surjective.

**Definition 2.15.** *If $T_N$ is exact, then $N$ is said to be a* ***flat*** *$A$-module.*

**Example**: Consider the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$$

[3]There are of course many possible languages of abstract nonsense. We are of course talking about the language of category theory.

If we tensor with $\mathbb{Z}/2\mathbb{Z}$, we get the sequence

$$0 \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2 \otimes 1} \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$$

But $(f \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = 0$.

**Proposition 2.16.** *For an $A$-module $N$, TFAE:*
*1) $N$ is flat*
*2) If $E$ is an exact sequence of $A$-modules, then $E \otimes N$ is exact.*
*3) If $f : M \to M'$ is injective, then $f \otimes 1 : M \otimes N \to M' \otimes N$ is injective.*

**Proposition 2.17.** *If $f : A \to B$ is a ring homomorphism and $M$ is a flat $A$-module, then $B \otimes_A M$ is a flat $B$-module.*

*Proof.* $(B \otimes_A M) \otimes_B N \cong M \otimes_A (N \otimes_B B) \cong M \otimes_A N$. □

## 2.5 Various smallfacts

If $m, n$ are coprime, then $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$. If $A$ is a ring, $\mathfrak{a}$ an ideal and $M$ an $A$-module, then $(A/\mathfrak{a}) \otimes_A M \cong M/\mathfrak{a}M$. If $(M_i)_{i \in J}$ is any family of $A$-modules, then $\oplus_{i \in J} M_i$ flat $\Leftrightarrow$ each $M_i$ is flat. $M[x] \cong A[x] \otimes_A M$. If $M, N$ are flat $A$-modules, then so is $M \otimes_A N$. If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of $A$-modules, and $M', M''$ are finitely generated, then so is $M$.

## 2.6 Direct limits

We will outline a construction for direct limits and state their universal property.

**Definition 2.18.** *A partially ordered set $I$ is said to be a* ***directed set*** *if for each pair $i, j \in I$ there exists a $k \in I$ such that $i \leq k$ and $j \leq k$.*

This roughly states that the partial order don't "seriously split" (in the graphical sense of the word). Imagine yourself walking a path with a friend, and suddenly the path splits. You and your friend choose different branches of the path. However, if the path is directed, this means that if you continue forward, you will meet again after some (finite?) time.

**Definition 2.19.** *Let $A$ be a ring, $I$ be a directed set, and let $(M_i)_{i \in I}$ be a family of $A$-modules index by $I$. For each pair with $i \leq j$, let $\mu_{ij} : M_i \to M_j$ be an $A$-module homomorphism. We demand the following:*
*1) $\mu_{ii} = id_{M_i}$ for all $i \in I$.*

*2)* $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ *whenever* $i \leq j \leq k$*. The modules* $M_i$ *and the homomorphisms* $\mu_{ij}$ *are said to form a* ***direct system*** $\boldsymbol{M} = (M_i, \mu_{ij})$ *over the directed set* $I$*.*

Condition 2) tells us that the following diagram commutes:

$$\begin{tikzcd} M_i \arrow[d, "\mu_{ij}"'] \arrow[dr, "\mu_{ik}"] & \\ M_j \arrow[r, "\mu_{jk}"'] & M_k \end{tikzcd}$$

We shall construct an $A$-module $M$ called the **direct limit** of the direct system $\boldsymbol{M}$. Let $C$ be the direct sum of the $M_i$. Its elements are formal sums $\Sigma x_i$ with $x_i \in M_i$ and $x_i = 0$ for almost all $i$. Let $D$ be the submodule of $C$ generated by all elements of the form $x_i - \mu_{ij}(x_i)$ where $i \leq j$ and $x_i \in M_i$. Now, let $M = C/D$ and let $\mu : C \to M$ be the projection, and let $\mu_i$ be the restriction of $\mu$ to $M_i$. The module $M$ and the family of homomorphisms $\mu_i : M_i \to M$ is the direct limit of the direct system $\boldsymbol{M}$. We write $M = \varinjlim M_i$, the homomorphisms being understood. It is clear from the construction that we have $\mu_i = \mu_j \circ \mu_{ij}$ whenever $i \leq j$. That is, the following diagram commutes:

$$\begin{tikzcd} M_i \arrow[r, "\mu_{ij}"] \arrow[d, "\mu_i"'] & M_j \arrow[dl, "\mu_j"] \\ \varinjlim M_i & \end{tikzcd}$$

**Proposition 2.20.** *Every element of* $\varinjlim M_i$ *can be written in the form* $\mu_i(x_i)$ *for some* $i \in I$ *and some* $x_i \in M_i$*.*

*Proof.* We consider $C$, the direct sum of the $M_i$. Let $x \in C$. Now, $x$ is a finite sum of $x_i$ with $x_i \in M_i$. We have $x_i \equiv \mu_{ij}(x_i) \pmod D$ for all $j \geq i$. Since this a finite sum and $I$ is a directed set, there exists a $k$ such that $k \geq i$ for all $i$ in the sum. Then $x = \Sigma x_i \equiv \Sigma \mu_{ik}(x_i)$. Again, using directedness, there exists an $l \geq k$, so (since all the $\mu_{ik}(x_i)$ are in $M_k$), $x \equiv \mu_{kl}(\Sigma \mu_{ik}(x_i))$. □

The direct limit is characterized up to isomorphism by the following universal property: Let $N$ be an $A$-module and for each $i \in I$ let $\alpha_i : M_i \to N$ be an $A$-module homomorphism such taht $\alpha_i = \alpha_j \circ \mu_{ij}$ whenever $i \leq j$. Then there exists a unique homomorphism $\alpha : \varinjlim M_i \to N$ such that $\alpha_i = \alpha \circ \mu_i$ for all $i \in I$. That is, for any other $A$-module making the above diagram commute, it must factor through $\varinjlim M_i$ (that is, $\varinjlim M_i$ is initial among all such objects in the category of $A$-modules. Of course, initial objects are unique up to isomorphism).

The previous proposition tells us that each $x \in \varinjlim M_i$ can be written in the form $\mu_i(x_i)$. Define $\alpha$ to be $x \mapsto \alpha_i \circ \mu_i(x_i)$.

$$\begin{tikzcd} M_i \arrow[r, "\mu_{ij}"] \arrow[d, "\mu_i"'] \arrow[dr, "\alpha_i"] & M_j \arrow[d, "\alpha_j"] \arrow[dl, "\mu_j"] \\ \varinjlim M_i \arrow[r, dotted, "\exists!\alpha"'] & N \end{tikzcd}$$

We have various small-facts which we will leave unproven (for now): tensor products commute with direct limits, that is $\varinjlim(M_i \otimes N) \cong (\varinjlim M_i) \otimes N$. $\varinjlim \mathfrak{R}_i$ is the nilradical of $\varinjlim A_i$.

# 3 Rings and modules of fractions

The formation of fractions let us "create units" from elements that are not zero-divisors. In $\mathbb{Q}$, we formally define $p/q$ to be all pairs of numbers $(p, q)$ with $q$ nonzero under the equivalence relation $(p, q) = (n, m)$ if and only if $pm - qn = 0$. However, that process is only of value if the underlying ring is an integral domain. However, it can be generalized.

**Definition 3.1.** *Let $A$ be any ring. A subset $S \subseteq A$ is* ***multiplicatively closed*** *if $1 \in S$ and $S$ is closed under multiplication.*

Let $S$ be any such multiplicatively closed set. We define a relation $\sim$ on $A \times S$ as follows:

$$(a, s) \sim (b, t) \Leftrightarrow (at - bs)u = 0 \text{ for some } u \in S$$

It is readily checked that this relation defines an equivalence relation. We now have fractions $a/s$ with addition and multiplication (well-)defined in the familiar way. We denote the resulting ring by $S^{-1}A$.

**Example:** Let $A = \mathbb{Z}$ and $S = \mathbb{Z} - \{0\}$. Then, of course, $S^{-1}A = \mathbb{Q}$ [4].

We have a ring homomorphism (the *fraction map*) $f : A \to S^{-1}A$ defined by $x \to x/1$. It is not in general injective. See example below.

[4]We could have used an $\cong$-sign instead here, but that really depends on how we define $\mathbb{Q}$ in the first place. If we think of $\mathbb{Q}$ just as some canonical set of fractions "out there", then of course we could only ever hope for an isomorphism, not an equality.

**Proposition 3.2.** *Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in $B$ for all $s \in S$. Then there is a unique homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.*

*Proof.* Uniqueness: Follows from

$$h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = h(f(s))^{-1} = g(s)^{-1}$$

Existence: Let $h(a/s) = g(a)g(s)^{-1}$. Well-definedness is easily checked. $\square$

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "f"'] & B \\ S^{-1}A \arrow[ur, "\exists! h"'] & \end{tikzcd}$$

The ring $S^{-1}A$ and the fraction map have the following properties:

1. $s \in S \Rightarrow f(s)$ is a unit in $S^{-1}A$.
2. $f(a) = 0 \Rightarrow as = 0$ for some $s \in S$.
3. Every element of $S^{-1}A$ is of the form $f(a)f(s)^{-1}$ for some $a \in A$ and some $s \in S$.

Conversely, for any other ring $B$ and homomorphism satisfying the above properties, there is a unique isomorphism $S^{-1}A \to B$.

**Example:** Let $\mathfrak{p}$ be a prime ideal of $A$. Then $S = A - \mathfrak{p}$ is multiplicatively closed. We write $A_\mathfrak{p}$ for $S^{-1}A$ in this case. The extension $f(\mathfrak{p})$ of $\mathfrak{p}$ in $A_\mathfrak{p}$ is an ideal $\mathfrak{m}$. It is easily seen that this ideal is maximal, and is the only maximal ideal in $A_\mathfrak{p}$. Hence $A_\mathfrak{p}$ is a local ring. The process of passing from $A$ to $A_\mathfrak{p}$ is called **localization at $\mathfrak{p}$**.

**Example:** $S^{-1}A = 0 \Leftrightarrow 0 \in S$. For any $f \in A$, we let $S = \{f^n\}_{n \geq 0}$. We write $A_f$ for $S^{-1}A$ ($f$ nilpotent $\Leftrightarrow A_f = 0$).

The construction of $S^{-1}A$ can be carried out with $A$ replaced by an $A$-module $M$ with the obvious replacements in the definitions. The same results apply. We get an $S^{-1}A$-module $S^{-1}M$.

**Proposition 3.3.** *$S^{-1}$ is a functor.*

*Proof.* Let $u : M \to N$ be an $A$-module homomorphism. It induces an obvious $S^{-1}A$-module homomorphism $S^{-1}u : S^{-1}M \to S^{-1}N$ defined by $m/s \mapsto u(m)/s$. It is easily verified that $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$. $\square$

$$\begin{tikzcd} M \arrow[d, "u"'] \arrow[dr, "u\circ v"] & & \mapsto & S^{-1}M \arrow[d, "S^{-1}u"'] \arrow[dr, "S^{-1}(v\circ u)"] & \\ N \arrow[r, "v"] & P & & S^{-1}N \arrow[r, "S^{-1}v"'] & S^{-1}P \end{tikzcd}$$

**Proposition 3.4.** *The functor $U_S : M \mapsto S^{-1}M$ is exact. (that is, it takes exact sequences to exact sequences)*

*Proof.* Easy. ☐

An easy consequence of this is the following results:

**Proposition 3.5.** *Let $N, P$ be submodules of an $A$-module $M$. Then*
*1) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$*
*2) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$*
*3) $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$.*

It turns out, once we know $S^{-1}A$, the ring of fractions, we also know any "module of fractions" $S^{-1}M$. Precisely,

**Proposition 3.6.** *Let $M$ be an $A$-module. There exists a unique isomorphism*

$$f : S^{-1}A\otimes_A \to S^{-1}M$$

*Proof.* Use the universal property of the tensor product. ☐

**Proposition 3.7.** *$S^{-1}A$ is a flat $A$-module.*

*Proof.* Let $N$ be any $A$-module. Then $S^{-1}A \otimes N \cong S^{-1}N$. The result follows from (3.4). ☐

**Proposition 3.8.** *Formation of fraction commutes with tensor product. Precisely, if $M, N$ are $A$-modules, then there exists a unique isomorphism*

$$f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$$

*such that*

$$(m/s) \otimes (n/t) \mapsto (m \otimes n)/st$$

## 3.1 Local properties

Localization can be viewed as "focusing attention at a point" (in a variety, points are represented by prime ideals). A property $P$ of a ring $A$ (or a module $M$) is said to be a local property if $A$ has $P \Leftrightarrow A_{\mathfrak{p}}$ has $P$ for each prime ideal $\mathfrak{p}$ of $A$.

