Commutative Algebra I

Craig Huneke [1]

Contents

Chapter 1

Rings, Ideals, and Maps

1 Notation and Examples

Throughout these notes, a ring R is considered a commutative unitary ring. That is, a triple $(R, +, \cdot)$ consisting of a set with two operations such that $(R, +)$ is an abelian group with additive identity 0, and multiplication is associative with identity 1, distributive: $a(b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$, and commutative: $ab = ba$.

Further, make note that there is no differentiation between the symbols $\subset$ and $\subseteq$. The symbol $\subsetneq$ will be used to represent a proper subset.

A ring is a *field* if for all non-zero elements $r \in R$, there exits $r' \in R$ (denoted r^{-1}) such that $rr' = 1$.

Example 1. The integers, $\mathbb{Z}$, and the fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings.

Example 2. Let $M_n(k)$ denote the $n \times n$ matrices over a field k. Choose any set of commuting matrices $A_1, \ldots, A_m \in M_n(k)$. Let R be the k-subalgebra generated by $A_1, \ldots, A_m$ in $M_n(k)$. I.e. all sums and products of them. Note that $\dim_k M_n(k) = n^2$. How big can $\dim_k R$ be?

Examples of building new rings from old ones

Example 3. Let R be a ring. Then $R[x]$, the polynomial ring over R, is $\{r_0 + r_1 x + \cdots + r_n x^n | r_i \in R, \ n \geqslant 0\}$ with the usual addition and multiplication of polynomials. Note that

$$r_0 + r_1 x + \cdots + r_n x^n = s_0 + s_1 x + \cdots + s_m x^m \iff n = m \text{ and } r_i = s_i \ \forall i.$$

Inductively, we define $R[x_1, \ldots, x_n]$ to be $R[x_1, \ldots, x_{n-1}][x_n]$.

Example 4 (Direct product)**.** Let I be an index set and R_i be rings for $i \in I$. Then the direct product is given by

$$\prod_{i \in I} R_i = \{(r_i)_{i \in I} | r_i \in R_i\}$$

with component-wise operations.

Example 5. The integers with modulo n arithmetic; $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$.

2   Homomorphisms and Isomorphisms

Let R, S be rings. A *homomorphism* $f : R \to S$ is a function from R to S preserving the operations, i.e, for all r, r' in R we have

$$
\begin{aligned}
f(r + r') &= f(r) + f(r') \\
f(rr') &= f(r)f(r') \\
f(1_R) &= 1_S
\end{aligned}
$$

Note that $f(0) = 0$ is forced.

An *isomorphism* is an homomorphism f which is injective and surjective. If there exists an isomorphism between R and S we say that R and S are *isomorphic* and write $R \simeq S$. Note that if $f : R \to S$ is an isomorphism, its set theoretic inverse f^{-1} is a homomorphism.

Definition. If $f : R \to S$ is a homomorphism (or "map") then the *kernel* of f is defined as $\ker f = \{r \in R \,|\, f(r) = 0\}$.

Examples of kernels and homomorphisms

Example 6. Let R be a ring. Then there exists a unique homomorphism f from $\mathbb{Z}$ to R given as follows: If $n \geqslant 0$ then

$$
\begin{aligned}
f(n) &= f(\overbrace{1 + \cdots + 1}^{n \text{ times}}) \\
&= f(1) + \cdots + f(1) \\
&= 1_R + \cdots + 1_R \\
&= n \cdot 1_R
\end{aligned}
$$

Similarly, if $n < 0$,

$$
f(n) = \overbrace{f(-1_R) + \cdots + f(-1_R)}^{|n| \text{ times}} = |n| \cdot (-1_R).
$$

Example 7. Let R be a ring and choose n elements $r_1, \ldots, r_n \in R$. Then there exists a unique homomorphism $f : \mathbb{Z}[x_1, \ldots, x_n] \to R$ such that $f(x_i) = r_i$. For a polunomial

$$
p(x_1, \ldots, x_n) = \sum_{v_i \geqslant 0} m_{\underline{v}} x_1^{v_1} \cdots x_n^{v_n}
$$

where $\underline{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ and $m_{\underline{v}} \in \mathbb{Z}$, the homomorphism f is given by

$$
f(p(x_1, \ldots, x_n)) = \sum_{v_i \geqslant 0} m_{\underline{v}} r_1^{v_1} \cdots r_n^{v_n}
$$

3 Ideals and Quotient Rings

A subset $I \subseteq R$ is said to be an *ideal* if I is a subgroup under addition and for all $r \in R$, $i \in I$, we have $ri \in I$.

Example 8. If $f : R \to S$ is a homomorphism, then the kernel of f is an ideal of R.

Example 9. Suppose $\{r_\lambda\}_{\lambda \in \Lambda} \subseteq R$. Then the ideal generated by this set, denoted (r_λ), or $(r_\lambda)R$, is the set of elements of the form

$$\sum_{\lambda \in \Lambda'} s_\lambda r_\lambda$$

where $\Lambda' \subseteq \Lambda$, $|\Lambda'| < \infty$, and $s_\lambda \in R$. This is the smallest ideal containing all of $\{r_\lambda\}_{\lambda \in \Lambda}$. We say that I is *finitely generated* if $I = (r_1, \ldots, r_n)$ for some $r_i \in R$, and *principal* if $I = (r)$ for some $r \in R$.

Example 10 (Direct Sum)**.** The direct sum is an ideal of the direct product (not necessarily a subring because it might not contain the multiplicative identity) and is defined as $\bigoplus R_i = \{(r_i) \in \prod R_i | r_i \neq 0$ for finitely many $i \in I\}$ (see Example 4).

Example 11. An arbitrary intersection of ideals is again an ideal. Note that the union of ideals is not necessarily an ideal, as it is not even an abelian group, in general. For example consider $2\mathbb{Z}$ and $3\mathbb{Z}$ in $\mathbb{Z}$.

Example 12. Given two ideals I, J the *product* is an ideal and $IJ = (ij)$ where $i \in I$ and $j \in J$. Note that in general $IJ \neq \{ij \mid i \in I, j \in J\}$; however this is true if one of the two ideals is principal.

Example 13. The *sum* of two ideals I, J is an ideal and is given by $I + J = \{i + j \mid i \in I, j \in J\}$

Example 14. Given two ideals I, J the *colon* is the ideal $I : J = \{r \in R \mid rJ \subseteq I\}$.

Example 15. If $R = \mathbb{Z}$ then every ideal is principal of the form (n) for some $n \geqslant 0$.

Proof. Let $I \subseteq \mathbb{Z}$ be an ideal, $I \neq (0)$. Note that $n \in I$ if and only if $-n \in I$. So without loosing generality, choose $n \in I$ least such that $n > 0$. To show that $I = (n)$, consider $m \in I$. Then $m = qn + r$ for $0 \leqslant r < n$. But this shows that $r = m - qn$ which is an element of I. Thus $r = 0$ and $I = (n)$. $\qquad\square$

Example 16. Let k be a field, $R = k[x]$. Then every ideal of R is principal.

Example 17. Let k be a field, $R = k[x, y]$. If $I = (x, y)$, that is the set of all $f \in R$ such that $f(0, 0) = 0$, then I is not principal. In fact $(x, y)^n$ requires $n + 1$ generators.

Let I be an ideal in a ring R. Then the *quotient ring*, denoted R/I, is the set $\{r + I | r \in R\}$ of additive cosets of I. We make this into a ring by

$$
\begin{aligned}
(r + I) + (s + I) &:= (r + s) + I \\
(r + I) \cdot (s + I) &:= rs + I
\end{aligned}
$$

We need to show that the product is well defined. First recall that $r + I = \{r + i | i \in I\}$ and we have $r + I = s + I$ if and only if there exists $i, i' \in I$ such that $r + i = s + i'$. This is equivalent to $r - s \in I$.

Now suppose $r + I = r' + I$ and $s + I = s' + I$. We want to show $rs + I = r's' + I$, i.e. $rs - r's' \in I$. So notice,

$$
rs - r's' = (r - r')s - r'(s' - s) \in I.
$$

The zero element in R/I is $0 + I = I$. The multiplicative identity is $1 + I$. In general we will write $\bar{r} = r + I$. There is a surjective homomorphism $\pi : R \to R/I$ defined by $\pi(r) = \bar{r}$ with $\ker(\pi) = I$.

Example 18. Let $R = \mathbb{Z}$. Then by example 15 we know that every ideal I is principal, say $I = (n)$. Then the map $\mathbb{Z} \to \mathbb{Z}/I$ is just $\mathbb{Z} \to \mathbb{Z}/(n)$ such that $m \mapsto \bar{m}$ for $m \in \mathbb{Z}$.

Example 19. Let $I = (x^2 + 1)$ be an ideal in the polynomial ring $\mathbb{R}[x]$ for $\mathbb{R}$ the real numbers. Then $\mathbb{R}[x]$ maps onto $\mathbb{C}$ via

$$
\mathbb{R}[x] \to \mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}
$$

Proposition 1 (Isomorphism Theorem). *Let $f : R \to S$ be a ring homomorphism and set $I = \ker f$. Then f factors as a surjection followed by an injection as in the following commutative diagram:*

In particular, if f is onto, then g is an isomorphism.

Proof. Note if $r \in R$, then we must have $(g(\bar{r}) =) g(\pi(r)) = f(r)$ giving the definition of g. To show g is well defined, suppose $\bar{r} = \bar{r'}$. This implies that $r - r' \in I$. Hence $f(r - r') = 0$ which gives $f(r) = f(r')$. So we have that $g(\bar{r}) = g(\bar{r'})$. The fact that g is a homomorphism is clear. We need to show g is injective. Suppose that $g(\bar{r}) = g(\bar{t})$. Then $f(r) = f(t)$ which gives $f(r - t) = 0$. Thus $r - t \in I$ and $\bar{r} = \bar{t}$. $\square$

Example 20. Let R be a ring and I an ideal of R. Let $IR[x]$ denote the ideal in $R[x]$ generated by $\{i \mid i \in I\}$. Then

$$
\frac{R[x]}{IR[x]} \simeq \left(\frac{R}{I}\right)[x]
$$

Proof. Apply proposition 1 with $R := R[x]$ and $S := (R/I)[x]$. Define $f : R \to S$ by $f(r_0 + r_1 x + \cdots + r_n x^n) = \overline{r_0} + \overline{r_1} x + \cdots + \overline{r_n} x^n$. This is onto and hence by the proposition we have established the isomorphism. $\square$

Theorem 2. *Let $I \subseteq R$ be an ideal.*

(1) *Every ideal $\overline{J}$ in $\overline{R} := R/I$ is of the form J/I where J is an ideal in R containing I and $J/I = \{\overline{j} \mid j \in J\}$. Moreover, if J is an ideal in R containing I, then J/I is an ideal in R/I.*

(2) *If J_1, J_2 are ideals in R containing I, then $\overline{J_1} = \overline{J_2}$ if and only if $J_1 = J_2$. Hence this correspondence is a one-to-one inclusion preserving correspondence between ideals of R/I and ideals in R containing I.*

(3) *If $J \supseteq I$ are ideals then $\overline{R}/\overline{J} \simeq R/J$*

Proof. Let $\overline{J} \subseteq \overline{R}$ be an ideal and define $J = \pi^{-1}(\overline{J})$ under the projection map $\pi : R \to R/I$. Since $\overline{0} \in \overline{J}$, we must have $I \subseteq J$. It is easy to see that J is an ideal and $J/I = \overline{J}$ by definition. Conversely, given an ideal J of R containing I, it is also easy to see that J/I is an ideal.

To show the second statement, note that if $J_1 = J_2$ then we have $\overline{J_1} = \overline{J_2}$. Conversely, suppose $\overline{J_1} = \overline{J_2}$ and let $j_i \in J_1$. Then there exists $j_2 \in J_2$ such that $\overline{j_1} = \overline{j_2}$. This implies that $j_1 - j_2 \in I$. But $I \subseteq J_2$ thus we have $j_1 = (j_1 - j_2) + j_2 \in J_2$. Hence $J_1 \subseteq J_2$. a similar argument shows that $J_2 \subseteq J_1$.

For the third statement, use proposition 1 with $S = \overline{R}/\overline{J}$ and the composition f of the surjections

$$R \xrightarrow{\ \pi\ } R/I \xrightarrow{\ \overline{\pi}\ } \overline{R}/\overline{J}.$$

with f below.

Note that the $\ker(f) = J$. $\square$

Remark. Suppose $I = (f)$ is a principal ideal in R and $\overline{g} \in \overline{R} = R/I$. Suppose we want to understand what $\overline{R}/(\overline{g})$ looks like. Set $\overline{J} := (\overline{g}) \subseteq \overline{R}$ and let J be as in the theorem. What is J?

By definition, $J = \pi^{-1}((\overline{g}))$ where $\pi : R \to R/(f)$. To understand the structure of J, consider an element $j \in J$, i.e. $\overline{j} \in (\overline{g})$. Equivalently j has the property that there exists an $\overline{r} \in \overline{R}$ such that $\overline{j} = \overline{r} \cdot \overline{g}$. But this is the same as saying $j - rg \in (f)$, that is for some $s \in R$, $j - rg = sf$. Thus $j = rg + sf$. This forces $J = (f, g)$. Therefore by the third part of theorem 2 we have that $\overline{R}/(\overline{g}) \simeq R/(f, g)$. By the same token, $R/(f, g) \simeq \tilde{R}/(\tilde{f})$ where $\tilde{R} = R/(g)$.

Example 21. Let $i \in \mathbb{C}$, $i^2 = -1$, and $\mathbb{Z}[i] = \{a + bi \mid a, b \in Z\}$. This ring is called the *Gaussian integers*. In order to analyze the quotient ring $\mathbb{Z}[x]/(5)$ consider the unique homomorphism $f : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by evaluating at i

(see example 7). From proposition 1 we have that $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$. So by the above remark we have that

$$
\begin{aligned}
\frac{\mathbb{Z}[i]}{(5)} \quad &\simeq \quad \frac{\mathbb{Z}[x]}{(x^2+1,5)} \\
&\simeq \quad \frac{\mathbb{Z}[x]/5\mathbb{Z}[x]}{(x^2+1)} \\
&\simeq \quad \frac{(\mathbb{Z}/5\mathbb{Z})[x]}{(x^2+1)} \\
&\simeq \quad \frac{\mathbb{Z}_5[x]}{(x-2)(x-3)}
\end{aligned}
$$

4 Prime Ideals

Given a ring R, an ideal I is *maximal* if there does not exist a proper ideal J such that $I \subsetneq J$. This is equivalent to R/I being a field. A proper ideal I is *prime* if whenever $ab \in I$ then $a \in I$ or $b \in I$. A ring is called a *domain* if for any elements a, b in the ring such that $ab = 0$ then $a = 0$ or $b = 0$. An ideal I in a ring R is prime if and only if R/I is a domain. Hence we have that maximal ideals are prime as fields are domains. On the other hand, the converse is not true, consider the ring $\mathbb{Z}$ with ideal (0).

Topology on Spec(R)   The set of prime ideals in a ring R is denoted $\mathrm{Spec}(R)$. For an example consider the ring $\mathbb{Z}$. Then $\mathrm{Spec}(\mathbb{Z})$ is all the ideals generated by a prime element and the zero ideal. Another example is $k[x]$, a polynomial ring over a field. This is a PID so $\mathrm{Spec}(k[x])$ is the set of ideals generated by an irreducible element and the zero ideal.

In general, if $f : R \to S$ is an homomorphism and $Q \in \mathrm{Spec}(S)$ then we have that $f^{-1}(Q)$ is in $\mathrm{Spec}(R)$. So we get an induced map $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$. A special case of this is if I is an ideal in a ring R and $\pi : R \to R/I$ is the projection map. If $\pi^* : \mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ is the induced map where $\mathrm{Spec}(R/I)$ is the set of ideals in the form P/I, with P a prime ideal in R such that $P \supseteq I$, then $\pi^*(P/I) = P$.

A topology on $\mathrm{Spec}(R)$ can be given by saying a set $V \subseteq \mathrm{Spec}(R)$ is closed if and only if there exists and ideal I in R such that $V = \{\mathfrak{p} \mid \mathfrak{p} \supseteq I\}$ (denoted $V(I)$). Open sets are given by $X - V(I) = U$ where $X = \mathrm{Spec}(R)$. This topology on $\mathrm{Spec}(R)$ is called the *Zariski topology*. Note that under this topology the induced map f^* is continuous. A basis of the open sets is $\{D(r)\}_{r \in R}$ where $D(r) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid r \notin \mathfrak{p}\}$. To see this notice that $D(r) = X - V(r)$ and if $U = X - V(I)$ then $U = \cup_{r \in I} D(r)$.

For an example, consider the ring $\mathbb{Z}$. Notice that $(0) \in \mathrm{Spec}(\mathbb{Z})$ but is not closed. For if $\{(0)\} = V(I)$ for some ideal I then $I = (0)$ and thus $V(I) = \mathrm{Spec}(\mathbb{Z})$, a contradiction. In fact, the closed points are maximal ideals.

Remark. Suppose that R is a domain. Then the intersection of any two nonempty open sets is non-empty, i.e. $\mathrm{Spec}(R)$ is irreducible.

Proof. Let U_1, U_2 be non-empty open sets, $U_i = X - V(I_i)$, $i = 1, 2$. Notice that $U_i = \emptyset$ if and only if $I_i = (0)$. This is true since $(0) \in \mathrm{Spec}(R)$. So $I_i \neq (0)$ iff $(0) \not\supseteq I_i$ iff $(0) \in X - V(I_i)$. Conversely, if $p \in U_i$ then $\mathfrak{p} \not\supseteq I_i$ and therefore $(0) \not\supseteq I_i$. This implies that $I_i \neq 0$. Therefore $I_1 \neq (0), I_2 \neq (0)$, and $(0) \in U_1 \cap U_2 \neq \emptyset$. $\qquad\square$

Nilradical and Jacobson Radical For $r \in R$ a ring, we say r is a *unit* if there exists an $s \in R$ such that $rs = 1$. Equivalently, $(r) = R$. Given an ideal I in a ring R, the *nilradical* of I (denoted $\sqrt{I}$) is defined as the set of all elements of the ring R whose powers are in I. An element r of the ring R is called *nilpotent* if some power of r is zero. The set of all nilpotent elements can be given by $\sqrt{0}$ and is denoted $\mathrm{Nilrad}(R)$. The *Jacobson radical* of R, denoted $\mathrm{Jac}(R)$ is the intersection of all maximal ideals in R.

Remark. The radical of I is an ideal and $V(\sqrt{I}) = V(I)$.

Proof. If $x \in \sqrt{I}$, $r \in R$ then $(xr)^n = x^n r^n \in I$ for all n sufficiently large. If $x, y \in \sqrt{I}$, say $x^n, y^m \in I$ then $(x+y)^{m+n-1}$ is also in I. Notice that

$$(x+y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i}$$

is in I since either $i \geqslant n$ or $m + n - 1 - i \geqslant m$.

To see the second part, let $\mathfrak{p} \in V(\sqrt{I})$. Then $\mathfrak{p} \supseteq \sqrt{I} \supseteq I$ and thus $\mathfrak{p} \in V(I)$. Conversely, let $\mathfrak{p} \in V(I)$ and $x \in \sqrt{I}$. Then $x^n \in I \subseteq \mathfrak{p}$ and hence $x \in \mathfrak{p}$. Therefore $\mathfrak{p} \supseteq \sqrt{I}$ and we have that $\mathfrak{p} \in V(\sqrt{I})$. $\qquad\square$

Remark. The ring R is said to be *reduced* if there are no non-zero nilpotent elements. For example, the ring $R/\sqrt{I}$ is always reduced since $\sqrt{\sqrt{I}} = \sqrt{I}$.

Lemma 3. *If R is a ring and x is non-nilpotent then there exist ideals maximal with respect to the exclusion of the set $S = \{x^n\}_{n=0}^{\infty}$ and any such ideal is prime.*

Proof. Let Σ be the set of ideals of R that do not meet S. Note that Σ is non-empty since the zero ideal does not meet S. By Zorn's lemma[1], we have that Σ has at least one maximal element I. Now assume that $ab \in I$ and that $a, b \notin I$. Hence we have that the ideals (I, a) and (I, b) have I as a proper subset and hence neither are elements of Σ. That is, there exists natural numbers n, m such that $x^n \in (I, a)$ and $x^m \in (I, b)$. So for some $i_1, i_2 \in I$ and $r, s \in R$ we have $x^n = i_1 + ra$ and $x^n = i_2 + sb$. The product

$$x^{n+m} = x^n x^m = (i_1 + ra)(i_2 + sb) = i_1 i_2 + i_1 sb + i_2 ra + abrs$$

is an element of I, a contradiction. So I is prime. $\qquad\square$

---

[1]Let S be a non-empty partially ordered set (i.e. we are given a relation $x \leqslant y$ on S which is reflexive and transitive and such that $x \leqslant y$ and $y \leqslant x$ together imply $x = y$). A subset T of S is a *chain* if either $x \leqslant y$ or $y \leqslant x$ for every pair of elements x, y in T. Then *Zorn's Lemma* may be stated as follows: if every chain T of S has an upper bound in S (i.e. if there exists $x \in S$ such that $t \leqslant x$ for all $t \in T$) then S has at least one maximal element.

