# NOTES FOR COMMUTATIVE ALGEBRA M5P55

AMBRUS PÁL

## 1. Rings and ideals

**Definition 1.1.** A quintuple $(A, +, \cdot, 0, 1)$ is a commutative ring with identity, if $A$ is a set, equipped with two binary operations; addition $+$ and multiplication $\cdot$, and two element $0, 1 \in A$ such that:

(1) the triple $(A, +, 0)$ is an abelian group,
(2) multiplication is associative:
$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$
commutative:
$$x \cdot y = y \cdot x$$
and distributive over addition:
$$x \cdot (y + z) = x \cdot y + x \cdot z,$$
(3) we have $x \cdot 1 = 1 \cdot x = x$.

It is rather usual to drop the dot from the notation when we write the product of elements, that is, to write $xy$ instead of $x \cdot y$. It is also a usual abuse of notation to let just the symbol $A$ denote this whole package.

*Remarks* 1.2. The identity element 1 is uniquely determined by its property in (3). We have $x \cdot 0 = 0$, and if $1 = 0$ in $A$, then $A$ has only one element. In this case we say that $A$ is the zero ring.

**Definition 1.3.** A ring homomorphism $f : A \to B$ is a mapping $f$ of a ring $A$ into a ring $B$ such that for all $x, y \in A$ we have:
$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y)$$
and $f(1) = 1$. The usual properties of ring homomorphisms can be proven from these assumptions. A subset $S$ of $A$ is a subring of $A$ if $S$ is an additive subgroup, closed under multiplication and contains $1 \in A$. In this case the inclusion map $f : S \to A$ is then a ring homomorphism.

*Remarks* 1.4. The composition of two homomorphisms is a homomorphism. An isomorphism between rings is a bijective homomorphism; this is the same condition as asking that the homomorphism has a inverse map which is also a homomorphism.

**Definition 1.5.** A subset $\mathfrak{a}$ of $A$ is an ideal of $A$ if $\mathfrak{a}$ is closed under addition and $A\mathfrak{a} = \mathfrak{a}A = \mathfrak{a}$. (Meaning that $ra \in \mathfrak{a}$ for every $r \in A$ and $a \in \mathfrak{a}$). Shorthand notation: $\mathfrak{a} \triangleleft A$. The quotient group $A/\mathfrak{a}$ is then a ring by the obvious multiplication:
$$(a + \mathfrak{a})(b + \mathfrak{a}) = (ab + \mathfrak{a}).$$

*Date*: March 23, 2017.

We call this ring the quotient ring $A/\mathfrak{a}$. The map $\pi : A \to A/a$ defined by $\pi(x) = x + \mathfrak{a}$ is a surjective ring homomorphism.

**Proposition 1.6.** *There is a bijective correspondence between the ideals $\mathfrak{b}$ containing $\mathfrak{a}$ and the ideals $\mathfrak{b}$ of $A/\mathfrak{a}$. Under this correspondence we get a bijection between prime ideals in $A$ containing $\mathfrak{a}$ and prime ideals in $A/\mathfrak{a}$.*

*Proof.* For every ideal $\mathfrak{b}$ containing $\mathfrak{a}$ let $\phi(\mathfrak{b}) = \{x + \mathfrak{a} | x \in \mathfrak{b}\}$; it is an ideal in $A/\mathfrak{a}$. For every ideal $\mathfrak{b}$ of $A/\mathfrak{a}$ let $\psi(\mathfrak{b}) = \{x \in A | x + \mathfrak{a} \in \mathfrak{b}\}$. This is an ideal of $A$ and contains $\mathfrak{a}$. If we can check that $\phi \circ \psi = id$ and $\psi \circ \phi = id$ then we are done. Let $\mathfrak{b}$ be an ideal of $A/\mathfrak{a}$. Then

$$\phi(\psi(\mathfrak{b})) = \{x + \mathfrak{a} | x \in \psi(b)\} = \{x + \mathfrak{a} | x \in \{x \in A | x + \mathfrak{a} \in \mathfrak{b}\}\},$$

which translates to saying that

$$\phi(\psi(\mathfrak{b})) = \{x + \mathfrak{a} | x + \mathfrak{a} \in \mathfrak{b}\}.$$

Therefore we get that $\phi(\psi(\mathfrak{b})) = \mathfrak{b}$. The other composition is similar. Since

$$A/\mathfrak{b} \cong (A/\mathfrak{a})/\phi(\mathfrak{a})$$

by the third isomorphism theorem, the second claim follows. □

**Definition 1.7.** If $f : A \to B$ is any ring homomorphism, the kernel of $f$ is the set of all $a \in A$ such that $f(a) = 0$. This is an ideal of $A$ and the image of $f$ is a subring of $B$, and $f$ induces a ring isomorphism:

$$A/\mathrm{Ker}(f) \cong \mathrm{Im}(f).$$

This is the first isomorphism theorem for rings. The notation $x \equiv y \mod \mathfrak{a}$ means that $x - y \in \mathfrak{a}$, and it was inspired by number theory, one of the progenitors of commutative algebra.

## 2. The most important example: polynomial rings

Let $R$ be a ring; we are going to introduce another ring $R[x]$, the polynomial ring in the variable $x$ with coefficients in $R$. As a set $R[x]$ can be described as formal sums:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i, \quad a_i \in R, m \in \mathbb{N},$$

where we consider two such sums

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \text{ and } b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \tag{2.0.1}$$

equal if $a_i = b_i$ $(\forall i = 0, 1, \ldots, \min(n, m))$, and $a_i = 0, b_i = 0$ $(\forall i > \min(n, m))$, if $a_i$ or $b_i$ is defined, respectively. In the ring $R$ the zero is 0, the unity element is 1, and we define the sum and product of the two elements listed in (2.0.1) above as:

$$\sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i \text{ and } \sum_{i=0}^{n+m} \left( \sum_{j+k=i} a_j b_k \right) x^i,$$

where $a_i = 0$, $b_i = 0$ for every index $i$ which is bigger than $n$, respectively $m$, by convention, and moreover $j, k$ are non-negative integers. More formally $R[x]$ is the set of functions:

$$\mathbb{N} \longrightarrow R, \quad i \mapsto a_i,$$

such that $a_i$ is zero for all but finitely many $i$. In this description $0 \in R[x]$ is the identically zero function, 1 is the function $0 \mapsto 1$, $i \mapsto 0$ for every other $i \in \mathbb{N}$, and addition and multiplication for two elements $i \mapsto a_i$, $i \mapsto b_i$ are defined as

$$i \mapsto a_i + b_i, \quad i \mapsto \sum_{j=0}^{i} a_i b_{j-i}.$$

**Proposition 2.1.** *The quintuple $(R[x], +, \cdot, 0, 1)$ is indeed a ring.*

This is easy check directly, but also follows from the principle of extension of identities (see Lemma 7.1, formulated using polynomials, just to make a vicious circle!)

**Definition 2.2.** We define the polynomial ring $R$ in the variables $x_1, x_2, \ldots, x_n$, denoted by $R[x_1, x_2, \ldots, x_n]$, as $R[x_1][x_2] \cdots [x_n]$. Its elements have the usual description as sums over multi-indexes:

$$R[x_1, x_2, \ldots, x_n] = \{ \sum_{i_1, i_2, \ldots, i_n} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} | a_{i_1 i_2 \ldots i_n} \in R, \text{ the sum is finite} \}.$$

## 3. Zero-divisors, nilpotent elements, units

**Definition 3.1.** A zero-divisor in a ring $A$ is an element $x$ such that there exists a nonzero element $y \in A$ with $xy = 0$. A ring with no nonzero zero-divisors is called an integral domain. An element $x \in A$ is nilpotent if there exists a natural number $n > 0$ such that $x^n = 0$. A nilpotent element is a zero-divisor (unless $A = 0$) since $x^{n-1}x = 0$. A unit in $A$ is an element $x$ such that there exists an element $y \in A$ with $xy = 1$. This $y$ is unique and is denoted by $x^{-1}$. The units of $A$ form a group with respect to multiplication, and this group is denoted by $A^*$.

**Definition 3.2.** The set of all multiples $ax$ of an element $x \in A$ is called the principal ideal generated by $x$ and is denoted by $(x)$ traditionally. Note that $x$ is a unit iff $(x) = A = (1)$. A field is a ring $A$ in which $1 \neq 0$ and every non-zero element is a unit. Every field is an integral domain. (If $xy = 0$, then $y = x^{-1}xy = 0$).

**Proposition 3.3.** *Let $A$ be a nonzero ring. Then the following are equivalent:*

*(1) the ring $A$ is a field,*
*(2) the only ideals in $A$ are $(0) = \{0\}$ and $(1)$,*
*(3) every homomorphism of $A$ into a non-zero ring $B$ is injective.*

*Proof.* $1 \Rightarrow 2$: Let $\mathfrak{a}$ be a nonzero ideal with $x \in \mathfrak{a}$ nonzero. Then $x$ is a unit and thus $\mathfrak{a} \supseteq (x) = (1)$.

$2 \Rightarrow 3$: Let $f : A \to B$ be a homomorphism and $B$ nonzero. Then $\mathrm{Ker}(f)$ is an ideal of $A$ and is either $(1)$ or 0. If it is $(1)$ then $f = 0$ which is impossible since $f(1) = 1$. Thus $\mathrm{Ker}(f) = 0$ and $f$ is injective.

$3 \Rightarrow 1$: Let $x$ be a nonzero element of $A$. Suppose that $x$ is not a unit so that $(x)$ is not equal to $(1)$. Then $A/(x)$ is a nonzero ring, and hence the natural homomorphism $\pi : A \to A/(x)$ is injective. But this means that $(x) = \mathrm{Ker}(f) = 0$ which is a contradiction. □

## 4. Prime ideals and maximal Ideals

**Definition 4.1.** An ideal $\mathfrak{p} \triangleleft A$ is prime if $\mathfrak{p} \neq (1)$ and if $xy \in \mathfrak{p}$ then either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Shorthand notation: $\mathfrak{a} \triangleleft_p A$. An ideal $\mathfrak{m}$ in $A$ is maximal if $\mathfrak{m} \neq (1)$ and if there is no ideal $\mathfrak{a}$ such that $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq (1)$. Shorthand notation: $\mathfrak{a} \triangleleft_m A$. The set of prime ideals of $A$ is denoted by $\operatorname{Spec}(A)$.

**Lemma 4.2.** *The ideal $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain, and it is maximal if and only if $A/\mathfrak{p}$ is a field.*

*Proof.* This first half of the claim is trivial, so we will only give a detailed argument for the second. Let $\mathfrak{m}$ be maximal. Then since there is a correspondence between ideals of $A/\mathfrak{m}$ and ideals containing $\mathfrak{m}$, the maximality of $\mathfrak{m}$ says that $A/\mathfrak{m}$ has no non-trivial ideals and Proposition 3.3 thus guarantees that $A/\mathfrak{m}$ is a field. Conversely, if $A/\mathfrak{m}$ is a field, then by the correspondence again, there are no ideals between $\mathfrak{m}$ and $A$. □

*Remark* 4.3. Note that this implies that maximal ideals are prime, but not necessarily vice versa. Also note that the zero ideal is prime if and only if $A$ is an integral domain.

**Proposition 4.4.** *If $f : A \to B$ is a ring homomorphism and $\mathfrak{b}$ is a prime ideal in $B$ then $f^{-1}(\mathfrak{b})$ is a prime ideal in $A$.*

*Proof.* The fact that $f^{-1}(\mathfrak{b})$ is an ideal is immediate. Let $xy \in f^{-1}(\mathfrak{b})$. Then $f(xy) \in \mathfrak{b}$ and therefore $f(x)f(y) \in \mathfrak{b}$, so either $f(x)$ or $f(y) \in \mathfrak{b}$, since $\mathfrak{b}$ is prime, and hence either $x$ or $y \in f^{-1}(\mathfrak{b})$. □

*Remark* 4.5. The corresponding statement about maximal ideals is not true in general, since if $A$ is any ring that is not a field and $F$ is any field containing $A$, then 0 is maximal in $F$ but its inverse image in $A$ is not maximal.