We have various local properties:

**Proposition 3.9.** *Let $M$ be an $A$-module. Then the following are equivalent:*
*1) $M = 0$*
*2) $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$ of $A$.*
*3) $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of $A$.*

*Proof.* Clearly $1 \Rightarrow 2 \Rightarrow 3$. Assume 3) is satisfied, but $M \neq 0$. Let $x$ be any non-zero element of $M$. The ideal $\mathrm{Ann}(x) = \mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$. Consider $x/1 \in M_{\mathfrak{m}}$. Since $M_{\mathfrak{m}} = 0$, $x/1 = 0$, so there is an element $m \in A - \mathfrak{m}$ such that $xm = 0$, but this is impossible since $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. □

**Proposition 3.10.** *Let $\phi : M \to N$ be an $A$-module homomorphism. TFAE:*
*1) $\phi$ is injective.*
*2) $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for each prime ideal $\mathfrak{p}$.*
*3) $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for each maximal ideal $\mathfrak{m}$.*
*(the same holds for "injective" replaced by "surjective" throughout)*

*Proof.* Use the exactness of $S^{-1}$ and the previous proposition. □

Flatness is a local property:

**Proposition 3.11.** *For any $A$-module $M$, TFAE:*
*1) $M$ is a flat $A$-module.*
*2) $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module for each prime ideal $\mathfrak{p}$.*
*3) $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module for each maximal ideal $\mathfrak{m}$.*

*Proof.* Omitted. □

## 3.2 Extended and contracted ideals

Recall the definition of extended and contracted ideals.

**Definition 3.12.** *Let $f : A \to B$ be a ring homomorphism. If $\mathfrak{b}$ is an ideal in $B$, then the ideal $f^{-1}(\mathfrak{b})$ is the* ***contraction of $\mathfrak{b}$ in** $A$. If $\mathfrak{a}$ is an ideal in $A$, then the ideal* generated by $f(\mathfrak{a})$ *is the* ***extension of $\mathfrak{a}$ in** $B$.*

**Proposition 3.13.** *1) Every ideal in $S^{-1}A$ is an extended ideal.*
*2) If $\mathfrak{a}$ is an ideal in $A$, then the contraction of the extension of $\mathfrak{a}$ (denoted by $\mathfrak{a}^{ec}$) equals $\cup_{s\in S}(a : s)$. Hence the extension of $\mathfrak{a}$ in $S^{-1}A$ equals $S^{-1}A$ if and only if $\mathfrak{a}$ meets $S$.*
*3) The prime ideals of $S^{-1}A$ are in one-to-one correspondence $\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$ with the prime ideals of $A$ not meeting $S$. 4) The operation $S^{-1}$ commutes with formation of finite sums, products, intersection and radicals.*

*Proof.* 1) Let $\mathfrak{b}$ be an ideal in $S^{-1}A$, and let $x/s \in \mathfrak{b}$. Then $x/1 \in \mathfrak{b}$, hence $x \in \mathfrak{b}^c$, thus $x/s \in \mathfrak{b}^{ce}$. So $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$. The reverse inclusion is easy: $f \circ f^{-1}(\mathfrak{b}) \subseteq \mathfrak{b}$.
2) $x \in \mathfrak{a}^{ec} = (S^{-1}\mathfrak{a})^c \Leftrightarrow x/1 = a/s$ for some $a \in \mathfrak{a}, s \in S \Leftrightarrow (xs - a)t = 0$ for some $t \in S \Leftrightarrow xst \in \mathfrak{a} \Leftrightarrow x \in \cup_{s\in S}(\mathfrak{a} : s)$.
3) If $\mathfrak{q}$ is a prime ideal in $S^{-1}A$, then obviousle its contraction is a prime ideal in $A$. Conversely, let $S^{-1}\mathfrak{p}$ be the extension of a prime ideal of $A$ in $S^{-1}A$ and let $(r/1)(s/1) \in S^{-1}\mathfrak{p}$. Then $rs/1 = p/q$ for some $p \in \mathfrak{p}$ and $q \in S$. We must have $\mathfrak{p} \cap S = \varnothing$, or else the extension is (1). We have $(rsq - p)t = 0$ for some $t \in S$. That is $rsqt \in \mathfrak{p}$, so $rs \in \mathfrak{p}$ since $qt \notin \mathfrak{p}$. So, say, $r \in \mathfrak{p}$, so $r/1 \in S^{-1}\mathfrak{p}$.
4) This is basically taken care of earlier. □

**Proposition 3.14.** *If $\mathfrak{N}$ is the nilradical of $A$, the nilradical of $S^{-1}A$ is $S^{-1}\mathfrak{N}$.*

**Proposition 3.15.** *Let $M$ be a finitely generated $A$-module, $S$ a multiplicatively closed subset of $A$. Then $S^{-1}(Ann(M)) = Ann(S^{-1}M)$. (we view $S^{-1}M$ as an $S^{-1}A$-module)*

*Proof.* Assuming the conclusion is true for two $A$-modules $M, N$, it is true for $M + N$:

$$\begin{aligned} S^{-1}(\mathrm{Ann}(M+N)) &= S^{-1}(\mathrm{Ann}(M) \cap \mathrm{Ann}(N)) \\ &= S^{-1}(\mathrm{Ann}(M)) \cap S^{-1}(\mathrm{Ann}(N)) \\ &= \mathrm{Ann}(S^{-1}M) \cap \mathrm{Ann}(S^{-1}N) \text{ by hypothesis} \\ &= \mathrm{Ann}(S^{-1}M + S^{-1}N) = \mathrm{Ann}(S^{-1}(M+N)) \end{aligned}$$

Hence it is enough to prove the proposition for $M$ generated by a single element $x$. Consider the sequence below:

$$0 \longrightarrow \mathrm{Ann}(M) \longrightarrow A \xrightarrow{\cdot x} M \longrightarrow 0$$

The sequence is obviously exact, so $M \cong A/\mathrm{Ann}(M)$. So

$$S^{-1}M \cong (S^{-1}A)/(S^{-1}\mathrm{Ann}(m)),$$

so $\mathrm{Ann}(S^{-1}M) = S^{-1}(\mathrm{Ann}(M))$. $\square$

### 3.3 Various small-facts

Let $S$ be a multiplicatively closed subset of $A$ and let $M$ be a finitely generated $A$-module. Then $S^{-1}M =$ if and only if there exists $s \in S$ such that $sM = 0$.

Let $\mathfrak{a}$ be an ideal in $A$ and let $S = 1 + \mathfrak{a}$. Then $S^{-1}\mathfrak{a}$ is contained in the Jacobson radical of $S^{-1}A$.

Let $T$ be another multiplicatively closed subset of $A$. And let $U$ be the image of $T$ in $S^{-1}A$. Then $(ST)^{-1}A \cong U^{-1}(S^{-1}A)$.

If $A_\mathfrak{p}$ has no nonzero nilpotent element for each prime $\mathfrak{p}$, then $A$ has no nonzero nilpotent elements either.

Example: If each $A_\mathfrak{p}$ is an integral domain, then $A$ is not necessarily an integral domain. Let $A = \mathbb{Z}/(6)$ and let $\mathfrak{p}_1 = (2)$ and $\mathfrak{p}_2 = (3)$. Then $A_{\mathfrak{p}_1} \cong \mathbb{Z}/(2)$ and $A_{\mathfrak{p}_2} \cong \mathbb{Z}/(3)$, and both are integral domains.

## 4 Primary decomposition

In some rings, it is possible to decompose an ideal into an intersection of "primary" ideals. The process is rather technical, however.

**Definition 4.1.** *An ideal $\mathfrak{q}$ in a ring $A$ is* ***primary*** *if $\mathfrak{q} \neq A$ and if $xy \in \mathfrak{q} \Rightarrow x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$. Or equivalently, $\mathfrak{q}$ is primary if and only if $A/\mathfrak{q} \neq 0$ and every zero-divisor in $A/\mathfrak{q}$ is nilpotent.*

Every prime ideal is primary. Also, the contraction of a primary ideal is primary.

**Proposition 4.2.** *Let $\mathfrak{q}$ be a primary ideal in a ring $A$. Then $r(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.*

*Proof.* It is enough to show that $r(\mathfrak{q})$ is prime. $\square$

If $\mathfrak{q}$ is a primary ideal, and $r(\mathfrak{q}) = \mathfrak{p}$ then $\mathfrak{q}$ is said to be $\mathfrak{p}$-primary.

**Proposition 4.3.** *If $r(\mathfrak{a})$ is maximal, then $\mathfrak{a}$ is primary. The powers of a maximal ideal $\mathfrak{m}$ are $\mathfrak{m}$-primary.*

**Proposition 4.4.** *If $\mathfrak{q}_i$ $(1 \leq i \leq n)$ are $\mathfrak{p}$-primary, then their intersection $\cap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary.*

**Proposition 4.5.** *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, $x \in A$. Then*
*1) $x \in \mathfrak{q} \Rightarrow (\mathfrak{q} : x) = (1)$*
*2) $x \notin \mathfrak{q} \Rightarrow (\mathfrak{q} : x)$ is $\mathfrak{p}$-primary, and therefore $r(\mathfrak{q} : x) = \mathfrak{p}$.*
*3) $x \notin \mathfrak{p} \Rightarrow (\mathfrak{q} : x) = \mathfrak{q}$.*

**Definition 4.6.** *A* ***primary decomposition*** *of an ideal $\mathfrak{a}$ in $A$ is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals $\mathfrak{q}_i$, that is, such that*

$$\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$$

*If moreover all the $r(\mathfrak{q}_i)$ are distinct and we have $\mathfrak{q}_j \not\supseteq \cap_{j \neq i} \mathfrak{q}_i$ $(1 \leq j \leq n)$, the composition is* ***minimal****. By* (4.4) *the first condition is achievable, so any primary decomposition may be reduced to a minimal one. If $\mathfrak{a}$ has a primary decomposition, then $\mathfrak{a}$ is* ***decomposable****.*

**Proposition 4.7** (1st uniqueness theorem)**.** *Let*

$$\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$$

*be a minimal decomposition of an ideal $\mathfrak{a} \subseteq A$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then the $\mathfrak{p}_i$ are precisely the set of prime ideals of the form $r(a : x)$ $(x \in A)$, and hence are independent of the decomposition.*

*Proof.* We have $(\mathfrak{a} : x) = (\cap \mathfrak{q}_i : x) = \cap(\mathfrak{q}_i : x)$, hence $r(\mathfrak{a} : x) = \cap_{i=1}^n r(\mathfrak{q}_i : x) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$, by the previous proposition. If $r(\mathfrak{a} : x)$ is prime, then $r(\mathfrak{a} : x) = \mathfrak{p}_j$ for some $j$. Hence every prime ideal of the form $r(\mathfrak{a} : x)$ is one of the $\mathfrak{p}_j$. Conversely, since the decomposition is minimal, there is an $i$ with $x_i \notin \mathfrak{q}_i$ and $x_i \in \cap_{j \neq i} \mathfrak{q}_j$. And by the previous proposition, $r(\mathfrak{a} : x_i) = \mathfrak{p}_i$. $\square$

The prime ideals $\mathfrak{p}_i$ above are said to **belong** to $\mathfrak{a}$, or to be **associated** with $\mathfrak{a}$. The minimal elements of the $\mathfrak{p}_i$ are called the **minimal** or **isolated** prime ideals belonging to $\mathfrak{a}$. The others are **embedded**.