Corollary 4. *Every ideal is contained in a maximal ideal*

Proof. Apply the lemma 3 to the ring $S = R/I$ and $x = 1 + I \in S$. So there exists an ideal J/I in S maximal with respect to not containing 1_S. I.e. if J/I is maximal in S then $J \supseteq I$ and J is maximal in R. □

Proposition 5. *Let R be a ring and I and ideal of R. The following are equivalent.*

(1) $x \in \sqrt{I}$

(2) For all ring homomorphisms $\phi : R \to k$ where k is a field, $\phi(x) \in (\phi(I))$. That is, the image of x in k is in the ideal generated by the image of I in k.

(3) $x \in \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $\mathfrak{p} \supseteq I$.

In particular, $\sqrt{I}$ is the intersection of all prime ideals containing I.

Proof. (1)⇒(2): Assume that $x \in \sqrt{I}$ and let k be a field. Consider a ring homomorphism $\phi : R \to k$. Since $(\phi(I))$ is an ideal of k it is either (1) or (0). The former case is clear so assume the latter. For all large n, $\phi(x^n) = 0$ so that $\phi(x)^n = 0$. But we are in a field, in particular a domain, hence $\phi(x) = 0$. (Note that we could have restated (2) to say for all ring homomorphism $\phi : R \to k$ such that $\phi(I) = 0$, $\phi(x) = 0$.)

(2)⇒(3): Suppose that $I \subseteq \mathfrak{p}$ for $\mathfrak{p}$ a prime ideal. Consider the composition

$$R \xrightarrow{\ \pi\ } R/\mathfrak{p} \overset{i}{\hookrightarrow} \kappa(\mathfrak{p}).$$
$$\underset{\phi}{\underbrace{\qquad\qquad\qquad}}$$

where $\kappa(\mathfrak{p})$ is the field of fractions of $R/\mathfrak{p}$. Choose $x \in R$ as in (2). Notice that $\phi(I) = 0$ since $I \subseteq \mathfrak{p}$. Therefore we have that $\phi(x) = 0$. Since i is an injection, we have that $x + \mathfrak{p} = 0$ in $R/\mathfrak{p}$ and thus $x \in \mathfrak{p}$.

(3)⇒(1): Assume that $x \notin \sqrt{I}$ and pass to R/I (assume $R = R/I$). Thus we have reduced to the case in which $x \in \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$ and $x \notin \sqrt{0}$. But by lemma 3, since x is not nilpotent, there exists a prime ideal P maximal with respect to the exclusion of $\{x^n\}_{n=0}^{\infty}$; a contradiction. □

Chinese Remainder Theorem

Definition. Two ideals I and J of a ring R are *comaximal* if $I + J = R$.

Example 22. If $n, m \in \mathbb{Z}$ are relatively prime, then (n) and (m) are comaximal.

Example 23. If k is a field, then for any two distinct elements $\alpha, \beta \in k$, the elements $(x - \alpha)$ and $(x - \beta)$ are comaximal in the polynomial ring $k[x]$. To see this notice

$$1 = \frac{1}{\beta - \alpha}(x - \alpha) - \frac{1}{\beta - \alpha}(x - \beta).$$

More generally, if $\mathfrak{m}_1$, $\mathfrak{m}_2$ are distinct maximal ideals then $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are comaximal since $\mathfrak{m}_1 \subsetneq \mathfrak{m}_1 + \mathfrak{m}_2$ implies $\mathfrak{m}_1 + \mathfrak{m}_2 = R$.

Theorem 6 (Chinese Remainder Theorem). *Let R be a ring and $I_1, \ldots, I_n$ ideals. If I_i and I_j are comaximal for all $i \neq j$, then*

(1) $R/I_1 \times \cdots \times R/I_n \simeq R/I_1 \cap \cdots \cap I_n$

(2) $I_1 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$.

Proof. First do the case $n = 2$. For simplicity, Let $I = I_1$ and $J = I_2$. By assumption there exists $i \in I$ and $j \in J$ such that $i + j = 1$. Since $IJ \subseteq I \cap J$ is always true, consider an element r of $I \cap J$. Then $ri + rj = r$ and $IJ \supseteq I \cap J$. Hence the second part holds.

For the first part, consider a map $f : R \to R/I \times R/J$ defined by $f(r) = (r+I, r+J)$. We need to prove that $\ker(f) = I \cap J$ and f is onto. By proposition 1 these two facts give the desired result. First notice that

$$f(r) = 0 \iff r + I = I, \ r + J = J$$
$$\iff r \in I \cap J.$$

Thus $\ker(f) = I \cap J$. Next let $(a + I, b + J)$ be an element of $R/I \times R/J$ and set $r = aj + bi$. Then

$$r + I = a + I \iff r - a \in I$$
$$\iff aj + bi - a \in I$$
$$\iff a(j - 1) + bi \in I$$
$$\iff a(-i) + bi \in I.$$

A similar argument can be made for b and J. Hence $f(r) = (a + I, b + J)$.

To complete the proof use induction on n. With out loosing any generality, assume $n > 2$. If $I_1 \cap \cdots \cap I_{n-1}$ and I_n are comaximal, then by the induction

$$R/I_1 \times \cdots \times R/I_{n-1} \simeq R/I_1 \cap \cdots \cap I_{n-1}$$

and

$$I_1 \cap \cdots \cap I_{n-1} = I_1 I_2 \cdots I_{n-1}.$$

By the case of $n = 2$ we may conclude that

$$R/I_1 \cap \cdots \cap I_{n-1} \times R/I_{n-1} \simeq R/I_1 \cap \cdots \cap I_{n-1}$$

and

$$(I_1 \cap \cdots \cap I_{n-1}) \cap I_n = (I_1 I_2 \cdots I_{n-1}) \cdot I_n.$$

In order to ensure $I_1 \cap \cdots \cap I_{n-1}$ and I_n are comaximal suppose they are not and argue by way of contradiction. That is assume $I_1 \cap \cdots \cap I_{n-1}$ and I_n are not comaximal. Then $(I_1 \cap \cdots \cap I_{n-1}) + I_n$ is a proper ideal and is contained in some maximal ideal $\mathfrak{m}$. Since $I_1 \cdots I_{n-1} \subseteq I_1 \cap \cdots \cap I_{n-1}$ we get that $I_1 \cdots I_{n-1} \subseteq \mathfrak{m}$. Since $\mathfrak{m}$ is prime there exists $1 \leqslant j \leqslant n - 1$ such that $I_j \subseteq \mathfrak{m}$. But then $I_j + I_n \subseteq \mathfrak{m}$, a contradiction. $\square$

Example 24. Recall from example 21 that

$$\frac{\mathbb{Z}[i]}{(5)} \simeq \frac{(\mathbb{Z}/5\mathbb{Z})[x]}{(x^2+1)} \simeq \frac{\mathbb{Z}_5[x]}{(x-2)(x-3)}.$$

Here the ideals $(x-2)$ and $(x-3)$ are comaximal.

Prime Avoidance

Theorem 7 (Prime Avoidance: Version 1). *Let $I_1, \ldots, I_n$ be ideals in a ring R, at most two are not prime. If J is another ideal and $J \subseteq \cup_{i=1}^{n} I_i$ then $J \subseteq I_j$ for some j.*

Proof. First assume $n = 2$ and that $J \nsubseteq I_1$, $J \nsubseteq I_2$. Choose elements $j_1 \in J - I_1$, $j_2 \in J - I_2$ and consider $j = j_1 + j_2$. Since $J \subseteq I_1 \cup I_2$ we have $j_1 \in I_2$ and $j_2 \in I_1$. But $j \in J$. So with out lose of generality, assume $j \in I_1$. Then $j_1 = j - j_2 \in I_1$, a contradiction.

By induction on n, we will prove the general case. Let $n > 2$ and choose I_1 to be prime. Assume that $J \nsubseteq I_j$ for all $j = 1, \ldots, n$. By the induction, for all $1 \leqslant j \leqslant n$, $J \nsubseteq \cup_{l \neq j} I_l$, so choose $a_j \in J - \cup_{l \neq j} I_l$ (note $a_j \in I_j$). Now consider

$$a = a_1 + a_2 a_3 \cdots a_n \in \bigcup_{j=1}^{n} I_j.$$

Suppose that $a \in I_j$ for some $j \geqslant 2$. Since $a_j \in I_j$, $a_2 a_3 \cdots a_n \in I_j$. Hence $a_1 = a - a_2 a_3 \cdots a_n \in I_j$, a contradiction.

If $a \in I_1$, then $a_2 a_3 \cdots a_n = a - a_1 \in I_1$. Since I_1 is prime, there exists an l such that $2 \leqslant l \leqslant n$ where $a_l \in I_1$, another contradiction. Therefore $a \in J$ is not contained in any I_j. In other words, $J \nsubseteq \cup_{j=1}^{n} I_j$. $\qquad\square$

Theorem 8 (Prime Avoidance: Version 2). *Let R be a ring and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals of R. Suppose $x \in R$, I is an ideal of R, and*

$$\{rx + i \mid r \in R, \ i \in I\} = (x) + I \nsubseteq \mathfrak{p}_j$$

for $1 \leqslant j \leqslant n$. Then there exists an $i \in I$ such that $x + i \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$.

Proof. We can assume $\mathfrak{p}_j \nsubseteq \mathfrak{p}_k$ for $j \neq k$. Assume by way of contradiction that the coset $x + I \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$ and fix v such that $x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_v$, $x \notin \mathfrak{p}_{v+1} \cup \cdots \cup \mathfrak{p}_n$. We know by version 1 that $I \nsubseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_v$. If so, $I \subseteq \mathfrak{p}_k$ for some $k \leqslant v$ and therefore $(x) + I \subseteq \mathfrak{p}_k$, a contradiction.

Choose $i_0 \in I \smallsetminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_v)$ and $r \in (\mathfrak{p}_{v+1} \cap \cdots \cap \mathfrak{p}_n) \smallsetminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_v)$ (This is possible since $\mathfrak{p}_{v+1} \cap \cdots \cap \mathfrak{p}_n \nsubseteq \mathfrak{p}_i$, $1 \leqslant i \leqslant v$). Then $x + r i_0 \in x + I$ and $x + r i_0 \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. $\qquad\square$

Example 25. Let $R = \mathbb{Z}_2[x, y]/(x, y)^2$. Then $(x, y)R \subseteq xR \cup yR \cup (x+y)R$ but $(x, y)R$ is not contained in any of them.

Proof. Every element in $(x, y)R$ can be represented by an element of the form $\alpha x + \beta y + (x, y)^2$ where $\alpha, \beta \in \mathbb{Z}_2$. Thus there are only 4 elements in $(x, y)R$; namely $x + y, x, y$, and 0. $\qquad\square$

Example 26. Let k be a field and $R = k[x]$ a polynomial ring in one variable. For an irreducible polynomial $f(x)$, $\mathfrak{p} = (f(x))$ is prime and $\sqrt{(f^n(x))} = \mathfrak{p}$.

Example 27. Consider the integers $\mathbb{Z}$. For $n > 0$, $\sqrt{(n)} = \bigcap_{(p) \supseteq (n)}(p) = \bigcap_{p|n}(p) = \prod_{p|n}(p)$. (Chinese remainder theorem)

Example 28. Let k be a field and $R = k[x]$ be a polynomial ring in one variable. Consider the ideal $I = (x^2, xy, y^2)$ of R. Then $\sqrt{I} = (x, y)$.

Example 29. Let $R = k[a, b, c, d]$ be a polynomial ring over in four variables over the field k. Consider the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \left(A^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} \right).$$

Let $I = (a^2 + bc, ab + bd, ac + cd, bc + d^2)$. Then $\sqrt{I} = (\det(A), \text{trace}(A))$.

Proof. We will first show that $(\det(A), \text{trace}(A)) \subseteq \sqrt{I}$. By proposition 5 it is enough to show that if homomorphism $\phi : R \to k$ such that $\phi(I) = 0$ then $\phi(\det(A)) = \phi(\text{trace}(A)) = 0$. Apply ϕ to the matrix A and let $\alpha, \beta, \gamma, \delta$ be the images of a, b, c, d respectively. Further let $M = \phi(A)$. Since $\phi(I) = 0$ we have that $M^2 = 0$. The characteristic polynomial is $T^2 - \text{trace}(M)T + \det(M) \cdot I$. So $m_M(T) = T^2$ and therefore $C_m(T)$ is also T^2. This implies that $\text{trace}(M) = \det(M) = 0$. So $\text{trace}(M) = \phi(\text{trace}(A))$, $\det(M) = \phi(\det(A))$.

To see the reverse inclusion, it is enough to show $I \subseteq (\text{trace}(A), \det(A))$ and $(\text{trace}(A), \det(A))$ is prime. $\qquad\square$

Example 30.

(1) (General set up) Let $R = k[x_1, \ldots, x_n]$, $S = k[t_1, \ldots, t_n]$ be polynomial rings over the field k. In general, a homomorphism ϕ can be defined from R to S by sending x_i to $f_i(t_1, \ldots, t_m)$ in S. This extends to a surjective homomorphism ϕ' from R to $k[f_1, \ldots, f_n]$ via $\phi(g(x_1, \ldots, x_n)) = g(f_1, \ldots, f_n)$. Notice that $k[f_1, \ldots, f_n]$ is a subring of S. So the kernel of ϕ' is a prime ideal in R. I.e. $\ker(\phi) = \{g(x_1, \ldots, x_n) \mid g(f_1, \ldots, f_n) = 0\}$.

(2) Let $\phi : k[x, y] \to k[t]$ defined by $x \mapsto t^2$ and $y \mapsto t^3$. The kernel of ϕ is $\{g(x, y) \mid g(t^2, t^3) = 0\}$. This is a prime ideal, say $\ker(\phi) = \mathfrak{p}$. Notice $x^3 - y^2 \in \ker \phi$.

   Claim. $\ker(\phi) = (x^3 - y^2)$

Let $R' = k[x,y]/(x^3 - y^2)$. Since $(x^3 - y^2) \subseteq \mathfrak{p}$ we have an induced homomorphism $\phi' : R' \to k[t^2, t^3]$. Consider the commutative diagram

where f is an isomorphism by proposition 1. Since $(x^3 - y^2) \subseteq \mathfrak{p}$, ϕ' is surjective.

Remark. If $\phi : V \to W$ is a homomorphism of vector spaces, and $\{v_i\}$ span V and if $\{\phi(v_i)\}$ are a basis for W, then ϕ is an isomorphism.

Proof. Clearly ϕ is onto since $\{\phi(v_i)\}$ are a basis. If $\phi(\sum \alpha_i v_i) = 0$ then $\sum \alpha_i \phi(v_i) = 0$ and thus $\alpha_i = 0$ for all i. That is, ϕ is one-to-one. $\square$

Given the remark, consider the vector space basis for R' and S. Notice that

$$S = k + kt^2 + kt^3 + kt^4 + kt^5 + \cdots$$

and $k[x,y]$ has a k-basis $\{x^i y^j\}_{i,j \geqslant 0}$. In R', $\{x^i y^j\}_{i,j \geqslant 0}$ are a generating set. Since $x^3 = y^2$ we can refine this generating set to $\{x^i, x^i y\}_{i \geqslant 0}$. Note that $\phi'(x^i) = t^{2i}$ and $\phi'(x^i y) = t^{2i+3}$ for $i \geqslant 0$. So under ϕ', $\{\phi'(x^i), \phi'(x^i y)\}$ is a k-basis of S. So the above remark shows ϕ' is an isomorphism. In particular, $\ker(\phi') = 0 + (x^3 - y^2)$ and thus $\ker(\phi) = (x^3 - y^2)$.

(3) Consider the map ϕ from $k[x,y,z]$ to $S = k[t^3, t^4, t^5]$ defined by $x \mapsto t^3$, $y \mapsto t^4$, and $z \mapsto t^5$. We have that ϕ is onto, but what is the kernel? Notice that the expressions $y^2 - xz, x^3 - yz, z^2 - x^2 y \in \ker(\phi)$.

Claim. The ideal $I = (y^2 - xz, x^3 - yz, z^2 - x^2 y)$ is the kernel of ϕ.

Let $R = k[x,y,z]/I$. A k-basis for S is $\{t^i\}_{i \geqslant 3, i=0}$. A k-generating set of R is $\{x^i y^j z^k\}_{i,j,k \geqslant 0}$. But we can refine this to $\{x^i, x^i y, x^i z\}_{i \geqslant 0}$. Apply ϕ to get the set

$$\{\phi(x^i) = t^3 i, \phi(x^i y) = t^{3i+4}, \phi(x^i z) = t^{3i+5}\}.$$

This is a k-basis of S. So ϕ is an isomorphism and $I = \ker(\phi)$.

(4) In general, if $a, b, c \in \mathbb{Z}^+$ such that $(a, b, c) = 1$ then if we map $k[x,y,z]$ into $k[t^a, t^b, t^c]$ via the map ϕ, then the kernel of ϕ is always (minimally) generated by the 2 or 3 elements which are exactly the least powers of x, y, z expressible as a product of the other two.

Going back to $k[t^3, t^4, t^5]$, notice that the three generators of the kernel of ϕ are excactly the 2×2 minors of

$$\begin{pmatrix} x & y & z \\ y & x^2 & z \end{pmatrix}$$

up to sign.

5 Unique Factorization Domains

Definition. A (non-zero) non-unit $r \in R$ is said to be *irreducible* if $r \neq ab$ where a and b are non-units. (Note that if u is a unit, $r = u(u^{-1}r)$.)

Remark. In a domain R, a non-unit r is irreducible if and only if (r) is maximal among principal (proper) ideals.

Proof. Suppose r is irreducible and $(r) \subseteq (s)$. Hence s divides r and there exists a t in R such that $st = r$. But then either t is a unit and $(r) = (s)$, or s is a unit and $(s) = R$.

Conversely, if (r) is maximal among proper principal ideals and $r = ab$, then since $(r) \subseteq (a)$ either $(a) = R$ (a is a unit) or $(r) = (a)$. In the latter case, r divides a as well. So, $rs = a$ for some s in R and thus $rsb = r$. Therefore $r(1 - sb) = 0$. Since R is a domain and $r \neq 0$, then $1 = sb$. $\square$

Definition. A ring R is a *unique factorization domain* (UFD, factorial in french) if R is a domain and

(1) For all irreducible elements $r \in R$, (r) is prime, and

(2) Any non-zero, non-unit r is a product of Irreducible elements.

Theorem 9. *Let R be an UFD. Then every element $r \in R$ which is non-zero and not a unit is uniquely a product*

$$r = a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$$

where $a_1, a_2, \ldots, a_k$ are irreducible elements, and $(a_i) \neq (a_j)$ for $i \neq j$ up to rearrangements and units.

Proof. First show uniqueness: Suppose

$$r = a_1^{n_1} \cdots a_k^{n_k} = b_1^{m_1} \cdots b_l^{m_l}$$

b_i irreducible, $(b_i) \neq (b_j)$ for $i \neq j$. By induction, it suffices to prove $(b_i) = (a_j)$ for some i, j. Then $b_i = a_j u$ for some u a unit. We cancel b_i and a_j up to units and the induction follows.

But

$$b_1 \mid a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$$

so,

$$a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \in (b_1).$$

But (b_1) is prime, so there exists and i, $1 \leqslant i \leqslant k$ such that $a_i \in (b_1)$. This implies $(a_i) \subseteq (b_1)$. But a_i is irreducible and thus $(a_i) = (b_1)$ by remark 5.

What is left is to prove existence: This is given by part (2) of the definition of UFD. $\qquad\square$

Definition. An element $e \in R$ is *idempotent* if $e^2 = e$.

Remark (See Atiyah, p. 20). For an idempotent e in R, $1 = e + (1-e)$, and $e^2 = e$ if and only if $e(1-e) = 0$. Further,

$$R \simeq Re \times R(1-e)$$

where Re has identity e and $R(1-e)$ has identity $(1-e)$.

Definition. A domain R is a *principal ideal domain* (PID) if every ideal is principal.

Example 31. $\mathbb{Z}$, $k[x]$, k a field.

Theorem 10. *If a ring R is a PID then it is also a UFD.*

To prove this theorem, we need to prove the following

(A) If a is irreducible then (a) is prime.

(B) Every element factors into irreducible factors.

But first some lemmas.

Lemma 11. *If R is a PID, then every ascending chain of ideals stabilizes. (Such a ring is said to be Noetherian.)*

Proof. Suppose

$$I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_i \subsetneqq \cdots$$

is an infinite ascending chain. We can write $I_i = (a_i)$. Let

$$I = \bigcup_{i=1}^{\infty} I_i.$$

This is an ideal. Therefore there exists $a \in R$ such that $(a) = I$. But then there exists an i such that $a \in I_i$. Then for all $j \geqslant i$

$$(a_i) \subsetneqq (a_j) \subseteq I = (a) \subseteq (a_i),$$

a contradiction. $\qquad\square$

Lemma 12. *Let R be a PID. The following are equivalent:*

(1) The element a is irreducible.