**Theorem 4.6.** *Every ring $A \neq 0$ has at least one maximal ideal.*

The proof will use Zorn's Lemma which we recall next. Let $S$ be a partially ordered set (sometimes called a poset), that is, one with a binary relation $\leq$ that is reflexive, transitive and anti-symmetric. A subset $T$ of $S$ is called a chain if any two elements of $T$ are comparable. That is to say that if $x, y \in T$ then either $x \leq y$ or $y \leq x$. An upper bound for a $T$ in $S$ is an element $x \in S$ such that $t \leq x$ for every $t \in T$. Finally, a maximal element in $S$ is an element $x \in S$ so that for all $y$ such that $x \leq y$, we have $x = y$.

**Theorem 4.7** (Zorn's Lemma)**.** *If $S$ is non-empty and every chain $T$ of $S$ has an upper bound in $S$ then $S$ has at least one maximal element.*

Zorn's Lemma is equivalent to the axiom of choice. We will not prove this, since it requires some non-trivial tools from set theory.

*Proof of Theorem 4.6.* Let $\Sigma$ be the set of all ideals not equal to (1) in $A$. Order $\Sigma$ by inclusion. $\Sigma$ is not empty, since $0 \in \Sigma$. We must show that every chain in $\Sigma$ has an upper bound in $\Sigma$. Let $(\mathfrak{a}_\alpha)$ be a chain of ideals in $\Sigma$, which means that for each pair of indices $\alpha, \beta$ we have either $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$ or $\mathfrak{a}_\beta \subseteq \mathfrak{a}_\alpha$.

Let $\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha$. We claim that $\mathfrak{a}$ is an ideal. Indeed, $\mathfrak{a}$ is clearly closed under multiplication by $A$, so we show closure under addition. Let $x, y \in \mathfrak{a}$. Then $x \in \mathfrak{a}_\alpha, y \in \mathfrak{a}_\beta$ for some $\alpha, \beta$. Then one of these ideals contains the other, since

they are elements of a chain and we therefore have $x, y$ contained in the same ideal and thus $x+y \in \mathfrak{a}$. Note that $1 \notin \mathfrak{a}$ since $1 \notin \mathfrak{a}_\alpha$ for all $\alpha$. Hence $\mathfrak{a} \in \Sigma$ and $\mathfrak{a}$ is an upper bound of the chain. Thus by Zorn's Lemma $\Sigma$ contains a maximal element. A maximal element in $\Sigma$ is an ideal that does not contain 1 such that there is no larger ideal in $\Sigma$ containing it; a maximal ideal in $A$. □

**Definition 4.8.** We say that a ring is *local* if it has a *unique* maximal ideal.

**Corollary 4.9.** *If $\mathfrak{a} \neq (1)$ is an ideal of $A$, there exists a maximal ideal of $A$ containing $\mathfrak{a}$.*

*Proof.* Note that $A/\mathfrak{a}$ has a maximal ideal $\mathfrak{m}$ by the above theorem. Denote by $\mathfrak{n}$ the corresponding ideal of $A$ containing $\mathfrak{a}$. We claim that $\mathfrak{n}$ is maximal in $A$. The claim is justified as follows: suppose that there is an ideal $\mathfrak{p}$ strictly between (1) and $\mathfrak{n}$. Then the ideal $\mathfrak{p} = \{x + \mathfrak{a} | x \in \mathfrak{p}\} \neq (1)$ is an ideal of $A/\mathfrak{a}$ that strictly contains $\mathfrak{m}$ which is a contradiction. □

**Corollary 4.10.** *Every non-unit of $A$ is contained in a maximal ideal. (Just let $\mathfrak{a} = (x)$).*

*Remark* 4.11. There exist rings with exactly one maximal ideal, for example fields. A ring $A$ with exactly one maximal ideal $\mathfrak{m}$ is called a local ring and the field $k = A/\mathfrak{m}$ is called the residue field of $A$.

**Lemma 4.12** (Prime avoidance I)**.** *Let $A$ be a ring and $I$ be an ideal of $A$. Let $\mathfrak{p}_1, \mathfrak{p}_2, , \ldots, \mathfrak{p}_n$ be prime ideals of $A$ such that $I \subseteq \bigcup_i \mathfrak{p}_i$. Then $I \subseteq \mathfrak{p}_j$ for some $j$.*

*Proof.* It will be enough to prove that if $I \not\subseteq \mathfrak{p}_j$ for all $j$ then $I \not\subseteq \bigcup_i \mathfrak{p}_i$. We are going to prove this by induction on $n$, the number of prime ideals. For $n = 1$, the claim is clear. Assume the result for $n-1$ prime ideals. Now suppose that $\mathfrak{p}_1, \mathfrak{p}_2, , \ldots, \mathfrak{p}_n$ are prime ideals of $A$ such that $I \not\subseteq \mathfrak{p}_j$ for $j = 1, 2, \ldots, n$. For each $i$ (where $1 \leq i \leq n$) we have $I \not\subseteq \mathfrak{p}_j$, for $j = 1, 2, \ldots, i-1, i+1, \ldots, n$, so by the induction hypothesis for each $i$ with $1 \leq i \leq n$ we can find an element $x_i \in I$ such that $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$. If for some $i$ we have $x_i \notin \mathfrak{p}_i$ then we are done. Otherwise, we have $x_i \in \mathfrak{p}_i$ for all $i$. Then it is easy to see that

$$y = \sum_{i=1}^{n} x_1 \cdots x_{i-1} x_{i+1} \cdots x_n$$

is an element of $I$ which is not in any $\mathfrak{p}_i$. This completes the proof. □

**Lemma 4.13** (Prime avoidance II)**.** *Let $A$ be a ring and $\mathfrak{p}$ be a prime ideal of $A$. Let $\mathfrak{a}_1, \mathfrak{a}_2, , \ldots, \mathfrak{a}_n$ be ideals of $A$ such that $\mathfrak{p} \supseteq \bigcap_i \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_j$ for some $j$. If $\mathfrak{p} = \bigcap_i \mathfrak{a}_i$ then $\mathfrak{p} = \mathfrak{a}_j$ for some $j$.*

*Proof.* Assume that the first claim is false. Then there is an $a_i \in \mathfrak{a}_i$ such that $a_i \notin \mathfrak{p}$ for every $i$. Then

$$a_1 a_2 \cdots a_n \in \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n \subseteq \mathfrak{p}$$

which is a contradiction as $\mathfrak{p}$ is a prime ideal. So the first claim is true. If $\mathfrak{p} = \bigcap_i \mathfrak{a}_i$ then $\mathfrak{p} \subseteq \mathfrak{a}_i$ for every $i$. So if $\mathfrak{p} \supseteq \mathfrak{a}_j$ for some $j$ then $\mathfrak{p} = \mathfrak{a}_j$. Therefore the second claim follows from the first. □

## 5. Nilradical and the Jacobson radical

**Proposition 5.1.** *The set $\mathcal{N}(A)$ of all nilpotent elements in a ring $A$ is an ideal and $A/\mathcal{N}(A)$ has no nilpotent elements $\neq 0$.*

*Proof.* If $x$ is nilpotent then so is $ax$ for all $a \in A$. Now let $x, y$ be nilpotent elements, say $x^n, y^m = 0$. Then

$$(x+y)^{n+m} = 0$$

since each term of the expansion must contain either a power of $x$ greater than $n$ or a power of $y$ greater than $m$. To see that $A/\mathcal{N}(A)$ has no nilpotent elements, note that $x+\mathcal{N}(A) \in A/\mathcal{N}(A)$ is nilpotent if and only if $x^n+\mathcal{N}(A) = 0$ in $A/\mathcal{N}(A)$ which is equivalent to saying that $x^n \in \mathcal{N}(A)$ which would imply that $x \in \mathcal{N}(A)$. □

The ideal $\mathcal{N}(A)$ defined above is called the nilradical of $A$. The following proposition gives another definition of $\mathcal{N}(A)$.

**Proposition 5.2.** *The nilradical of $A$ is the intersection of all the prime ideals.*

*Proof.* Let $R'$ denote the intersection all prime ideals of $A$. Then if $f$ is nilpotent, then $f^n = 0$ for some $n > 0$. Since $0 \in \mathfrak{p}$ for all ideals and $\mathfrak{p}$ is prime, we have that $f \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ and hence $f \in R'$.

Conversely, we will show that if $f$ is not nilpotent, then it is not in the intersection of all prime ideals. Suppose that $f$ is not nilpotent. Then let $\Sigma$ be the set of all ideals $\mathfrak{a}$ such that no power of $f$ is in $\mathfrak{a}$. Ordering $\Sigma$ by inclusion we can apply Zorn's Lemma to conclude that it has a maximal element, $\mathfrak{p}$. We shall show that $\mathfrak{p}$ is prime by showing that $x, y \notin \mathfrak{p}$ implies $xy \notin \mathfrak{p}$. Indeed, if $x, y \notin \mathfrak{p}$ then $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ properly contain $\mathfrak{p}$ and thus are not elements of $\Sigma$ by the maximality of $\mathfrak{p}$. Thus it follows that there exist some $n, m$ so that

$$f^n \in \mathfrak{p} + (x), f^m \in \mathfrak{p} + (y),$$

which clearly implies that $f^{n+m} \in \mathfrak{p} + (xy)$ which implies that $xy \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is prime and does not contain $f$ as required. □

The Jacobson radical $\mathcal{J}(A)$ of $A$ is the intersection of all the maximal ideals of $A$. It can be characterised as follows:

**Proposition 5.3.** *$x \in \mathcal{J}(A)$ if and only if $1 - xy$ is a unit in $A$ for all $y \in A$.*

*Proof.* $\Rightarrow$: Suppose $1-xy$ is not a unit for some $y \in A$. Then by Corollary 4.10 the element $1-xy$ is contained in some maximal ideal $\mathfrak{m}$ of $A$. But since $x \in \mathcal{J}(A) \subseteq \mathfrak{m}$ we have $1 - xy \in \mathfrak{m} \Rightarrow 1 \in \mathfrak{m}$ which is absurd.

$\Leftarrow$: Suppose $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Since $x$ and $\mathfrak{m}$ generate A we have $m + xy = 1$ for some elements $m \in \mathfrak{m}$ and $y \in A$. Thus $1 - xy \in \mathfrak{m}$ contradicting the fact that $1 - xy$ is a unit. □

If $\mathfrak{a}$ is any ideal of $A$ then the radical of $\mathfrak{a}$ is

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}.$$

**Proposition 5.4.** *The radical of an ideal $\mathfrak{a}$ is the intersection of the prime ideals which contain $\mathfrak{a}$.*

*Proof.* Proposition 5.2 applied to $A/\mathfrak{a}$ tells us that the nilradical of $A/\mathfrak{a}$ is the intersection of all prime ideals of $A/\mathfrak{a}$ which is in correspondence with the set of all prime ideals containing $\mathfrak{a}$. □

**Definition 5.5.** Let $I$ be an index set, and for every $i \in I$ let $R_i$ be a ring. Then we may equip the direct product set

$$\prod_{i\in I} R_i$$

with the structure of a ring as follows. We define 0 and 1 as

$$\prod_{i\in I} 0 \quad \text{and} \quad \prod_{i\in I} 1,$$

respectively, while addition and multiplication are defined coordinate-wise:

$$\prod_{i\in I} a_i + \prod_{i\in I} b_i = \prod_{i\in I} (a_i + b_i),$$

$$\prod_{i\in I} a_i \cdot \prod_{i\in I} b_i = \prod_{i\in I} (a_i \cdot b_i).$$

It is easy to see that with this structure $\prod_{i\in I} R_i$ is a ring, and it will be called the direct product of the $R_i$. The key property of direct products is that the direct product of homomorphisms is a homomorphism: if $h_i : R \to R_i$ is a ring homomorphism (for every $i \in I$), then

$$\prod_{i\in I} h_i : R \to \prod_{i\in I} R_i$$

is a ring homomorphism, too.