**Proposition 4.8.** *Let $\mathfrak{a}$ be decomposable. The any prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ contains a minimal prime ideal belong to $\mathfrak{a}$.*

**Proposition 4.9.** *If $\mathfrak{a}, \mathfrak{q}_i, \mathfrak{p}_i$ are as before, then*

$$\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A | (\mathfrak{a} : x) \neq \mathfrak{a}\}$$

*In particular, if the zero ideal is decomposable, then the set of zero-divisors of $A$ is the union of the prime ideals belonging to $0$.*

**Proposition 4.10.** *Let $S \subseteq A$ be multiplicatively closed, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.*
*1) $S \cap \mathfrak{p} \neq \varnothing \Rightarrow S^{-1}\mathfrak{q} = S^{-1}A$.*
*2) If $S \cap \mathfrak{p} = \varnothing$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and its contraction is $\mathfrak{q}$.*

*Proof.* Easy. □

We denote the contraction of $S^{-1}\mathfrak{a}$ by $S(\mathfrak{a})$:

**Proposition 4.11.** *Let $S$ be multiplicatively closed and let $\mathfrak{a}$ be decomposable. Let $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$, and suppose the $\mathfrak{q}_i$ are numbered so that $S$ meets $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$, but not the rest of the $\mathfrak{p}_i$. Then*

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i \quad S(\mathfrak{a}) = \textstyle\bigcap_{i=1}^{m} \mathfrak{q}_i$$

**Definition 4.12.** *A set $\Sigma$ of prime ideals belonging to $\mathfrak{a}$ is said to be **iso-lated** if $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ and $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.*

**Proposition 4.13** (2nd uniqueness theorem)**.** *Let $\mathfrak{a}$ be a decomposable ideal. Let $\mathfrak{a} = \cap i = 1^n \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$ and let $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}$ be an isolated set of prime ideals of $\mathfrak{a}$. Then $\mathfrak{q}_{i_1} \cap \ldots \cap \mathfrak{q}_{i_m}$ is independent of the decomposition.*

*Proof.* Let $S = A - \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$. We have

$$\mathfrak{p}' \in \Sigma \Rightarrow \mathfrak{p}' \cap S = \varnothing$$

$$\mathfrak{p}' \notin \Sigma \Rightarrow \mathfrak{p}' \nsubseteq \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \Rightarrow \mathfrak{p}' \cap S \neq \varnothing$$

The result follows form (4.11) and the independency of the $\mathfrak{p}_i$. □

## 4.1 Various small-facts and examples

If $\mathfrak{a} = r(\mathfrak{a})$, then $\mathfrak{a}$ has no embedded prime ideals. In $\mathbb{Z}[t]$, the ideal $\mathfrak{m} = (2, t)$ is maximal and the ideal $\mathfrak{q} = 4, t)$ is $\mathfrak{m}$-primary, but is not a power of $\mathfrak{m}$.

**Example 1:** It is easily checked that $(x) \cap (y) \cap (x^2, y^2)$ is a primary decomposition of $(x^2y, y^2x)$. Since $r(x^2, y^2) = (x, y)$, and $(x) \subset (x, y)$, the isolated prime ideals are $(x), (y)$ and $(x, y)$ is an embedded prime ideal.

**Example 2:** Let $J = (x^3, x^2y)$. Assuming that $J$ is decomposable, we want to find its minimal prime ideal. From Example 4 in Section 1 and from Proposition (4.7), we know that $(x)$ is one of the associated prime ideals. From Example 3 in Section 1, we know also that $r(J) = (x)$, so $(x)$ must be minimal.

**Example 3:** Continouing, we want to show that $(x, y)$ is an embedded prime ideal of $J$ in $k[x, y]$. From Proposition (4.7), it is enough to find an element $f \in k[x, y]$ such that $(J : f) = (x, y)$ (certainly $(x, y)$ is a prime ideal). It is straightforward to verify that $(J : x^2) = (x, y)$.

# 5 Integral dependence

Considering $\mathbb{R}$ as a subring of $\mathbb{C}$, we know that the element $i \in \mathbb{C}$ satisfies a polynomial equation $(i)^2 + 1 = 0$. We say that $i$ is integral over $\mathbb{R}$. More generally:

**Definition 5.1.** *Let $B$ be a ring, $A$ a subring such that $1 \in A$. An element $x \in B$ is said to be integral over $A$ if $x$ is a root in a monic polynomial with coefficients in $A$. That is, if there exists $a_i$ such that*

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

Example: Let $B = k(x)$ (that is, the ring of rational functions), and $A = k[x]$. Clearly, $A \subseteq B$ and $A$ may be considered a subring of $B$. Assume $f \in B$ is integral over $A$. $f$ is on the form $f = g/h$ (we may, as usual, assume $g$ and $h$ have no common factor). That is, we have an equation

$$(g/h)^n + k_1(g/h)^{n-1} + \ldots + k_n = 0$$

Multiplying by $h^n$ on both sides, we get

$$g^n + k_1 h g^{n-1} + \ldots + k^n h^n = 0$$

So $h$ divides $g^n$, contrary to assumption, so $h = \pm 1$, so $f \in A$. This shows that no element strictly inside $k(x)$ is integral over $k[x]$.

**Proposition 5.2.** *TFAE:*
*1) $x \in B$ is integral over $A$*
*2) $A[x]$ is a finitely generated $A$-module.*
*3) $A[x]$ is contained in a subring $C$ of $B$ such that $C$ is a finitely-generated $A$-module.*
*4) There exists a faithful $A[x]$-module $M$ which is finitely generated as an $A$-module.*

*Proof.* $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4$ are easy. □

**Proposition 5.3.** *Let $x_i (1 \leq i \leq n)$ be elements of $B$, each integral over $A$. Then $A[x_1, \ldots, x_n]$ is a finitely-generated $A$-module.*

*Proof.* By induction on $n$. □

**Proposition 5.4.** *The set $C$ of elements of $B$ which are integral over $A$ is a subring of $B$ containing $A$.*

The ring $C$ is called the **integral closure** of $A$ in $B$[5]. If $C = A$ then $A$ is **integrally closed** in $B$. If $C = B$, the ring $B$ is said to be **integral over A**.

**Proposition 5.5.** *Let $A \subseteq B \subseteq C$ be rings and let $B$ be integral over $A$ and $C$ integral over $B$. Then $C$ is integral over $A$.*

**Proposition 5.6.** *Let $A \subseteq B$ be rings and let $C$ be the integral closure of $A$ in $B$. Then $C$ is integrally closed in $B$.*

**Proposition 5.7.** *Let $A \subseteq B$ be rings. $B$ integral over $A$.*
*1) If $\mathfrak{b}$ is an ideal of $B$ and $\mathfrak{a} = \mathfrak{b}^c = A \cap \mathfrak{b}$, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.*
*2) If $S$ is a multiplicatively closed subset of $A$, then $S^{-1}B$ is integral over $S^{-1}A$.*

## 5.1 Going-up

**Proposition 5.8.** *Let $A \subseteq B$ be integral domains, $B$ integral over $A$. Then $B$ is a field if and only if $A$ is a field.*

*Proof.* Doing tricks with the integral dependence polynomial. □

[5] The example in the beginning showed that the integral closure of $k[x]$ in $k(x)$ is $k[x]$ itself.

**Proposition 5.9.** *Let $A \subseteq B$ be rings, $B$ integral over $A$. Let $\mathfrak{q}$ be a prime ideal of $B$ and let $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

*Proof.* $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. $\square$

Contraction is "injective":

**Proposition 5.10.** *Let $A \subseteq B$ be rings, $B$ integral over $A$. Let $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of $B$ such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q} \cap A = \mathfrak{q}'A = \mathfrak{p}$. Then $\mathfrak{q} = \mathfrak{q}'$.*

*Proof.* $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Let $\mathfrak{m}$ be the extension of $\mathfrak{p}$ in $A_\mathfrak{p}$, and let $n, n'$ be the extensions of $\mathfrak{q}, \mathfrak{q}'$ respectively. Since $\mathfrak{m}$ is maximal, it follows from the previous proposition that both $n, n'$ are maximal, hence $n = n'$. Hence $\mathfrak{q} = \mathfrak{q}'$. $\square$

**Proposition 5.11.** *Let $A \subseteq B$ be rings. $B$ integral over $A$. Let $\mathfrak{p}$ be a prime ideal of $A$. Then there exists a prime ideal $\mathfrak{q} \subseteq B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ ($\mathfrak{p}$ is the contraction of $\mathfrak{q}$ in $A$).*

$$\begin{tikzcd}
A \arrow[r, hook] & B \\
\mathfrak{p} \arrow[u, hook] \arrow[r, hook, dotted, "\exists"] & \mathfrak{q} \arrow[u, hook, dotted, "\exists"']
\end{tikzcd}$$

*Proof.* Consider the commutaive diagram (in which the horizontal arrows are injections):

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\
A_\mathfrak{p} \arrow[r] & B_\mathfrak{p}
\end{tikzcd}$$

Now, let $n$ be the maximal ideal of $B_\mathfrak{p}$. Then its contraction in $A_\mathfrak{p}$ is maximal since $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. The rest follows from the commutativity of the diagram. $\square$

This gives us the "Going-up"-theorem:

**Proposition 5.12.** *Let $A \subseteq B$ be rings. $B$ integral over $A$. Let $\mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_n$ be a chain of prime ideals of $A$ and $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$ ($m < n$) a chain of prime ideals in $B$ such that for $i$, $\mathfrak{p}_i$ is the contraction of $\mathfrak{q}_i$. Then the chain*

$\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$ *may be extended to a longer chain* $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_n$ *such that* $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ *for all* $i$*.*

$$\begin{tikzcd}
\mathfrak{p}_1 \arrow[r] \arrow[d] & \ldots \arrow[r] \arrow[d] & \mathfrak{p}_m \arrow[r] \arrow[d] & \mathfrak{p}_{m+1} \arrow[r] \arrow[d, dotted] & \ldots \arrow[r] & \mathfrak{p}_n \arrow[d, dotted] \\
\mathfrak{q}_1 \arrow[r] & \ldots \arrow[r] & \mathfrak{q}_m \arrow[r, dotted] & \mathfrak{q}_{m+1} \arrow[r, dotted] & \ldots \arrow[r] & \mathfrak{q}_n
\end{tikzcd}$$

*Proof.* Go to $A/\mathfrak{p}_1$. □

## 5.2 Going-down

**Proposition 5.13.** *Let* $A \subseteq B$ *be rings,* $C$ *the integral closure of* $A$ *in* $B$*. Let* $S \subseteq A$ *be multiplicatively closed. Then* $S^{-1}C$ *is the integral closure of* $S^{-1}A$ *in* $S^{-1}B$*.*

*Proof.* ... □

An integral domain is said to be **integrally closed** if it is integrally closed in its field of fractions. Our example in the beginning showed that $k[x]$ was integrally closed. Likewise, $\mathbb{Z}$ is integrally closed. By the same method, every unique factorization domain is integrally closed.

Integral closure is a local property:

**Proposition 5.14.** *Let* $A$ *be an integral domain. TFAE:*
*1)* $A$ *is integrally closed.*
*2)* $A_{\mathfrak{p}}$ *is integrally closed for each prime ideal* $\mathfrak{p}$*.*
*3)* $A_{\mathfrak{m}}$ *is integrally closed for each maximal ideal* $\mathfrak{m}$*.*

*Proof.* Let $K$ be the field of fractions of $A$ and $C$ the integral closure of $A$ in $K$ and let $f : A \to C$ be the inclusion mapping. Then $A$ integrally closed $\Leftrightarrow$ $f$ is surjective. By (5.13), $f_{\mathfrak{p}}$ surjective $\Leftrightarrow$ $A_{\mathfrak{p}}$ is integrally closed. The claim follows from (3.10). □

As usual, let $A \subseteq B$ be rings. Let $\mathfrak{a}$ be an ideal of $\mathfrak{a}$. An element of $B$ is said to be **integral over** $\mathfrak{a}$ if it satisfies an equation of integral dependence in which all the coefficients lie in $\mathfrak{a}$. The **integral closure** of $\mathfrak{a}$ in $B$ is the set of all such elements.