(2) The ideal (a) is maximal.

Proof. This is clear from remark 5. □

Now we are ready to prove the theorem.

Proof of Theorem 10. (A) is a consequence of lemma 12, since maximal ideals are prime. For (B) let $a \in R$, a is non-unit, non-zero. There exits a maximal ideal $\mathfrak{m}$ containing a. Since R is a PID, $\mathfrak{m} = (a_1)$, a_1 is irreducible by lemma 12. So, $a = a_1 b_1$. If b_1 is a unit, done. If not, $(a) \subsetneq (b_1)$. Repeat with b_1 in place of a.

There exists an irreducible a_2 such that $b_1 = a_2 b_2$. Therefore

$$(a) \subsetneq (b_1) \subsetneq (b_2)$$

If b_2 is a unit then $a = a_1 a_2 b_2$. If not, continue. By lemma 11, this chain stops and we have our factorization. □

Chapter 2

Modules

1 Notation and Examples

For a commutative ring R, an abelian group $(M, +)$ is an R-*module* if there exists a map $R \times M \to M$ defined by $(r, m) \mapsto rm$ satisfying the following properties for all $r, s \in R$ and $m, n \in M$:

   (i) $1 \cdot m = m$

   (ii) $(r + s)m = rm + sm$

   (iii) $r(m + n) = rm + rn$

   (iv) $(rs)m = r(sm)$

Example 32. Let $R = \mathbb{Z}$. A $\mathbb{Z}$-module is an abelian group.

Proof. Let M be a $\mathbb{Z}$-module and $n \in \mathbb{Z}$, $m \in M$. Property (ii) and (iv) force that

$$
n \cdot m =
\begin{cases}
\overbrace{m + \cdots + m}^{n-\text{times}} & \text{if } n > 0 \\
0 & \text{if } n = 0 \\
\underbrace{(-m) + \cdots + (-m)}_{|n|-\text{times}} & \text{if } n < 0
\end{cases}
$$

This action forces (i) and (iii) to hold. $\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Example 33. If $R = k$ a field, then modules are exactly vector spaces over k.

Example 34. If $f : R \to S$ is a ring homomorphism, then

   (a) S is an R-module;

   (b) any S-module is an R-module.

In particular, R is a module over itself with respect to the usual multiplication.

Proof. For (a), if $r \in R$ and $s \in S$, define $rs = f(r)s$. Similarly for (b), if $r \in R$ and $m \in M$, for M an S-module, define $r \cdot m = f(r)m$. The R-module M is said to be obtained from the S-module M by *restriction of scalars*. $\square$

Example 35. Let k be a field and $R = k[t]$ a polynomial ring with indeterminate t. Let V be an R-module. By examples 33 and 34, V is a vector space over k. But this vector space comes with an action of t on V. That is,

$$t : V \to V$$
$$v \mapsto t \cdot v.$$

Note by example 33, for any $v_1, v_2 \in V$,

$$t(v_1 + v_2) = tv_1 + tv_2.$$

By example 34, if $\alpha \in k$ and $v \in V$,

$$t(\alpha v) = (t\alpha)v = \alpha(tv).$$

Therefore, t is an endomorphism from V to V; i.e. a linear transformation.

The definition of a module force that if $p(t) = \alpha_0 + \alpha_1 t + \cdot + \alpha_n t^n$, then

$$p(t) \cdot v = \alpha_0 v + \alpha_1(tv) + \cdot + \alpha_n(t^n v).$$

The converse also holds: given a vector space V and a linear transformation $T : V \to V$ we can make V into a $k[t]$-module by $tv = T(v)$ for all $v \in V$.

Example 36. If $R = k[t_1, \ldots, t_n]$ is a polynomial ring over a field with n variables, then an R-module M is a vector space V with n linear transformations $T_1, \ldots, T_n$ which commute.

Example 37. Suppose $\{M_i\}$ are R-modules. We define the *direct sum* of a module as

$$\bigoplus_i M_i = \{(m_i) \mid m_i \in M_i, \text{ all but finitely many } m_i = 0\}.$$

This is an R-module. The *direct product* is defined as

$$\prod_i M_i = \{(m_i) \mid m_i \in M_i\}.$$

When the index set is finite, the notions of direct sum and direct product coincide.

2 Submodules and Maps

Definition. If M, N are R-modules, then an *R-homomorphism* $\phi : M \to N$ is an homomorphism of abelian groups such that $\phi(rm) = r\phi(m)$ for all $r \in R$. An R-homomorphism is an *isomorphism* if it is surjective and injective. As with rings, the kernel of an R-homomorphism is the set of all elements that get mapped to zero.

Example 38. Let M, N be R-modules. Define $\mathrm{Hom}_R(M, N)$ to be the set of R-homomorphisms from M to N. This becomes an R-module with addition and multiplication defined as follows: for any f, g in $\mathrm{Hom}_R(M, N)$, $r \in R$,

$$(f + g)(m) := f(m) + g(m)$$

$$(r \cdot f)(m) := rf(m)$$

Note. If k is a field, $V \simeq k^n$, $\mathrm{Hom}_k(V, V) \simeq M_n(k)$ where $M_n(k)$ is the set of $n \times n$ matrices with elements from k.

Definition. An R-module F is a *free module* if $F \simeq \bigoplus_i R_i$ where $R_i \simeq R$. In other words, F is free if it has a basis.

Example 39. Every vector space V over a field k is free. Choose a basis $\{v_i\}$ of V. Then $V \simeq \bigoplus_i kv_i$, $kv_i \simeq k$.

Definition. Suppose that M is an R-module. We say that $\{x_i\}_{i \in I}$, $x_i \in M$, *generate* M if for all $x \in M$ there exists an equality (not necessarily unique)

$$x = \sum_i r_i x_i$$

such that $r_i \in R$ and all but finitely many r_i are zero. The R-module M is said to be *finitely generated* if I is a finite set. I.e., there exists $x_1, \ldots, x_k \in M$ such that $M = \{r_1 x_1 + \cdots + r_k x_k \mid r_i \in R\} = Rx_1 + \cdots + Rx_k = \langle x_1, \ldots, x_k \rangle$.

Remark. Let M be an R-module with a generating set $\{x_i\}_{i \in I}$. In this case, let $F \simeq \bigoplus_i R_i$ where $R_i \simeq R$. Consider the elements $e_i = (0, 0, \ldots, 1, 0, \ldots) \in F$, where the one is is the ith position. There exists a homomorphism $F \to M$ defined by $e_i \mapsto x_i$. Thus

$$(r_1, r_2, \ldots) \mapsto \sum_i r_i x_i \in M.$$

This is a surjective map and well defined since F is free.

Submodules and Quotient Modules   If M is an R-module, a *submodule* N of M is a subgroup $N \subseteq M$ such that the restricted operations make N an R-module. If N is a submodule of M, we can define a *quotient module*, denoted M/N as follows: the group structure is as a quotient group and $r(m + N) = rm + N$. For instance, if $M = R$, then the submodules are exactly the ideals.

Example 40. Kernels and images of homomorphisms are submodules of their respective modules, e.g. if $N \subseteq M$, the natural projection $\pi : M \to M/N$ defined by $x \mapsto x + N$ is an homomorphism with $\ker(\pi) = N$ and $\mathrm{im}(\pi) = M/N$.

The next three theorems are generalized versions of proposition 1 and theorem 2. They are stated without proof.

Theorem 13 (Isomorphism Theorem). *Let R be a ring and $f : M \to N$ an R-homomorphism. Set $K = \ker(f)$. Then f factors as a surjection followed by an injection as in the following commutative diagram:*

$$
\begin{array}{ccc}
M & \xrightarrow{\ f\ } & N \\
{\scriptstyle \pi}\big\downarrow & \nearrow{\scriptstyle g} & \\
M/K & &
\end{array}
$$

In particular, if f is onto, then g is an isomorphism.

Theorem 14. *Let R be a ring and $N \subseteq M$ be R-modules. Then there exists a one-to-one inclusion preserving correspondence between submodules of M/N and submodules of $K \subseteq M$ such that $N \subseteq K$:*

$$K \longleftrightarrow K/N.$$

Theorem 15. *Let $N \subseteq K \subseteq M$ be R-modules. Define $\overline{M} := M/N$ and $\overline{K} := K/N \subseteq \overline{M}$. Then*

$$M/K \simeq \overline{M}/\overline{K}.$$

Definition. If $N, K \subseteq M$ are R-submodules and $I \subseteq R$, then we define

$$
IM = \left\{ \sum_j i_j m_j \mid i_j \in I, m_j \in M \right\} \subseteq M
$$

$$N + K = \{ n + k \mid n \in N, k \in K \}$$

Remark. The objects IM and $N + K$ in definition 2 are submodules of the R-module M. Further, $N + K$ is the smallest submodule of M containing N and K.

Theorem 16 (Diamond Isomorphism). *If $N, K \subseteq M$ are R-submodules, then there is an isomorphism theorem:*

$$\frac{N + K}{N} \simeq \frac{K}{K \cap N}.$$

Proof. Let f be the composition map from K to $N + K/N$

$$
K \hookrightarrow N + K \xrightarrow{\ \pi\ } N + K/N
$$
$$
\underset{f}{\searrow\nearrow}
$$

defined by $k \mapsto k + N$. Notice that f is surjective and by theorem 13 we have that

$$K/\ker(f) \simeq N + K/N.$$

Finally

$$\ker(f) = \{k \in K : f(k) = 0\} = \{k \in K : k + N = N\} = K \cap N.$$

$\square$

Lemma 17. *Let R be a ring and M an R-module. Then $\mathrm{Hom}_R(R, M) \simeq M$.*

Proof. Define a homomorphism $\Phi : \mathrm{Hom}_R(R, M) \to M$ by $\Phi(\phi) = \phi(1)$. Check that Φ is an isomorphism. $\square$

Remark. From the lemma we know that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}) \simeq \mathbb{Q}$. Let $\phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ be a non-zero $\mathbb{Z}$-homomorphism, so that there exists $\alpha \in \mathbb{Q}$ such that $\phi(\alpha) \neq 0$. Without loosing generality, say $\phi(\alpha) = n$, with $n > 0$. So,

$$n = \phi(\alpha) = \phi(m \cdot \frac{1}{m} \cdot \alpha) = m \cdot \phi(\frac{1}{m}\alpha) \in \mathbb{Z}.$$

Since m is arbitrary, we have arrived at a contradiction. Hence $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$.

3   Tensor Products

Definition. Let M, N, P be R-modules. An R-*bilinear map* $f : M \times N \to P$ defined by $(m, n) \mapsto f(m, n)$ is a map such that

(i) If we fix $x \in M$ and then define $f_x : N \to P$ by $x \mapsto f(x, n)$, then f_x is an R-module homomorphism.

(ii) Similarly, fixing $y \in N$ and defining $f_y : N \to P$ by $m \mapsto f(m, y)$ is an R-module homomorphism.

Theorem 18. *Given R-modules M, N, there exists an R-module T and a bilinear map $g : M \times N \to T$ such that*

(i) *Given any other R-module P and bilinear map $f : M \times N \to P$, there exists a unique R-module homomorphism $\alpha : T \to P$ such that*

is a commutative diagram.

(ii) *Further, T and g are unique in the following sense: If T', g' is another pair satisfying (i), then there exists an isomorphism i such that*



is a commutative diagram as well.

Definition. The R-module T in the above theorem is called the *tensor product* of M and N (over R) and is written $T = M \otimes_R N$.

Proof. For (i), let F be a free module $\bigoplus R_{(m,n)}$ with $m \in M$, $n \in N$ and $R_{(m,n)} \simeq R$. Denote the element with a 1 in the $(m,n)^{th}$ slot and 0 elsewhere by $[m,n]$. Hence $F = \bigoplus R[m,n]$.

Let C be the R-submodule of F generated by all elements of the following form: $m_i \in M$, $n_i \in N$, $r \in R$.

(1) $[m_1 + m_2, n] - [m_1, n] - [m_2, n]$

(2) $[rm, n] - r[m, n]$

(3) $[m, n_1 + n_2] - [m, n_1] - [m, n_2]$

(4) $[m, rn] - r[m, n]$

Set $T = F/C$ and define the map $g : M \times N \to T$ by $(m, n) \mapsto [m, n] + C$. g is clearly bilinear. Define $[m, n] + C$ by $m \otimes n$. Now let P be an R-module and $f : M \times N \to P$ be a bilinear map.

$$M \times N \xrightarrow{\ \ g\ \ } T$$
$$\searrow_{f} \quad$$
$$P$$
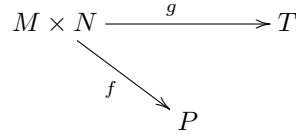
Note that T is generated as an R-module by elements $m \otimes n$ since F is generated as an R-module by $[m, n]$.

A typical element in T looks like $\sum_i m_i \otimes n_i$, not $m \otimes n$. $(r_i(m_i \otimes n_i) = r_i m_i \otimes n_i = m_i' \otimes n_i)$

We have no choice for α: $\alpha(m \otimes n) = f(m, n)$ is forced, and then to make this a homomorphism, we must set $\alpha(\sum m_i \otimes n_i) = \sum f(m_i, n_i)$. To see α is well-defined, first observe the map $F \xrightarrow{\Phi} P : [m, n] \mapsto f(m, n)$ gives an R-module homomorphism. To see α is well-defined, it suffices to prove $\Phi(C) = 0$. Then Φ induces a well-defined homomorphism

$$T/C \to P \ : \ t + C \mapsto \Phi(t) \ (m \otimes n \mapsto f(m, n)).$$
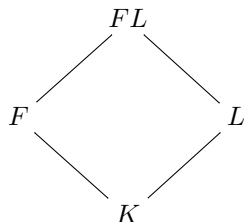
It's enough to prove Φ sends the specified generators of C to zero, and it does.

For (ii), if T, g and T', g' are two such tensor products, then by

$$M \times N \xrightarrow{\ \ g\ \ } T$$
$$\searrow_{g'} \quad \exists! \ \alpha \ \nearrow \ \uparrow_{\beta}$$
$$T'$$
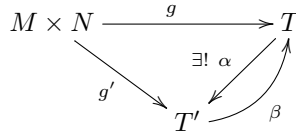
it is easy to check $\alpha \circ \beta = 1_{T'}$ and $\beta \circ \alpha = 1_T$. $\qquad\square$

Example 41. Let F and L be two field extensions of a field K, and let FL be their compositum, so that we have a diagram of fields

$$
\begin{array}{ccc}
 & FL & \\
\diagup & & \diagdown \\
F & & L \\
\diagdown & & \diagup \\
 & K &
\end{array}
$$

There exists a K-bilinear map from $F \times L \to FL$ and therefore there exists a K-homomorphism $F \otimes_K L \to FL$. This is an isomorphism if and only if one of the two equivalent conditions hold.

(1) Every set $\{x_i\}$ of elements in F which are linearly independent over K are linearly independent over L.

(2) Every set $\{y_j\}$ of elements in L which are linearly independent over K are linearly independent over F.

Exact Sequences

Definition. A sequence of modules and homomorphisms

$$\cdots \longrightarrow M_{i_1} \xrightarrow{\phi_{i+1}} M_i \xrightarrow{\phi_i} M_{i-1} \longrightarrow \cdots$$

is said to be *exact* if for all i, $\ker(\phi_i) = \mathrm{im}(\phi_{i+1})$. It is said to be a *complex* if $\mathrm{im}(\phi_{i+1}) \subseteq \ker(\phi_i)$, equivalently, $\phi_i \circ \phi_{i+1} = 0$. A *short exact sequence* (s.e.s.) is a sequence

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

which is exact. This means

(1) α is injective, i.e. $\ker(\alpha) = 0$.

(2) β is surjective, i.e. $\mathrm{im}(\beta) = C$.

(3) $\ker(\beta) = \mathrm{im}(\alpha)$

Example 42. Given R-modules $N \subseteq M$,

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$$

is a s.e.s.

Proposition 19. *Let R be a ring and M, N, Q, M_i, N_i be R-modules. Also let I be an ideal in R.*

(1) $M \otimes N \simeq N \otimes M$

(2) $(M \otimes N) \otimes Q \simeq M \otimes (N \otimes Q)$

(3) $R/I \otimes M \simeq M/IM$

(4) $(\bigoplus_i M_i) \otimes N \simeq \bigoplus_i (M_i \otimes N)$

(5) *If K is a field, V, W vector spaces, $\{v_i\}$ a basis of V and $\{w_j\}$ a basis of W, then $\{v_i \otimes w_j\}$ are a basis of $V \otimes_K W$. In particular,*

$$\dim_K(V \otimes_K W) = (\dim_K V)(dim_K W).$$

(6) *If $IM = IN = 0$, then M and N are R/I modules and $M \otimes_{R/I} N \simeq M \otimes_R N$.*

(7) *IF $\phi : M \to N$ is a homomorphism, then there exists an induced homomorphism $\phi \otimes 1 : M \otimes Q \to N \otimes Q$ by $(\phi \otimes 1)(m \otimes q) = \phi(m) \otimes q$.*

(8) *If $M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$ is exact, then*

$$M_1 \otimes N \xrightarrow{\alpha \otimes 1} M_2 \otimes N \xrightarrow{\beta \otimes 1} M_3 \otimes N \longrightarrow 0$$

is exact (right exactness).

(9) *Hom, $\bigotimes$ adjointness*

$$\mathrm{Hom}_R(M \otimes_R N, Q) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, Q))$$

Proof. (1) Notice the bilinear map $M \times N \to T$ is exactly the same as the bilinear map $N \times M \to T$ by "flipping". So both $M \otimes N$ and $N \otimes M$ solve the same universal problem. $M \otimes N \simeq N \otimes M$ where $m \otimes n \mapsto n \otimes m$.

(2) Exercise.

(3) We will show that M/IM has the correct universal property. Denote cosets in R/I by $\_$ and define the map $R/I \times M \to M/IM$ by $(\overline{r}, m) \mapsto \overline{rm}$. This is well-defined: $\overline{r} = \overline{s} \Leftrightarrow r - s \in I \Rightarrow (r - s)m \in IM \Rightarrow \overline{rm} = \overline{sm}$ in M/IM.

It is bilinear, e.g. $(\overline{r} + \overline{s}, \overline{m}) \mapsto \overline{(r + s)m} = \overline{rm} + \overline{sm}$.

Does there exist a unique R-module homomorphism h such that

commutes? Define $\alpha : M \to Q$ by $\alpha(m) = g(\overline{1}, m)$. This is a R-module homomorphism by the bilinearity of g.

Remark. In general, if $h : M \to N$ is an R-module homomorphism and if $I \cdot h(M) = 0$, for I an ideal in R, then there exists an induced homomorphism $\overline{h}$ such that the following diagram commutes.

$$
\begin{array}{ccc}
M & \xrightarrow{\quad h \quad} & N \\
& \searrow_{\pi} \quad \nearrow_{\overline{h}} & \\
& M/IM &
\end{array}
$$

Claim. $I \cdot \alpha(M) = 0$

To see this, let $m \in M$ and $\alpha(m) = g(\overline{1}, m)$. For $i \in I$,

$$i \cdot \alpha(m) = i \cdot g(\overline{1}, m) = g(i \cdot \overline{1}, m) = g(\overline{i}, m) = g(\overline{0}, m) = 0.$$

Hence there exists an induced R-module homomorphism $\overline{\alpha} : M/IM \to Q$. Further we have that

$$g(\overline{r}, m) = r \cdot g(\overline{1}, m) = r \cdot \alpha(m) = r \cdot \overline{\alpha}(\overline{m}) = \overline{\alpha}(\overline{rm}).$$

So the diagram commutes for any bilinear map g, that is, $M/IM \simeq R/I \otimes_R M$.

(4) Exercise.

(5) Note, in general, that using (4) and induction, if F is the free module $\sum Rv_i$ and $G = \sum Rw_i$ then $F \otimes_R G = \sum_{i,j} R(v_i \otimes w_j)$. Using (3) with $I = 0$, we see that $R \otimes_R N \simeq N$. e.g.

$$R^2 \otimes R^2 = (R \oplus R) \otimes R^2 \simeq (R \otimes R^2) \oplus (R \otimes R^2) \simeq R^2 \oplus R^2 \simeq R^4.$$

Now apply this to vector spaces which are free k-modules to get (5).

(6) Exercise.

(7) Exercise.