*Remark* 5.6. Proposition 5.2 can be reformulated as follows: there is an injective ring homomorphism:

$$R/\mathcal{N}(R) \longrightarrow \prod_{\mathfrak{p}\lhd_p R} R/\mathfrak{p}.$$

This map is just (induced by) the direct product of the quotient maps $R \to R/\mathfrak{p}$ (where $\mathfrak{p} \lhd_p R$). Similarly there is an injective ring homomorphism:

$$R/\mathcal{J}(R) \longrightarrow \prod_{\mathfrak{m}\lhd_m R} R/\mathfrak{m}.$$

## 6. Localisation of Rings

**Definition 6.1.** A subset $S$ of a ring $A$ is called multiplicative (or multiplicatively closed) if $1 \in S$, $0 \notin S$, and $ab \in S$ whenever $a, b \in S$.

**Examples 6.2.** Let $A$ be a ring and $a \in A$ be such that $a^n \neq 0$ for all $n \in \mathbb{N}$. Then $S = \{1, a, a^2, \ldots, a^n, \ldots\}$ is a multiplicative set. If $\mathfrak{p} \lhd A$ is a prime ideal, then $S = A - \mathfrak{p}$ is a multiplicative set. For any family $\{\mathfrak{p}_i\}_{i\in I}$ of prime ideals of $A$, the set $A - \bigcup_{i\in I} \mathfrak{p}_i$ is multiplicative. For any ring $A$, the set of units of $A$ is a multiplicative set, so is the set of elements of $A$ that are not zero divisors. If $I$ is a proper ideal of a ring $A$, then $S = 1 + I$ is a multiplicative set.

**Definition 6.3.** Let $A$ be a ring and $S \subset A$ be a multiplicative set. Define a relation $\sim$ on the set $A \times S$ by $(a, s) \sim (b, t)$ if and only if there is a $u \in S$ such that $u(at - bs) = 0$. It is easy to see that $\sim$ is an equivalence relation. Denote the equivalence class of $(a, s)$ under $\sim$ by $a/s = \frac{a}{s}$. Let us denote the set of all

equivalence classes under $\sim$ by $S^{-1}A$. Define binary operations of addition and multiplication on $S^{-1}A$ as follows:

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st},$$
$$\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}.$$

It is easy to verify that these operations are well-defined and make $S^{-1}A$ into a ring with zero $0/1$ and unity $1/1$. Since $A$ is commutative, so is $S^{-1}A$.

**Lemma 6.4.** *Let $A$ be a ring and $S \subset A$ a multiplicative set. There is a ring homomorphism $f : A \to S^{-1}A$ given by $f(x) = x/1$. The map $f$ is injective if and only if $S$ contains no zero divisors.*

*Proof.* It is easy to see that $f$ is a ring homomorphism. If $f$ is injective and $S$ contains a zero divisor $u$, then there is a non-zero $a \in A$ such that $ua = 0$. But then we have $a/1 = ua/u = 0/1 = 0$, contradicting that $f$ is injective. Therefore $S$ does not contain zero divisors. Conversely, if $S$ contains no zero divisors, then for $u \in S$ such that $u(a - b) = 0$ implies $a = b$. Therefore $f$ is injective. □

Throughout the chapter, the letter $f$ will denote the canonical homomorphism $f : A \to S^{-1}A$ of Lemma 6.4.

**Example 6.5.** In general, the homomorphism $f$ is not injective. Let $k$ be a field and consider the ring $A = k[x, y]/(xy)$ and the multiplicatively closed set $S = \{1, x, x^2, \ldots, x^n, \ldots\}$. Note that in this case $f(y) = y/1 = xy/x = 0$, so $f$ is not injective. Also $f(A) = k[x]$ and $S^{-1}A = k[x, x^{-1}]$.

The following is the universal property of localisation.

**Lemma 6.6.** *Let $A$ be a ring and $S \subset A$ a multiplicative set. 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 exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.*

*Proof.* Define $h : S^{-1}A \to B$ by $h(a/s) = g(a)g(s)^{-1}$ for all $a \in A$ and $s \in S$. Then $h$ is a well-defined ring homomorphism and clearly, for any $a \in A$, we have

$$h \circ f(a) = h(a/1) = g(a)g(1)^{-1} = g(a).$$

Moreover if $h' : S^{-1}A \to B$ is such that $g = h' \circ f$, then for any $a \in A$ we have $h' \circ f(a) = g(a)$. Since $h'$ is a ring homomorphism, for any $s \in S$ we have $h'(s^{-1}) = h'(s/1)^{-1} = g(s)^{-1}$. Thus $h' = h$, proving the uniqueness of $h$. □

For every ideal $I$ of $A$ let

$$S^{-1}I = \{i/s \in S^{-1}A | i \in I, s \in S\}$$

denote the ideal generated by $f(I)$ in $S^{-1}A$. The following properties of localisation of rings are routine verifications and are hence left as exercises.

**Proposition 6.7.** *Let $S \subset A$ be a multiplicative subset of a ring $A$. Let $I_1, I_2, \ldots, I_n$ be ideals of $A$. Then*

(a) $S^{-1}(I_1 + \cdots + I_n) = S^{-1}I_1 + \cdots + S^{-1}I_n$,
(b) $S^{-1}(I_1 \cdots I_n) = S^{-1}I_1 \cdot S^{-1}I_2 \cdots S^{-1}I_n$,
(c) $S^{-1}(\bigcap_{i=1}^n I_i) = \bigcap_{j=1}^n S^{-1}I_j$,
(d) $r(S^{-1}I) = S^{-1}(r(I))$ *for every* $I \lhd A$.

We shall now see that the ideals of $S^{-1}A$ can described in terms of ideals of $A$. Then we characterise the prime ideals of $S^{-1}A$ in terms of prime ideals of $A$.

**Proposition 6.8.** *Every ideal of $S^{-1}A$ is of the form $S^{-1}I$ for some ideal $I$ of $A$.*

*Proof.* Let $J$ be any ideal of $S^{-1}A$. Let $f$ denote the canonical homomorphism of Lemma 6.4. Put $I = f^{-1}(J)$. Clearly $I$ is an ideal of $A$. We claim that $J = S^{-1}I$. Let $a/s \in J$. Since $J$ is an ideal, $s \cdot a/s = a \in J$, and so $a \in I$. This implies that $J \subseteq S^{-1}I$. The other containment is clear as $f(I) \subseteq J$. Therefore $J = S^{-1}I$. □

We now prove the most important property of localisation of rings.

**Theorem 6.9.** *The only prime ideals of $S^{-1}A$ are $S^{-1}\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of $A$ such that $\mathfrak{p} \cap S = \emptyset$. Thus prime ideals of $S^{-1}A$ are in bijective correspondence with the prime ideals of $A$ that do not intersect $S$.*

*Proof.* First, we prove that $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$ for any prime ideal $\mathfrak{p}$ not intersecting $S$. Assume that $a/s \cdot b/t \in S^{-1}\mathfrak{p}$ for some $a/s, b/t \in S^{-1}A$. This implies that $v(abu - cst) = 0$ for some $u, v \in S$ and $c \in \mathfrak{p}$. Then $ab(uv) = cstv \in \mathfrak{p}$ which gives $ab \in \mathfrak{p}$, as $\mathfrak{p} \cap S = \emptyset$. But this implies that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, as $\mathfrak{p}$ is prime. So $S^{-1}\mathfrak{p}$ is prime, too.

Also note that $f^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$; if $a \in A$ lies in $S^{-1}\mathfrak{p}$ then there is an $s \in S$ such that $sa \in \mathfrak{p}$, and hence $a \in \mathfrak{p}$, as $\mathfrak{p}$ is a prime and $s \notin \mathfrak{p}$. So $\mathfrak{p}$ is uniquely determined by $S^{-1}\mathfrak{p}$. Now let $\mathfrak{q}$ be a prime ideal of $S^{-1}A$. Then $\mathfrak{q} = S^{-1}\mathfrak{p}$, where $\mathfrak{p} = f^{-1}(\mathfrak{q})$. Since the inverse image of a prime ideal under a ring homomorphism is a prime ideal, we have $\mathfrak{p} \in \mathrm{Spec}(A)$. Clearly $\mathfrak{p} \cap S = \emptyset$ and the claim follows. □

## 7. Cramer's rule for commutative rings

**Lemma 7.1.** *Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. If $f$ is zero evaluated on any $n$-tuple of elements of $\mathbb{Z}$, then it is zero.*

*Proof.* The proof is by induction on the number of variables of $f$. The case $n = 1$ is clear, since $f$ vanishes on an infinite set. In general

$$f(x_1, \ldots, x_n) = \sum_j f_j(x_1, \ldots, x_{n-1}) x_n^j,$$

where the $f_j$ are polynomials with integer coefficients. By plugging in any $(n-1)$-uple of elements of $\mathbb{Z}$ into the first $n-1$ variables we get a polynomial in $x_n$ which vanishes on $\mathbb{Z}$. It is therefore zero, and hence the $f_j$ are also zero, by the induction hypothesis. □

*Remark* 7.2. This simple claim above can be informally reformulated (or reinterpreted) as the following principle: a polynomial identity holds for every ring $R$ if and only if it holds for the integers $\mathbb{Z}$. (Simply apply the lemma to the difference of the two sides of the identity!) For example the binomial identity:

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}$$

holds in $\mathbb{Z}$, so it is true in every ring. Of course we could prove the claim the same way for every $R$ as it was done (hopefully) for integers, using induction on $n$. But the point of the principle is that we do not need to do it for any particular identity, if we already convinced ourselves one way or another for the integers. We

might even use a proof which uses non-algebraic methods, for example analysis, if we wish. This is a useful point for a lazy mathematician. In the following I will assume that you know what Cramer's rule is for (say complex) numbers, and reformulate it essentially as an identity in all rings. By the above I do not need to give any proofs!

**Definition 7.3.** Let $R$ be a commutative ring with unity. The determinant of an $n \times n$ matrix $A = (a_{ij})_{i,j=1}^n$ with coefficients in $R$, where $n$ is a positive integer, is the expression:

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)},$$

where $S_n$ is the permutation group on the letters $\{1, 2, \ldots, n\}$, and for every $\pi \in S_n$ the symbol $\operatorname{sgn}(\pi) = \pm 1$ denotes the sign of $\pi$, considered as an element of $R$.