**Proposition 5.15.** *Let* $C$ *be the integral closure of* $A$ *in* $B$ *and let* $\mathfrak{a}^e$ *be the extension of* $\mathfrak{a}$ *in* $C$*. The the integral closure of* $\mathfrak{a}$ *in* $B$ *is the radical of* $\mathfrak{a}^e$*.*

*Proof.* If $x \in B$ is integral over $\mathfrak{a}$, we have an equation

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

with $a_i \in \mathfrak{a}$. Then $x \in C$ and $x^n \in \mathfrak{a}^e$, or $x \in r(\mathfrak{a}^e)$. Conversely, if $x \in r(ia^e)$, then $x^n = \sum a_i x_i$ for some $n$ where $a_i \in \mathfrak{a}$ and $x_i \in C$. Then $M = A[x_1, \ldots, x_n]$ is a finitely generated $A$-module with $x^n M \subseteq \mathfrak{a} M$. The claim follows from the Cayley-Hamilton-theorem. $\square$

**Proposition 5.16.** *$A \subseteq B$ integral domains. $A$ integrally closed. Let $x \in B$ be integral over an ideal $\mathfrak{a}$ of $A$. Then $x$ is algebraic over the field of fractions $K$ of $A$, and the coefficients of its minimal polynomial in $K$ all lies in $r(\mathfrak{a})$.*

*Proof.* Clearly $x$ is algebraic over $K$. Let $L$ be an extension field of $K$ containing all the conjugates $x_i$ of $x$. Each $x_i$ satisfies the same equation of integral dependence as $x$, so they are all integral over $\mathfrak{a}$. The coefficients of the minimal polynomial of $x$ over $K$ are linear combinations of the $x_i$, and since the integral closure of $A$ is closed under multiplication and addition (previous proposition, the radical is an ideal), the $x_i$ are integral over $\mathfrak{a}$. Again, by the previous proposition, they must all lie in $r(\mathfrak{a})$. $\square$

**Proposition 5.17** ("Going down")**.** *Let $A \subseteq B$ be integral domains, $A$ integrally closed, $B$ integral over $A$. Let $\mathfrak{p}_1 \supseteq \ldots \mathfrak{p}_n$ be a chain of prime ideals of $A$, and let $\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_m$ $(m < n)$ be a chain of prime ideals of $B$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ $(1 \leq i \leq m)$. Then the chain $\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_m$ may be extended to a chain $\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i (1 \leq i \leq n)$.*

*Proof.* Omitted for now. It is a conundrum of polynomial equations, contractions and fraction rings. $\square$

### 5.3 Various

Let $A$ be a subring of $B$ such that $B$ is integral over $A$, and let $f : A \to \Omega$ be a homomorphism of $A$ into an algebraically closed field $\Omega$. Then $f$ can be extended to a homomorphism of $B$ into $\Omega$.

If $A$ is a subring of $B$ and $B - A$ is closed under multiplication, then $A$ is integrally closed in $B$.

**Example 1:** Consider $A = \mathbb{C}[x, y]/(y^2 - x^5)$. We want to find the field of fractions $K(A)$ of $A$. Since every second power of $y$ vanishes, $A$ has the form $A = \mathbb{C}[x] + \mathbb{C}[x]y$ under the relation $y^2 = x^5$. Now, what does a fraction in $K(A)$ look like? It is enough to find all fractions of the form $1/h$, where $h \in A$. $h$ is of the form $h = f + gy$ for some $f, g \in \mathbb{C}[x]$. So

$$\frac{1}{h} = \frac{1}{f+gy} = \frac{f-gh}{f^2-g^2y^2} = \frac{f-gy}{f^2-g^2x^5} = H + Gy$$

where $H, G$ are rational function of $x$. Thus the field of fractions looks like

$$K(A) = \mathbb{C}(x)[y]/(y^2 - x^5)$$

**Example 2:** Let $A, B$ be integral domains, $A$ a subring of $B$. Assume their field of fractions are equal to, say, $K$. Assume also that $B$ is integrally closed and that $B$ is integral over $A$. We will show that $B$ is the integral closure of $A$.

*Proof.* Let $x \in K$ with $x$ integral over $A$. Then $x$ is also integral over $B$ (since $A$ is a subring of $B$). But $B$ is integrally closed, so $x \in B$. That is, the integral closure of $A$ lies inside B.
On the other hand, assume $x \in B$. Then $x$ is integral over $A$. $\square$

**Example 3:** Let $A = k[x, y, z]/(xy^2 - z^2)$. Assume that $A$ is an integral domain. We will find its field of fractions and its integral closure. To find the field of fractions, are allowed to divide by $A - \{0\}$. However, let us first localize in $(y)$. That is, we are allowed to divide by $y$. Then our ring $A_y$ looks like (here $S = \{0, y, y^2, \ldots\}$)

$$A_y = k[x, y, z, \frac{1}{y}]/(xy^2 - z^2) = k[x, y, z, \frac{1}{y}]/(x - \frac{z^2}{y^2}) = k[y, z, \frac{1}{y}] = k[y, \frac{z}{y}]x$$

Allowing ourselves to divide by everything but zero, we may change our brackets into parantheses, so

$$K(A) = k(\frac{z}{y}, y)$$

Now, let $B = A_y = k[y, \frac{z}{y}]$. $A$ is naturally a subring of $B$ (since $A, B$ are integral domains and $B$ is $A_y$). Since $B$ is a polynomial ring, it is integrally closed. The equation $(\frac{z}{y}) - x = 0$ in $A$ implies that $B$ is integral over $A$. It follows from Example 2 that $B$ is the integral closure of $A$.

## 6 Chain conditions

We now arrive at the socalled Noetherian and Artinian properties. They are fundamental to the whole of algebra.

Throughout, let $\Sigma$ denote some specified partially ordered set.

**Proposition 6.1.** *TFAE:*
*1) Every increasing sequence $(x_i)$ in $\Sigma$ is stationary.*
*2) Every non-empty subset of $\Sigma$ has a maximal element.*

If $\Sigma$ is the set of submodules of a module $M$, ordered by $\subseteq$, then 1) is called the **ascending chain condition** (usually a.c.c.). A module satisfying a.c.c. is said to be **Noetherian**. If, however, $\Sigma$ is ordered by $\supseteq$, then 1) is the **descending chain condition** (usually d.c.c.). A module satisfying d.c.c. is **Artinian**.

**Examples:** Anything finite satisfies both d.c.c. and a.c.c. The ring $\mathbb{Z}$ satisfies a.c.c but not d.c.c. The same applies to $k[x]$ on ideals. The polynomial ring $k[x_1, x_2, \ldots]$ satisfies neither chain condition.

Noetherian modules are more important than Artian modules:

**Proposition 6.2.** *$M$ is a Noetherian $A$-module $\Leftrightarrow$ every submodule of $M$ is finitely generated.*

*Proof.* $\Rightarrow$ Let $N$ be a submodule of $M$ and let $\Sigma$ be the set of all finitely generated submodules of $N$. Since $M$ is Noetherian, $\Sigma$ has a maximal element $L$. Choose $x \in N$, $x \notin L$ and consider $L + Ax$. This is finitely generated and strictly contains $L$, so $N = L$.
$\Leftarrow$ Consider $M_1 \subseteq M_2 \subseteq \ldots$. □

**Proposition 6.3.** *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of $A$-modules. Then*
*1) $M$ is Noetherian $\Leftrightarrow$ $M'$ and $M''$ are Noetherian.*
*2) $M$ is Artinian $\Leftrightarrow$ $M'$ and $M''$ are Artinian.*

**Proposition 6.4.** *If $M_i (1 \leq i \leq n)$ are Noetherian/Artinian $A$-modules, so is $\oplus_{i=1}^{n} M_i$.*

*Proof.* Induction on

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0$$

□

A ring $A$ is said to be **Noetherian/Artinian** if it satisfies a.c.c/d.c.c. on ideals. Any field is both Noetherian and Artinian. Any prinicipal ideal domain is Noetherian.

**Proposition 6.5.** *Let $A$ be a Noetherian/Artinian ring, $M$ a finitely generated $A$-module. Then $M$ is Noetherian/Artinian.*

*Proof.* Use (2.5), (6.3),(6.4). $\square$

**Proposition 6.6.** *Let $A$ be a Noetherian/Artinian ring, $\mathfrak{a}$ an ideal of $A$. Then $A/\mathfrak{a}$ is Noetherian/Artinian.*

A chain of submodules of a module $M$ is a sequence $(M_i)$ $(0 \leq i \leq n)$ of submodules of $M$ such that

$$M = M_0 \supset M_1 \supset \ldots \supset M_n = 0 \text{ strict inclusions}$$

The **length** of the chain is $n$, that is, the number of $\supset$-symbols. A **composition series** of $M$ is a maximal chain, that is a chain in which no extra submodules can be inserted. Equivalently, a chain in which each quotient $M_{i-1}/M_i$ is simple.

The length of a composition series is an invariant:

**Proposition 6.7.** *Suppose that $M$ has a composition series of length $n$. Then every composition series of $M$ has length $n$, and every chain in $M$ can be extended to a composition series.*

**Proposition 6.8.** *$M$ has a composition series $\Leftrightarrow$ $M$ satisfies both a.c.c and d.c.c.*

*Proof.* $\Rightarrow$: Obvious.
$\Leftarrow$: Let $M = M_0$. Since $M$ is Noetherian, it has a maximal submodule $M_1$, and so on. The chain stops because $M$ is Artinian. $\square$

We call a module satisfying both a.c.c and d.c.c a module of **finite length**. We denote the length of $M$ by $l(M)$.

**Proposition 6.9.** *The length $l(M)$ is an additive function on the class of $A$-modules of finite length. That is, if*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

*is an exact sequence, then $l(M) = l(M') + l(M'')$.*

When our module is a $k$-vector space, we have the following proposition:

**Proposition 6.10.** *For $k$-vector spaces $V$, TFAE:*
*1) finite dimension*
*2) finite length*
*3) a.c.c*
*4) d.c.c.*
*Moreover, if any of the above conditions are satisfied, then length = dimension.*

*Proof.* $1 \Rightarrow 2$, $2 \Rightarrow 3$, and $2 \Rightarrow 4$ are easy. We prove $3 \Rightarrow 1$. The implication $4 \Rightarrow 1$ is similar.

Assume 1) is false. That is, the dimension is infite. Then there exists an infinite sequence $(x_n)_{n>1}$ of linearly independent elements of $V$. Let $U_n$ be the vector space spanned by $x_1, \dots, x_n$. Then the sequence $(U_n)$ is infinite and strictly ascending. □

**Proposition 6.11.** *Let $A$ be a ring in which the zero ideal is a product $\mathfrak{m}_1 \dots \mathfrak{m}_n$ of maximal ideals. Then $A$ is Noetherian if and only if $A$ is Artinian.*

# 7 Noetherian Rings

We restate the little we so far know about Noetherian rings:

**Proposition 7.1.** *For a Noetherian ring $A$, the following are equivalent:*
*1) Every non-empty set of ideals in $A$ has a maximal element.*
*2) Every ascending chain of ideals in $A$ is stationary.*
*3) Every ideal in $A$ is finitely generated.*

**Proposition 7.2.** *If $A$ is Noetherian and $\phi : A \to B$ is a surjective homomorphism, then $B$ is Noetherian.*

*Proof.* This is just restating (6.6). □

**Proposition 7.3.** *Let $A$ be a subring of $B$. Assume $A$ is Noetherian and $B$ finitely-generated $A$-module. Then $B$ is Noetherian as a ring.*

**Proposition 7.4.** *If $A$ is Noetherian and $S$ is a multiplicatively closed subset of $A$, then $S^{-1}A$ is Noetherian.*

*Proof.* The ideals in $S^{-1}A$ are in 1-1 correspondence with the contracted ideals of $A$. □

**Example:** The above proposition tells us that $\mathbb{Q}$ and $k(x)$ are Noetherian. The next famous theorem is a generalization of the fact that any polynomial ring over a field is Noetherian:

**Proposition 7.5** (Hilbert's basis theorem)**.** *If $A$ is Noetherian, then the polynomial ring $A[x]$ is Noetherian.*

*Proof.* Let $\mathfrak{a}$ be an ideal in $A[x]$. Let $I$ be the set of leading coefficients of elements of $\mathfrak{a}$. It is an ideal in $A$. Since $A$ is Noetherian, $I$ is finitely-generated by, say, $a_i(1 \leq i \leq n)$. Each $a_i$ has a representative $f_i$ of degree $r_i$ in $\mathfrak{a}$. Let $r = \max\{r_i\}$. The $f_i$ generate an ideal $\mathfrak{a}'$ in $A[x]$, it is clear that $\mathfrak{a}' \subseteq \mathfrak{a}$.

Let $f \in \mathfrak{a}$. Then $f = ax^m +$ lower terms with $a \in I$. If $m \geq r$, write $a = \sum a_i u_i$, with $u_i \in A$. Then $f - \sum u_i f_i x^{m-r_i}$ is a polynomial in $\mathfrak{a}$ of degree $< m$. Continuing this way, we can write $f$ as $f = g + h$ with $h \in \mathfrak{a}'$ and $g$ of degree $< r$.