(8) As an R-module, $M_3 \otimes_R N$ is generated by "decomposable" tensors, $m \otimes n$, $m \in M_3$, $n \in N$. But there exists an $x \in M_2$ such that $\beta(x) = m$ and so $(\beta \otimes 1)(x \otimes n) = m \otimes n$ and thus $\beta \otimes 1$ is onto. Note that $\ker(\beta \otimes 1) \supseteq \operatorname{im}(\alpha \otimes 1)$. For let $x \in M_1$, $n \in N$;

$$(\beta \otimes 1)((\alpha \otimes 1)(x \otimes n)) = \beta\alpha(x) \otimes n = 0 \otimes n = 0.$$

Therefore, there exists an induced map

$$\frac{M_2 \otimes N}{\operatorname{im}(\alpha \otimes 1)} \xrightarrow{\overline{\beta \otimes 1}} M_3 \otimes N \longrightarrow 0.$$

It is enough to show $\overline{\beta \otimes 1}$ is an isomorphism. We will construct $h : M_3 \otimes N \to M_2 \otimes N/\operatorname{im}(\alpha \otimes 1)$ such that $(\overline{\beta \otimes 1}) \circ h = h \circ (\overline{\beta \otimes 1}) = \operatorname{id}$. Consider the R-bilinear map

$$g : M_3 \times N \longrightarrow \frac{M_2 \otimes N}{\operatorname{im}(\alpha \otimes 1)}.$$

Let $x \in M_3$, $n \in N$ and define $g(x, n) = \overline{y \otimes n}$ in $\overline{M_2 \otimes N}$ where $\beta(y) = x$. We want to prove that g is well defined, i.e. if $\beta(y) = x = \beta(z)$, then for $n \in N$

$$y \otimes n + \operatorname{im}(\alpha \otimes 1) = z \otimes n + \operatorname{im}(\alpha \otimes 1).$$

This can be restated as $(y - z) \otimes n = y \otimes n - z \otimes n \in \operatorname{im}(\alpha \otimes 1)$. However $\beta(y - z) = \beta(y) - \beta(z) = x - x = 0$. So there exists $u \in M_1$ such that $\alpha(u) = y - z$. Then $(y - z) \otimes n = \alpha(u) \otimes n = (\alpha \otimes 1)(u \otimes n) \in \operatorname{im}(\alpha \otimes 1)$, and therefore g is well defined. Then g induces a R-homomorphism

$$h : M_3 \otimes N \longrightarrow \frac{M_2 \otimes N}{\operatorname{im}(\alpha \otimes 1)}$$

$$x \otimes n \longmapsto g(x, n)$$

Now let $x \in M_3$, $n \in N$. If we compute $(\overline{\beta \otimes 1})(h(x \otimes n))$ where $\beta(y) = x$, we have

$$\begin{aligned}(\overline{\beta \otimes 1})(h(x \otimes n)) &= (\overline{\beta \otimes 1})(y \otimes n) \\ &= \beta(y) \otimes n \\ &= x \otimes n,\end{aligned}$$

so that $(\overline{\beta \otimes 1})h = \operatorname{id}$. Conversely

$$\begin{aligned}h((\overline{\beta \otimes 1})(y \otimes n)) &= h(\beta(y) \otimes n) \\ &= y \otimes n,\end{aligned}$$

and therefore $\overline{\beta \otimes 1}$ is an isomorphism, that is $\operatorname{im}(\alpha \otimes 1) = \ker(\beta \otimes 1)$ and the sequence is exact.

Example 43. For $x \in R$, x is said to be a *non-zero divisor* if the map from R to R defined by $r \mapsto rx$ is one-to-one. (i.e. $rx = 0 \Rightarrow r = 0$) Let $x \in R$ be a non-zero divisor. Then

$$0 \longrightarrow R \xrightarrow{x} R \longrightarrow R/Rx \longrightarrow 0$$

is an exact sequence. Now let M be an R-module. So

$$R \otimes_R M \xrightarrow{x} R \otimes_R M \longrightarrow R/xR \otimes_R M \longrightarrow 0,$$

that is

$$M \xrightarrow{x} M \longrightarrow M/xM \longrightarrow 0,$$

is exact. Notice that if x is also a non-zerodivisor on M, then

$$0 \longrightarrow M \xrightarrow{x} M \longrightarrow M/xM \longrightarrow 0$$

is also exact.

Remark. The map $M \xrightarrow{x} M$ being one-to-one is equivalent to x being a non-zero divisor of M. In fact, explicitly, this means $xm = 0 \Rightarrow m = 0$ for $m \in M$. For example, if $M = R/Rx$ then

$$R/xR \xrightarrow{x} R/xR$$

is the zero map, hence not one-to-one.

Remark. Since $M \otimes N \simeq N \otimes M$, $\mathrm{Hom}_R(M \otimes N, Q) \simeq \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, Q))$. (9) Homomorphisms from $M \otimes N$ to Q correspond to bilinear maps from $M \times N$ to Q. A bilinear map from $M \times N$ to Q is a linear map from M to $\mathrm{Hom}_R(N, Q)$. That is exactly an element of $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, Q))$. $\qquad\square$

4 Operations on Modules

Definition. In analogy with the colon operation defined for ideals, given an ideal $I \subseteq R$ and R-modules $N \subseteq M$ we define the R-submodule

$$N :_M I = \{m \in M : mI \subseteq N\} \subseteq M.$$

Similarly, given $N, L \subseteq M$ two R-submodules we can define the ideal

$$N :_R L = \{r \in R : rL \subseteq N\} \subseteq R.$$

In particular, if $N = 0 \subseteq M$ and $L = M$ we define the *annihilator* of M as

$$\mathrm{ann}(M) = 0 :_R M = \{r \in R : rM = 0\} \subseteq R.$$

Definition. If M is an R-module, M is said to be *flat* if whenever

$$0 \longrightarrow N_1 \xrightarrow{\alpha} N_2 \xrightarrow{\beta} N_3 \longrightarrow 0$$

is a short exact sequence of R-modules, then

$$0 \longrightarrow N_1 \otimes M \xrightarrow{\alpha \otimes 1} N_2 \otimes M \xrightarrow{\beta \otimes 1} N_3 \otimes M \longrightarrow 0$$

is also exact; equivalently, $\alpha \otimes 1$ is one-to-one. If $f : A \to B$ is a homomorphism of rings, we say f is *flat homomorphism* if B is a is a flat A-module (B is an A-module via f: $a \cdot b = f(a) \cdot b$).

Example 44. Any free module is flat.

Remark. M is finitely generated if and only if there exists a free module R^k mapping onto M.

Proof. If M is finitely generated and $R^k \xrightarrow{\phi} M \longrightarrow 0$, $\phi(e_i) = x_i$, then $\ker(\phi)$ is a submodule of R^k and $\ker(\phi) = \{(r_1, \ldots, r_k) \in R^k \mid \sum_i r_i x_i = 0\}$ where

$$0 \longrightarrow \ker(\phi) \longrightarrow R^k \xrightarrow{\phi} M \longrightarrow 0.$$

$\qquad\square$

Note. Elements in the kernel of ϕ are called *syzygies*.

Theorem 20 (Nakayama's Lemma, NAK)**.** *Let R be a ring, $I \subseteq R$ and M a finitely generated R-module. If $IM = M$, then there exists $x \in I$ such that $(1 + x)M = 0$.*

Remark. If there exists an $x \in I$ such that $(1 + x)M = 0$ then for all $u \in M$, $u = -xu \in IM$. So $M = IM$.

Proof. Let $M = \langle m_1 \ldots m_k \rangle$. For each $1 \leqslant i \leqslant k$, we can write

$$m_i = \sum_j x_{ij} u_j \quad u_j \in M, x_{ij} \in I.$$

But since M is finitely generated, we have $u_j = \sum_l r_{jl} m_l$ where $r_{jl} \in R$. Therefore,

$$m_i = \sum_j x_{ij} u_j$$

$$= \sum_j x_{ij} \left(\sum_l r_{jl} m_l \right)$$

$$= \sum_l \left(\sum_j x_{ij} r_{jl} \right) m_l$$

$$= \sum_l y_{il} m_l$$

$$= y_{i1} m_1 + \cdots + y_{ik} m_k$$

where $y_{il} = \sum_j x_{ij} r_{jl}$. Thus we have a system of linear equations

$$\begin{pmatrix} -y_{11} + 1 & -y_{12} & \cdots & -y_{1k} \\ -y_{21} & -y_{22} + 1 & \cdots & -y_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ -y_{k1} & -y_{k2} & \cdots & -y_{kk} + 1 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Recall that for a square matrix A, $\mathrm{adj}(A) \cdot A = \det(A) \cdot I$ where I is the identity matrix. Let A be the above matrix composed of the y_{ik}'s. Hence

$$\mathrm{adj}(A) \cdot A \begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

or, by the recollection,

$$\begin{pmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Thus for $1 \leqslant i \leqslant k$ we have $\det(A) \cdot m_i = 0$. This forces $\det(A) \cdot M = 0$. Now modulo I the matrix A is the identity matrix. Hence $\det(A) \equiv 1 \pmod{I}$, i.e. there exists an $x \in I$ such that $\det(A) = 1 + x$. $\qquad\square$

Corollary 21. *If $I \subseteq \operatorname{jac}(R)$ and M is finitely generated with $IM = M$, then $M = 0$.*

Proof. By NAK, there exists an $x \in I$ such that $(1 + x)M = 0$. So it is enough to show that $1 + x$ is a unit. This is true if and only if $1 + x$ is not in any maximal ideal. But $x \in \bigcap \mathfrak{m}$, $\mathfrak{m}$ maximal, implies $1 + x$ is not in any maximal ideal. $\qquad\square$

Corollary 22. *Suppose that $I \subseteq \operatorname{jac}(R)$. Assume M is an R-module, $N \subseteq M$ and M/N is finitely generated. If $M = N + IM$ then $M = N$.*

Proof. Notice that $I(M/N) = M/N$. Let $u \in M$ and consider $u + N \in M/N$. Write $u = n + y$ for $n \in N$ and $y \in IM$ where $y = \sum a_i y_i$. Then $u + N = y + N = \sum a_i(y_i + N) \in I(M/N)$. Apply NAK to M/N, using the first corollary we get that $M/N = 0$. $\qquad\square$

Chapter 3

Localization

1 Notation and Examples

A subset $W \subseteq R$ is said to me *multiplicatively closed* if $1 \in W$ and for any two elements $w_1, w_2 \in W$, $w_1 w_2 \in W$. Two main examples of this are as follows.

Example 45. If $x \in R$, not nilpotent, then $W = \{x^n\}_{n=0}^{\infty}$ is multiplicatively closed.

Example 46. If $\mathfrak{p} \in \mathrm{Spec}R$ the $W = R \smallsetminus \mathfrak{p}$ is a multiplicatively closed set. In particular, if R is a domain, then $W = R \smallsetminus \{0\}$ is multiplicatively closed as well.

The idea in this chapter is to construct a ring in which all elements of W become units, i.e., solving the following universal problem: If $g : R \to S$ is a ring homomorphism such that $g(w)$ are units in S for all $w \in W$, then there is a unique ring L, and a unique homomorphism h such that the following diagram commutes.

$$
\begin{array}{ccc}
R & \longrightarrow & L \\
& {\scriptstyle g}\searrow & \downarrow {\scriptstyle h} \\
& S &
\end{array}
$$

Construction   For a ring R, M an R-module and W a multiplicatively closed set, consider elements in the set $R \times W$ (respectively $M \times W$). Put an equivalence relation $\sim$ on $R \times W$ by: $(r_1, w_1) \sim (r_2, w_2)$ if and only if there exists a $w \in W$ such that $(r_1 w_2 - r_2 w_1)w = 0$. This does define an equivalence relation: Reflexivity and symmetry are clear. For transitivity, let $(r_1, w_1) \sim (r_2, w_2)$ and $(r_2, w_2) \sim (r_3, w_3)$. Hence there exists a $w, w' \in W$ such that $(r_1 w_2 - r_2 w_1)w = 0$ and $(r_2 w_3 - r_3 w_2)w' = 0$. Notice that $ww'[w_3(r_1 w_2 - r_2 w_1) + w_1(r_2 w_3 - r_3 w_2)] = 0$. Simplifying we find $(r_1 w_3 - r_3 w_1)w_2 ww' = 0$.

We denote the equivalence class or (r, w) by $\frac{r}{w}$ or $w^{-1}r \in R \times W/ \sim$ (similarly, $\frac{m}{w}$). The set of equivalence classes in $R \times W/ \sim$ we will denote $W^{-1}R$ (

or R_W) and similarly, $M \times W/\sim$ denoted $W^{-1}M$. We have to make $W^{-1}R$ a ring by defining

$$\frac{r_1}{w_1} + \frac{r_2}{w_2} := \frac{r_1 w_2 + r_2 w_1}{w_1 w_2}$$

$$\frac{r_1}{w_1} \cdot \frac{r_2}{w_2} := \frac{r_1 r_2}{w_1 w_2}.$$

We make $W^{-1}M$ a module over this ring $W^{-1}R$ by defining

$$\frac{m_1}{w_1} + \frac{m_2}{w_2} := \frac{m_1 w_2 + m_2 w_1}{w_1 w_2}$$

$$\frac{r}{w_1} \cdot \frac{m}{w_2} := \frac{rm}{w_1 w_2}.$$

Exercise 1. Check for the well-defined property then show that $W^{-1}R$ is really a commutative ring and $W^{-1}M$ is really a module over $W^{-1}R$.

Remark. The identity of $W^{-1}R$ is $\frac{1}{1}$ or $\frac{w}{w}$ for all $w \in W$. Also, there exists a ring map (sometimes called the *canonical map*) $R \to W^{-1}R$ defined by $r \mapsto \frac{r}{1}$.

Definition. Let R be a ring and M, R-module and W a multiplicatively closed set. The *localization* of R with respect to W, is the ring $W^{-1}R$. Similarly, the *localization* of M with respect to W is the $W^{-1}R$-module $W^{-1}M$.

Remark. If $W = \{x^n\}_{n=0}^{\infty}$ (see example 45) then we denote $W^{-1}R$ by R_x. Likewise if W is a complement of a prime $\mathfrak{p}$ (see example 46) then we denote $W^{-1}R$ by $R_{\mathfrak{p}}$.

Proposition 23. *The ring $W^{-1}R$ has the following universal property:*

$$R \xrightarrow{\hspace{3cm}} W^{-1}R$$
$$\,_f \searrow \qquad \nearrow\, \exists! g$$
$$S$$

Given a ring homomorphism such $f(w)$ is a unit in S for all $w \in W$, then there exists a unique ring homomorphism $g : W^{-1}R \to S$ making the diagram commute.

Proof. Define $g(\frac{r}{w}) = f(w)^{-1} f(r)$. This is forced since

$$g(r) = g(\frac{w}{1} \cdot \frac{r}{w}) = g(w) \cdot g(\frac{r}{w}),$$

but $g(w) = f(w)$ and $g(r) = f(r)$ are forced. Therefore $f(w)^{-1} f(r) = g(\frac{r}{w})$ is forced.

The reader should check that g really is a ring homomorphism. $\qquad\square$

Remark. Let U, W be multiplicatively closed in R. The set $UW = \{uw \mid u \in U, w \in W\}$ is also multiplicatively closed. (Caution, it could happen that $0 \in UW$). Then

$$(UW)^{-1}R \simeq U^{-1}(W^{-1}R)$$

This can be checked since the right hand side has the same universal property as the left hand side.

Remark. If $0 \in W$ then $W^{-1}R = 0$

Theorem 24. *Let M, N, L be R-modules and W a multiplicatively closed set.*

(1) *If $M \xrightarrow{\alpha} N \xrightarrow{\beta} L$ is an exact sequence, then $M_W \xrightarrow{\alpha_W} N_W \xrightarrow{\beta_W} L_W$ is also an exact sequence of R_W-modules.*

(2) $M \otimes_R R_W \simeq M_W$

Proof. First given $\alpha : M \to N$, define $\alpha_W : M_W \to N_W$ by $\alpha_W(\frac{x}{w}) = \frac{\alpha}{w}$. This is a well-defined R_W-module homomorphism. Let $\frac{n}{w} \in \ker(\beta_W)$ where $n \in N$ and $w \in W$. Since

$$\frac{0}{1} = 0 = \beta_W\left(\frac{n}{w}\right) = \frac{\beta(n)}{w}$$

there exists a $u \in W$ such that $u(0 \cdot w - \beta(n)) = 0$. Hence $un \in \ker(\beta) = \operatorname{im}(\alpha)$ because $u\beta(un) = 0$ implies $\beta(un) = 0$. So there exists $m \in M$ such that $\alpha(m) = un$. Then

$$\alpha_W\left(\frac{m}{uw}\right) = \frac{\alpha(m)}{uw} = \frac{un}{uw} = \frac{n}{w}$$

and therefore $\ker(\beta_W) \subseteq \operatorname{im}(\alpha_W)$.

Conversely, if $\frac{n}{w} \in \alpha_W(\frac{m}{u})$, then

$$\beta_W\left(\frac{n}{w}\right) = \beta_W \circ \alpha_W\left(\frac{m}{u}\right) = \frac{\beta \circ \alpha(m)}{u} = \frac{0}{u} = 0.$$

To show the second part, define $\theta : M \times R_W \to M_w$ by $\theta(m, \frac{r}{u}) = \frac{rm}{u}$ where $m \in M$, $u \in W$, and $r \in R$. This is a bilinear map, so we get an induced map

$$M \otimes R_W \xrightarrow{\phi} M_W$$
$$m \otimes \frac{r}{u} \mapsto \frac{rm}{u}.$$

Claim 1. The map ϕ is one-to-one and onto.

To show ϕ is onto, just note that $\phi(m \otimes \frac{1}{u}) = \frac{m}{u}$. Now suppose that

$$\phi\left(\sum_{i=1}^{n} m_i \otimes \frac{r_i}{u_i}\right) = 0.$$

Fist note that with out any loss of generality all the u_i's are the same, say u. Then

$$\sum m_i \otimes \frac{r_i}{u} = \sum m_i r_i \otimes \frac{1}{u} = \left(\sum m_i r_i\right) \otimes \frac{1}{u}$$

which is of the form $m \otimes \frac{1}{u}$. Thus we have $\phi(m \otimes \frac{1}{u}) = 0$ so $\frac{m}{u} = 0$. But this is true if and only if there exists a $w \in W$ such that $wm = 0$. Then

$$m \otimes \frac{1}{u} = m \otimes \frac{w}{wu} = wm \otimes \frac{1}{wu} = 0 \otimes \frac{1}{wu} = 0.$$

$\square$

Corollary 25. *The map $R \to R_W$ is flat.*

Proof. This follows from the canonical isomorphisms of the tensor product and the definition of a flat homomorphism (see definition on page 26). $\square$

Corollary 26. *If I is an ideal, M an R-module, and W a multiplicatively closed set, then*

$$W^{-1}(M/IM) \simeq W^{-1}M/I(W^{-1}M).$$

In particular,

$$W^{-1}(R/I) \simeq W^{-1}R/W^{-1}I.$$

In other words, localization commutes with quotients.

Proof. Apply the theorem to the left hand side and then use the canonical isomorphisms of the tensor product to obtain the right hand side. $\square$

Example 47. Given the polynomial ring $k[x, y]$ in two indeterminates over a field k, the structure of the ring

$$\left(\frac{k[x, y]}{(xy)} \right)_x$$

can be determined using the previous corollary. That is,

$$\left(\frac{k[x, y]}{(xy)} \right)_x \simeq \frac{k[x, x^{-1}, y]}{(xy)k[x, x^{-1}, y]}.$$

Notice that $(xy)k[x, x^{-1}, y] = (y)k[x, x^{-1}, y]$. So substituting and applying the corollary again we obtain

$$\left(\frac{k[x, y]}{(xy)} \right)_x \simeq k[x]_x \simeq k[x, x^{-1}].$$

2   Ideals and Localization

Example 48. Let R be a domain with W a multiplicatively closed set in R, $0 \notin W$. Then $W^{-1}R$ is still a domain.

Proof. Suppose $\frac{r}{w} \cdot \frac{r'}{w'} = 0$. This means there exists $w'' \in W$ such that $w''rr' = 0$. Since $w'' \neq 0$, either $r = 0$ or $r' = 0$. Thus either $\frac{r}{w} = 0$ or $\frac{r'}{w'} = 0$. $\square$

Definition. If R is a domain and $W = R - \{0\}$, then $W^{-1}R$ is a field called the *field of fractions* of R, e.g. if $R = \mathbb{Z}$, then the field of fractions is $\mathbb{Q}$.

Theorem 27. *Let R be a ring, W a multiplicatively closed set of R.*

(1) *If I is an ideal of R then $W^{-1}I$ is an ideal of $W^{-1}R$ where*

$$W^{-1}I = \left\{ \frac{i}{w} \mid i \in I, w \in W \right\}.$$

(2) *If J is an ideal in $W^{-1}R$ then*

$$J \cap R = \left\{ i \in R \mid \frac{i}{1} \in J \right\}.$$

(3) *The previous two statements give a one-to-one inclusion preserving correspondence between $\mathrm{Spec}(W^{-1}R)$ and primes $\mathfrak{p}$ in R such that $\mathfrak{p} \cap W = \emptyset$*

Proof. For the first part, use the definition of addition and multiplication in the ring $W^{-1}R$.

In general, if $\phi : R \to S$ is a ring homomorphism, $J \subseteq S$, then $\phi^{-1}(J)$ is an ideal in R. Apply this to the canonical map from R into $W^{-1}R$ and we have that $\phi^{-1}(J) = J \cap R$ is an ideal. Further, if $\frac{i}{w} \in J$ then $w\frac{i}{w} = \frac{i}{1}$ implies that $i \in J \cap R$. Thus $\frac{i}{w} \in W^{-1}(J \cap R)$ and the second statement follows.