The $i, j$ minor of $A$ is, by definition, the determinant $M_{ij}$ of the $(n-1) \times (n-1)$ matrix that results from deleting the $i$-th row and the $j$-th column of $A$. A basic fact is the expansion formula:

**Theorem 7.4.** *Let $A = (a_{ij})_{i,j=1}^n$ be as above and let $i \in \{1, 2, \ldots, n\}$. Then its determinant $\det(A)$ is given by:*

$$\det(A) = (-1)^{i+1} a_{i1} M_{i1} + (-1)^{i+2} a_{i2} M_{i2} + \cdots + (-1)^{i+n} a_{in} M_{in}.$$

This is the expansion with respect the $i$-th row of the matrix $A$. There is a similar expansion with respect to columns, which can be derived as follows. The transpose $A^T$ of the matrix $A$ is $A^T = (a_{ji})_{i,j=1}^n$. Since $\det(B^T) = \det(B)$ for every square matrix $B$, we get as an immediate corollary of the theorem above the following result:

**Theorem 7.5.** *Let $A = (a_{ij})_{i,j=1}^n$ be as above and let $i \in \{1, 2, \ldots, n\}$. Then its determinant $\det(A)$ is given by:*

$$\det(A) = (-1)^{i+1} a_{1i} M_{1i} + (-1)^{i+2} a_{2i} M_{2i} + \cdots + (-1)^{i+n} a_{ni} M_{ni}.$$

Every matrix which has either two identical rows or two identical columns has zero determinant. Hence the two results above imply that expansions in the "wrong" way are zero:

**Theorem 7.6.** *Let $A = (a_{ij})_{i,j=1}^n$ be as above and let $i, j \in \{1, 2, \ldots, n\}$ such that $i \neq j$. Then we have:*

$$\begin{aligned} 0 &= (-1)^{j+1} a_{i1} M_{j1} + (-1)^{j+2} a_{i2} M_{j2} + \cdots + (-1)^{j+n} a_{in} M_{jn} \\ &= (-1)^{j+1} a_{1i} M_{1j} + (-1)^{j+2} a_{2i} M_{2j} + \cdots + (-1)^{j+n} a_{ni} M_{nj}. \end{aligned}$$

These results can be expressed in one elegant statement. The Cramer adjoint of $A$ is the matrix $A^\vee = ((-1)^{i+j} M_{ji})_{i,j=1}^n$. Cramer's rule is the following

**Theorem 7.7.** *We have:*

$$A \cdot A^\vee = A^\vee \cdot A = \det(A) I_{n \times n},$$

*where $\cdot$ denotes the usual matrix multiplication and $I_{n \times n}$ is the $n \times n$ identity matrix.*

## 8. Modules

**Definition 8.1.** Let $A$ be a commutative ring with unity. A module over $A$ is an abelian group $(M, 0, +)$ with additional structure $\cdot : A \times M \to M$ (called the $A$-multiplication) such that the following hold for every $\lambda, \mu \in A$ and $x, y \in M$:

$$\begin{aligned} \lambda \cdot (x + y) &= \lambda \cdot x + \lambda \cdot y, \\ \mu \cdot (\lambda \cdot x) &= (\mu\lambda) \cdot x, \\ 1 \cdot x &= x, \\ (\mu + \lambda) \cdot x &= \mu \cdot x + \lambda \cdot x. \end{aligned}$$

**Examples 8.2.** 1) Any ideal of $A$ is an $A$-module. In particular, $A$ itself is an $A$-module. 2) If $A$ is a field $k$ then an $A$-module is precisely a $k$-vector space. 3) If $A = \mathbb{Z}$ then a $\mathbb{Z}$-module is the same as an abelian group. (Just define the action $nx = x + \cdots + x$). 4) If $A = k[x]$ where $k$ is a field, then an $A$-module is a $k$-vector space $V$ with a linear transformation $T$. Define $f\cdot : V \to V$ by $fv = f(T)(v)$ (for every $v \in V$).

**Definition 8.3.** Let $M$ and $N$ be $A$-modules. We say that a function $f : M \to N$ is an $A$-module homomorphism if $f(x+y) = f(x)+f(y)$ and f$(ax) = af(x)$. If $A$ is a field, then these are just the properties of a linear transformation. Note that the composition of $A$-module homomorphisms is again an $A$-module homomorphism. Thus by defining addition and multiplication in an obvious way, we can turn the set of all $A$-module homomorphisms from $M$ to $N$ into an $A$-module. This $A$-module is denoted $\mathrm{Hom}_A(M, N)$. Sometimes we might just write $\mathrm{Hom}(M, N)$ and you'll have to guess what the ring is.

**Definition 8.4.** A submodule $N$ of $M$ is a subgroup of $M$ which is closed under multiplication by elements of $A$. The abelian group $M/N$ then inherits an $A$-module structure by $a(x + N) = ax + N$. This is well defined, and as for ideals, there is a bijective order preserving correspondence between submodules of $M/N$ and submodules of $M$ which contain $N$. We define the sum and intersection of modules in the same way we did for ideals of rings. We define $(N : M) = \{a \in A | aM \subseteq N\}$. This is an ideal of A. In particular, $(0 : M) = \{a \in A | aM = 0\}$ is called the annihilator of $M$ and we denote it by $\mathrm{Ann}(M)$.

**Definition 8.5.** The kernel of a module homomorphism is the set of all $x \in M$ such that $f(x) = 0$. It is a submodule of $M$. The image of $f$ is the set of all $f(x) \in N$ with $x \in M$. The cokernel of $f$ is $\mathrm{Coker}(f) = N/\mathrm{Im}(f)$. If $M'$ is a submodule of $M$ and $M' \subseteq \mathrm{Ker}(f)$ then we have an induced map $f : M/M' \to N$ given by the rule $f(x + M') = f(x)$. This is well defined (you should check this) and in particular if $M' = \mathrm{Ker}(f)$ then by the first isomorphism theorem we have that $M/\mathrm{Ker}(f) = \mathrm{Im}(f)$.

**Definition 8.6.** We say that an $A$-module $M$ be a finitely generated if there is a finite set of elements $m_1, m_2, \ldots, m_n$ of $M$ such that every element of $M$ can be written as an $A$-linear combination of these. In this case we say that $m_1, m_2, \ldots, m_n$ generates $M$. An example of a finitely generated $A$-module is $A^{\oplus n} = \{(a_1, a_2, \ldots, a_n) | a_i \in A\}$, equipped with coordinate-wise addition and $A$-multiplication. In fact every finitely generated $A$-module is a quotient of $A^{\oplus n}$ for some $n$.

**Lemma 8.7.** *Let $A$ be a ring, let $M$ be a finitely generated $A$-module and let $I$ be an ideal of $A$ such that $IM = M$. Then there is an $a \in I$ such that $(1-a)M = 0$.*

*Proof.* If $M = 0$ then there is nothing to prove. So let $M \neq 0$ be generated by $m_1, m_2, \ldots, m_n$. Since $IM = M$, there exist $x_{ij} \in I$ for $1 \leq i, j \leq n$ such that

$$\begin{pmatrix} 1-x_{11} & -x_{12} & \ldots & -x_{1n} \\ -x_{21} & 1-x_{22} & \ldots & -x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -x_{n1} & -x_{n2} & \ldots & 1-x_{nn} \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Multiplying the above relation on the left by the adjoint $T^\vee$ of the square matrix $T$ on the left we get

$$\det(T) \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

using Cramer's rule, so $\det(T)M = 0$. But since $T \equiv I_{n\times n} \mod I$, we have $\det(T) \equiv 1 \mod I$, so $\det(T) = 1-a$ for some $a \in I$. This completes the proof. □

**Corollary 8.8** (Nakayama's lemma)**.** *Let $A$ be a ring and let $M$ be a finitely generated $A$-module. Suppose that $I$ is an ideal of $A$ such that $I \subseteq \mathcal{J}(A)$. If $IM = M$ then $M = 0$.*

*Proof.* From lemma above there is an $a \in I$ such that $(1-a)M = 0$. But $a$ lies in $\mathcal{J}(A)$, so $1-a$ is a unit of $A$. Therefore we get that $M = 0$. □

*Second proof.* Let $m_1, m_2, \ldots, m_n$ be a minimal generating set for $M$ (as an $A$-module). Since $IM = M$ there are $a_1, a_2, \ldots, a_n \in I$ such that

$$m_1 = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n.$$

Since $a_1 \in I \subseteq \mathcal{J}(A)$, we have $1 - a_1 \in A^*$, so by multiplying with its inverse we get that

$$m_1 = (1-a_1)a_2 m_2 + \cdots + (1-a_1)a_n m_n.$$

Therefore $m_2, \ldots, m_n$ is still a generating set, which is a contradiction unless $n = 0$, and hence $M = 0$. □

## 9. Localisation of Modules

**Definition 9.1.** Let $A$ be a ring, let $S \subset A$ be a multiplicative set and let $M$ be an $A$-module. Define a relation $\sim$ on the set $M \times S$ by by $(m, s) \sim (n, t)$ if and only if there is a $u \in S$ such that $u(tm - sn) = 0$. It is easy to see that $\sim$ is an equivalence relation. Denote the equivalence class of $(m, s)$ under $\sim$ by $m/s = \frac{m}{s}$. Let us denote the set of all equivalence classes under $\sim$ by $S^{-1}M$. Define binary operations of addition $+ : S^{-1}M \times S^{-1}M \to S^{-1}M$ and multiplication $\cdot : S^{-1}A \times S^{-1}M \to S^{-1}M$ on $S^{-1}M$ as follows:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

It is easy to verify that these operations are well-defined and make $S^{-1}M$ into an $S^{-1}A$-module with zero $0/1$.

**Definition 9.2.** Let $A$ be a ring and $\mathfrak{p}$ be a prime ideal of $A$. Then $S = A - \mathfrak{p}$ is a multiplicative set. Then the ring $S^{-1}A$ is called the localisation of $A$ at $\mathfrak{p}$ and is denoted by $A_{\mathfrak{p}}$.

We shall now see that $A_{\mathfrak{p}}$ is a local ring; that is why this process is called localisation.

**Theorem 9.3.** *Let $A$ be a ring and $\mathfrak{p}$ be a prime ideal of $A$. Then $a \in A_{\mathfrak{p}}$ is a unit if and only if $a \notin \mathfrak{p}A_{\mathfrak{p}}$. Therefore $A_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.*

*Proof.* Suppose $a/s \in A_{\mathfrak{p}}$ is a unit. Then there exists $b/t \in A_{\mathfrak{p}}$ such that $a/s \cdot b/t = 1$, so for some $u \in S$ (here $S = A - \mathfrak{p}$) we have $u(ab - st) = 0$. Therefore $uab = ust \in S$, and so $a \notin \mathfrak{p}$. Conversely if $a/s \notin \mathfrak{p}A_{\mathfrak{p}}$, then $a \in S$, so $a/s \in A_{\mathfrak{p}}^*$. Therefore $\mathfrak{p}A_{\mathfrak{p}}$ is the unique maximal ideal of $A_{\mathfrak{p}}$ and the ring $A_{\mathfrak{p}}$ is local. This completes the proof. □

**Example 9.4.** $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, p \not| b\}$, where $p$ is a prime number, is an example of localisation of $\mathbb{Z}$ at the prime ideal $(p)$.

The following result illustrates the use of localisation at prime ideals to obtain a property of modules.

**Proposition 9.5.** *Let $A$ be a ring and let $M$ be an $A$-module. Then $M = 0$ if and only if $M_{\mathfrak{p}} = 0$ for all maximal ideals $\mathfrak{p}$ of $A$.*

*Proof.* ($\Rightarrow$) follows trivially. We shall prove the nontrivial implication ($\Leftarrow$). Suppose that $M \neq 0$. Choose any nonzero $x \in M$. Let $I = \mathrm{Ann}(x) = \{a \in A | ax = 0\}$. Clearly, $1 \notin I$, so $I$ is proper. Therefore $I$ is contained in a maximal ideal $\mathfrak{p}$ of $A$. We claim that $M_{\mathfrak{p}} \neq 0$. Indeed if $M_{\mathfrak{p}}$ were 0, we would have $x = 0$ in $M_{\mathfrak{p}}$, so then we would find an element $u \in A - \mathfrak{p}$ with $ux = 0$, giving that $u \in I$. But this contradicts that $I \subseteq \mathfrak{p}$. Hence the proposition follows. □

## 10. Chain conditions

**Lemma 10.1.** *Let $\Sigma$ be a poset. Then the following are equivalent:*

1. *Any nonempty subset of $\Sigma$ has a maximal element.*
2. *Any ascending chain of elements of $\Sigma$ is stationary.*

*Proof.* ($\Rightarrow$): let

$$x_1 \leq x_2 \leq \cdots \leq x_n \leq \cdots$$

be an ascending chain of elements of $\Sigma$. The set of these has a maximal element, say $x_n$. Then $x_n = x_{n+1} = \ldots$ and hence the chain is stationary. ($\Leftarrow$): let $S$ be nonempty subset of $\Sigma$ which has no maximal element. We are going to construct an ascending chain of elements of $S$ recursively:

$$x_1 < x_2 < \cdots < x_n < \cdots$$

as follows. Let $x_1$ be any element of $S$. If the first $n$ elements are already chosen, let $x_{n+1} \in S$ be an element larger than $x_n$. This is possible because $S$ has no maximal element. This is a contradiction so the claim follows. □

**Definition 10.2.** Let $A$ be a ring. An $A$-module $M$ is called Noetherian if every ascending chain of $A$-submodules of $M$ is stationary. It is called Artinian if every descending chain of $A$-submodules of $M$ is stationary. A ring $A$ is called a Noetherian (Artinian) ring if $A$ is Noetherian (respectively Artinian) as an $A$-module.