Let $M$ be the $A$-module generated by $x, x^2, \ldots, x^{r-1}$. What we just showed was that $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$. But $M$ was finitely-generated $A$-module, so $M$ is Noetherian. $\mathfrak{a} \cap M$ is a submodule of a Noetherian module $M$, so is finitely-generated. Since $\mathfrak{a}'$ is finitely-generated, so is $\mathfrak{a}$. $\square$

**Proposition 7.6.** *Let $B$ be a finitely-generated $A$-algebra. If $A$ is Noetherian, then so is $B$.*

**Proposition 7.7.** *Let $A \subseteq B \subseteq C$ be rings. Let $A$ be Noetherian. Let $C$ be a finitely-generated $A$-algebra, and let $C$ satisfy either of the following equivalent conditions:*
*1) finitely generated $B$-module*
*2) integral over $B$*
*Then $B$ is finitely generated as an $A$-algebra.*

*Proof.* $\varnothing$ for now. $\square$

**Proposition 7.8.** *Let $k$ be a field, $E$ a finite-generated $k$-algebra. If $E$ is a field, then it is a finite algebraic extension of $k$.*

## 7.1 Primary decomposition in Noetherian rings

We say that an ideal $\mathfrak{a}$ is **irreducible** if

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow (\mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c})$$

In other words, if it cannot be written as an intersection two distinct ideals. However:

**Proposition 7.9.** *In a Noetherian ring $A$ every ideal is a finite intersection of irreducible ideals.*

*Proof.* Assume the claim is false. Let $\Sigma$ be the set of ideals which are not a finite intersection of irreducible ideals. Since $A$ is Noetherian, $\Sigma$ has a maximal element $\mathfrak{a}$. It is reducible, so $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{b} \supset \mathfrak{a}$ and $\mathfrak{c} \supset \mathfrak{a}$. But since $\mathfrak{a}$ was maximal, $\mathfrak{b}, \mathfrak{c}$ are both a finite intersection of irreducible ideals, hence so is $A$. Contradiction. $\square$

**Proposition 7.10.** *In $A$ Noetherian ring every irreducible ideal is primary.*

*Proof.* Let $\mathfrak{a}$ ba an irreducible ideal in $A$ and let $xy \in \mathfrak{a}$ with $y \notin \mathfrak{a}$. Consider the chain of ideals $(\mathfrak{a} : x) \subseteq (ia : x^2) \subseteq \ldots$. By a.c.c., this chain is stationary, so we have $(\mathfrak{a} : x^n) = (\mathfrak{a} : x^{n+1})$ for some $n$.

Now, if $a \in (y)$, then $ax \in \mathfrak{a}$. And if $a \in (x^n)$, then $a = bx^n$ for some $b$, hence $bx^{n+1} \in \mathfrak{a}$. That is $b \in (\mathfrak{a} : x^{n+1}) = (\mathfrak{a} : x^n)$. So $bx^n \in \mathfrak{a}$, that is, $a \in \mathfrak{a}$. It follows that $(x^n) \cap (y) = \mathfrak{a}$. Since $\mathfrak{a}$ was chosen to be irreducible, and $y \notin \mathfrak{a}$, it follows that $x^n \in \mathfrak{a}$.

Thus $\mathfrak{a}$ is primary. $\square$

Thus every ideal in a Noetherian ring admits a primary decomposition, which we schizophrenically repeat below:

**Proposition 7.11.** *In a Noetherian ring every ideal has a primary decomposition.*

**Proposition 7.12.** *In a Noetherian ring $A$, every ideal contains a power of its radical.*

*Proof.* Let $x_1, \ldots, x_k$ generate $r(\mathfrak{a})$ with $x_i^{n_i} \in \mathfrak{a}(1 \leq i \leq k)$. Let $m = (\sum_{i=1}^k n_i) - k + 1$. Then $r(\mathfrak{a})^m$ is generated by the products $x_1^{r_1} \cdots x_k^{r_k}$ with $\sum_{i=1}^k r_i = m$. Claim: We must have $r_i \leq n_i$ for at least one $i$. Assume the contrary, i.e. that $r_i < n_i$ for all $i$. Then $\sum_{n=1}^k (r_i - n_i) \leq -k$, so $1-k \leq -k$, that is, $1 \leq 2k$, which is impossible. So each such product lies in $\mathfrak{a}$, and therefore $r(\mathfrak{a})^m \subseteq \mathfrak{a}$. $\square$

Which gives us the following very important result:

**Proposition 7.13.** *Let $A$ be a Noetherian ring, $\mathfrak{m}$ a maximal ideal of $A$, $\mathfrak{q}$ any ideal of $A$. TFAE:*
*1) $\mathfrak{q}$ is $\mathfrak{m}$-primary.*
*2) $r(\mathfrak{q}) = \mathfrak{m}$.*
*3) $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some $n > 0$.*

*Proof.* $1 \Rightarrow 2$ By definition.
$2 \Rightarrow 1$ By (4.3).
$2 \Rightarrow 3$ By (7.12).
$3 \Rightarrow 2$ By taking radicals. $\mathfrak{m} = r(\mathfrak{m}^n) \subseteq r(\mathfrak{q}) \subseteq r(\mathfrak{m}) = \mathfrak{m}$. □

**Proposition 7.14.** *Let $\mathfrak{a} \neq (1)$ be an ideal in a Noetherian ring $A$. Then the prime ideals belonging to $\mathfrak{a}$ are precisely the prime ideals occuring in the set of ideals $\{(\mathfrak{a} : x)\}_{x \in A}$.*

# 8 Artin rings

Recall that an Artin (or Artinian if you want to use more letters) is a ring satisfying d.c.c on ideals. Artin rings are very well-behaved - almost too much so.

**Proposition 8.1.** *In an Artin ring every prime ideal is maximal.*

*Proof.* Let $\mathfrak{p}$ be a prime ideal in an artin ring $A$. Then $A/\mathfrak{p}$ is an Artinian integral domain. Let $x \in A/\mathfrak{p}$ be nonzero. By d.c.c. we have $(x^n) = (x^{n+1})$ for some $n$. Hence $x^n = yx^{n+1}$ for some $y \in A/\mathfrak{p}$. Since we live in an integral domain, we may cancel $x^n$ on both sides, giving us $1 = xy$, hence $x$ has an inverse, hence $A/\mathfrak{p}$ is a field, hence $\mathfrak{p}$ is maximal. □

Thus the nilradical is equal the Jacobson radical in an Artin ring.

**Proposition 8.2.** *An Artin ring has only a finite number of maximal ideals.*

*Proof.* Let $\Sigma$ be the set of finite intersections $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r$ where the $\mathfrak{m}_i$ are maximal ideals. By d.c.c., $\Sigma$ has a minimal element $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$, say. Let $\mathfrak{m}$ be any maximal ideal. We have $\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ from the minimality of $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$. Thus $\mathfrak{m} \supseteq \mathfrak{m}_i$ for some $i$, thus $\mathfrak{m} = \mathfrak{m}_i$. That is, $\mathfrak{m}$ was one of the finitely many $\mathfrak{m}_i (1 \leq i \leq n)$. □

**Proposition 8.3.** *In an Artin ring the nilradical is nilpotent.*

*Proof.* Exercise for now! □

**Definition 8.4.** *A* ***chain*** *of prime ideals is a strictly increasing sequence*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$$

*The* ***length*** *of the chain is $n$. The* ***dimension*** *of $A$ is to be the supremum of all lengths of all chains of prime ideals in $A$. It is an integer $\leq 0$ or $+\infty$.*

A field has dimension 0 ((0) is the only prime ideal). $\mathbb{Z}$ has dimension 1.

**Proposition 8.5.** *A ring $A$ is Artin $\Leftrightarrow$ $A$ is Noetherian and* $\dim A = 0$.

*Proof.* $\Rightarrow$: By (8.1), $\dim A = 0$. Let $\mathfrak{m}_i$ be the distinc maximal ideals of $A$. Then $\Pi_{i=1}^n \mathfrak{m}_i^k \subseteq (\cap_{i=1}^n \mathfrak{m}_i)^k = \mathfrak{R}^k = 0$ for some $k$ (where $\mathfrak{R}$ denotes the nilradical). Hence by (6.11), $A$ is Noetherian.
$\Leftarrow$: The zero ideal is decomposable, so $A$ has only a finite number of minimal prime ideals, and they are all maximal since $\dim A = 0$. In a Noetherian ring, the nilradical is nilpotent, so we have $\mathfrak{R}^k = 0$ for some $k$. Also, $\mathfrak{R} = \cap_{i=1}^n \mathfrak{m}_i$ where $\mathfrak{m}_i$ are the maximal ideals in $A$. Hence $\Pi_{i=1}^n \mathfrak{m}_i^k = 0$. Hence $A$ is Artin. $\square$

**Proposition 8.6.** *If $A$ is an Artin local ring with maximal ideal $\mathfrak{m}$, then $\mathfrak{m}$ is the nilradical of $A$. Hence every element of $\mathfrak{m}$ is nilpotent and $\mathfrak{m}$ itself is nilpotent. Hence every element of $A$ is either a unit or nilpotent.*

**Example:** $\mathbb{Z}/(p^n)$.

**Proposition 8.7.** *Let $A$ be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal. Then exactly one of the following statements are true:*
*1)* $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$
*2)* $\mathfrak{m}^n = 0$ *for some $n$, in which case $A$ is an Artin local ring.*

*Proof.* Use Nakayama's lemma and take radicals. $\square$

**Proposition 8.8** (Structure theorem for Artin rings)**.** *An Artin ring $A$ is uniquely – up to isomorphism – a finite direct product of Artin local rings.*

*Proof.* Omitted. $\square$

**Proposition 8.9.** *Let $A$ be an Artin local ring. TFAE:*
*1) Every ideal in $A$ is principal.*
*2) The maximal ideal $\mathfrak{m}$ is principal.*
*3)* $\dim_k(m/m^2) \leq 1$

*Proof.* $1 \Rightarrow 2 \Rightarrow 3$ should be clear.
$3 \Rightarrow 1$: If $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$, then $\mathfrak{m} = \mathfrak{m}^2$, hence $\mathfrak{m} = 0$ by Nakayamas' lemma, and therefore $A$ is a field, and thus the only proper ideal in $A$ is the zero ideal which certainly is principal.

Now, assume $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$. Then $\mathfrak{m}$ is principalm, say $\mathfrak{m} = (x)$. Ket $\mathfrak{a}$ be any nontrivial ideal of $A$. Since $\mathfrak{m}$ is nilpotent, there exist an integer $r$ such that $\mathfrak{a} \subseteq \mathfrak{m}^r$ and $\mathfrak{a} \not\subseteq \mathfrak{m}^{r+1}$. There exists an $y \in \mathfrak{a}$ such that $y = ax^r$ but $y \notin (x^{r+1})$. Consequently, $a \notin (x)$, so $a$ is a unit in $A$. Hence $x^r \in \mathfrak{a}$, therefore $\mathfrak{m}^r = (x^r) \subseteq \mathfrak{a}$, hence $\mathfrak{a} = \mathfrak{m}^r = (x^r)$. So $\mathfrak{a}$ is principal. $\square$

# 9 Discrete Valuation Rings

More later?

For now we state only the definition of a discrete valuation ring:

**Definition 9.1.** *Let $K$ be a field. A* ***discrete valuation*** *on $K$ is a surjective mapping $v : K^\star \to \mathbb{Z}$ such that*
*1) $v(xy) = v(x) + v(y)$*
*2) $v(x+y) \geq \min(v(x), v(y))$*
*The set consisting of $0$ and all $x \in K^\star$ such that $v(x) \geq 0$ is a ring, called the* ***valuation ring*** *of $v$. It is a valuation ring of the field $K$.*

**Definition 9.2.** *An integral domain $A$ is a discrete valuation ring if there is a discrete valuation $v$ of its field of fractions $K$ such that $A$ is the valuation ring of $v$.*

**Example:** Let $K = \mathbb{Q}$. Let $p$ be a fixed prime. Then any nonzero $x \in \mathbb{Q}$ may be written uniquely as $p^a y$ where $a \in \mathbb{Z}$ and both numerator and denumerator of $y$ are prime to $p$. Define $v_p(x) = a$. The valuation ring of $v_p$ is the local ring $\mathbb{Z}_(p)$.

# 10 Completions

Given a ring it is possible to define a topology on it. This in turn let us talk about convergence in rings, which leads us to consider "completing" the ring such that every sequence converges. Many of the concepts developed in this chapter will only be tools in the next chapter about dimension theory.

## 10.1 Topologies and completions

Let $G$ be a topological abelian group. If $\{0\}$ is closed in $G$, then $G$ is Hausdorff. If $a \in G$, then $T_a(x) = x + a$ is a homeomorphism of $G$ onto itself, thus the topology of $G$ is uniquely determined by the neighbourhoods of $0$ in $G$.