For the third statement, consider $\mathfrak{q} \in \mathrm{Spec}(R)$ and $\mathfrak{q} \cap W = \emptyset$. Then since

$$W^{-1}(R/\mathfrak{q}) \simeq W^{-1}R/W^{-1}\mathfrak{q}$$

we can apply the above general remark to the domain $R/\mathfrak{q}$. We see that $W^{-1}(R/\mathfrak{q})$ is a domain and so $W^{-1}\mathfrak{q} \in \mathrm{Spec}(W^{-1}R)$. ($W \cap \mathfrak{q} = \emptyset$ implies that $W^{-1}\mathfrak{q} = W^{-1}R$)

Conversely, if $Q \in \mathrm{Spec}(W^{-1}R)$ then $Q \cap R = \mathfrak{q}$ is prime. (This is true for general homomorphisms) By (2) we have that $W^{-1}\mathfrak{q} = Q$. $\qquad\square$

Remark. If I_1 and I_2 are ideals, it is possible that $W^{-1}I_1 = W^{-1}I_2$ without $I_1 = I_2$.

Example 49. Let $R = k[x, y]$ be a polynomial ring in two variables over a field and $W = \{y^n\}_{n \geqslant 0}$. Consider the ideals $I_1 = (x^2, xy)$ and $I_2 = (x)$. Then $W^{-1}I_1 = W^{-1}I_2$ but $W^{-1}I_1 \cap R = (x)$.

Remark. In general, if $I \subseteq R$ is an ideal, then

$$W^{-1}I \cap R = \{r \in R \mid \exists \, w \in W \text{ with } w \cdot r \in I\} = \bigcup_{w \in W} I : w.$$

This contains I if I is not prime. If I is prime,

$$\bigcup_{w \in W} I : w = I.$$

Corollary 28. *If* $\mathfrak{p} \in \mathrm{Spec}(R)$ *then* $R_{\mathfrak{p}}$ *is local with maximal ideal* $\mathfrak{p}R_{\mathfrak{p}}$.

Proof. We know that $\mathrm{Spec}(R_{\mathfrak{p}})$ is the set of primes Q in R such that $Q \cap R_{\mathfrak{p}} = \emptyset$, i.e. primes Q such that $Q \subseteq \mathfrak{p}$. $\qquad\square$

Proposition 29. *Let R be a ring, $R[x]$ a polynomial ring over x. Suppose $Q_1 \subseteq Q_2 \subseteq Q_3$ for prime ideals of $R[x]$. If*

$$Q_1 \cap R = Q_2 \cap R = Q_3 \cap R$$

then $Q_1 = Q_2$ or $Q_2 = Q_3$.

Proof. Set $q = Q_1 \cap R = Q_2 \cap R = Q_3 \cap R$. Then

$$R/q[x] \simeq R[x]/qR[x].$$

Also set $Q_1' = Q_1/qR[x]$, $Q_2' = Q_2/qR[x]$, $Q_3' = Q_3/qR[x]$. In R/q we have

$$Q_1' \cap R/q = Q_2' \cap R/q = Q_3' \cap R/q,$$

so without loss of generality we can assume $R = R/q$ is a domain with $Q_1 = Q_1'$, $Q_2 = Q_2'$ and $Q_3 = Q_3'$ and

$$Q_1 \cap R = Q_2 \cap R = Q_3 \cap R = 0.$$

Let $W = R \smallsetminus \{0\}$. Then $W \cap Q_i = \emptyset$, therefore

$$W^{-1}Q_1 \subseteq W^{-1}Q_2 \subseteq W^{-1}Q_3$$

is a chain of primes in $W^{-1}(R[x]) = R[x] \otimes_R W^{-1}R = (W^{-1}R)[x]$. But $W^{-1}R$ is a field, so $(W^{-1}R)[x]$ is a polynomial ring over a field, and this means:

$$\mathrm{Spec}((W^{-1}R)[x]) = \{0\} \cup \{f(x)\},$$

where $f(x) \neq 0$ is a irreducible polynomial. Hence the longest chain of primes has length two (because $(W^{-1}R)[x]$ has Krull dimension equal to one), therefore $W^{-1}Q_1 = W^{-1}Q_2$ or $W^{-1}Q_2 = W^{-1}Q_3$, which implies

$$Q_1 = Q_2 \quad \text{or} \quad Q_2 = Q_3.$$

$\qquad\square$

Theorem 30 (Local - Global Principle)**.** *Let R be a ring and M and R-module. The following are equivalent:*

(1) $M = 0$;

(2) $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$.

(3) $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$ maximal in $\mathrm{Spec}(R)$.

Proof. Clearly $(1) \Rightarrow (2) \Rightarrow (3)$. Now assume (3) and by way of contradiction suppose $M \neq 0$, i.e. there exists $x \in M$, $x \neq 0$. This means $\mathrm{ann}(x) = \{y \in R : yx = 0\} \neq R$, therefore there exists a maximal ideal $\mathfrak{m} \in \mathrm{Spec}(R)$ such that $\mathrm{ann}(x) \subseteq \mathfrak{m}$.

Claim. $\frac{x}{1} \neq 0$ in $M_\mathfrak{m}$.

Proof of the Claim. Assume $\frac{x}{1} = 0$, then there exists $w \in R \smallsetminus \mathfrak{m}$ such that $xw = 0$ in R. Therefore $w \in \mathrm{ann}(x) \subseteq \mathfrak{m}$, which is a contradiction.

So the claim holds, but this is a contradiction since we assumed $M_\mathfrak{m} = 0$. $\square$

Corollary 31. *Let $f : M \to N$ be an homomorphism of R-modules. Then f is injective (respectively surjective, isomorphism) if and only if the homomorphisms $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ are injective (respectively surjective, isomorphism) for all $\mathfrak{p}$ in $\mathrm{Spec}(R)$.*

Proof. Note that $f_\mathfrak{p}\left(\frac{m}{s}\right) = \frac{f(m)}{s}$ for $s \notin \mathfrak{p}$. Also

$$\begin{cases} f \text{ is injective} & \Longleftrightarrow \ker f = 0. \\ f \text{ is surjective} & \Longleftrightarrow \mathrm{coker} f = 0. \\ f \text{ is isomorphism} & \Longleftrightarrow \ker f = \mathrm{coker} f = 0. \end{cases}$$

But the Local-Global Principle says that it is enough to check $(\ker f)_\mathfrak{p}$ and $(\mathrm{coker} f)_\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Finally, since $\otimes_R R_\mathfrak{p}$ is flat, we get $(\ker f)_\mathfrak{p} = \ker f_\mathfrak{p}$ and $(\mathrm{coker} f)_\mathfrak{p} = \mathrm{coker} f_\mathfrak{p}$. Hence

$$\begin{cases} f \text{ is injective} & \Longleftrightarrow f_\mathfrak{p} \text{ is injective for all } \mathfrak{p} \in \mathrm{Spec}(R). \\ f \text{ is surjective} & \Longleftrightarrow f_\mathfrak{p} \text{ is surjective for all } \mathfrak{p} \in \mathrm{Spec}(R). \\ f \text{ is isomorphism} & \Longleftrightarrow f_\mathfrak{p} \text{ is isomorphism for all } \mathfrak{p} \in \mathrm{Spec}(R). \end{cases}$$

$\square$

Remark. If M is generated by $x_1, \dots, x_n$, then for all multiplicatively closed sets W, $W^{-1}M$ is generated by $\frac{x_1}{1}, \dots, \frac{x_n}{1}$

Proof. Assume $x_1, \dots, x_n$ generate M, then there is a surjective R-homomorphism

$$\varphi : R^n \to M$$
$$e_i \mapsto x_i$$

φ is surjective, therefore φ_W is also surjective, i.e.

$$\varphi_W : W^{-1}R^n \to W^{-1}M$$
$$\frac{e_i}{1} \longmapsto \frac{x_i}{1}$$

is a presentation for $W^{-1}M$, which is generated by $\varphi_W\left(\frac{e_1}{1}\right) = \frac{x_1}{1}, \dots, \varphi_W\left(\frac{e_n}{1}\right) = \frac{x_n}{1}$. $\square$

Remark. If R is local and M is finitely generated then all minimal generating sets of M have the same number of elements; namely the dimension of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$ where $\mathfrak{m}$ is the unique maximal ideal.

Proof. By Nakayama's Lemma $M = Rx_1 + \ldots Rx_n$ if and only if $M = Rx_1 + \ldots + Rx_n + \mathfrak{m}M$. Therefore $x_1, \ldots, x_n$ minimally generate M if and only if their images $\overline{x}_1, \ldots, \overline{x}_n$ form a $k = R/\mathfrak{m}$-basis for the vector space $M/\mathfrak{m}M$. $\qquad\square$

Example 50. Suppose R has nontrivial idempotents, say e. Then R itself is generated by $\{1\}$, but it is also minimally generated by $\{e, 1 - e\}$

Definition. If M is an R-module, the *support of M* is the set of prime ideals $\mathfrak{p}$ in $\mathrm{Spec}(R)$ such that $M_\mathfrak{p} \neq 0$. This set is denoted $\mathrm{Supp}(M)$.

Proposition 32. *If M is finitely generated then*

$$\mathrm{Supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq \mathrm{ann}(M)\} = V(\mathrm{ann}(M))$$

Proof. $M_\mathfrak{p} = 0$ if and only if there exists $s \notin \mathfrak{p}$ such that $sM = 0$ if and only if there exists $s \notin \mathfrak{p}$ such that $s \in \mathrm{ann}(M)$ if and only if $\mathrm{ann}(M) \not\subseteq \mathfrak{p}$. $\qquad\square$

3 UFD's and Localization

Theorem 33. *Let R be a ring and let W be a multiplicatively closed set.*

(1) If R is UFD then $W^{-1}R$ is UFD.

(2) Suppose there exists a set of prime elements $\Lambda = \{x_i\} \subseteq W$ which are NZD such that every element $w \in W$ can be written as

$$w = \prod_i x_i^{a_i}.$$

If $W^{-1}R$ is UFD and R satisfies ACC (Ascending Chain Condition) then R is UFD.

To prove this theorem we need some further results.

Lemma 34. *Let R, W and Λ be as above. Then every $r \in R$ can be written in the form $r = wr'$ for some $w \in W$ and $x_i \nmid r'$ for all $x_i \in \Lambda$.*

Proof. If $x_i \nmid r$ for all $x_i \in \Lambda$ then take $r' = r$ and $w = 1$. Otherwise $r = r_1 x_i$ for some $r_1 \in R$, $x_i \in \Lambda$. Note that $(r) \subsetneq (r_1)$. Repeat the process with r_1 in place of r. Inductively we get a chain

$$(r) \subsetneq (r_1) \subsetneq (r_2) \subsetneq \ldots$$

which must stabilize at some point since R is Noetherian. If $(r_n) = (r_{n+1})$ this means that x_i does not divide r_n for all $x_i \in \Lambda$. But then $r = wr_n$ for some $w \in W$ by construction. $\qquad\square$

Lemma 35. *Suppose that $\left(\frac{z}{1}\right) \subseteq W^{-1}R$ is a prime ideal. Write $z = wz'$ as in Lemma 34. Then*

$$\left(\frac{z}{1}\right) = \left(\frac{z'}{1}\right) \quad and \quad \left(\frac{z'}{1}\right) \cap R = (z') \;\; is \; prime \; in \; R.$$

Proof. Clearly $\left(\frac{z}{1}\right) = \left(\frac{z'}{1}\right)$ since $\frac{w}{1}$ is invertible in $W^{-1}R$. Also $(z') \subseteq R$ is a prime since $\left(\frac{z'}{1}\right)$ is a prime in $W^{-1}R$. Moreover we have:

$$\left(\frac{z'}{1}\right) \cap R = \bigcup_{w \in W} (z' : w),$$

therefore we are done if we prove that $(z' : w) = (z')$ for all $w \in W$. Let $r \in (z' : w)$, then there exists $s \in R$ such that $wr = z's$. By definition of Λ in Theorem 33 there exists $a_1, \ldots, a_n$ integers such that $w = \prod_i x_i^{a_i}$. Therefore

$$x_1^{a_1} \cdot \ldots \cdot x_n^{a_n} r = z's.$$

Hence $x_i | z's$ but $x_i \nmid z'$ for all i, and since the x_i's are prime we get $x_i | s$ for all i. So we can cancel the x_i's one at a time to get $r = z't$ for some $t \in R$, i.e. $r \in (z')$. $\qquad\square$

Proof of Theorem 33. (1) Recall that to prove that a domain is UFD we only need to show that every irreducible element is prime, provided we have ACC (Ascending Chain Condition) on principal ideals. R is UFD, hence a domain, therefore $W^{-1}R$ is a domain. If $x \in R$ is irreducible then x is prime, therefore $W^{-1}(x) = \left(\frac{x}{1}\right)$ is prime in $W^{-1}R$ provided $W \cap (x) = \emptyset$. Set

$$W' := \{x \in R : \exists w \in W, x | w\}$$

Claim. $W^{-1}R = (W')^{-1}R$

Proof of the Claim. Let $x \in W'$ and write $xy = w \in W$. in $W^{-1}R$ w is a unit, then

$$1 = w^{-1}xy = x(w^{-1}y) = y(w^{-1}x)$$

so x and y are also units. This means that $W^{-1}R$ satisfies the same property as $(W')^{-1}R$ and therefore they are isomorphic. $\qquad\square$

By the Claim we can assume without loss of generality that $W = W'$. Let $\frac{b}{w} \in W^{-1}R$ and write $b = x_1 \cdot \ldots \cdot x_n$ a product of primes (R is UFD). Then

$$\frac{b}{w} = \frac{1}{w}\frac{x_1}{1} \cdots \frac{x_n}{1}.$$

Now $\frac{x_i}{1}$ is either a unit (if $x_i \in W'$) or a prime element (if $x_i \notin W'$).
(2) It suffices to show that every irreducible element $r \in R$ is prime. There are two cases:

(1) $\frac{r}{1}$ is a unit in $W^{-1}R$, i.e. $r \in W$. Since every element in W is a product of x_i's in Λ, but also r is irreducible, we have that $r = x_j$ for some j, and hence it is prime.

(2) $\frac{r}{1}$ is not a unit, then there exists a prime ideal $\left(\frac{z}{1}\right) \subseteq W^{-1}R$ such that $\frac{r}{1} \in \left(\frac{z}{1}\right)$. Therefore there exist $s \in R$ and $w \in W$ such that

$$\frac{r}{1} = \frac{z}{1}\frac{s}{w} \;\Rightarrow\; wr = zs.$$

Without loss of generality we can replace z with z' of Lemma 35 to assume $x_i \nmid z$ for all $x_i \in \Lambda$. By Lemma 35 z is prime and $z|wr$ but $z \nmid w$, therefore $z|r$. Finally r is irreducible, hence $(r) = (z)$ is prime.

$$\square$$

Corollary 1. *If R is a UFD, so is $R[x_1, \ldots, x_n]$.*

Proof. By induction we can assume $n = 1$ (write $x := x_1$). Let $W := R \smallsetminus \{0\}$. Since R is UFD, W satisfies the conditions of Theorem 33 (2), and it satisfies them not only for R but also for $R[x]$. Therefore $R[x]$ is UFD if $W^{-1}R[x]$ is UFD. Finally $W^{-1}R[x] = (W^{-1}R)[x] = K[x]$ where $K = W^{-1}R$ is a field, therefore it is a PID and hence a UFD. $\hspace{2em}\square$

Example 51. Consider

$$R := \frac{\mathbb{C}[x_1, x_2, x_3, x_4]}{(x_1^2 + x_2^2 + x_3^2 + x_4^2)} \simeq \frac{\mathbb{C}[u, v, s, t]}{(uv - st)} =: S$$

via the isomorphism $u = x_1 + ix_2$, $v = x_1 - ix_2$, $s = x_3 + ix_4$, $t = x_3 - ix_4$. S is clearly not UFD, and so is R.

Example 52. Consider $n \geq 5$ and

$$R := \frac{\mathbb{C}[x_1, \ldots, x_n]}{(x_1^2 + \ldots + x_n^2)} \simeq \frac{\mathbb{C}[u, v, x_3, \ldots, x_n]}{(uv + x_3^2 + \ldots x_n^2)} =: S.$$

Then u is prime since $S/uS \simeq \frac{\mathbb{C}[v, x_3, \ldots, x_n]}{(x_3^2 + x_4^2 + x_5^2)}$ is a domain. Also $S_u \cong (\mathbb{C}[u, x_3, x_4, x_5])_u$ is a UFD, hence S is a UFD by Theorem 33 (2), and so is R.

Chapter 4

Chain Conditions

Definition. Let $(S, \leq)$ be a partially ordered set. Then S satisfies:

(1) The *ascending chain condition (ACC)* if every ascending chain

$$s_1 \leq s_2 \leq \ldots$$

of elements in S stabilizes, i.e. there exists $n \in \mathbb{N}$ such that $s_n = s_{n+1} = s_{n+2} = \ldots$.

(2) The *descending chain condition (DCC)* if every descending chain

$$t_1 \geq t_2 \geq \ldots$$

of elements in S stabilizes, i.e. there exists $m \in \mathbb{N}$ such that $t_m = t_{m+1} = t_{m+2} = \ldots$.

1 Noetherian Rings

Definition. A ring R is *Noetherian* if the set of all ideals satisfies ACC with respect to the inclusion. This means that every ascending chain of ideals has a maximal element, i.e., if

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq I_{i+1} \subseteq \cdots$$

is a chain of ascending ideals I_j, then there exists n sufficiently large such that $I_n = I_{n+1}$.

Proposition 36. *The ring R is Noetherian if and only if every ideal in R is finitely generated.*

Proof. Assume R is Noetherian and let I be and ideal in R. Let $f_1 \in I$. If $(f_1) = I$ we are done. If not, choose $f_2 \in I \setminus (f_1)$. If $(f_1, f_2) = I$ then stop. Incuctively, we have a chain,

$$(f_1) \subseteq (f_1, f_2) \subseteq (f_1, f_2, f_3) \subseteq \cdots .$$

Since R is Noetherian, this chain stops and it can only stop when I is generated by these elements.

Conversely, if we have an ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq I_{i+1} \subseteq \cdots ,$$

let $J = \cup_{i=1}^{\infty} I_i$. This is an ideal, hence $J = (f_1, \ldots, f_n)$, and there exists an N sufficiently large such that $(f_1, \ldots, f_n) \subseteq I_N$. Therefore

$$J \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq J.$$

So $I_N = I_{N+1}$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Example 53. Examples of Noetherian Rings:

(1) The integers $\mathbb{Z}$.

(2) Any field.

(3) If k is a field, then $k[x]$ is Noetherian.

Theorem 37 (Hilbert Basis Theorem). *If R is a Noetherian ring, then $R[x_1, \ldots, x_n]$ is Noetherian.*

Proof. By induction on n, it suffices to prove the case when $n = 1$ since $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. We want to prove $R[x]$ is Noetherian. Let

$$f(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_n x^n$$

be an element of $R[x]$ such that $r_n \neq 0$. Define $\text{in}(f) = r_n$. If $I \subseteq R[x]$ is an ideal, then

$$\text{in}(I)_j = \{\text{in}(f) \mid f \in I, \ \deg(f) \leqslant j\} \cup \{0\}.$$

Notice that $\text{in}(I)_j$ is an ideal in R: take $a \in \text{in}(I)_j$ and $r \in R$, then if $ra = 0$ clearly $ra \in \text{in}(I)_j$. If $ra \neq 0$ then we have

$$ax^i + \text{lower degree terms}$$

is an element of I, with $i \leqslant j$, therefore

$$(ra)x^i + \text{lower degree terms} \in I,$$

which means $ra \in \text{in}(I)_j$. To prove that $\in I_j$ is closed under the sum pick $a, b \in \text{in}(I)_j$, then there exist

$$f(x) = ax^i + \ldots \qquad g(x) = bx^k + \ldots$$

with $k \leq i \leq j$ without loss of generality. Then $a + b = \text{in}(f + x^{i-k} g)$ which has degree $i \leq j$.

Now let $I \subseteq R[x]$ be an ideal. Notice:

$$\text{in}(I)_0 \subseteq \text{in}(I)_1 \subseteq \text{in}(I)_2 \subseteq \ldots$$

is an ascending chain of ideals in R, which is Noetherian by assumption. Therefore there exists $N \in \mathbb{N}$ such that

$$\mathrm{in}(I)_N = \mathrm{in}(I)_{N+1} = \dots$$

Also $\mathrm{in}(I)_j$ is finitely generated for all $0 \le j \le N$, hence choose generators $r_{j1}, \dots, r_{jm_j}$ for $\in I_j$, for all $0 \le j \le N$. Pick now $f_{ji} \in I$ such that $\mathrm{in}(f_{ji}) = r_{ji}$.

Claim. $I = (f_{01}, \dots, f_{0m_0}, \dots, f_{N1}, \dots, f_{Nm_N}) =: J$.