**Proposition 10.3.** *Let $A$ be a ring and $M$ be an $A$-module. Then the following are equivalent:*

*(1) The module $M$ is Noetherian.*
*(2) Every $A$-submodule of $M$ is finitely generated.*

*Proof.* ($\Rightarrow$): let $N$ be $A$-submodule of $M$ which is not finitely generated. We are going to construct an ascending chain of finitely generated $A$-submodules of $N$ recursively:

$$N_1 \subset N_2 \subset \cdots \subset N_n \subset \cdots$$

as follows. Let $N_1$ be the zero module. If the first $n$ submodules are already chosen, let $x_n \in N$ be an element not in $N_n$. This is possible because $N$ is not finitely generated. Let $N_{n+1}$ be generated by $N_n$ and $x_n$ (i.e. the smallest $A$-submodule containing both). This module is also finitely generated (as $N_n$ is). This is a contradiction.

($\Leftarrow$): let

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

be an ascending chain of $A$-submodules of $M$. The union $N$ of these $A$-submodules is also an $A$-submodule, and hence it is generated by a finite set $m_1, m_2, \ldots, m_r$. For some index $n$ we have $m_1, m_2, \ldots, m_r \in M_n$ already. Then $m_1, m_2, \ldots, m_r$ generates $M_n$ and hence $M_n = N$. So $M_n = M_{n+1} = \ldots$ and hence the chain is stationary. □

**Proposition 10.4.** *Let $A$ be a ring, let $M$ be an $A$-module and $N$ be an $A$-submodule of $M$. Then $M$ is Noetherian (Artinian) if and only if $N$ and $M/N$ are Noetherian (respectively Artinian).*

*Proof.* We will give the proof in the Noetherian case, the argument in the Artinian case is the same. Suppose that $M$ is Noetherian. An ascending chain of $A$-submodules of $N$ is also an ascending chain of $A$-submodules of $M$. Also, an ascending chain of $A$-submodules of $M/N$ corresponds to an ascending chain of $A$-submodules of $M$ containing $N$. Hence it follows that $N$ and $M/N$ are Noetherian.

Now assume that $N$ and $M/N$ are Noetherian. Consider an ascending chain of submodules of $M$:

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

Since the ascending chain

$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \cdots \subseteq (M_n + N)/N \subseteq \cdots$$

is stationary, there is an $n_0 \in \mathbb{N}$ such that $(M_n + N)/N = (M_{n_0} + N)/N$ for all $n \geq n_0$. But the ascending chain

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots \subseteq M_n \cap N \subseteq \cdots$$

of submodules of $N$ must be stationary, too, so there is an $n_1 \in \mathbb{N}$ such that $M_n \cap N = M_{n_1} \cap N$ for all $n \geq n_1$. Taking $n_2 = \max\{n_0, n_1\}$, it is easy to see that $M_n = M_{n_2}$ for all $n \geq n_2$. Therefore it follows that $M$ is Noetherian. □

**Corollary 10.5.** *Let $A$ be a Noetherian (Artinian) ring and let $M$ be a finitely generated $A$-module. Then $M$ is Noetherian (respectively Artinian).*

*Proof.* Because $M$ is the quotient of a finitely generated free $A$-module $A^{\oplus n}$, it will be enough to prove that the latter is Noetherian (respectively Artinian). But this follows from the proposition above by induction on $n$. □

**Corollary 10.6.** *Let $A$ be a ring and let $M$ be an $A$-module. Let*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

*be a finite chain of $A$-submodules. Then $M$ is Noetherian (Artinian) if and only if $M_{i+1}/M_i$ are Noetherian (respectively Artinian) for each $i$.*

*Proof.* This follows from induction from Proposition 10.4. □

**Lemma 10.7.** *Let $A$ be a Noetherian ring and $S \subset A$ be a multiplicative set. Then $S^{-1}A$ is Noetherian.*

*Proof.* Let $J$ be a non-empty set of ideals of $S^{-1}A$. Let $\phi : A \to S^{-1}A$ be the homomorphism given by $a \mapsto \frac{a}{1}$. Consider the collection $\{\phi^{-1}(I) | I \in J\}$ of ideals of $A$. Since $A$ is Noetherian, this has a maximal element, say $\phi^{-1}(I_0)$. Then $I_0 = S^{-1}(\phi^{-1}(I_0))$ is a maximal element of $J$. Therefore $S^{-1}A$ is Noetherian. □

## 11. Primary Decomposition

**Definition 11.1.** A proper ideal $\mathfrak{q}$ of a ring $R$ is primary if for all $x, y \in R$ such that $xy \in \mathfrak{q}$ implies that either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n \in \mathbb{Z}$.

**Proposition 11.2.** *Let $\mathfrak{q}$ be an ideal in a ring $R$. If $r(\mathfrak{q}) = \mathfrak{m}$ is a maximal ideal, then $\mathfrak{q}$ is primary. In particular, any power of a maximal ideal is primary.*

*Proof.* Since $r(\mathfrak{q})$ is the intersection of all prime ideals containing $\mathfrak{q}$, if this intersection is a maximal ideal $\mathfrak{m}$, then $\mathfrak{m}$ is the unique prime ideal containing $\mathfrak{q}$ and $R/\mathfrak{q}$ is a local ring with $\mathcal{N}(R/\mathfrak{q}) = \mathcal{J}(R/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$. In such a ring an element is a zero-divisor if and only if it is not a unit, and the latter holds if and only if the element is nilpotent. Therefore $\mathfrak{q}$ is primary. Since for a maximal ideal $\mathfrak{m}$ we have $r(\mathfrak{m}^n) = \mathfrak{m}$, the second claim follows. □

**Proposition 11.3.** *If $\mathfrak{q}$ is a primary ideal, then its radical $r(\mathfrak{q})$ is a prime ideal, the smallest prime ideal containing $\mathfrak{q}$.*

*Proof.* Let $xy \in r(\mathfrak{q})$, so that $(xy)^m = x^m y^m \in \mathfrak{p}$ for some $m \in \mathbb{Z}$. If $x^m$ is in $\mathfrak{q}$ then $x \in r(\mathfrak{q})$, so assume that $x^m$ is not in $\mathfrak{q}$. Then $y^m$ is a zero divisor in $R/\mathfrak{q}$, so there exists $n \in \mathbb{Z}$ such that $(y^m)^n \in \mathfrak{q}$, as $\mathfrak{q}$ is primary, and then $y \in r(\mathfrak{q})$. The second statement holds for any ideal $I$ whose radical is prime, since $r(I)$ is the intersection of all prime ideals containing $I$. □

A primary ideal is said to be $\mathfrak{p}$-primary if its radical is the prime ideal $\mathfrak{p}$.

**Lemma 11.4.** *If $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary ideals, then $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is a $\mathfrak{p}$-primary ideal, too.*

*Proof.* Let $x, y$ be elements of the ring $R$ such that $xy \in \mathfrak{q}$ and $x \in R - \mathfrak{q}$. Then there is an index $j$ such that $x$ is not in $\mathfrak{q}_j$, so because the latter is a primary ideal we get that $y$ is in the radical of $\mathfrak{q}_j$, which is $\mathfrak{p}$. This implies that for all $1 \leq i \leq n$ there exists $a_i \in \mathbb{N}$ such that $y^{a_i} \in \mathfrak{q}_i$, and then $y^{\max\{a_i\}} \in \bigcap_{i=1}^n \mathfrak{q}_i$, so $\mathfrak{q}$ is primary.

As we saw in the exercises we have $r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n r(\mathfrak{q}_i) = \mathfrak{p}$, so $\mathfrak{q}$ is $\mathfrak{p}$-primary, too. □

Let $R$ be a ring and $I$ an ideal of $R$. We say that $I$ is irreducible if for any two ideals $J, K$ of $R$ such that $I = J \cap K$ we have either $I = J$ or $J = K$.

**Proposition 11.5.** (*a*) *A prime ideal is irreducible.* (*b*) *An irreducible ideal in a Noetherian ring is primary.*

*Proof.* (*a*) Let $\mathfrak{p}$ be a prime ideal, and write $\mathfrak{p} = I \cap J$. Since then $\mathfrak{p} \supseteq IJ$, by the second prime avoidance lemma we have $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$. Without the loss of generality we may say that $\mathfrak{p} \supseteq I$. Then $\mathfrak{p} = I \cap J \supseteq I$, so that we must have $I = \mathfrak{p}$.

(*b*) By passage to the quotient, we may assume that the 0 ideal is irreducible and we must show that it is primary. So suppose $xy = 0$ and $x \neq 0$. Consider the chain of ideals

$$\operatorname{Ann}(y) \subseteq \operatorname{Ann}(y^2) \subseteq \cdots \subseteq \operatorname{Ann}(y^n) \subseteq \cdots$$

Since $R$ is Noetherian, this chain stabilises, so there exists an $n$ such that $\operatorname{Ann}(y^n) = \operatorname{Ann}(y^{n+k})$ for all $k$. We claim that $(x) \cap (y^n) = 0$. Indeed, if $a \in (x)$ then $ay = 0$, and if $a \in (y^n)$ then $a = by^n$ for some $b \in R$, and hence $by^{n+1} = ay = 0$. So $b \in \operatorname{Ann}(y^{n+1}) = \operatorname{Ann}(y^n)$, therefore $a = by^n = 0$. Since the ideal (0) is irreducible, we must then have $y^n = 0$, and this shows that (0) is primary. □

Let $R$ and $I$ be as above. A primary decomposition of $I$ is an expression of $I$ as a finite intersection of primary ideals, say $I = \bigcap_{i=1}^n \mathfrak{q}_i$.

**Theorem 11.6** (Noether)**.** *Any proper ideal in a Noetherian ring admits a primary decomposition.*

*Proof.* Let $I$ be a proper ideal in the Noetherian ring $R$. We claim $I$ is a finite intersection of irreducible ideals; by part (*b*) of Proposition 11.5 this gives the desired result. To see this: suppose that the set of proper ideals which cannot be written as a finite intersection of irreducible ideals is nonempty, and choose a maximal element $I$. Then $I$ is reducible, so we may write $I = J \cap K$ where each of $J$ and $K$ is strictly larger than $I$. But being strictly larger than $I$ each of $J$ and $K$ can be written as a finite intersection of irreducible ideals, and hence so can $I$, which is a contradiction. □

**Lemma 11.7.** *Let $R$ be ring, let $\mathfrak{q} \lhd R$ be a $\mathfrak{p}$-primary ideal, and let $x \in R$.*

(*a*) *If $x \in \mathfrak{q}$ then $(\mathfrak{q} : (x)) = R$.*
(*b*) *If $x \notin \mathfrak{q}$ then $(\mathfrak{q} : (x))$ is $\mathfrak{p}$-primary.*
(*c*) *If $x \notin \mathfrak{p}$ then $(\mathfrak{q} : (x)) = \mathfrak{q}$.*

*Proof.* (*a*) If $x \in \mathfrak{q}$ then $1 \cdot (x) = (x) \subseteq \mathfrak{q}$ so $1 \in (\mathfrak{q} : (x))$. (*b*) If $y \in (\mathfrak{q} : (x))$, then $xy \in \mathfrak{q}$. By assumption $x \notin \mathfrak{q}$, so $y^n \in \mathfrak{q}$ for some $n$ and thus $y \in r(\mathfrak{q}) = \mathfrak{p}$. So $\mathfrak{q} \subseteq (\mathfrak{q} : (x)) \subseteq \mathfrak{p}$; taking radicals we get $r((\mathfrak{q} : (x))) = \mathfrak{p}$. Moreover, if $yz \in (\mathfrak{q} : (x))$ with $y \notin r(\mathfrak{q} : (x)) = \mathfrak{p}$, then $xyz = y(xz) \in \mathfrak{q}$, so $xz \in \mathfrak{q}$, thus $z \in (\mathfrak{q} : (x))$. We get that $(\mathfrak{q} : (x))$ is primary.