**Proposition 10.1.** *Let $H$ be the intersection of all neighborhoods of $0$ in $G$. Then*
*1) $H$ is a subgroup.*
*2) $H$ is the closure of $\{0\}$.*
*3) $G/H$ is Hausdorff.*
*4) $G$ is Hausdorff $\Rightarrow H = 0$.*

For simplicity, let us assume that $G$ is first-countable - that is, 0 has a countable neighbourhood basis. Simplifying even further, we assume $G$ has a countable neighbourhood basis consisting of subgroups. That is, we have a sequence

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n \supseteq \ldots$$

and $U \subseteq G$ is a neighborhood of 0 if and only if it contains some $G_n$.

**Example:** The p-adic topology on $\mathbb{Z}$, in which $G_n = p^n\mathbb{Z}$. (this will make sense later on)

**Proposition 10.2.** *In our situation, the subgroups $G_n$ are both open and closed.*

*Proof.* For any $g \in G_n$, $g+G_n$ is a neighborhood of $g$, since $g+G_n \subseteq G_n$, this shows that $G_n$ is open. Therefore, for any $h$, $h+G_n$ is open, so $\cup_{h \notin G_n}(h+G_n)$ is open. This is the complement of $G_n$ in $G$, so $G_n$ is closed. $\square$

Hence we will do well not comparing this topology to the topology of the real numbers.

**Definition 10.3.** *A* ***Cauchy sequence*** *in $G$ is defined to be a sequence $(x_n)$ such that for any neighborhood $U$ of 0, there exists an integer $N$ such that $x_n - x - m \in U$ for all $n, m \geq N$.*

*Two Cauchy sequences $(x_n)$ and $(y_n)$ are* ***equivalent*** *if $x_n - y_n \to 0$ in $G$.*

We now construct the completion of $G$ with respect to a topology given by subgroups $G_n$. Suppose $(x_n)$ is a Cauchy sequence in $G$. Then the image of $x_n$ in $G/G_n$ is ultimately a constant, say $\xi_n$. Considering

$$G/G_{n+1} \xrightarrow{\theta_{n+1}} G/G_n$$

it is clear that $\xi_{n+1} \mapsto \xi_n$ under the projection $\theta_{n+1}$. Thus a Cauchy sequence $(x_n)$ defines a coherent sequence $(\xi_n)$ such that

$$\theta_{n+1}(\xi_{n+1}) = \xi_n \text{ for all } n$$

It should be clear that equivalent Cauchy sequences defines the same coherent sequence $(\xi_n)$. Also, given any coherent sequence, we can construct a Cauchy sequence definining it. The resulting abelian group of all coherent sequences is denoted by $\hat{G}$ and is called the **completion** of $G$ with respect to $G_n$.

Slightly more generally, let $\{A_n\}$ be any sequence of groups and homomorphisms

$$\theta_{n+1} : A_{n+1} \to A_n$$

We call this an **inverse system**, and the group of all coherent sequences $(a_n)$ ($a_n \in A_n$ and $\theta_{n+1}(a_{n+1}) = a_n$) is called the **inverse limit** of the system. We write $\varprojlim A_n$, the homomorphisms being understood.

With this notation, $\hat{G} \cong \varprojlim G/G_n$.

There is an obvious homomorphism $\phi : G \to \hat{G}$, namely, $x \mapsto (x)$, where $(x)$ is the constant sequence. $\phi$ is not in general injective, in fact $\mathrm{Ker}\phi = \cap U$, where $U$ runs through all neighborhoods of 0.

If $H$ is another topological group and $f : G \to H$ is a continous homomorphism, then $f$ sends Cauchy sequences to Cauchy sequences, and therefore $f$ induces a continous homomorphism $\hat{f} : \hat{G} \to \hat{H}$. The following diagram commutes:

$$\begin{tikzcd} \hat{G} \arrow[r, "\hat{f}"] \arrow[dr, "\widehat{g \circ f}"'] & \hat{H} \arrow[d, "\hat{g}"] \\ & K \end{tikzcd}$$

Notice that in the inverse system $\{G/G_n\}$, $\theta_{n+1}$ is always surjective. Such an inverse system is called a **surjective system**, or a *flasque* system. Suppose now we have inverse systems $\{A_n\}, \{B_n\}, \{C_n\}$ and homomorphisms such that the following diagram commutes for all $n$:

$$\begin{tikzcd} 0 \arrow[r] & A_{n+1} \arrow[r] \arrow[d] & B_{n+1} \arrow[r] \arrow[d] & C_{n+1} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & A_n \arrow[r] & B_n \arrow[r] & C_n \arrow[r] & 0 \end{tikzcd}$$

The diagram induces homomorphisms $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$, but this sequence is not always right-exact. However:

**Proposition 10.4.** *If* $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ *is an exact sequence of inverse system, then*

$$0 \longrightarrow \varprojlim A_n \longrightarrow \varprojlim B_n \longrightarrow \varprojlim C_n$$

*is exact. If* $\{A_n\}$ *is a surjective system, then the sequence is also right-exact.*

*Proof.* Let $A = \Pi_{n=1}^{\infty} A_n$ and define $d^A : A \to A$ by $d^A(a_n) = a_n - \theta_{n+1}(a_{n+1})$. Then $\mathrm{Ker} d^A \cong \varprojlim A_n$. Now, use the snake lemma. $\square$

**Proposition 10.5.** *Let $0 \to G' \to G'' \to 0$ be an exact sequence of groups. Let $G$ have the topology defined by a sequence $(G_n)$ of subgroups, and give $G'$ and $G''$ the induced topologies. Then*

$$0 \to \widehat{G'} \to \widehat{G} \to \widehat{G''} \to 0$$

*is exact.*

If $\phi : G \to \hat{G}$ is an isomorphism, then $G$ is complete. Note that the completion is complete.

Likewise, for an $A$-module $M$, let $G = M$ and $G_n = \mathfrak{a}^n M$ for an ideal $\mathfrak{a} \subseteq A$. This defines the $\mathfrak{a}$-topology on $M$, and the completion $\hat{M}$ is a topological $\hat{A}$-module.

**Example:** $A = k[x]$. Let $\mathfrak{a} = (x)$. Then $\hat{A} = k[[x]]$, the ring of formal power series.

## 10.2 Filtrations

An infinite chain $M = M_0 \supseteq M_1 \supseteq \dots$ where the $M_i$ are submodules of $M$ is called a **filtration** of $M$ and denoted by $(M_n)$. It is an **$\mathfrak{a}$-filtration** if $\mathfrak{a}M_n \subseteq M_{n+1}$, and a **stable** $\mathfrak{a}$-filtration if $\mathfrak{a}M_n = M_{n+1}$ for all sufficiently large $n$.

**Proposition 10.6.** *If $(M_n), (M'_n)$ are stable $\mathfrak{a}$-filtrations of $M$, then there is an integer $n_0$ such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for alle $n \leq 0$. Hence all stable $\mathfrak{a}$-filtrations determine the same topology on $M$.*

*Proof.* Because they are stable, it is enough to take $M'_n = \mathfrak{a}^n M$. Since $\mathfrak{a}M_n \subseteq M_{n+1}$ for all $n$, we have $\mathfrak{a}^n M \subseteq M_n$. Also $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$ say, implies $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subseteq \mathfrak{a}^n M = M'_n$. Now use symmetry. □

## 10.3 Graded rings and modules

The prototype of graded rings are polynomial rings.

**Definition 10.7.** *A **graded ring** is a ring $A$ together with countable family $(A_n)_{n \geq 0}$ of subgroups of the additive group $A$ such that $A = \oplus_{n=0}^{\infty} A_n$ and $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$. $A_0$ is a subring of $A$ and each $A_n$ is a $A_0$-module.*

**Definition 10.8.** ***A graded** $A$**-module** is a $A$-module $M$ together with a graded ring $A$ and a countable family of submodules $(M_n)_{n \geq 0}$ such that $M = \oplus_{n=0}^{\infty} M_n$ and $A_m M_n \subseteq M_{n+m}$. Each $M_n$ is an $A_0$-module. An element $x \in M$ is **homogeneous** if $x \in M_n$ for some $n$ (we call $n$ the **degree** of $x$).*

Any element $y \in M$ can be written as a finite sum of $y_n$ with $y_n \in M_n$. Each $y_n$ are called the **homogeneous components of** $y$.

A **homomorphism of graded $A$-modules** is an $A$-module homomorphism $f : M \to N$ such that $f(M_n) \subseteq N_n$ for all $n$.

If $A$ is a graded ring, we let $A_+ = \oplus_{n>0} A_n$. $A_n$ is an ideal of $A$.

**Proposition 10.9.** *Let $A$ be a graded ring. TFAE:*
*1) $A$ is Noetherian*
*2) $A_0$ is Noetherian and $A$ is finitely generated as an $A_0$-algebra.*

*Proof.* $2 \Rightarrow 1$ is just Hilbert's basis theorem. $A_0 \cong A/A_+$, so $A_0$ is Noetherian. [...] $\square$

If $A$ is a non-graded ring and $\mathfrak{a}$ is an ideal in $A$, then we can form the graded ring $A^\star = \oplus_{n=0}^{\infty} \mathfrak{a}^n$. Similarly, if $M$ is an $A$-module and $M_n$ is an $\mathfrak{a}$-filtration of $M$, then $M^\star = \oplus_n M_n$ is a graded $A^\star$-module.

If $A$ is Noetherian, $\mathfrak{a}$ is finitely generated by $x_1, \ldots, x_r$, so $A^\star = A[x_1, \ldots, x_r]$, and is also Noetherian again by Hilbert's basis theorem.

**Proposition 10.10.** *Let $A$ be a Noetherian ring, $M$ a finitely-generated $A$-module, $(M_n)$ an $\mathfrak{a}$-filtration of $M$. TFAE:*
*1) $M^\star$ is a finitely-generated $A^\star$-module.*
*2) The filtration $(M_n)$ is stable.*

**Proposition 10.11** (Artin-Rees lemma)**.** *Let $A$ be a Noetherian ring, $\mathfrak{a}$ an ideal of $A$, $M$ a finitely-generated $A$-module, $(M_n)$ a stable $\mathfrak{a}$-filtration of $M$. If $M'$ is a submodule of $M$, then $(M' \cap M_n)$ is a stable $\mathfrak{a}$-filtration of $M'$.*

*Proof.* We have $\mathfrak{a}(M' \cap M_n) \subseteq \mathfrak{a}M' \cap \mathfrak{a}M_n \subseteq M' \cap M_{n+1}$, hence $(M' \cap M_n)$ is an $\mathfrak{a}$-filtration. It defines a graded $A^\star$-module which is a submodule of $M^\star$, and is therefore finitely generated. Now use the previous proposition. $\square$

**Proposition 10.12.** *There exists an integer $k$ such that*

$$(\mathfrak{a}^n M) \cap M' = \mathfrak{a}^{n-k}((\mathfrak{a}^k M) \cap M')$$

**Proposition 10.13.** *Let $A$ be a Noetherian ring, $\mathfrak{a}$ an ideal, $M$ a finitely-generated $A$-module and $M'$ a submodule of $M$. Then the filtrations $\mathfrak{a}^n M'$ and $(\mathfrak{a}^n M) \cap M'$ have bounded difference. In particular, the $\mathfrak{a}$-topology on $M'$ coincides with the topology induced by the $\mathfrak{a}$-topology of $M$.*

It follows immediately by (10.5) that

**Proposition 10.14.** *Let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

*be an exact sequence of finitely-generated modules over a Noetherian ring $A$. Let $\mathfrak{a}$ be an ideal of $A$. Then the sequence of $\mathfrak{a}$-adic completions*

$$0 \longrightarrow \widehat{M'} \longrightarrow \widehat{M} \longrightarrow \widehat{M''} \longrightarrow 0$$

*is exact.*

We need a little observation:

**Proposition 10.15.** *$\mathfrak{a}$-adic completion commutes with finite direct sums.*

*Proof.* It is enough to consider the case $n = 2$. $x_n \oplus y_n$ give rise to a Cauchy sequence in $G_1 \oplus G_2$ if and only if $x_n, y_n$ give rise to Cauchy sequences in $G_1, G_2$ respectively. □

**Proposition 10.16.** *Let $A$ be any ring. $M$ a finitely-generated $A$-module. Then $\hat{A} \otimes_A M \to \hat{M}$ is surjective. If moreover $A$ is Noetherian, then $\hat{A} \otimes_A M \to \hat{M}$ is an isomorphism.*

*Proof.* If $F = A^n$, then $\hat{A} \otimes_A F \cong \hat{F}$. If $M$ is finitely generated, we have an exact sequence

$$0 \longrightarrow L \longrightarrow F \longrightarrow M \longrightarrow 0$$

And we have the following commutative diagram:

$$\begin{tikzcd}
 & \hat{A} \otimes_A N \arrow[r] \arrow[d, "\gamma"] & \hat{A} \otimes_A F \arrow[r] \arrow[d, "\beta"] & \hat{A} \otimes_A M \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & \hat{N} \arrow[r] & \hat{F} \arrow[r, "\delta"] & \hat{M} \arrow[r] & 0
\end{tikzcd}$$

The top line is exact by exactness properties tensor products. By (10.5), $\delta$ is surjective. $\beta$ is an isomorphism, so $\alpha$ is surjective, proving the first claim.