Proof of the Claim. Clearly $J \subseteq I$. Conversely assume by way of contradiction that $I \ne J$. Then choose $f \in I$ of least degree such that $f \notin J$. If $\deg f = k$, then $\mathrm{in}(f) \in \mathrm{in}(I)_k$. There are two cases:

- $k \ge N$: under this assumption $\mathrm{in}(f) \in \mathrm{in}(I)_N = (r_{N1}, \dots, r_{Nm_N})$. Write:

$$\mathrm{in}(f) = \sum_{l=1}^{m_N} s_l r_{Nl}$$

  with $s_l \in R$ and consider

$$g := f - \sum_{l=1}^{m_N} s_l x^{k-N} f_{Nl}.$$

  This polynomial has coefficient zero in degree k, since

$$\mathrm{in}(f) = \sum_{l=1}^{m_N} s_l r_{Nl} = \mathrm{in}\left(\sum_{l=1}^{m_N} s_l x^{k-N} f_{Nl}\right).$$

  By minimality in the choice of f we have $g \in J$, therefore:

$$f = g + \sum_{l=1}^{m_N} s_l x^{k-N} f_{Nl} \in J$$

  which is a contradiction. Therefore $I = J$ in this case.

- If $k < N$ proceed as in the previous case: pick f of least degree such that $f \in I \setminus J$ and write

$$\mathrm{in}(f) = \sum_{l=1}^{m_k} s_l r_{kl}.$$

  Again cancel the leading term of f, which is $\mathrm{in}(f)x^k$, using $f_{k1}, \dots, f_{km_k}$:

$$g := f - \sum_{l=1}^{m_k} s_l f_{kl} \in J$$

  and therefore $f\ inJ$, contradiction. Hence again $I = J$.

So I is finitely generated and $R[x]$ is Noetherian. $\qquad\qquad \square$

Remark. If R is Noetherian and $I \subseteq R$ is an ideal, then R/I is Noetherian.

Remark. If R is Noetherian and W is multiplicatively closed, then R_W is Noetherian.

Proof. Let $J_1 \subseteq J_2 \subseteq \ldots$ be an ascending chain of ideals in R_W. Then there exists $N \in \mathbb{N}$ such that $J_N \cap R = J_{N+1} \cap R = \ldots$ which implies

$$J_N = (J_N \cap R)R_W = (J_{N+1} \cap R)R_W = J_{N+1} = \ldots.$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \square$

2   Noetherian Modules

Definition. Let R be a ring and let M be a R-module. The following are equivalent:

(1) Every submodule of M is finitely generated.

(2) M satisfies ACC on submodules.

(3) Any ordered set of submodules has a maximal element with respect to containment.

Such a module M is said to be Noetherian.

Proof. The proof is the same as the one given for ideals. $\qquad\qquad \square$

Proposition 38.   *(1) If $N \subseteq M$ is a submodule and M is Noetherian, then M/N is Noetherian.*

   (2) If $N \subseteq M$ is a submodule and both N and M/N are Noetherian, then M is Noetherian.

Proof. (1) Immediate from the definition and the 1-1 correspondence:

$$\{K/N \subseteq M/N \text{ submodule}\} \overset{1-1}{\longleftrightarrow} \{N \subseteq K \subseteq M \text{ submodule}\}.$$

(2) Suppose we have an ascending chain of submodules of M:

$$M_1 \subseteq M_2 \subseteq \ldots$$

Then consider:

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \ldots \subseteq N$$

and

$$\frac{M_1 + N}{N} \subseteq \frac{M_2 + N}{N} \subseteq \ldots \subseteq M/N.$$

By assumption there exists $n \in \mathbb{N}$ such that

$$M_n \cap N = M_{n+1} \cap N \quad \text{and} \quad \frac{M_n + N}{N} = \frac{M_{n+1} + N}{N}.$$

Claim. $M_n = M_{n+1}$.

Proof of the Claim. It is enough to show that if $x \in M_{n+1}$, then $x \in M_n$. Notice that $x + N \in \frac{M_{n+1}+N}{N} = \frac{M_n+N}{N}$, hence there exists $y \in M_n$ such that

$$x + N = y + N.$$

Therefore $x - y \in N$ and $x - y \in M_{n+1}$, and so:

$$x - y \in M_{n+1} \cap N = M_n \cap N.$$

Finally, since $y \in M_n$ and $x - y \in M_n$:

$$x = y + (x - y) \in M_n.$$

$\square$

Proposition 39. *Let R be a Noetherian ring and let M be a R-module. The following are equivalent:*

(1) M is Noetherian.

(2) M is finitely generated.

Proof. (1) $\Rightarrow$ (2) Since M is Noetherian every submodule, in particular M itself, is finitely generated.
(2) $\Rightarrow$ (1) Let $M = <x_1, \ldots, x_n>$ and consider the map:

$$f : R^n \to M$$
$$e_i \mapsto x_i$$

where $<e_1, \ldots, e_n>$ is the standard basis of R^n. R is a Noetherian, so is a Noetherian R-module. Therefore R^n is Noetherian and $R^n/\ker f \simeq M$ is Noetherian too. $\square$

Remark 1. If M is Noetherian, then $R/\mathrm{ann}(M)$ is Noetherian.

Proposition 40. *Let M be a Noetherian R-module and let $f : M \to M$ be a surjective homomorphism. Then f is an isomorphism.*

Proof. Let $f^n := f \circ f \circ \ldots \circ f$ the composition of f with itself n times. Note that f^n is surjective for all n and moreover:

$$\ker f \subseteq \ker f^2 \subseteq \ldots \subseteq \ker f^n \subseteq \ldots \subseteq M.$$

Since M is Noetherian there exists $n \in \mathbb{N}$ such that

$$\ker f^n = \ker f^{n+1}.$$

Let now $x \in \ker f$. Since f^n is surjective there exists $y \in M$ such that $x = f^n(y)$. Apply f to get
$$0 = f(x) = f^{n+1}(y)$$

and hence $y \in \ker f^{n+1} = \ker f^n$. This means:

$$0 = f^n(y) = x,$$

i.e. f is injective and so it is an isomorphism. $\qquad\qquad\qquad\qquad \square$

Remark 2. This is no longer true if we switch surjective and injective in Proposition 40. For instance consider:

$$\mathbb{Z} \longrightarrow \mathbb{Z}$$

$$1 \longmapsto 2$$

which is injective but not surjective.

3   Artinian Rings

Definition. If the set of ideals in a ring R satisfies DCC then R is said to be *Artinian*.

Example 54.   (1) Fields are Artinian.

   (2) Any finite ring, e.g. $\mathbb{Z}/n\mathbb{Z}$ is Artinian.

   (3) Let k be a field and
$$R = k[x_1, \ldots, x_n]/I$$
     be a quotient such that $\dim_k \leq \infty$. Then R is Artinian.

   (4) Let k be a field and $k \subseteq R$ be a subring of $M_n(k)$ the $n \times n$ matrices with coefficients in k. Then R is Artinian since $\dim_k R \leq \infty$.

Remark 3. If R is Artinian, then it is Noetherian. However the converse is not true, for instance $R = k[x]$ is Noetherian but

$$R \supseteq (x) \supseteq (x^2) \supseteq \ldots$$

is a descending chain which does not stabilize.

Remark 4. If R_1, R_2 are Artinian then $R_1 \times R_2$ is Artinian.

Proposition 41. *if R is Artinian, then every prime is maximal and there are only finitely many maximal ideals.*

Proof. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and pass to $R/\mathfrak{p}$. Relabel it as R so that without loss of generality we can assume that R is a domain and we have to prove that it is in fact a field. Assume not and pick $x \in R$, $x \neq 0$ which is not a unit. Then consider
$$R \supseteq (x) \supseteq (x^2) \supseteq \ldots$$
that has to stabilize since R is Artinian. So there is $n \in \mathbb{N}$ such that $(x^n) = (x^{n+1})$. So there exists $a \in R$ such that $x^n = ax^{n+1}$ and, since R is a domain,

we can cancel x^n and get $1 = ax$, i.e. x is a unit. This is a contradiction, therefore R is a field and $\mathfrak{p}$ is maximal.

Assume now that there are infinitely many distinct maximal ideals in R, say $\{\mathfrak{m}_i\}_{i=1}^{\infty}$. Consider:

$$\mathfrak{m}_1 \supseteq (\mathfrak{m}_1 \cap \mathfrak{m}_2) \supseteq (\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3) \supseteq \ldots$$

Again since R is Artinian there exists $k \in \mathbb{N}$ such that

$$(\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_k) = (\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_k \cap \mathfrak{m}_{k+1}).$$

But this means $(\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_k) \subseteq \mathfrak{m}_{k+1}$ and therefore, since they are maximal (prime was enough) there exists $i \in \{1, \ldots, k\}$ such that $\mathfrak{m}_i \subsetneq \mathfrak{m}_{k+1}$, contradicting the maximality of $\mathfrak{m}_i$. Hence there are just finitely many maximal ideals in R. $\qquad\square$

Theorem 42. *Let R be a ring. The following facts are equivalent:*

(1) R is Artinian.

(2) R is Noetherian and there exist only finitely many prime ideals, and all of them are maximal.

Proof. $(1) \Rightarrow (2)$ By Proposition 41 we only need to show that R is Noetherian. List all the maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$.

Claim. There exists $k \in \mathbb{N}$ such that $(\mathfrak{m}_1 \ldots \mathfrak{m}_n)^k = 0$.

Proof of the Claim. Set $I = \mathfrak{m}_1 \ldots \mathfrak{m}_n$, then

$$I \supseteq I^2 \supseteq I^3 \supseteq \ldots \supseteq I^k = I^{k+1}$$

for some k since R is Artinian. Assume $I^k \neq 0$ and consider:

$$\Lambda := \{J \subseteq R : JI^k \neq 0\}.$$

Note that $I \in \Lambda$, so $\Lambda \neq \emptyset$. Therefore there exists a minimal element J, and this has to be a principal ideal, otherwise there exists $x \in J$ such that $xI^k \neq 0$ (this is because $JI^k \neq 0$) and so $(x)I^k \neq 0$ and $(x) \subseteq J$. So set $J = (x)$. Notice that

$$(xI)I^k = xI^{k+1} = xI^k \neq 0$$

so $xI \in \Lambda$ and $xI \subseteq (x) = J$. By minimality it has to be $xI = (x)$ and since $I = \mathfrak{m}_1 \ldots \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n = \mathrm{Jac}(R)$ it has to be $x = 0$ by NAK. This is a contradiction, hence $I^k = (\mathfrak{m}_1 \ldots \mathfrak{m}_n)^k = 0$.

By Chinese Remainder Theorem we have:

$$R = \frac{R}{(\mathfrak{m}_1 \ldots \mathfrak{m}_n)^k} \simeq \frac{R}{\mathfrak{m}_1^k} \times \ldots \times \frac{R}{\mathfrak{m}_n^k}.$$

R is Artinian, hence each $R/\mathfrak{m}_i^k$ is Artinian, and if each $R/\mathfrak{m}_i^k$ is Noetherian, then so is R. So assume $R = R/\mathfrak{m}^k$ for some maximal ideal $\mathfrak{m}$, so that we reduced to the case in which there is only one maximal ideal, and its k-th power is zero. To prove that R is Noetherian induct on the least k such that $\mathfrak{m}^k = 0$:

- If $k = 1$ then $\mathfrak{m} = 0$ and R is a field, and hence Noetherian.

- If $k > 1$ then by induction $R/\mathfrak{m}^{k-1}$ is Noetherian. Note that $\mathrm{ann}(\mathfrak{m}^{k-1}) = \mathfrak{m}$, so that $\mathfrak{m}^{k-1}$ is a $R/\mathfrak{m}$-module, i.e. a vector space. Now any vector subspace of $\mathfrak{m}^{k-1}$ is an ideal in R, so that $\dim_{R/\mathfrak{m}} \mathfrak{m}^{k-1} \leq \infty$, since R is Artinian, so DCC is satisfied on ideals. Hence $\mathfrak{m}^{k-1}$ is a Noetherian R-module and since both $R/\mathfrak{m}^{k-1}$ and $\mathfrak{m}^{k-1}$ are Noetherian, R is Noetherian too.

$(2) \Rightarrow (1)$ Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the maximal ideals in R. These are all the primes in R, so

$$\sqrt{(0)} = \mathfrak{m}_1 \cap \ldots \mathfrak{m}_n,$$

so, since R is Noetherian, there exists $N \gg 0$ such that $(\mathfrak{m}_1 \ldots \mathfrak{m}_n)^N = 0$. By Chinese Remainder Theorem

$$R \simeq \frac{R}{\mathfrak{m}_1^N} \times \ldots \frac{R}{\mathfrak{m}_n^N}.$$

A product of Artinian rings is artininan, so it is enough to show that $R/\mathfrak{m}^N$ is Artinian for some ring R with a unique maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^N = 0$. Induct on N:

- If $N = 1$ then R is a field, and hence Artinian.

- If $N > 1$ by induction $R/\mathfrak{m}^{N-1}$ is Artinian. Also $\mathfrak{m}^{N-1}$ is a $R/\mathfrak{m}$-vector space of finite dimension, since R is Noetherian. Let

$$R \supseteq I_1 \supseteq I_2 \supseteq \ldots$$

be a descending chain of ideals. Then going modulo $\mathfrak{m}^{N-1}$:

$$\frac{R}{\mathfrak{m}^{N-1}} \supseteq \frac{I_1 + \mathfrak{m}^{N-1}}{\mathfrak{m}^{N-1}} \supseteq \frac{I_2 + \mathfrak{m}^{N-1}}{\mathfrak{m}^{N-1}} \supseteq \ldots$$

must stabilize, and also

$$R \cap \mathfrak{m}^{N-1} \supseteq I_1 \cap \mathfrak{m}^{N-1} \supseteq I_2 \cap \mathfrak{m}^{N-1} \supseteq \ldots$$

must stabilize because $\mathfrak{m}^{N-1}$ is a finite dimensional vector space. Therefore there exists $M \gg 0$ such that

$$I_M + \mathfrak{m}^{N-1} = I_{M+1} + \mathfrak{m}^{N-1} \quad \text{and} \quad I_M \cap \mathfrak{m}^{N-1} = I_{M+1} \cap \mathfrak{m}^{N-1}.$$

This implies $I_M \subseteq I_{M+1} + \mathfrak{m}^{N-1}$ and so:

$$I_M \subseteq I_M \cap (I_{M+1} + \mathfrak{m}^{N-1}) = I_{M+1} + (I_M \cap \mathfrak{m}^{N-1}) = I_{M+1} + (I_{M+1} \cap \mathfrak{m}^{N-1}) \subseteq I_{M+1},$$

which means $I_M = I_{M+1}$ and the chain stabilizes.

$\square$

Definition. A R-module M is said to be Artinian if it satisfies DCC on submodules.

Remark 5. R is Artinian as a ring if and only if R is Artinian as a module over itself.

Remark 6. If $N \subseteq M$ is a submodule, then M is Artinian if and only if N and M/N are Artinian.

Chapter 5

Primary Decomposition

1 Definitions and Examples

Definition. An ideal $I \subseteq R$ is said to be *irreducible* if

$$I = J \cap K \implies J = I \text{ or } K = I.$$

Definition. An ideal $\mathfrak{q} \subseteq R$ is said to be *primary* if whenever $xy \in \mathfrak{q}$ and $x \notin \sqrt{\mathfrak{q}}$, it has to be $y \in \mathfrak{q}$.

Example 55. In $\mathbb{Z}$ we have $(m) \cap (n) = (lcm(m,n))$, hence an ideal (k) is irreducible if and only if $k \neq lcm(m,n)$ unless $k = m$ or $k = n$. This is equivalent to require that $k = p^l$ for some $p \in \mathbb{Z}$ prime and some integer l. Primary ideals in $\mathbb{Z}$ are also of this form. In fact if $\mathfrak{q} = (p^l)$ and $xy \in \mathfrak{q}$, then $p^l | xy$. Assume $x \notin \sqrt{\mathfrak{q}} = (p)$, then $p \nmid x$ and hence $p^l | y$, that is $y \in \mathfrak{q}$.

Remark 7. If $\mathfrak{q} \subseteq R = \mathbb{Z}$, then

$\mathfrak{q}$ primary $\iff$ $\mathfrak{q}$ irreducible $\iff$ $\mathfrak{q} = (p^l)$ for some p prime and some $l \in \mathbb{N}$.

Proposition 43 (Noether)**.** *If R is a Noetherian ring and $\mathfrak{q} \subseteq R$ is irreducible, then $\mathfrak{q}$ is primary.*

Proof. Suppose not, and let $ab \in \mathfrak{q}$ such that $a \notin \sqrt{\mathfrak{q}}$ and $b \notin \mathfrak{q}$. Notice that it has to be $a^n \notin \mathfrak{q}$ for all $n > 0$. For $n \in \mathbb{N}$ consider:

$$\mathfrak{q} : a^n = \{r \in R : ra^n \in \mathfrak{q}\}$$

and notice that

$$\mathfrak{q} \subseteq (\mathfrak{q} : a) \subseteq (\mathfrak{q} : a^2) \subseteq \dots$$

Since R is Noetherian the chain stabilizes, i.e. there exists $k \in \mathbb{N}$ such that $(\mathfrak{q} : a^k) = (\mathfrak{q} : a^{k+1}) = \dots$

Claim. $\mathfrak{q} = (\mathfrak{q} : a^k) \cap (\mathfrak{q} + Ra^k)$ and furthermore $\mathfrak{q} \neq (\mathfrak{q} : a^k)$ and $\mathfrak{q} \neq (\mathfrak{q} + Ra^k)$.

Proof of the Claim. Clearly $\mathfrak{q} \subseteq (\mathfrak{q} : a^k) \cap (\mathfrak{q} + Ra^k)$. Let $r \in (\mathfrak{q} : a^k) \cap (\mathfrak{q} + Ra^k)$, then $r = c + da^k$, with $c \in \mathfrak{q}$ and $d \in R$. Also

$$a^k(c + da^k) = ra^k \in \mathfrak{q},$$

therefore $da^{2k} \in \mathfrak{q}$, i.e. $d \in (\mathfrak{q} : a^{2k}) = (\mathfrak{q} : a^k)$. Finally $da^k \in \mathfrak{q}$ and hence $r = c + da^k \in \mathfrak{q}$.

Furthermore $\mathfrak{q} \neq \mathfrak{q} : a^k$ since $ba^k = (ba)a^{k-1} \in \mathfrak{q}$, hence $b \in ((\mathfrak{q} : a^k) \smallsetminus \mathfrak{q})$ and also $a^k \in (Ra^k \smallsetminus \mathfrak{q}) \subseteq ((\mathfrak{q} + Ra^k) \smallsetminus \mathfrak{q})$.

$\square$

Remark 8. The converse of Proposition 43 is not true. For instance in $k[x, y]$ the ideal $(x, y)^2 = (x^2, xy, y^2)$ is primary (a justification is given later) but it is not irreducible, in fact:

$$(x, y)^2 = (x^2, y) \cap (x, y^2).$$

Proposition 44. *Let R be a ring.*

(1) If $\mathfrak{q}$ is primary, then $\sqrt{\mathfrak{q}} = \mathfrak{p}$ is prime (we often say that $\mathfrak{q}$ is $\mathfrak{p}$-primary).

(2) If $\sqrt{\mathfrak{q}} = \mathfrak{m}$ is maximal, then $\mathfrak{q}$ is $\mathfrak{m}$-primary.

Proof. (1) Suppose that $ab \in \sqrt{\mathfrak{q}}$ and $a \notin \sqrt{\mathfrak{q}}$. There exists $n >> 0$ such that $a^n b^n \in \mathfrak{q}$, but $a^m \notin \mathfrak{q}$ for all $m \geq 1$. Since $\mathfrak{q}$ is primary it has to be $b^n \in \mathfrak{q}$, and hence $b \in \sqrt{\mathfrak{q}}$, which is prime.

(2) Suppose $ab \in \mathfrak{q}$ and $a \notin \mathfrak{m} = \sqrt{\mathfrak{q}}$. Then $\mathfrak{m} + Ra = (1)$, therefore there exists $r \in R$ and $m \in \mathfrak{m}$ such that $1 = ra + m$. Since $m \in \mathfrak{m} = \sqrt{\mathfrak{q}}$ there exists $n \in \mathbb{N}$ such that $m^n \in \mathfrak{q}$, therefore:

$$1 = 1^n = (m + ra)^n = m^n + sa$$

for some $s \in R$. Finally

$$b = m^n b + sab \in \mathfrak{q}$$

and so $\mathfrak{q}$ is $\mathfrak{m}$-primary. $\square$

Remark 9. The converse of Proposition 44 (1) is not true in general if $\sqrt{\mathfrak{q}} = \mathfrak{p}$ is not maximal.

2 Primary Decomposition

Definition. Let R be a ring. An ideal I is said to have a *primary decomposition* if we can write

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n,$$

where each $\mathfrak{q}_i$ is primary.

In this section we prove that every Noetherian ring has a primary decomposition. Such a decomposition is not unique:

Example 56.

$$(x^2, xy) = (x) \cap (x^2, xy, y^n) \ \text{ for all } n \geq 2.$$

However it has some degree of uniqueness.