(*c*) In any case $\mathfrak{q} \subseteq (\mathfrak{q} : (x))$. If $x \notin \mathfrak{p} = r(\mathfrak{q})$ and $y \in (\mathfrak{q} : (x))$, then $xy \in \mathfrak{q}$; since no power of $x$ is in $\mathfrak{q}$, we must have $y \in \mathfrak{q}$. □

We say that a primary decomposition $I = \bigcap_{i=1}^n \mathfrak{q}_i$ of $I$ is minimal if (*i*) the $r(\mathfrak{q}_i)$ are distinct, and (*ii*) we have $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ for every index $i$. Clearly ever ideal

which has a primary decomposition has a minimal primary decomposition, too, by Lemma 11.4.

**Theorem 11.8** (First Uniqueness Theorem)**.** *Let $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be any minimal primary decomposition of the ideal $I$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then the ideals $\mathfrak{p}_i$ are precisely the prime ideals of the form $r((I : (x)))$ as $x$ ranges through elements of $R$. In particular, they are independent of the choice of minimal primary decomposition.*

*Proof.* For every $x \in R$ we have $(I : (x)) = (\bigcap_{i=1}^{n} \mathfrak{q}_i : (x)) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : (x))$, so $r((I : x)) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i : (x)) = \bigcap_{x \notin \mathfrak{q}_i} \mathfrak{p}_i$ by two of the exercises. So if $r(I : (x))$ is prime then $r(I : (x)) = \mathfrak{p}_i$ for some $i$ by the second prime avoidance lemma. Conversely, for each $i$, by the minimality of the decomposition, there exists $x_i \notin \mathfrak{q}_i$ with $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j$ and then Lemma 11.7 implies $r(I : (x_i)) = \mathfrak{p}_i$. □

## 12. Artinian Rings and Modules

**Definition 12.1.** Let $A$ be a ring and let $M$ be an $A$-module. We say that $M$ is a simple $A$-module (or just simple) if it is not the zero module and every $A$-submodule of $A$ is either 0 or $M$ itself. A composition series of $M$ of length $n$ is a descending chain:

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

such that the quotient modules $M_i/M_{i+1}$ are all simple.

**Proposition 12.2.** *For an $A$-module $M$ the following conditions are equivalent:*

1. *The module $M$ is both Noetherian and Artinian.*
2. *The module $M$ has a composition series.*

*Proof.* ($\Rightarrow$): We are going to construct a composition series

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

as follows. Since $M$ is Noetherian, there must exist a proper maximal $A$-submodule, say $M_1$ (or $M$ is zero and the claim is trivial). If $M_1$ is the zero module, we have a composition series. Otherwise it has a proper maximal $A$-submodule, say $M_2$. We continue in this way: since $M$ is also Artinian, the process must eventually terminate, yielding a composition series. ($\Leftarrow$): as every simple module is Noetherian and Artinian, this follows easily from Corollary 10.6. □

**Proposition 12.3.** *If $M$ has a composition series of length $n$, every composition series of $M$ has length $n$.*

*Proof.* Induction on the length of a composition series. □

The common length of all composition series of $M$ is called the length of $M$, and it is usually denoted by $l(M)$. We say that a module $M$ has finite length if $M$ has a composition series. The following claim is easy:

**Proposition 12.4.** *If*

$$0 \longrightarrow K \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0.$$

*is an exact sequence of $R$-modules with finite length, then*

$$l(K) + l(N) = l(M) + l(P). \quad \square$$

**Examples 12.5.** 1. A field $k$ is an Artinian ring. 2. A finite dimensional vector space over a field $k$ is an Artinian $k$-module. 3. A finite module is Artinian. In particular $\mathbb{Z}/n\mathbb{Z}$ is an Artinian $\mathbb{Z}$-module. 4. If $k$ is a field and $A = k[x]$, then

$$(x) \supset (x^2) \supset \cdots \supset (x^n) \supset \cdots$$

is an infinite strictly descending chain of ideals of $A$. Thus $A$ is not Artinian.

Example 4 above shows that the natural analogue of Hilbert's Basis Theorem is not true for Artinian rings.

**Lemma 12.6.** *An Artinian integral domain is a field.*

*Proof.* Let $A$ be an Artinian integral domain and let $x \in A$ be nonzero. Since the decreasing sequence of ideals

$$(x) \supseteq (x^2) \supseteq \cdots \supseteq (x^n) \supseteq \cdots$$

must be stationary, there exists an $n \in N$ such that $(x^n) = (x^{n+1})$. Since $(x^n) = (x^{n+1})$ we have $x^n = x^{n+1}y$ for some $y \in A$. Since $A$ is a domain and $x \neq 0$, we get $xy = 1$. It follows that $A$ is a field. □

**Corollary 12.7.** *In an Artinian ring every prime ideal is maximal.*

*Proof.* Let $A$ be an Artinian ring and $\mathfrak{p}$ be a prime ideal of $A$. Then $A/\mathfrak{p}$ is an Artinian integral domain, which has to be a field by the above. Hence $\mathfrak{p}$ must be a maximal ideal of $A$. □

We have the following immediate

**Corollary 12.8.** *If $A$ is an Artinian ring, then the nilradical of $A$ is the same as the Jacobson radical of $A$.* □

**Lemma 12.9.** *Let $A$ be an Artinian ring. Then $A$ has only finitely many maximal ideals.*

*Proof.* Suppose that the claim is false; then we can find an infinite set $\{\mathfrak{m}_n | n \in \mathbb{N}\}$ of distinct maximal ideals of $A$. Since the descending sequence of ideals

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n \supseteq \cdots$$

must be stationary, for some $n \in \mathbb{N}$ we have

$$\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_{n+1} \subseteq \mathfrak{m}_{n+1}.$$

Since $\mathfrak{m}_{n+1}$ is a prime ideal, by the second prime avoidance lemma $\mathfrak{m}_{n+1}$ contains $\mathfrak{m}_i$ for some $1 \leq i \leq n$. Because $\mathfrak{m}_i$ is maximal, we get $\mathfrak{m}_{n+1} = \mathfrak{m}_i$, which is a contradiction. □

We say that an ideal $I$ is nilpotent if there is a natural number $n$ such that $I^n = 0$.

**Lemma 12.10.** *Let $A$ be an Artinian ring. Then the nilradical of $A$ is nilpotent.*

*Proof.* The descending chain

$$\mathcal{N}(A) \supseteq \mathcal{N}(A)^2 \supseteq \cdots \supseteq \mathcal{N}(A)^n \supseteq \cdots$$

is stationary, so for some $k \in \mathbb{N}$ we have $\mathcal{N}(A)^k = \mathcal{N}(A)^l$ for all $l \geq k$. We claim that $\mathcal{N}(A)^k = 0$. Assume the contrary. Then the collection

$$C = \{I \lhd A | I \text{ is an ideal such that } I\mathcal{N}(A)^k \neq 0\}$$

is nonempty (as $\mathcal{N}(A)^l \in C$ for all $l$), and has a minimal element, say $I$, since $A$ is Artinian. Since $I\mathcal{N}(A)^k \neq 0$, there exists an element $x \in I$ such that $x\mathcal{N}(A)^k \neq 0$. The minimality of $I$ in $C$ implies that $I = (x)$. Also, $(x\mathcal{N}(A)^k)\mathcal{N}(A)^k = x\mathcal{N}(A)^k \neq 0$, and hence $x\mathcal{N}(A)^k \subseteq I$. The minimality of $I$ again implies that $(x)\mathcal{N}(A)^k = I$. Therefore $(x\mathcal{N}(A)^k) = (x)$, so $x = xy$ for some $y \in \mathcal{N}(A)^k$. Since $y$ is nilpotent we have $y^r = 0$ for some $r$, and hence $x = xy = xy^2 = \cdots = xy^r = 0$. We get that $I = (x) = 0$, a contradiction. So $\mathcal{N}(A)^k = 0$ and $\mathcal{N}(A)$ is nilpotent. □

**Lemma 12.11.** *For a vector space $V$ over a field $k$, the following are equivalent:*

*(1) The vector space $V$ is finite dimensional over $k$.*
*(2) The vector space $V$ is a Noetherian $k$-module.*
*(3) The vector space $V$ is an Artinian $k$-module.*

*Proof.* (1) ⇒ (2): If $V$ is a finite dimensional vector space over $k$ then every $k$-submodule of $V$ is a subspace of $V$ which is finite dimensional and hence, finitely generated. Therefore, $V$ is a Noetherian $k$-module. (2) ⇒ (3): If $V$ is a Noetherian $k$-module, then $V$ is finitely generated, so it has a finite basis. Given any nonempty collection $C$ of $k$-submodules (that is, vector subspaces) of $V$, we can choose a subspace of least dimension, which serves as a minimal element of $C$. Therefore $V$ is Artinian. (3) ⇒ (1): Suppose that $V$ is Artinian but not a finite dimensional vector-space over $k$. Then we can find an infinite subset $\{e_n | n \in \mathbb{N}\}$ of linearly independent vectors in $V$. Then

$$\langle e_1, e_2, \ldots, e_n, \ldots\rangle \supseteq \langle e_2, e_3, \ldots, e_n, \ldots\rangle \supseteq \cdots \supseteq \langle e_m, e_{m+1}, \ldots, e_n, \ldots\rangle \supseteq \cdots$$

is an infinite strictly decreasing chain of $k$-submodules of $V$, a contradiction. This completes the proof. □

**Lemma 12.12.** *Let $A$ be a ring and $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ be maximal ideals of $A$ (not necessarily distinct). Suppose that $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = 0$. Then $A$ is Noetherian if and only if $A$ is Artinian.*

*Proof.* First assume that $A$ is Noetherian. Consider the finite descending chain:

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = 0$$

Let $M_i = \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n$. Since $A$ is noetherian, the module $M_i/M_{i+1}$ is also Noetherian for all $i$ by Proposition 10.4. But $M_i/M_{i+1}$ is an $A/\mathfrak{m}_{i+1}$ module, that is, a vector space over the field $A/\mathfrak{m}_{i+1}$. Therefore $M_i/M_{i+1}$ is Artinian by Lemma 12.11. Using Propostion 10.4 again we get that $A$ is Artinian. The other implication can be proved similarly. □

**Definition 12.13.** The Krull dimension of a ring $A$ is the supremum of all natural numbers $n$ such that there is an ascending chain:

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

of proper prime ideals of $A$. Therefore it is a natural number or $\infty$. It is denoted by $\dim(A)$. Clearly $\dim(A) = 0$ if and only if every prime ideal of $A$ is maximal.

We are now set to prove the main equivalent characterisation of Artinian rings. A noetherian ring may not be Artinian; for example, $\mathbb{Z}$ is Noetherian but not Artinian. The next theorem will imply that an Artinian ring is always Noetherian, so the descending chain condition is stronger than the ascending chain condition.

**Theorem 12.14.** *A ring $A$ is Artinian if and only if $A$ is Noetherian and* $\dim(A) = 0$.

*Proof.* Suppose that $A$ is an Artinian ring. Then every prime ideal of $A$ is maximal by Corollary 12.7, and hence $\dim(A) = 0$. By Lemma 12.9 the ring $A$ has only finitely many maximal ideals, say $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_n$. By Corollary 12.8 and Lemma 12.10 we also know that

$$\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n = \mathcal{J}(A) = \mathcal{N}(A)$$

is nilpotent. So there is a $k \in \mathbb{N}$ such that $(\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n)^k = 0$. This along with Lemma 12.12 implies that $A$ is Noetherian.