Assume now that $A$ is Noetherian. Then $\lambda$ is also surjective by what we just have proved. So the bottom line is exact. Chase the diagram a little, and the result pops out. □

Thus, in the language of abstract nonsense:

**Proposition 10.17.** *Let $A$ be Noetherian. The functor $M \mapsto \hat{A} \otimes_A M$ is exact on the category of finitely-generated $A$-modules.*

**Proposition 10.18.** *If $A$ is Noetherian, $\hat{A}$ its $\mathfrak{a}$-adic completion, then*
*1)* $\hat{\mathfrak{a}} := \hat{A}\mathfrak{a} \cong \hat{A} \otimes_A \mathfrak{a}$
*2)* $\widehat{(\mathfrak{a}^n)} = (\hat{\mathfrak{a}})^n$
*3)* $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$
*4)* $\hat{\mathfrak{a}}$ *is contained in the Jacobson radical of* $\hat{A}$*.*

**Proposition 10.19.** *Let $A$ be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal. Then the $\mathfrak{m}$-adic completion $\hat{A}$ of $A$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$.*

*Proof.* By (10.18), we have $\hat{A}/\hat{\mathfrak{m}} \cong A/\mathfrak{m}$, so $\hat{A}/\hat{\mathfrak{m}}$ is a field and $\hat{\mathfrak{m}}$ is a maximal ideal. From (10.18) no. 4, it follows that $\mathfrak{m}$ is the only maximal ideal of $\hat{A}$. $\square$

**Proposition 10.20** (Krulls' theorem)**.** *Let $A$ be a Noetherian ring, $\mathfrak{a}$ an ideal, $M$ a finitely-generated $A$-module and $\hat{M}$ the $\mathfrak{a}$-completion of $M$. Then the kernel $E = \cap_{n=1}^{\infty}\mathfrak{a}^n M$ of $M \to \hat{M}$ consists of those $x \in M$ annihilated by some element of $1 + \mathfrak{a}$.*

In particular, if $M = A$ and $A$ is an integral domain, the kernel is trivial.

**Proposition 10.21.** *If $A$ is Noetherian, $\mathfrak{a}$ an ideal of $A$ contained in the Jacobson radical of $A$ and $M$ a finitely-generated $A$-module, then the $\mathfrak{a}$-topology on $M$ is Hausdorff.*

A trivial corollary of the previous proposition is the following important observation:

**Proposition 10.22.** *Let $A$be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $M$ a finitely-generated $A$-module. Then the $\mathfrak{m}$-topology of $M$ is Hausdorff. In particular, the $\mathfrak{m}$-topology of $A$ is Hausdorff.*

## 10.4 The associated graded ring

Let $A$ be a ring and $\mathfrak{a}$ an ideal of $A$. Define

$$G_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}$$

where we define $\mathfrak{a}^0 = A$.

**Example:** Let $A = k[x]$ and $\mathfrak{a} = (x)$. Then

$$G_{(x)}(A) = A/(x) \oplus (x)/(x^2) \oplus (x^2/x^3) \oplus \dots$$

The first factor contains no elements of degree $\geq 1$. The second factor contains only elements of degree 1, and so on. Thus the associated graded ring can be seen as a way of "sorting" a ring into its "degrees" (whatever that's supposed to mean!). Multiplying $x^n$ with $x^m$ gives us a monomial $x^{n+m}$, which should lie in $(x^{n+m})/(x^{n+m+1})$. This rule of multiplication makes $G(A)$ a graded ring. We call $G(A)$ the **associated graded ring**.

Similarly, if $M$ is an $A$-module and $(M_n)$ is an $\mathfrak{a}$-filtration of $M$, we define

$$G(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$$

which is a graded $G(A)$-module. Let $G_n(M)$ denote $M_n/M_{n+1}$.

**Proposition 10.23.** *Let $A$ be a Noetherian ring, $\mathfrak{a}$ an ideal of $A$. Then*
*1) $G_{\mathfrak{a}}(A)$ is Noetherian.*
*2) $G_{\mathfrak{a}}(A)$ and $G_{\hat{\mathfrak{a}}}(\hat{A})$ are isomorphic as graded rings.*
*3) If $M$ is a finitely-generated $A$-module and $(M_n)$ is a stable $\mathfrak{a}$-filtration of $M$, then $G(M)$ is a finitely-generated graded $G_{\mathfrak{a}}$-module.*

*Proof.* 1) Since $A$ is Noetherian, $\mathfrak{a}$ is finitely generated by, say, $x_1, \ldots, x_n$. Let $\bar{x_1}, \ldots, \bar{x_n}$ be the images in $\mathfrak{a}/\mathfrak{a}^2$. Then $G(A) = (A/\mathfrak{a})[\bar{x_1}, \ldots, \bar{x_n}]$. Since $A/\mathfrak{a}$ is Noetherian, $G(A)$ is Noetherian by Hilbert's basis theorem.

2) From (10.18).

3) Since $(M_n)$ is a stable $\mathfrak{a}$-filtration of $M$ it must exists an $n_0$ such that $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ for all $r \geq 0$, hence $G(M)$ is generated by $\oplus_{n \neq n_0} G_n(M)$. Each $G_n(M)$ is Noetherian and annihilated by $\mathfrak{a}$, so they are finitely generated $A/\mathfrak{a}$-modules. Therefore $\oplus_{n \leq n_0} G_n(M)$ is generated by a finite number of elements, hence $G(M)$ is finitely generated. □

**Proposition 10.24.** *Let $\phi : A \to B$ be a homomorphism of filtered groups ($\phi(A_n) \subseteq B_n$), and let $G(\phi) : G(A) \to G(B)$, $\hat{\phi} : \hat{A} \to \hat{B}$ be the induced homomorphisms of the associated graded and completed groups. Then*
*1) $G(\phi)$ injective $\Rightarrow \hat{\phi}$ injective.*
*2) $G(\phi)$ surjective $\Rightarrow \hat{\phi}$ surjective.*

...

**Proposition 10.25.** *If $A$ is a Noetherian ring, $\mathfrak{a}$ an ideal of $A$, then the $\mathfrak{a}$-completion $\hat{A}$ of $A$ is Noetherian.*

# 11 Dimension theory

The goal of this chapter is to establish the Dimension Theorem, which tells us that three seemingly different notions of dimension actually are equal.

## 11.1 The Poincaré series

Let $A = \oplus_{n=0}^{\infty} A_n$ be a Noetherian graded ring. By (10.9) $A_0$ is a Noetherian ring and $A$ is generated as an $A_0$-algebra by some finite set $x_1, \ldots, x_s$, which we assume are homogenous of degrees $k_1, \ldots, k_s$, all positive, of course.

Let $M$ be a finitely-generated graded $A$-module. Then $M$ is generated by a finite number of homogeneous elements, say $m_1, \ldots, m_t$, of degrees $r_j = \deg m_j$. Every element of $M_n$ is of the form $\sum f_j m_j$ with $f_j \in A$ homogeneous of degree $n - r_j$. Thus each $M_n$ is finitely generated as an $A_0$-module.

Let $\lambda$ be an additive function with values in $\mathbb{Z}$ on the class of all finitely-generated $A_0$-modules. The Poincaré series of $M$ with respect to $\lambda$ is

$$P(M, t) = \sum_{n=0}^{\infty} \lambda(M_n) t^n \in \mathbb{Z}[[t]]$$

We have a famous theorem:

**Proposition 11.1** (Hilbert, Serre). *$P(M, t)$ is a rational function in $t$ of the form*

$$\frac{f(t)}{\prod_{i=1}^{s}(1 - t^{k_i})}$$

*where $f(t) \in \mathbb{Z}[t]$.*

*Proof.* We prove the theorem by induction on $s$, the number of generators of $A$ over $A_0$ (i.e. the number of generators of $A$ as an $A_0$-algebra, or as $A = A_0[x_1, \ldots, x_s]$).

Let $s = 0$. That means $A_n = 0$ for all $n > 0$. Since $M$ is finitely-generated, there is a generator of $M$ of largest degree $v$. Since every element of $A$ has degree 0, no element of $M$ can have degree greater than $v$. So $M_n = 0$ for all sufficiently large $n$. Hence $P(M, t)$ is a polynomial, and we're okay.

Assume the theorem is true for $s - 1$. Multiplication my $x_s$ is an $A$-module homomorphism of $M_n$ into $M_{n+k_s}$, hence gives rise to an exact sequence:

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0 \tag{1}$$

Let $K = \oplus_n K_n$ and $L = \oplus_n L_n$. These are both finitely generated (because we have an exact sequence with $M$ in the middle and $M$ is finitely generated) and both are annihilated by $x_s$, hence they are $A_0[x_1, \ldots, x_{s-1}]$ modules (which will allow us to use the inductive hypothesis). We apply $\lambda$ to the above exact sequence:

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0$$

We multiply by $t^{n+k_s}$ and sum with respect to $n$:

$$t^{k_s} P(K,t) - t^{k_s} P(M,t) + P(M,t) - g_1(t) - P(L,t) + g_2(t) = 0$$

where $g_1(t)$ and $g_2(t)$ are the "beginnings" of $P(M,t), P(L,t)$ respectively. Isolating $P(M,t)$ and applying the inductive hypothesis, we get

$$\begin{aligned} (1 - t^{k_s})P(M,t) &= P(L,t) - t^{k_s} P(K,t) + g(t) && (2) \\ &= \frac{f_1(t) - t^{k_s} f_2(t) + g(t) \prod_{i=1}^{s-1}(1 - t^{k_i})}{\prod_{i=1}^{s-1}(1 - t^{k_i})} && (3) \end{aligned}$$

which is just what we want. □

We shall denote the order of the pole at $t = 1$ by $d(M)$. We consider the case when all the generators of $A$ are of degree 1.

**Proposition 11.2.** *Let each $k_i = 1$. Then for all sufficiently large $n$, $\lambda(M_n)$ is a polynomial in $n$ of degree $d(M) - 1$.*

*Proof.* Let $d = d(M)$. By (11.1), we infer that $\lambda(M_n)$ equals the coefficient of $t^n$ in $f(t)(1-t)^{-s}$. Cancelling powers of $(1-t)$, we may assume $s = d$ and $f(1) \neq 0$. Suppose $f(t) = \sum_{n=1}^{N} a_k t^k$. Since

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k$$

(which can easily be proven by induction on $d$), we have

$$\lambda(M_n) = \sum_{k=0}^{N} a_k \binom{d+n-k-1}{d-1}$$

for all $n \geq N$. This is a polynomial of degree $d-1$ (this can easily by shown by induction on $d$). □

The polynomial $\lambda(M_n)$ is called the **Hilbert polynomial** of $M$ with respect to $\lambda$.

**Proposition 11.3.** *If $x \in A_k$ is not a zero-divisor in $M$ (that is $xm = 0 \Rightarrow m = 0$), then $d(M/xM) = d(M) - 1$.*

*Proof.* If $x$ is not a zero-divisor, then $K_n = 0$ in (1). Thus $P(K, t) = 0$. So from (2), we see that $P(L, t)$'s pole is of degree one less than the pole of $P(M, t)$. Since $L \cong M/xM$, the result follows. $\square$

## 11.2 The characteristic polynomial

The previus subsection dealt with the general situation in which $\lambda(M)$ was any additive function on finitely-generated $A$-modules. From now on, we will let $\lambda(M) = l(M)$ where $l(M)$ denotes the length of a finitely-generated $A_0$-module $M$. $A_0$ will also be Artinian.