Theorem 45 (Noether)**.** *Let R be a Noetherian ring. Then every ideal $I \subseteq R$ has a primary decomposition.*

Proof. Since irreducible ideals are primary it suffices to prove that every ideal is a finite intersection of irreducible ideals. Let

$$\Lambda := \{J \subseteq R : J \text{ is not an intersection of finitely many irreducible ideals}\}.$$

Suppose $\Lambda \neq \emptyset$ and choose $I \in \Lambda$ maximal (this is possible since R is Noetherian). I itself cannot be irreducible (since $I \in \Lambda$), hence $I = J \cap K$ with $I \subsetneq J$ and $I \subsetneq K$. Since I is maximal in Λ we have $J \notin \Lambda$ and $K \notin \Lambda$. Therefore we can write J and K as finite intersections of irreducible ideals, say $J = J_1 \cap \ldots \cap J_j$ and $K = K_1 \cap \ldots \cap K_k$. But then:

$$I = J \cap K = J_1 \cap \ldots \cap J_j \cap K_1 \cap \ldots \cap K_k$$

can be written as a finite intersection of irreducible ideals. This is a contradiction since $I \in \Lambda$, therefore $\Lambda = \emptyset$ and every ideal $I \subseteq R$ has a primary decomposition. $\square$

The main effort in this section from now on is to try to make the primary decomposition as unique as possible.

Lemma 46. *Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be $\mathfrak{p}$-primary ideals. Then $\mathfrak{q}_1 \cap \mathfrak{q}_2$ is $\mathfrak{p}$-primary.*

Proof. Let $ab \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ and assume $a \notin \sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2}$. Since $\sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2} = \sqrt{\mathfrak{q}_1} \cap \sqrt{\mathfrak{q}_2} = \mathfrak{p}$ we have that $a \notin \sqrt{\mathfrak{q}_1} = \sqrt{\mathfrak{q}_2} = \mathfrak{p}$. But they both are primary, therefore $b \in \mathfrak{q}_1$ and $b \in \mathfrak{q}_2$, that is $b \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ and $\mathfrak{q}_1 \cap \mathfrak{q}_2$ is $\mathfrak{p}$-primary. $\square$

Definition. A primary decomposition $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ is *minimal* if

(1) No one of the $\mathfrak{q}_i$'s can be deleted, that is

$$\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$$

for all $i = 1, \ldots, n$.

(2) $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ whenever $i \neq j$.

Remark 10. It follows immediately from Noether's Theorem 45 and Lemma 46 that if R is Noetherian, then every ideal $I \subseteq R$ has a minimal primary decomposition.

Theorem 47. *Let R be a Noetherian ring, let $I \subseteq R$ be an ideal and let $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a minimal primary decomposition of I. Then the following facts are equivalent for a prime $\mathfrak{p} \supseteq I$:*

(1) $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ *for some i.*

(2) There exists $x \in R$ such that $I : x = \mathfrak{p}$.

(3) There exists an embedding $R/\mathfrak{p} \hookrightarrow R/I$.

Proof. (1) $\Rightarrow$ (2) Let $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ and let $m \geq 1$ be such that $\mathfrak{p}^m \subseteq \mathfrak{q}_i$. Such m exists since R is Noetherian. Set $J := \mathfrak{q}_1 \cap \ldots \cap \hat{\mathfrak{q}}_i \cap \ldots \cap \mathfrak{q}_n$. We have:

$$J\mathfrak{p}^m \subseteq J\mathfrak{q}_i \subseteq J \cap \mathfrak{q}_i = I.$$

Choose $N \geq 1$ such that $J\mathfrak{p}^N \subseteq I$ and $J\mathfrak{p}^{N-1} \not\subseteq I$. This N exists since the decomposition is minimal, therefore $J \not\subseteq I$, and it is finite since $N \leqslant m$. Choose $y \in J\mathfrak{p}^{N-1} \smallsetminus \mathfrak{q}_i$. Notice that

$$I : y = \left(\bigcap_j \mathfrak{q}_j\right) : y = \bigcap_j (\mathfrak{q}_j : y) = R \cap R \cap \ldots \cap (\mathfrak{q}_i : y) \cap \ldots \cap R = (\mathfrak{q}_i : y)$$

because $y \in J\mathfrak{p}^{N-1} \subseteq J \subseteq \mathfrak{q}_j$ for all $j \neq i$. Also notice that $y\mathfrak{p} \subseteq J\mathfrak{p}^N \subseteq I$ by definition of y, hence

$$\mathfrak{p} \subseteq I : y = \mathfrak{q}_i : y.$$

Finally, let $z \in \mathfrak{q}_i : y$, then $zy \in \mathfrak{q}_i$, with $y \notin \mathfrak{q}_i$. Since $\mathfrak{q}_i$ is primary there exists $n \geq 1$ such that $z^n \in \mathfrak{q}_i$, which means $z \in \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. Therefore $\mathfrak{q}_i : y \subseteq \mathfrak{p}$ and this forces $\mathfrak{p} = I : y$.

(2) $\Rightarrow$ (3) Note that $x \notin I$. Define:

$$\varphi : R \to R/I$$
$$r \mapsto \overline{rx}$$

Then φ is a R-homomorphism and $\ker \varphi = \mathfrak{p}$, thus there is an induced monomorphism:

$$\hat{\varphi} : R/\mathfrak{p} \hookrightarrow R/I.$$

(3) $\Rightarrow$ (1) Consider

$$\psi : R \to R/I$$

such that $\ker \psi = \mathfrak{p}$. Set $x = \psi(1)$ modulo I, then $x \notin I$. Note that

$$I : x = (\mathfrak{q}_1 : x) \cap \ldots \cap (\mathfrak{q}_n : x) = \mathfrak{p},$$

so that, using the fact that $\mathfrak{p}$ is prime, there exists i such that

$$\mathfrak{q}_i : x \subseteq \mathfrak{p} = (\mathfrak{q}_1 : x) \cap \ldots \cap (\mathfrak{q}_n : x) \subseteq \mathfrak{q}_i : x,$$

and clearly

$$\sqrt{\mathfrak{q}_i : x} \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{q}_i : x}.$$

This implies $\sqrt{\mathfrak{q}_i : x} = \mathfrak{p}$. As a consequence $x \notin \mathfrak{q}_i$, otherwise $\mathfrak{p} = \sqrt{\mathfrak{q}_i : x} = R$, which gives a contradiction. Then, let $y \in \sqrt{\mathfrak{q}_i : x}$, so that there exists $n \geq 1$ such that $xy^n \in \mathfrak{q}_i$. But $x \notin \mathfrak{q}_i$ and $\mathfrak{q}_i$ is primary. This implies $(y^n)^m \in \mathfrak{q}_i$ for some $m \geq 1$, that is $y \in \sqrt{\mathfrak{q}_i}$. Finally, one always has $\sqrt{\mathfrak{q}_i} \subseteq \sqrt{\mathfrak{q}_i : x}$, so that $\sqrt{q_i : x} = \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. $\qquad\square$

Corollary 2. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. If $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \ldots \cap \mathfrak{q}'_m$ are minimal prime decompositions, then $n = m$ and, after re-indexing, $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}'_i}$ for all $i = 1, \ldots, n$.*

Proof. Let $\mathfrak{a} := \{\mathfrak{p} : \mathfrak{p} \text{ is prime and } \mathfrak{p} = I : x \text{ for some } x \in R\}$. Then

$$\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\} = \mathfrak{a} = \{\sqrt{\mathfrak{q}'_1}, \ldots, \sqrt{\mathfrak{q}'_m}\}$$

and they all are distinct. So it has to be $n = m$ and $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}'_i}$ after re-indexing. $\qquad\square$

Definition. Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Let $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a minimal primary decomposition. Then the prime ideals $\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}$ are called *associated primes* to R/I and we denote

$$\mathrm{Ass}(R/I) := \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}.$$

Proposition 48. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Then $x \in R$ is a zero divisor modulo I if and only if there exists $\mathfrak{p} \in \mathrm{Ass}(R/I)$ such that $x \in \mathfrak{p}$. In other words*

$$\bigcup_{\mathfrak{p} \in \mathrm{Ass}(R/I)} \mathfrak{p} = \{\text{zero divisors modulo } I\}.$$

Proof. Suppose $x \in \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(R/I)$. Since $\mathfrak{p}$ is associated there exists $r \in R$ such that $\mathfrak{p} = I : r$. If $x \in I$ then it is zero modulo I. So suppose $x \in R \smallsetminus I$. Since $x \in \mathfrak{p} = I : r$, we have $rx \in I$. Notice that $r \notin I$ since $I : r = \mathfrak{p} \neq (1)$, therefore x is a zero divisor modulo I.
Conversely assume r is a zero divisor modulo I. So there exists $y \notin I$ such that $ry \in I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$. Since $y \notin I$ there exists $\mathfrak{q}_i$ such that $y \notin \mathfrak{q}_i$. Since $ry \in I \subseteq \mathfrak{q}_i$ it has to be $r \in \sqrt{\mathfrak{q}_i} \in \mathrm{Ass}(R/I)$. $\qquad\square$

Definition. Let R be a ring and let $I \subseteq R$ be an ideal. A prime ideal $\mathfrak{p} \supseteq I$ is said to be a *minimal prime* of I if there is no prime ideal $\mathfrak{q}$ such that

$$I \subseteq \mathfrak{q} \subsetneq \mathfrak{p}.$$

We denote the set of all minimal primes of I by $\mathrm{Min}(I)$.

Proposition 49. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Then minimal primes of I exist and they are a finite number. In fact, every minimal prime of I is an associated prime of R/I.*

Proof. Let $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a minimal primary decomposition and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ for all $i = 1, \ldots, n$ be the associated primes. Take $\mathfrak{p}_i$ minimal among $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ (minimal in the sense that there is no $\mathfrak{p}_j$ such that $\mathfrak{p}_j \subsetneq \mathfrak{p}_i$). Notice that in general there might be more than one prime among $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ satisfying this condition. In that case just pick one. Assume that $\mathfrak{p}$ is a prime such that $I \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$. Then

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n \subseteq \mathfrak{p}$$

and, since $\mathfrak{p}$ is prime, we get $\mathfrak{q}_j \subseteq \mathfrak{p}$ for some j. Also, taking radicals, we get $\mathfrak{p}_j \subseteq \mathfrak{p}$. So $\mathfrak{p}_j \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$ and, by minimality of $\mathfrak{p}_i$, it has to be $\mathfrak{p}_j = \mathfrak{q} = \mathfrak{p}_i$. This proves that $\mathfrak{p}_i$ is a minimal prime of I, and therefore minimal primes of I exist. Now take $\mathfrak{p} \supseteq I$ a minimal prime of I. With the same argument we can show that $I \subseteq \mathfrak{p}_j \subseteq \mathfrak{p}$ for some j, and hence $\mathfrak{p}_j = \mathfrak{p}$ by definition of minimal prime. Therefore every minimal prime of I is an associated prime of R/I. In particular this means that there are only finitely many minimal primes of I. $\qquad \square$

Remark 11. Not every associated prime is a minimal prime. For instance:

$$I = (x^2, xy) = (x) \cap (x^2, y) \subseteq k[x, y] = R.$$

In this case $\mathrm{Min}(I) = \{(x)\} \subsetneq \mathrm{Ass}(R/I) = \{(x), (x, y)\}$.

Proposition 50. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Let $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a minimal primary decomposition and suppose $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ is a minimal prime of I. Then:*

$$\mathfrak{q}_i = \bigcup_{s \notin \mathfrak{p}_i} (I : s).$$

Proof. Let $r \in (I : s)$ for some $s \notin \mathfrak{p}_i$. Then $rs \in I \subseteq \mathfrak{q}_i$, and therefore $r \in \mathfrak{q}_i$ because it is primary.

Conversely notice that $\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{p}_i$, otherwise there would be $\mathfrak{q}_j \subseteq \mathfrak{p}_i$ and hence $\mathfrak{p}_j \subseteq \mathfrak{p}_i$. The decomposition is minimal, so the two primes cannot be equal, but this would contradict the fact that $\mathfrak{p}_i$ is a minimal prime of I. So we can pick $s \in \bigcap_{j \neq i} \mathfrak{q}_j \smallsetminus \mathfrak{p}_i$. Let $x \in \mathfrak{q}_i$, then $xs \in \bigcap_{j=1}^n \mathfrak{q}_j = I$, which means $x \in (I : s)$ for $s \notin \mathfrak{p}_i$. $\qquad \square$

Corollary 3. *Primary components whose radicals are minimal primes are independent of the primary decomposition.*

Proof. If $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ is a minimal primary decomposition and $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ is a minimal prime of I, then by Proposition 50 we have

$$\mathfrak{q}_i = \bigcup_{s \notin \mathfrak{p}_i} (I : s).$$

In particular the right hand side is independent of the chosen decomposition, and so is $\mathfrak{q}_i$. $\qquad \square$

Theorem 51 (Yao). *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Let*

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = I = \mathfrak{q}'_1 \cap \ldots \cap \mathfrak{q}'_n$$

be minimal primary decompositions, with $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}'_i}$. Then, for all $1 \leq i \leq n$

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{i-1} \cap \mathfrak{q}'_i \cap \mathfrak{q}_{i+1} \cap \ldots \cap \mathfrak{q}_n$$

is still a minimal primary decomposition of I.

Remark 12. We know from Chapter 1 that

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \supseteq I \\ \mathfrak{p} \text{ prime}}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \text{Min}(I)} \mathfrak{p}.$$

Then this is the unique minimal primary decomposition of $\sqrt{I}$.

Chapter 6

Integral Closure

1 Definitions and Notation

Definition. Let $R \subseteq S$ be rings. An element $s \in S$ is *integral* over R if there exists a monic polynomial $f(t) \in R[t]$ such that $f(s) = 0$. Trivially, if $r \in R$, then r is integral over R. We say that S is integral over R if every element of S is integral over R.

Example 57. The irrational number $\sqrt{2}$ is integral over $\mathbb{Z}$ because it satisfies the polynomial $t^2 - 2$.

Example 58. The rational number $1/2$ is not integral over $\mathbb{Z}$.

Example 59. If e is idempotent in S, then e is integral over R. That is, e is a root of $t^2 - t$.

Definition. We say R is *integrally closed in S* if $s \in S$ integral over R implies that $s \in R$. The set of all elements of S integral over R is called the *integral closure of R in S*. If R is a domain with fraction field K, then the *integral closure* of R is the set of all elements in K that are integral over R. We say that R is *integrally closed* if R is integrally closed in K.

Remark. If $K \subseteq L$ are fields, then L is integral over K if and only if L is algebraic over K.

Definition. For rings $R \subseteq S$, S is said to be *module-finite* over R if S is finitely generated as an R-module. S is said to be *finite as an R-algebra* if there exists $s_1, s_2, \ldots, s_n$ in S such that $S = R[s_1, s_2, \ldots, s_n]$.

Remark. If S is module-finite, then S is finite as an R-algebra, but not the converse.

Example 60. Given a field k, the polynomial ring $k[x]$ is finite as an algebra, but not as a k-module

Lemma 52. *Let $R \subseteq S \subseteq T$ be rings. Suppose S is module-finite over R and T is module-finite over S, then T is module-finite over R.*

Proof. Let $T = St_1 + \cdots + St_n$ and $S = Rs_1 + \cdots + Rs_m$. Then $T = \sum_{i,j} Rs_i t_j$. That is, the $s_i t_j$'s generate T. $\qquad\square$

Theorem 53. *Let $R \subseteq S$ be rings. The following are equivalent:*

(1) *S is module-finite over R;*

(2) *$S = R[s_1, s_2, \ldots, s_n]$, where $s_i \in S$ and each one is integral over R;*

(3) *S is a finitely generated R-algebra and S is integral over R.*

Proof. (3)$\Rightarrow$ (2) Easy exercise.

(2)$\Rightarrow$ (1) Induct on n. For $n = 1$, we have that $S = R[s]$ and there exists a monic polynomial $p(t) = t^m + r_1 t^{m-1} + \cdots + r_m$ with $r_i \in R$ such that $p(s) = 0$.

Claim. $S = R \cdot 1 + R \cdot s + \cdots + R \cdot s^{m-1}$

Proof of the Claim. Let the right hand side of the claim be defined as N. Clearly, $1, s, s^2, \ldots, s^{m-1} \in S$, so that $N \subseteq S$. Conversely, if $w > m - 1$, write

$$s^m = -(r_1 s^{m-1} + \cdots + r_m)$$

Hence if we multiply by s^{w-m} we get

$$s^w = -(r_1 s^{w-1} + \cdots + r_m s^{w-m}).$$

Inductively we get $s^w \in N$ for all $w \in \mathbb{N}$. This proves the claim.

For $n > 1$, let $T = R[s_1, \ldots, s_{n-1}]$ and $S = T[s_n]$. Notice that by induction, T is module-finite over R and that S is module finite over T. Hence by lemma 52 S is module-finite over R.

(1)$\Rightarrow$ (3): Write $S = R \cdot s_1 + \cdots + R \cdot s_n$, then $S = R[s_1, \ldots, s_n]$, so S is a finitely generated R-algebra. To show S is integral over R, let $u \in S$ and notice $us_i \in S$. So there exists equations $us_i = \sum_{j=1}^n r_{ij} s_j$ where $r_{ij} \in R$ for $i = 1, 2, \ldots, n$. This implies

$$\sum_{j=1}^n (u \cdot \delta_{ij} - r_{ij}) = 0 \tag{6.1}$$

for all $i = 1, 2, \ldots, n$. Let

$$A = \begin{pmatrix} u - r_{11} & & -r_{ij} \\ & \ddots & \\ -r_{ij} & & u - r_{nn} \end{pmatrix}$$

Then 6.1 can be written as

$$
A \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.
$$

Multiplication by the adjoint of A yields

$$
\begin{pmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.
$$

Hence $\det(A) \cdot s_i = 0$ for all i. Thus $\det(A)S = 0$. In particular, $\det(A) \cdot 1 = 0$. But if t is a variable, and we let we let

$$
\tilde{A} = \begin{pmatrix} t - r_{11} & & -r_{ij} \\ & \ddots & \\ -r_{ij} & & t - r_{nn} \end{pmatrix},
$$

then $\det(\tilde{A})(t)$ is a monic polynomial in t with coefficients in R and $\det(\tilde{A})(u) = 0$. Hence u is integral over R. $\qquad\square$

Corollary 54. *Let $R \subseteq S$ be rings and T be the integral closure of R in S. Then $R \subseteq T \subseteq S$ and T is a ring.*

Proof. Let $u, v \in T$, then u, v are integral over R. By (2) $\Rightarrow$ (3) of theorem 53, $R[u, v]$ is integral over R, that is $R[u, v] \subseteq T$. Hence $u \cdot v$ and $u + v$ are integral over R. Thus T is a ring. $\qquad\square$

2 Going-Up

Remark. If W is a multiplicatively closed set in R and $R \subseteq S$ is an integral extension, then so is $R_W \subseteq S_W$. (Just use the same equations for $\frac{s}{1} \in S_W$.) Moreover, in general, if s is integral over R and $w \in R$, then ws in integral over R since $R[s]$ is integral over R. (You could also multiply the integral equation for s by w^n.)

Theorem 55 (Lying Over)**.** *Let $R \subseteq S$ be an integral extension of rings, then $i^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective. I.e. for all $\mathfrak{q} \in \mathrm{Spec}(R)$, there exists $Q \in \mathrm{Spec}(S)$ such that $Q \cap R = \mathfrak{q}$.*

Proof. Let $\mathfrak{q} \in \mathrm{Spec}(R)$. Then $R_{\mathfrak{q}} \to S_{\mathfrak{q}}$ is integral. Suppose we prove that there exists $Q \in \mathrm{Spec}(S_{\mathfrak{q}})$ such that $Q \cap R_{\mathfrak{q}} = \mathfrak{q}R_{\mathfrak{q}}$. Set $Q' = Q \cap S \in \mathrm{Spec}(S)$

and compute

$$
\begin{aligned}
Q' \cap R &= (Q \cap S) \cap R \\
&= Q \cap (S \cap R) \\
&= Q \cap R \\
&= (Q \cap S_{\mathfrak{q}}) \cap R \\
&= Q \cap (S_{\mathfrak{q}} \cap R).
\end{aligned}
$$

But if $s/t \in S_{\mathfrak{q}} \cap R$ (for $s \in S$ and $t \in R \smallsetminus \mathfrak{q}$), there exist $r \in R$ and $u \in R \smallsetminus \mathfrak{q}$ such that

$$us = utr \in R.$$

Therefore

$$\frac{s}{t} = \frac{us}{ut} \in R_{\mathfrak{q}},$$

and this shows $S_{\mathfrak{q}} \cap R = R_{\mathfrak{q}} \cap R$. Hence

$$
\begin{aligned}
Q' \cap R &= Q \cap (S_{\mathfrak{q}} \cap R) \\
&= Q \cap (R_{\mathfrak{q}} \cap R) \\
&= (Q \cap R_{\mathfrak{q}}) \cap R \\
&= \mathfrak{q} R_{\mathfrak{q}} \cap R \\
&= \mathfrak{q}
\end{aligned}
$$

Let us change the notation: without loss of generality, $(R, \mathfrak{m})$ is local and $\mathfrak{q} = \mathfrak{m}$. $R \to S$ is integral. First suppose $\mathfrak{m}S \neq S$. Then there exists a prime ideal Q in S such that $\mathfrak{m}S \subseteq Q$. But then $\mathfrak{m} \subseteq \mathfrak{m}S \cap R \subseteq Q \cap R \subseteq R$. Since $\mathfrak{m}$ is maximal, $Q \cap R = \mathfrak{m}$ proving the theorem for this case.