For the converse we will need the analogue of Lemma 12.10: the nilradical in a Noetherian ring $A$ is nilpotent. Indeed the nilradical is finitely generated: $\mathcal{N}(A) = (x_1, x_2, \dots, x_n)$. There is a positive integer $m$ such that $x_i^m = 0$ for every index $i$. Every element of $\mathcal{N}(A)$ is an $R$-linear combination of the $x_i$, so its $mn$-th power is zero, too, by the pigeonhole principle. Also note that every ideal $\mathfrak{n} \lhd A$ contains a power of its radical. Because $A$ is Noetherian, so is the quotient ring $A/\mathfrak{n}$, so by the above its nilradical is nilpotent, and the remark follows. By Noether's theorem (0) has a primary decomposition. Because $A$ has zero dimension, every prime ideal appearing in this decomposition is maximal. By the above the product of some power of these maximal ideals is (0). This along with Lemma 12.12 implies that $A$ is Artinian. □

The next result is called the structure theorem for Artinian rings:

**Theorem 12.15.** *An Artinian ring $A$ is the finite direct product of Artinian local rings.*

**Definition 12.16.** Two ideals $\mathfrak{a}, \mathfrak{b}$ of a ring $R$ are *coprime* if $\mathfrak{a} + \mathfrak{b} = R$.

Now let $R$ be a ring and let $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ be ideals of $R$. Consider the homomorphism:

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

given by the rule $x \mapsto (x + \mathfrak{a}_1, x + \mathfrak{a}_2, \cdots, x + \mathfrak{a}_n)$. We will need the following

**Lemma 12.17.** *(i) If $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$.*
*(ii) The map $\phi$ is surjective if and only if $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime whenever $i \neq j$.*
*(iii) The map $\phi$ is injective if and only if $\bigcap \mathfrak{a}_i = (0)$.*

The proof is left as an exercise.

*Proof of Theorem 12.15.* Let $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_n$ be the maximal ideals of $A$ (all pairwise different, of course). We saw that $\prod_{i=1}^{n} \mathfrak{m}_i^k = 0$ for some $k > 0$. Clearly the ideals $\mathfrak{m}_i$ and $\mathfrak{m}_j$ are coprime whenever $i \neq j$, so there is an $x \in \mathfrak{m}_i$ and $y \in \mathfrak{m}_j$ such that $x + y = 1$. Then

$$1 = 1^{2k} = (x + y)^{2k} \in \mathfrak{m}_i^k + \mathfrak{m}_j^k$$

by the binomial theorem. Therefore the ideals $\mathfrak{m}_i^k$ and $\mathfrak{m}_j^k$ are coprime whenever $i \neq j$, so $\bigcap \mathfrak{m}_i^k = \prod \mathfrak{m}_i^k = 0$, and hence the map

$$\phi : A \longrightarrow \prod_{i=1}^{n}(A/\mathfrak{m}_i^k), \quad x \mapsto (x + \mathfrak{m}_1^k, x + \mathfrak{m}_2^k, \cdots, x + \mathfrak{m}_n^k)$$

is an isomorphism by the above. Now we only need to show that $A/\mathfrak{m}_i^k$ is a local Artinian ring. As the quotient of an Artinian ring, it is Artinian. Note that in $A/\mathfrak{m}_i^k$ the nilradical is $\mathfrak{m}_i/\mathfrak{m}_i^k$, since the $k$-th power of any element of this ideal is zero, but it is also a maximal ideal. As the nilradical is the intersection of all prime ideals, all prime ideals of $A/\mathfrak{m}_i^k$ contain $\mathfrak{m}_i/\mathfrak{m}_i^k$, but the latter is maximal, so they are all equal to it. So this ring has a unique prime, and hence maximal ideal. □

## 13. Graded rings, graded modules and the Artin–Rees lemma

**Definition 13.1.** A graded ring is a ring $R$ with a family $(R_n)_{n\in\mathbb{N}}$ of subgroups of the additive group of $R$ such that $R = \bigoplus_{n=0}^{\infty} R_n$ and $R_m R_n \subseteq R_{n+m}$ for every $m, n \in \mathbb{N}$. A graded $R$-module over such an $R$ is an $R$-module $M$ with a family $(M_n)_{n\in\mathbb{N}}$ of subgroups of $M$ such that $M = \bigoplus_{n=0}^{\infty} M_n$ and $R_m M_n \subseteq M_{n+m}$ for every $m, n \in \mathbb{N}$. We say that an $x \in M$ is homogeneous of degree $n$ if $x \in M_n$.

**Example 13.2.** Consider the polynomial ring $R[x_1, \dots, x_r]$ over the ring $R$. If we set $R_n$ to be the $R$-module generated by $\{x_1^{i_1} \cdots x_r^{i_r} \mid i_1 + \cdots + i_r = n\}$, then $R[x_1, \dots, x_r] = \bigoplus_{n=0}^{\infty} R_n$ and the family $(R_n)_{n\in\mathbb{N}}$ equips $R[x_1, \dots, x_r]$ with the structure of a graded ring. If $R, (R_n)_{n\in\mathbb{N}}$ is a graded ring, then $R$ with the family $(R_n)_{n\in\mathbb{N}}$ is a graded $R$-module.

**Definition 13.3.** Let $R$ be any ring and let $\mathfrak{a} \lhd R$. An $\mathfrak{a}$-filtration of an $R$-module $M$ is an infinite descending chain:

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

of $R$-submodules of $M$ such that $\mathfrak{a}M_n \subseteq M_{n+1}$ for every $n \in \mathbb{N}$. We say that an $\mathfrak{a}$-filtration as above is stable if $\mathfrak{a}M_n = M_{n+1}$ for sufficiently large $n$.

**Notation 13.4.** Let $R$ and $\mathfrak{a} \lhd R$ be as above. Then we may form the graded ring $R^{\mathfrak{a}} = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$ (where $\mathfrak{a}^0 = R$ by convention). If $M$ is an $R$-module equipped with an $\mathfrak{a}$-filtration $(M_n)_{n\in\mathbb{N}}$ then $M^{\mathfrak{a}} = \bigoplus_{n=0}^{\infty} M_n$ is a graded $R^{\mathfrak{a}}$-module, as $\mathfrak{a}^m M_n \subseteq M_{m+n}$.

**Lemma 13.5.** *Let $R$ be a Noetherian ring, let $\mathfrak{a} \lhd R$, let $M$ be a finitely generated $R$-module, and let $(M_n)_{n\in\mathbb{N}}$ be an $\mathfrak{a}$-filtration of $M$. Then the following are equivalent:*

*(i) $M^{\mathfrak{a}}$ is a finitely generated $R^{\mathfrak{a}}$-module,*
*(ii) the $\mathfrak{a}$-filtration $(M_n)_{n\in\mathbb{N}}$ is stable.*

*Proof.* As $R$ is Noetherian, the ideal $\mathfrak{a}$ is finitely generated, for example $\mathfrak{a} = \langle x_1, \dots, x_r \rangle$. Then $R^{\mathfrak{a}}$ is finitely generated by $x_1, \dots, x_r$ as an $R$-algebra, so it is Noetherian by Hilbert's basis theorem. Since $R$ is Noetherian and $M$ is finitely generated, we get that $M$ is Noetherian. Therefore $M_n$ is finitely generated for each $n$. Hence so is each $Q_n = \oplus_{r=0}^{n} M_r$. The $R^{\mathfrak{a}}$-submodule

$$M_n^{\mathfrak{a}} = M_0 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots \mathfrak{a}^r M_n \oplus \cdots$$

generated by $Q_n$ in $M^{\mathfrak{a}}$ is finitely generated as an $R^{\mathfrak{a}}$-module. The $M_n^{\mathfrak{a}}$ form an ascending chain, whose union is $M^{\mathfrak{a}}$. Since $R^{\mathfrak{a}}$ is Noetherian, we get that $M^{\mathfrak{a}}$ is finitely generated as an $R^{\mathfrak{a}}$ module $\Leftrightarrow$ it is Noetherian $\Leftrightarrow$ the chain $M_n^{\mathfrak{a}}$ is stationary $\Leftrightarrow$ we have $M^{\mathfrak{a}} = M_m^{\mathfrak{a}}$ for some $m \in \mathbb{N} \Leftrightarrow$ we have $M_{m+k} = \mathfrak{a}^k M_m$ for all $k \in \mathbb{N} \Leftrightarrow$ the filtration is stable. □

**Theorem 13.6** (Artin–Rees lemma)**.** *Let $R$ be a Noetherian ring, let $\mathfrak{a} \lhd R$, let $M$ be a finitely generated $R$-module, and let $(M_n)_{n\in\mathbb{N}}$ be a stable $\mathfrak{a}$-filtration of $M$. If $M'$ is an $R$-submodule of $M$ then $(M' \cap M_n)_{n\in\mathbb{N}}$ is a stable $\mathfrak{a}$-filtration of $M'$.*

*Proof.* We have

$$\mathfrak{a}(M' \cap M_n) \subseteq \mathfrak{a}M' \cap \mathfrak{a}M_n \subseteq M' \cap M_{n+1},$$

so $(M' \cap M_n)_{n\in\mathbb{N}}$ is an $\mathfrak{a}$-filtration. Hence it defines a graded $R^{\mathfrak{a}}$-module which is a submodule of $M^{\mathfrak{a}}$ and therefore finitely generated, since $R^{\mathfrak{a}}$ is Noetherian. The claim now follows from Lemma 13.5 above. □

**Lemma 13.7.** *Let $R, \mathfrak{a}$ and $M$ be as above. Let $(M_n)_{n\in\mathbb{N}}, (M'_n)_{n\in\mathbb{N}}$ be two stable $\mathfrak{a}$-filtrations of $M$. Then there is a positive integer $n_0$ such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for every $n \in \mathbb{N}$.*

*Proof.* We may assume without the loss of generality that $M'_n = \mathfrak{a}^n M$. Since $\mathfrak{a}M_n \subseteq M_{n+1}$ for all $n$, we have $\mathfrak{a}^n M = \mathfrak{a}^n M_0 \subseteq M_n$. By stability $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$ for some $n_0$, and hence $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subseteq \mathfrak{a}^n M$. □

## 14. Poincaré series

Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a Noetherian graded ring and let $M = \bigoplus_{n=0}^{\infty} M_n$ be a finitely generated graded $R$-module.

**Lemma 14.1.** *For every $n$ the $R_0$-module $M_n$ is finitely generated.*

*Proof.* Note that $M_{\geq n} = \bigoplus_{k=n}^{\infty} M_k$ is an $R$-submodule of $M$, so it is Noetherian, as $R$ is Noetherian and $M$ is finitely generated. Therefore its quotient $M_n = M_{\geq n}/M_{\geq n+1}$ is also Noetherian as an $R$-module, and hence as an $R_0$-module, too. Hence it is finitely generated as an $R_0$-module. □

**Definition 14.2.** Now assume that $R_0$ is Artinian. Then each $M_n$ is Artinian, since it is finitely generated over an Artinian ring. Therefore it has a composition series, and its length $l(M_n)$ is well-defined. The Poincaré series of $M$ is the generating function of the $l(M_n)$, that is, the power series:

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

**Theorem 14.3** (Hilbert, Serre)**.** *The power series $P(M,t)$ is a rational function in $t$ of the form $f(t)/\prod_{j=1}^{s}(1-t^{k_j})$, where $f(t) \in \mathbb{Z}[t]$.*

*Proof.* The ideal $R_+ = \bigoplus_{n=1}^{\infty} R_n \lhd R$ is finitely generated, since $R$ is Noetherian. Therefore there is a finite number of homogeneous elements $m_1, m_2, \ldots, m_s \in R_+$ which generate $R_+$. Set $k_j = \deg(m_j)$. We are going to prove the claim by induction on $s$. If $s = 0$ then $R_n = 0$ for every positive $n$, and hence $M$ is actually finitely generated as an $R_0$-module. Therefore $M_n = 0$ for every sufficiently large $n$, so $P(M,t)$ is a polynomial in this case.