**Example:** Let $A = k[x_1, \ldots, x_s]$. The $x_i$ are independent indeterminates. Any field $k$ is Artinian. Then $A_n$ is an $A_0$-module generated by the monomials $x_1^{m_1} \cdots x_s^{m_s}$ with $\sum m_i = n$. There are $\binom{s+n-1}{s-1}$ of these[6], hence $\lambda(A_n) = \binom{s+n-1}{s-1}$, hence $P(A, t) = (1-t)^{-s}$.

**Proposition 11.4.** *Let $A$ be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{q}$ an $\mathfrak{m}$-primary ideals, $M$ a finitely-generated $A$-module, $(M_n)$ a stable $\mathfrak{q}$-filtration of $M$. Then*
*1) $M/M_n$ is of finite length for all $n \geq 0$.*
*2) For all sufficiently large $n$, the length of $M/M_n$ is a polynomial $g(n)$ of degree $\leq s$, the least numbers of generators of $\mathfrak{q}$.*
*3) The degree and leading coefficient of $g(n)$ depend only on $M$ and $\mathfrak{q}$, not on the filtration.*

*Proof.* 1) Let $G(A) = \oplus_n \mathfrak{q}^n/\mathfrak{q}^{n+1}$, $G(M) = \oplus_n M_n/M_{n+1}$. Since every element of $G_0(A) = A/\mathfrak{q}$ is either nilpotent or a unit, the image of $\mathfrak{m}$ is the only ideal in $A/\mathfrak{q}$, so $\dim A/\mathfrak{q} = 0$, hence $G_0(A)$ is Artin. $G(A)$ is Noetherian and $G(M)$ is a finitely-generated $G(A)$-module by (10.23). Each $G_n(M) = M_n/M_{n+1}$ is a Noetherian $A/\mathfrak{q}$-module, and since $A/\mathfrak{q}$ is Artin, they are of finite length. In fact, since $l(M)$ is an additive function, we have

$$l(M/M_n) = \sum_{r=1}^{n} l(M_{r-1}/M_r)$$

[6] An induction argument should help you count this.

2) Since $A$ is Noetherian, $\mathfrak{q}$ is finitely-generated by, say, $x_i (1 \leq i \leq s)$. The images $\bar{x_i}$ in $\mathfrak{q}/\mathfrak{q}^2$ generate $G(A)$ as an $A/\mathfrak{q}$-algebra. Each $\bar{x_i}$ has degree 1. By (11.2) we have $l(M_n/M_{n+1}) = f(n)$ where $f(n)$ is a polynomial in $n$ of degree $\leq s-1$ for sufficiently large $n$. From our summation formula above, we have $l(M/M_{n+1}) - l(M/M_n) = f(n)$, hence $l_n$ is a polynomial of degree $\leq s$ for large enough values of $n$.

3) Let $(M'_n)$ be another stable $\mathfrak{q}$-filtration of $M$ and let $g'(n) = l(M/M'_n)$. The two filtrations have bounded difference,, that is, there exists some $n_0$ such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \geq 0$. Consequently, $g(n+n_0) \geq g'(n)$ and $g'(n+n_0) \geq g(n)$. Letting $n \to \infty$, we see that $g$ and $g'$ must have the same degree and leading coefficient. $\square$

The polynomial $g(n)$ corresponding to the filtration $(\mathfrak{q}^n M)$ is denoted by $\chi_{\mathfrak{q}}^M(n)$. We have $\chi_{\mathfrak{q}}^M(n) = l(M/\mathfrak{q}^n M)$ for large enough $n$. If $M = A$, we write $\chi_{\mathfrak{q}}(n)$. We call $\chi_{\mathfrak{q}}$ the **characteristic polynomial** of the $\mathfrak{m}$-primary ideal $\mathfrak{q}$. Thus

**Proposition 11.5.** *For large n, the length $l(A/\mathfrak{q}^n)$ is a polynomial $\chi_{\mathfrak{q}}(n)$ of degree $\leq s$ where $s$ is the least number of generators of $\mathfrak{q}$.*

**Proposition 11.6.** *Let $A, \mathfrak{m}, \mathfrak{q}$ be as above. Then*

$$\deg \chi_{\mathfrak{q}}(n) = \deg \chi_{\mathfrak{m}}(n)$$

*Proof.* Since $A$ is Noetherian and $\mathfrak{q}$ is $\mathfrak{m}$-primary, we have - for some natural number $r$ - that $\mathfrak{m} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^r$, hence $\mathfrak{m}^n \supseteq \mathfrak{q}^n \supseteq \mathfrak{m}^r n$. And therefore

$$\chi_{\mathfrak{m}}(n) \leq \chi_{\mathfrak{q}}(n) \leq \chi_{\mathfrak{m}}(rn)$$

Now, let $n \to \infty$. $\square$

Thus we have found an invariant, namely the common degree of the $\chi_{\mathfrak{q}}$. We denote this degree by $d(A)$. This choice of notation is not arbitrary. We have $d(A) = d(G_{\mathfrak{m}}(A))$ where $d(G_{\mathfrak{m}}(A))$ is the order of the pole of the Poincaré series of $A$.

## 11.3 Dimension theory of Noetherian local rings

Let $A$ be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal. Define $\delta(A)$ to be the least numbers of generators of an $\mathfrak{m}$-primary ideal of $A$. We can restate (11.6):

**Proposition 11.7.** $\delta(A) \geq d(A)$

**Proposition 11.8.** *Let $A, \mathfrak{m}, \mathfrak{q}$ as before. Let $M$ be a finitely-generated $A$-module, $x \in A$ a nonzerodivisor in $M$ and $M' = M/xM$. Then*

$$\deg \chi_{\mathfrak{q}}^{M'} \leq \deg_{\mathfrak{q}}^{M} - 1$$

*Proof.* Let $N = xM$. Then $N \cong M$ as $A$-modules. Let $N_n = N \cap \mathfrak{q}^n M$. We have exact sequences

$$0 \longrightarrow N/N_n \longrightarrow M/\mathfrak{q}^n M \longrightarrow M'/\mathfrak{q}^n M' \longrightarrow 0$$

Let $g(n) = l(N/N_n)$. Then

$$g(n) - \chi_{\mathfrak{q}}^{M}(n) + \chi_{\mathfrak{q}}^{M'}(n) = 0$$

for large $n$. The Artin-Rees lemma implies that $(N_n)$ is a stable $\mathfrak{q}$-filtration, so by (11.4), $g(n)$ and $\chi_{\mathfrak{q}}^{M}(n)$ have the same leading term. The result follows. $\square$

**Proposition 11.9.** *If $A$ is a Noetherian local ring, $x$ a non-zero-divisor in $A$, then $d(A/(x)) < d(A)$ (strictly less!).*

*Proof.* Let $M = A$. $\square$

**Proposition 11.10.** $d(A) \geq \dim A$

*Proof.* If $d = d(A) = 0$, then $l(M/M_n)$ is constant for some large $n$. Thus there exists $n$ such that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. Hence by Nakayama (since $A$ is local), we have $\mathfrak{m}^n = 0$. Thus, by (8.7), $A$ is Artin and $\dim A = 0$.

Assume $d > 0$ and assume the statement holds for all rings of dimension $< d$. Let $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \mathfrak{p}_r$ be a chain of prime ideals in $A$ (strict inclusions). Let $x \in \mathfrak{p}_1$ with $x \notin \mathfrak{p}_0$ and let $A' = A/\mathfrak{p}_0$ and let $x'$ be the image of $x$ in $A'$. Then $x' \neq 0$ and $A'$ is an integral domain, hence by (11.9), we have

$$d(A'/(x')) < d(A')$$

If $\mathfrak{m}'$ is the maximal ideal of $A'$, then $l(A/\mathfrak{m}^n) \geq l(A'/mm'^n)$, and therefore $d(A) \geq d(A')$. Therefore

$$d(A'/(x')) \leq d(A) - 1 = d - 1$$

By the inductive hypothesis, the length of any chain of prime ideals in $A'/(x')$ is $\leq d-1$. But the images of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in $A'/(x')$ form a chain of length $r-1$, hence $r - 1 \leq d - 1$, and consequently $r \leq d$. Hence $\dim A \leq d = d(A)$. $\square$

**Proposition 11.11.** *If $A$ is a Noetherian local ring,* $\dim A$ *is finite.*

**Definition 11.12.** *If $A$ is any ring, $\mathfrak{p}$ a prime ideal in $A$, then the **height** of $\mathfrak{p}$ is the supremum of lengths of chains of prime ideals $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r = \mathfrak{p}$ ending at $\mathfrak{p}$.*

Thus height$\mathfrak{p} = \dim A_{\mathfrak{p}}$.

**Proposition 11.13.** *Let $A$ be a Noetherian local ring of dimension $d$. Then there exists and $\mathfrak{m}$-primary ideal in $A$ generated by $d$ elements $x_1, \ldots, x_d$, and therefore* $\dim A \geq \delta(A)$.

*Proof.* We will construct generators $x_j$ such that every prime ideal containing $(x_1, \ldots, x_i)$ have height $\geq i$ for each $i$. Suppose $i > 0$ and that we already have constructed $x_1, \ldots, x_{i-1}$. Now, let

$$P = \{\mathfrak{p}_j |\text{ minimal prime ideals of } (x_1, \ldots, x_{s-1}) \text{ with height} = i - 1\}$$

This collection is finite but could be empty (note that since $A$ is Noetherian, every ideal has a decomposition). Since $i - 1 < d = \dim A = \text{height}\mathfrak{m}$, we have $\mathfrak{m} \neq \mathfrak{p}_j$ for each $j$ and therefore $\mathfrak{m} \neq \cup_{j=1}\mathfrak{p}_j$. Choose $x_i \in \mathfrak{m}$, $x_i \notin \cup\mathfrak{p}_j$. Let $\mathfrak{q}$ be any prime containing $(x_1, \ldots, x_i)$. Then $\mathfrak{q}$ contains some minimal prime ideal $\mathfrak{p}$ of $(x_1, \ldots, x_{i-1})$. If $\mathfrak{p} = \mathfrak{p}_j$ for some $j$, we have $x_i \in \mathfrak{q}$, $x_i \notin \mathfrak{p}$, hence $\mathfrak{q} \supset \mathfrak{p}$, and therefore height $\mathfrak{q} \geq i$. If $\mathfrak{p} \neq \mathfrak{p}_j$ for all $j$, then height $\mathfrak{p}$ is strictly greater than $i - 1$ (since $\mathfrak{p} \notin P$), so height $\mathfrak{p} \geq i$, hence height $\mathfrak{q} \geq i$. Thus every prime ideal containing $(x_1, \ldots, x_i)$ has height $\geq i$.

Now consider $(x_1, \ldots, x_d)$. If $\mathfrak{p}$ is a prime ideal belonging to this ideal, then $\mathfrak{p}$ has height $\geq d$, and so $\mathfrak{p} = \mathfrak{m}$. Hence $(x_1, \ldots, x_d)$ must be $\mathfrak{m}$-primary. $\square$

**Proposition 11.14** (Dimension theorem)**.** *For any Noetherian ring $A$ the following three integers are equal:*
*1) the maximum length of chains of prime ideals in $A$, i.e.* $\dim A$
*2) the degree of the characteristic polynomial, $\chi_{\mathfrak{m}}(n) = l(A/\mathfrak{m}^n)$, i.e. $\delta(A)$*
*3) the least number of generators of an $\mathfrak{m}$-primary ideal of $A$, i.e. $d(A)$.*

*Proof.* $\delta(A) \geq d(A) \geq \dim(A) \geq \delta(A)$ $\square$

**Example:** Let $R = \mathbb{C}[x, y]_{(x,y)}$ and $A = R/(x^2, xy)$ and let $\mathfrak{m}$ be the maximal ideal in $A$. We want to find $\chi_{\mathfrak{m}}(n)$. This is really an exercise in counting. We grade $A$ by the filtration $A_n = \mathfrak{m}^n A$. How many monomials are there of degree 1? Two, of course - namely $x, y,$. Thus 2 is the length of $\mathfrak{m}/\mathfrak{m}^2$. How many are there of degree 2? Only one! Poor $x^2, xy$ are killed.

Of degree 3 there is also only one, namely $y^3$. Generally, for $n > 1$, we have $l(A_n/A_{n+1}) = 1$. Thus $l(A/A_n) = 2 + 1 + 1 + \ldots + 1 = 2 + (n-1) = n + 1$ which is of degree 1, so $\dim A = 1$.