Now assume that $s > 0$ and we know the theorem for $s-1$. Multiplication by $m_s$ furnishes an exact sequence:

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{\cdot m_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0.$$

Let $K = \bigoplus_{n=0}^{\infty} K_n$ and $L = \bigoplus_{n=0}^{\infty} L_n$. These are both finitely generated $R$-modules annihilated by $m_s$, and hence they are finitely generated $R_0[m_1, \ldots, m_{s-1}]$-modules,

too. Therefore by the induction hypothesis their Poincaré series are of the form $g(t)/\prod_{j=1}^{s-1}(1-t^{k_j})$ and $h(t)/\prod_{j=1}^{s-1}(1-t^{k_j})$, where $g(t), h(t) \in \mathbb{Z}[t]$. Using the additivity of the length we get that

$$l(K_n) - l(M_n) + l(M_{n+k_s}) - l(K_{n+k_s}) = 0,$$

and hence

$$(1-t^{k_s})P(M,t) = P(L,t) - t^{k_s}P(K,t) + r(t),$$

where $r(t)$ is a polynomial. The claim is now clear. □

The following claim is proved in the exercises:

**Corollary 14.4.** *If the ideal $R_+$ is generated by $R_1$ then $l(M_n)$ is a polynomial in $n$ for large $n$.* □

## 15. Hilbert functions

**Definition 15.1.** Let $R$ be a ring and let $\mathfrak{a} \lhd R$ be an ideal. The associated graded ring is:

$$G_{\mathfrak{a}}(R) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}, \text{ with } \mathfrak{a}^0 = R.$$

The multiplication of this graded ring is defined as follows: for each $x_n \in \mathfrak{a}^n$ let $\overline{x}_n$ denote the image of $x_n$ in $\mathfrak{a}^n/\mathfrak{a}^{n+1}$. Define $\overline{x}_m\overline{x}_n$ to be $\overline{x_m x_n}$, that is, the image of $x_m x_n$ in $\mathfrak{a}^{m+n}/\mathfrak{a}^{m+n+1}$. One needs to check that $\overline{x_m x_n}$ does not depend on the particular representatives chosen. Now if $M$ is an $R$-module and $(M_n)_{n\in\mathbb{N}}$ is an $\mathfrak{a}$-filtration of $M$ then we set:

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

which is a graded $G_{\mathfrak{a}}(R)$-module in a natural way. Let $G_n(M)$ denote $M_n/M_{n+1}$.

**Lemma 15.2.** *Let $R$ be a Noetherian ring and let $\mathfrak{a} \lhd R$. Then:*

(*i*) *the ring $G_{\mathfrak{a}}(R)$ is Noetherian,*
(*ii*) *if $M$ is a finitely generated $R$-module, and $(M_n)_{n\in\mathbb{N}}$ is a stable $\mathfrak{a}$-filtration of $M$ then $G(M)$ is a finitely generated $G_{\mathfrak{a}}(R)$-module.*

*Proof.* (*i*) Since $R$ is Noetherian, the ideal $\mathfrak{a}$ is finitely generated, so we have $\mathfrak{a} = \langle m_1, m_2, \ldots, m_s\rangle$. Let $\overline{m}_i$ be the image of $m_i$ in $\mathfrak{a}/\mathfrak{a}^2$ for every index $i$. Then $G_{\mathfrak{a}}(R) = R/\mathfrak{a}[\overline{m}_1, \overline{m}_2, \ldots, \overline{m}_s]$. As $R/\mathfrak{a}$ is Noetherian, the same holds for $G_{\mathfrak{a}}(R)$ by Hilbert's basis theorem.

(*ii*) By assumption there is an $n_0$ such that $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ for every $r \in \mathbb{N}$, so $G(M)$ is generated by $\bigoplus_{n\le n_0} G_n(M)$. Each $G_n(M)$ is Noetherian and annihiliated by $\mathfrak{a}$, so they are finitely generated $R/\mathfrak{a}$-modules. Hence $\bigoplus_{n\le n_0} G_n(M)$ is a generated by a finite number of elements as an $R/\mathfrak{a}$-module, so $G(M)$ is finitely generated as a $G_{\mathfrak{a}}(R)$-module. □

**Proposition 15.3.** *Let $R$ be a local Noetherian ring, let $\mathfrak{m}$ be its maximal ideal, let $M$ be a finitely generated $R$-module, and let $(M_n)_{n\in\mathbb{N}}$ be a stable $\mathfrak{m}$-filtration of $M$. Then:*

(*i*) *the $R$-module $M/M_n$ is of finite length, for every $n \in \mathbb{N}$,*
(*ii*) *for all sufficiently large $n$ this length is a polynomial $g(n)$,*

(*iii*) *the degree and the leading coefficient of $g(n)$ depends only on $M$, not on the filtration chosen.*

*Proof.* (*i*) By Lemma 15.2 the graded module $G(M)$ is finitely generated over the Noetherian ring $G_{\mathfrak{m}}(R)$. Since $G_{\mathfrak{m}}(R)_0$ is the field $R/\mathfrak{m}$, it is Artinian. Therefore $M_n/M_{n+1}$ has finite length by Lemma 14.1. So the $R$-module $M/M_n$ has finite length, too.

(*ii*) Let $m_1, m_2, \dots, m_s$ generate $\mathfrak{m}$. Then the images $\overline{m}_i$ of the $m_i$ in $\mathfrak{m}/\mathfrak{m}^2$ generate $G_{\mathfrak{m}}(R)$ as an $R/\mathfrak{a}$-algebra, and each $\overline{m}_i$ has degree 1. So we may use Corollary 14.4 to conclude that $l(M_n/M_{n+1}) = f(n)$ where $f(n)$ is a polynomial for large $n$. From part (*i*) we get that $l(M/M_n) - l(M/M_{n+1}) = f(n)$, which implies that $l(M/M_n)$ is also a polynomial for large $n$.

(*iii*) Let $(\widetilde{M}_n)_{n\in\mathbb{N}}$ be another stable $\mathfrak{m}$-filtration of $M$ and set $\widetilde{g}(n) = l(M/\widetilde{M}_n)$. By Lemma 13.7 there is a positive integer $n_0$ such that $M_{n+n_0} \subseteq \widetilde{M}_n$ and $\widetilde{M}_{n+n_0} \subseteq M_n$ for every $n \in \mathbb{N}$, and hence $g(n+n_0) \geq \widetilde{g}(n)$ and $\widetilde{g}(n+n_0) \geq g(n)$. Since $g$ and $\widetilde{g}$ are polynomials for large $n$, we have $\lim_{n\to\infty} g(n)/\widetilde{g}(n) = 1$, and therefore $g$ and $\widetilde{g}$ have the same degree and leading coefficient. □

**Notation 15.4.** The common degree of the polynomials above is denoted by $d_R(M)$, or by $d(M)$, if $R$ is clear from the context. Let $\chi^M(n)$ denote the polynomial for the stable $\mathfrak{m}$-filtration $(\mathfrak{m}^n M)_{n\in\mathbb{N}}$.

**Proposition 15.5.** *Let $R, \mathfrak{m}$ and $M$ be as above, and let $x \in R$ be an element such that multiplication by $x$ on $M$ is injective. Set $M' = M/xM$. Then*

$$d(M') \leq d(M) - 1.$$

*Proof.* Let $N = xM$. Since $N$ is isomorphic to $M$ as $R$-modules via multiplication by $x$. Set $N_n = N \cap \mathfrak{m}^n M$. Then we have exact sequences

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

If we set $g(n) = l(N/N_n)$, then we have

$$g(n) - \chi^M(n) + \chi^{M'}(n) = 0$$

for large $n$. By the Artin–Rees lemma $(N_n)_{n\in\mathbb{N}}$ is a stable $\mathfrak{m}$-filtration of $N$. Since $N \cong M$, by part (*iii*) of Proposition 15.3 above $g(n)$ and $\chi^M(n)$ has the same degree and leading term. The claim is now clear. □

## 16. The dimension of local Noetherian rings

**Theorem 16.1.** *Let $R$ be a local Noetherian ring. Then* $\dim(R) \leq d(R)$.

*Proof.* We prove the claim by induction on $d(R)$. If $d(R) = 0$ then $l(R/\mathfrak{m}^n)$ is constant for all large $n$, hence $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some $n$, so $\mathfrak{m}^n = 0$ by Nakayama's lemma. Thus $R$ is Artinian, and so $\dim(R) = 0$. Suppose now that $d(R) > 0$ and let $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r$ be any chain of ideals in $R$. Let $x \in \mathfrak{p}_1 - \mathfrak{p}_0$ and let $R' = R/\mathfrak{p}_0$. Let $x'$ be the image of $x$ in $R'$. Then $x' \neq 0$ and $R'$ is an integral domain so by Lemma 15.5 we have

$$d(R'/(x')) \leq d(R') - 1.$$

Also if $\mathfrak{m}'$ is the unique maximal ideal of $R'$ then $R'/\mathfrak{m}'^n$ is the homomorphic image of $R/\mathfrak{m}^n$, and hence $d(R') \leq d(R)$. So we get that

$$d(R'/(x')) \leq d(R) - 1.$$

Hence by the induction hypothesis the length of any chain of prime ideals in $R'/(x')$ is $\leq d(R)-1$. But the images of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in $R'/(x')$ form a chain of length $r-1$, so $r-1 \leq d(R)-1$ and consequently $r \leq d(R)$. The claim follows. □

We get the following immediate

**Corollary 16.2.** *If $R$ is a local Noetherian ring then* $\dim(R)$ *is finite.* □

Another application is the following theorem, which we will prove assuming Hilbert's Nullstellensatz in the exercises:

**Theorem 16.3.** *We have* $\dim(\mathbb{C}[x_1, x_2, \ldots, x_n]) = n$. □

## 17. Appendix: elements integral over a ring

**Theorem 17.1.** *Let $R$ be a ring and let $A \subseteq R$ be a subring. Let $x \in R$. Then the following are equivalent:*

(a) *there are $a_0, \ldots, a_{n-1} \in A$ such that*
$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$
(b) *The $A$-module $A[x]$ is finitely generated.*
(c) *There is a subring $B \subseteq R$ which contains $A$, $x$ and it is finitely generated as an $A$-module.*

Here $A[x]$ denotes ring generated by $A$ and $x$. It consists of polynomials in $x$ with coefficients in $A$.

*Proof.* First assume $(a)$. Let $M$ be the $A$-module generated by $1, x, \ldots, x^{n-1}$. By assumption:
$$x^{n+j} = -a_{n-1}x^{n+j-1} - \ldots - a_0 x^j$$
for every non-negative integer $j$. By induction on $j$ we get that $x^{n+j} \in M$ for every such $j$ and hence $M = A[x]$. Therefore as an $A$-module $A[x]$ is finitely generated.

Assume now that $(b)$ holds. Then the choice $B = A[x]$ clearly satisfies the conditions of $(c)$. Finally assume that $(c)$ is true. Let $y_1, \ldots, y_n$ be a finite set of generators for the $A$-module $B$. Since $x \in B$ we get that $xy_i \in B$ for every $i = 1, \ldots, n$, and hence $xy_i = \sum_{j=1}^n a_{ij} y_j$ with some $a_{ij} \in A$. Let $\mathcal{A}$ be the matrix $(a_{ij})_{i,j=1}^n$ and let $d = \det(xI - \mathcal{A})$. By Cramer's rule we have $dy = 0$ for every $y \in B$. Since $1 \in B$ we get that $x$ satisfies the monic polynomial relation $\det(tI - \mathcal{A}) = 0$ in the variable $t$. □

**Definition 17.2.** Let $R$ be a ring and let $A \subseteq R$ be a subring. We say that $x \in R$ is integral over $A$ if it satisfies the three equivalent conditions of Theorem 17.1. Let $P \in A[x]$ be monic polynomial such that $P(x) = 0$. The relation $P(x) = 0$ is called an equation of integral dependence of $x$ over $A$.