If $\mathfrak{m}S = S$, write $\sum_{i=1}^{n} r_i s_i = 1$ for $r_i \in \mathfrak{m}$ and $s_i \in S$. By theorem 53, $B = R[s_1, \ldots, s_n]$ is a finite R-module. Notice that we have $\mathfrak{m}B = B$. Hence NAK implies that $B = 0$, a contradiction. $\qquad\square$

Remark. Suppose $R \subseteq S$ is an integral extension and $J \subseteq S$ is an ideal. Then the injection

$$\frac{R}{J \cap R} \hookrightarrow \frac{S}{J}$$

is an integral extension.

Theorem 56 (Going-Up). *Let $R \subseteq S$ be an integral extension of rings. Let $\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ be a chain of primes in R. Let $Q_0 \in \operatorname{Spec}(S)$ such that $Q_0 \cap R = \mathfrak{q}_0$. Then there exists a chain $Q_0 \subseteq Q_1 \subseteq \cdots \subseteq Q_n$ of primes in S such that $Q_i \cap R = \mathfrak{q}_i$ for $i = 0, 1, \ldots, n$.*

Proof. By induction, it is enough to show there exists Q_1 such that $Q_0 \subseteq Q_1$, $Q_1 \cap R = \mathfrak{q}_1$, $Q_0 \cap R = \mathfrak{q}_0$, and $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$. By the remark, $R/\mathfrak{q}_0 \hookrightarrow S/Q_0$ is integral and $\mathfrak{q}_1/\mathfrak{q}_0 \in \operatorname{Spec}(R/\mathfrak{q}_0)$. Lying over gives a prime $Q_1/Q_0 \in \operatorname{Spec}(S/Q_0)$ such that $Q_1/Q_0 \cap R/\mathfrak{q}_0 = \mathfrak{q}_1/\mathfrak{q}_0$. Retracting back to S and R gives us the desired result. $\qquad\square$

Theorem 57 (Incomparable)**.** *Let $R \subseteq S$ be an integral extension of rings. Suppose that $Q, Q' \in \mathrm{Spec}(S)$ and that $Q \subseteq Q'$. If $Q \cap R = Q' \cap R$ then $Q = Q'$.*

Proof. Consider $R/Q \cap R \subseteq S/Q$ (still integral). Without loss of generality, $R \subseteq S$ are domains, $Q' \in \mathrm{Spec}(S)$, $Q' \cap R = 0$ and we want to prove $Q' = 0$. Let $W = R - \{0\}$. Then $R_W \subseteq S_W$ is integral and $Q'S_W$ is a proper prime (since $Q' \cap W = \emptyset$). We have reduced to: $k \subseteq S$ is integral where k is a field and S a domain, $Q' \cap k = 0$. This implies $Q' = 0$.

Hence by the following lemma the theorem is proved. □

Lemma 58. *Let $R \subseteq S$ be an integral extension of domains. Then S is a field if and only if R is a field.*

Proof. Assume that R is a field and let $u \in S$, $u \neq 0$. There exists an equation of least degree $u^n + \alpha_1 u^{n-1} + \cdots + \alpha_n = 0$, $\alpha_i \in R$. By choice of n, $\alpha_n \neq 0$. Hence $u(u^{n-1} + \cdots + \alpha_{n-1}) = -\alpha_n \in R$ and u is a unit in S.

Now assume that S is a field and let $u \in R$, $u \neq 0$. Since S is a field, $u^{-1} \in S$. Since S is integral over R, there exists an equation

$$(u^{-1})^n + r_1(u^{-1})^{n-1} + \cdots + r_n = 0$$

for $r_i \in R$. Multiplication by u^n and solving for 1 shows that the inverse of u is an element of R. □

Definition. The *Krull dimension* of a ring R, denoted $\dim R$, is the supremum on n of the set of chains

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

where $\mathfrak{p}_i \in \mathrm{Spec}(R)$.

Example 61. (1) If k is a field, $\dim k = 0$.

(2) $\dim \mathbb{Z} = 1$.

(3) If k is a field, $\dim k[x] = 1$.

Theorem 59. *Let $R \subseteq S$ be an integral extension of rings. Then $Q \in \mathrm{Spec}(S)$ is maximal if and only if $Q \cap R = \mathfrak{q}$ is maximal in R.*

Proof. Notice that $R/Q \cap R \subseteq S/Q$ is an integral extension of domains. The rest follows for lemma 58. □

Example 62. The polynomial ring $S = k[x, y, z]$ where k is a field is integral over $R = k[x^3, y^5, z^9]$.

Proof. Consider the following, polynomials: $t^3 - x^3$, $t^5 - y^5$, $t^9 - z^9 \in R[t]$. Use theorem 53 so say that S is integral over R. □

Theorem 60. *Let $R \subseteq S$ be an integral extension of rings, then $\dim R = \dim S$*

Proof. Let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ be a chain in R. By lying over, there exists Q_0 over P_0 and by going up, there exists

$$
\begin{array}{ccccccc}
Q_0 & \subsetneq & Q_1 & \subsetneq \cdots \subsetneq & Q_n \\
\downarrow & & \downarrow & & \downarrow \\
P_0 & \subsetneq & P_1 & \subsetneq \cdots \subsetneq & P_n
\end{array}
$$

and all the Q_i's are distinct. Hence $\dim R \leqslant \dim S$.

Conversely,

$$
\begin{array}{ccccccc}
Q_0 & \subsetneq & Q_1 & \subsetneq \cdots \subsetneq & Q_n & & \in \operatorname{Spec}(S) \\
\downarrow & & \downarrow & & \downarrow \\
Q_0 \cap R & \subsetneq & Q_1 \cap R & \subsetneq \cdots \subsetneq & Q_n \cap R
\end{array}
$$

where the $Q_i \cap R$ are distinct by incomparability. Thus $\dim R \geqslant \dim S$.   □

Example 63.   (1) If R is an Artinian ring, then $\dim R = 0$ (since every prime is maximal).

(2) Consider the extension $\mathbb{Z} \subseteq \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is integral over Z, $\dim \mathbb{Z}[i] = 1$.

Remark. If R is Noetherian and $\dim R = 0$, then R is Artinian.

3   Normalization and Nullstellensatz

Theorem 61 (Neother Normalization Lemma)**.** *Let k be a field and S a finitely generated k-algebra. Then there exists $y_1, y_2, \ldots, y_d$ in S which are algebraically independent over k such that S is integral (even module-finite) over the subring $k[y_1, y_2, \ldots, y_d] = R \subseteq S$.*

Definition. For k a field and S a ring such that $k \subseteq S$, $y_1, y_2, \ldots, y_d \in S$ are *algebraically independent* over k if for any non-zero polynomial $p(T_1, T_2, \ldots, T_d) \in k[T_1, T_2, \ldots, T_d]$, $p(y_1, y_2, \ldots, y_d) \neq 0$. Equivalently, $k[y_1, y_2, \ldots, y_d]$ is isomorphic to $k[T_1, T_2, \ldots, T_d]$.

Example 64. Let k be a field and $S = k[t^2, t^3] \simeq k[x, y]/(y^2 - x^3)$. We have that t^2 is algebraically independent over k, so let $R = k[t^2]$, i.e. a polynomial ring in one variable. Notice that $(t^3)^2 - (t^2)^3 = 0$. For $p(T) = T^2 - t^6 \in R[T]$, $p(t^3) = 0$. Thus S is integral over R.

Lemma 62. *Let k be a field and $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. Then for all N sufficiently large, there exists a change of variables,*

$$x_n' = x_n$$
$$x_{n-1}' = x_{n-1} - x_n^N$$
$$x_{n-2}' = x_{n-2} - x_n^{N^2}$$
$$\vdots$$
$$x_1' = x_1 - x_n^{N^{n-1}}$$

such that when we write $f(x_1, \ldots, x_n) = g(x_1', \ldots, x_n')$,

$$g(x_1', \ldots, x_n') = \alpha(x_n')^L + (x_n')^{L-1} g_1(x_1', \ldots, x_{n-1}') + \cdots + g_L(x_1', \ldots, x_{n-1}')$$

where $\alpha \neq 0$, $\alpha \in k$ and $g_1, g_2, \ldots, g_L \in k[x_1', \ldots, x_{n-1}']$.

Proof. Write $f = \sum_{\alpha \in I} \lambda_\alpha \underline{x}^\alpha$ where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $|I| < \infty$, $\lambda_\alpha \in k$, $\lambda_\alpha \neq 0$, $\underline{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Choose $N > \max_{\alpha \in I}\{\alpha_i\}$. Rewrite f using the change of variable (notice that $k[x_1, \ldots, x_n] = k[x_1', \ldots, x_n']$). So

$$f = \sum_{\alpha \in I} \lambda_\alpha (x_1' + x_n^{N^{n-1}})_1^\alpha (x_2' + x_n^{N^{n-2}})_2^\alpha \cdots (x_{n-1}' + x_n^N)_1^\alpha x_n^{\alpha_n}.$$

We have to rewrite as a polynomial in x_n. The highest degree contribution from the α-monomial is $x_N^{\alpha_1 N^{n-1} + \alpha_n N^{n-2} + \cdots + \alpha_n}$. Since $N > \alpha_i$ for all α_i appearing, if $L = \alpha_1 N^{n-1} + \alpha_n N^{n-2} + \cdots + \alpha_n$, then this is the base N expansion of L. This is unique. Hence f becomes monic up to a non-zero element of k as no cancellation occurs. $\qquad\square$

Example 65. Let $f(x_1, x_2, x_3, x_4) = x_1 x_4 - x_2 x_3$ and $x_4 = x_4' + x_1$. Keep x_1, x_2, x_3 fixed. Then

$$f(x_1, x_2, x_3, x_4) = x_1(x_4' + x_1) - x_2 x_3 = x_1^2 + x_4' x_1 - x_2 x_3$$

Proof of Noether Normalization Lemma; Theorem 61. We can write $S = k[t_1, \ldots, t_n]$. Induct on n. If $n = 0$ there is nothing to prove. Assume that $n > 0$.

Case 1. $t_1, \ldots, t_n$ are algebraically independent over k.

If this is the case, then take $y_i = t_i$, then $R = S$.

Case 2. There exists a non-zero polynomial $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ such that $f(t_1, \ldots, t_n) = 0$. With out loss of generality, using the lemma, we can assume that

$$f = t_n^L + t_n^{L-1} g_1(t_1, \ldots, t_{n-1}) + \cdots + g_L(t_1, \ldots, t_{n-1}).$$

Then we have an integral extension

$$k \subseteq k[t_1, \ldots, t_{n-1}] \overset{\text{integral}}{\subseteq} k[t_1, \ldots, t_n] = S.$$

By induction, there exists $y_1, \ldots, y_d \in k[t_1, \ldots, t_{n-1}]$. algebraically independent over k such that

$$k[y_1, \ldots, y_d] \overset{\text{integral}}{\subseteq} k[t_1, \ldots, t_{n-1}] \overset{\text{integral}}{\subseteq} S.$$

Therefore S is integral over $k[y_1, \ldots, y_d]$.

$\square$

Example 66. Let k be a field and consider the ring $k[x, y, u, v]$ such that

$$\begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} u & v \end{pmatrix} = \begin{pmatrix} xu & xv \\ yu & yv \end{pmatrix} \quad \text{and} \quad \det \begin{pmatrix} xu & xv \\ yu & yv \end{pmatrix} = 0.$$

If $S = k[xu, xv, yu, yv]$, find a polynomial subring over which S is integral.

Let $f(x_1, x_2, x_3, x_4) = x_1 x_4 - x_2 x_3$. Then $f(xu, yu, xv, yv) = 0$. If we let $x_4' = x_4 - x_1$ as in example 65, then

$$f(x_1, x_2, x_3, x_4) = x_1^2 + x_4' x_1 - x_2 x_3 = g(x_1, x_2, x_3, x_4')$$

and $g(xu, yu, xv, yv) = 0$. Since g is monic in x_1, xu is integral over the polynomial ring $k[yu, xv, yv - xu] \subseteq S$ and $yu, xv, yv - xu$ are algebraically independent.

Corollary 63. *Let K and L be fields, L a finitely generated K-algebra. Then L is algebraic over K. In particular, if $K = \overline{K}$ (the algebraic closure of K), then $L = K$.*

Proof. By the normalization lemma, there exists $y_1, \ldots, y_d$ algebraically independent over K such that $K[y_1, \ldots, y_d] \subseteq L$ is integral. Since L is a field, we must have $K[y_1, \ldots, y_d]$ is a field. Hence $d = 0$ and L is algebraic over K. $\square$

Theorem 64. *Let $S = k[t_1, \ldots, t_n]$ be a finitely generated k-algebra, and let $\mathfrak{m}$ be a maximal ideal of S. Then there exists a canonical embedding $k \hookrightarrow S/\mathfrak{m} = L$ and L is algebraic over k.*

Proof. There exists a map

$$k \overset{\hookrightarrow}{\longrightarrow} S \longrightarrow S/\mathfrak{m}.$$
$$\phi$$

Since k is a field and $\phi \neq 0$, $\ker(\phi) = 0$. But $L = k[\overline{t_1}, \ldots, \overline{t_n}]$, $\overline{t_i} = t_i + \mathfrak{m}$. Apply the corollary to finish the proof. $\square$

Corollary 65. *Let k be an algebraically closed field, $R = k[x_1, \ldots, x_n]$. Then every maximal ideal $\mathfrak{m}$ of R has the form:*

$$\mathfrak{m} = (x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n)$$

where $\alpha_i \in k$. Conversely, all such ideals are maximal.

Proof. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\phi_\alpha : k[x_1, \ldots, x_n] \to k$ be the evaluation map $f(x_1, \ldots, x_n) \mapsto f(\alpha_1, \ldots, \alpha_n)$. This is a surjective ring homomorphism so $R/\ker(\phi_\alpha) \simeq k$; i.e. $\mathfrak{m}_\alpha = \ker(\phi_\alpha)$ is maximal. Clearly $(x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n) \subseteq \mathfrak{m}_\alpha$. By the Taylor expansion,

$$f(x_1, \ldots, x_n) = f(\alpha_1, \ldots, \alpha_n) + \sum_i (x_i - \alpha_i)\frac{\partial f}{\partial x_i}(\alpha) + \text{other terms in } (x_i - \alpha_i)$$

Hence $f(\underline{x}) \equiv f(\alpha) \pmod{(x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n)}$. So all said ideals are maximal.

Let $\mathfrak{m}$ be maximal in R. By theorem 64 the map $\overline{k} = k \hookrightarrow R/\mathfrak{m}$ implies that $k = R/\mathfrak{m}$. Hence there exists $\alpha_i \in k$ where $\alpha_i \mapsto x_i + \mathfrak{m}$ for all $i = 1, \ldots, n$. I.e. $\alpha_i + \mathfrak{m} = x_i + \mathfrak{m}$, thus $x_i - \alpha_i \in \mathfrak{m}$. Therefore $(x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n) \subseteq \mathfrak{m}$ and by above we have equality. $\qquad\square$

Theorem 66 (Hilbert's Nullstellensatz)**.** *Let k be a field, $R = k[x_1, \ldots, x_n]$, and I an ideal of R. Then*

$$\sqrt{I} = \bigcap_{\mathfrak{m} \supseteq I} \mathfrak{m}$$

where $\mathfrak{m}$ are maximal ideals in R.

Proof. First reduce to the case k is algebraically closed. Let $\overline{k}$ be the algebraic closure of k. We now have an integral extension $R = k[x_1, \ldots, x_n] \subseteq \overline{k}[x_1, \ldots, x_n] = S$. Suppose we prove the theorem for S. Then for all $I \subseteq R$,

$$\sqrt{IS} = \bigcap_{\mathfrak{n} \supseteq IS} \mathfrak{n}$$

where $\mathfrak{n}$ is maximal in S. Hence

$$\sqrt{IS} \cap R = \left(\bigcap_{\mathfrak{n} \supseteq IS} \mathfrak{n}\right) \cap R = \bigcap_{\mathfrak{n} \supseteq IS} (\mathfrak{n} \cap R) = \bigcap_{\mathfrak{m} \supseteq I} \mathfrak{m}$$

where $\mathfrak{m}$ is maximal in R. And since $\sqrt{IS} = \bigcap \mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Spec}(S)$ containing IS, by going up

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

Hence without loss of generality, $k = \overline{k}$. Let $f \in \bigcap_{\mathfrak{m} \supseteq I} \mathfrak{m}$ for $\mathfrak{m}$ maximal in R. Suppose $f \notin \sqrt{I}$ and consider $R[y] = k[x_1, \ldots, x_n, y]$.
Claim. $(\sqrt{I}, yf - 1) = R[y]$.

If not, then $(\sqrt{I}, yf - 1) \subseteq \mathfrak{m}$ for $\mathfrak{m}$ maximal in $R[y]$, i.e. $\mathfrak{m} = (x_1 - \alpha, \ldots, x_n - \alpha_n, y - \beta)$. Hence $I \subseteq (x_1 - \alpha, \ldots, x_n - \alpha_n)$ and $\beta f(\alpha_1, \ldots, \alpha_n) - 1 = 0$. But by assumption, $f \in (x_1 - \alpha, \ldots, x_n - \alpha_n)$, and thus $f(\alpha_1, \ldots, \alpha_n) = 0$. A contradiction.

Now write

$$1 = \sum_i h_i(\underline{x}, y)g_i(\underline{x}) + l(\underline{x}, y)(xf - 1)$$

where $g_i(\underline{x}) \in \sqrt{I}$. Substitute y with $1/f$ to get $1 = \sum h_i(\underline{x}, 1/f)g_i(\underline{x})$. Hence for $N \gg 0$ we have that

$$f^N = \sum_i f^N h_i(\underline{x}, 1/f)g_i(\underline{x}) \in \sqrt{I}.$$

That is, $f \in \sqrt{I}$.

$\square$

4 Going-Down

Proposition 67. *Let $A \subseteq B$ be rings and C the integral closure of A in B. If $S \subseteq A$ is multiplicatively closed, then C_S is the integral closure of A_S in B_S.*

Proof. Clearly , C_S is in the integral closure of A_S in B_S. Conversely, for any $x/s \in B_S$ which is integral over A_S we have

$$\left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s} = 0.$$

This gives the following equality,

$$\frac{x^n + a_1 x^{n-1} + \cdots + a_n s^{n-1}}{s^n} = 0 \in B_S.$$

Thus there is a $t \in S$ such that $t^n(x^n + a_1 x^{n-1} + \cdots + a_n s^{n-1}) = 0$ in B. That is, tx is integral over A, i.e. $tx \in C$. Hence $\frac{x}{s} = \frac{tx}{ts} \in C_S$. $\square$

Recall. As defined on page 55, an integral domain is called integrally closed if it is integrally closed in the fraction field.

Proposition 68. *Let A be a domain. The following are equivalent:*

(1) A is integrally closed;

(2) $A_\mathfrak{p}$ is integrally closed for all primes $\mathfrak{p}$ in A;

(3) $A_\mathfrak{m}$ is integrally closed for all maximal $\mathfrak{m}$ in A.

Proof. Let K be the fraction field of A, and let C be the integral closure of A in K. Let $f : A \hookrightarrow C$ be the inclusion map. But f is an isomorphism iff $f_\mathfrak{p}$ is an isomorphism for all $\mathfrak{p} \in \mathrm{Spec}(A)$ iff $f_\mathfrak{m}$ is an isomorphism for all $\mathfrak{m} \in \mathrm{Spec}(A)$. $\square$

Remark. Let $A \subseteq B$ be rings and $A \subseteq C \subseteq B$. Then C is the integral closure of A in B if and only if the statement is true locally.

Definition. Let $A \subseteq B$ be rings and I an ideal of A. Then we say $x \in B$ is *integral over I* if x satisfies

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

with $a_i \in I$.

Lemma 69. *Let $A \subseteq C \subseteq B$, A, B be rings, C the integral closure of A in B, and I an ideal of A. Then the integral closure over I in B is $\sqrt{IC}$.*

Proof. Choose $x \in B$ integral over I. Then $x^n + a_1 x^{n-1} + \cdots + a_0 = 0$ where $a_i \in I$ and thus

$$x^n = -(a_1 x^{n-1} + \cdots + a_0) \in IC.$$

I.e. $x \in \sqrt{IC}$.

Now choose $x \in \sqrt{IC}$. Then $x^n = \sum_{i=1}^{m} a_i x_i$ with $a_i \in I$, $x_i \in C$. Let $M = A[x_1, \ldots, x_m]$. Then M is finite as an A-module, M is faithful, and $x^n \in M \subseteq IM$. Therefore x^n (and even more so x) is integral over I by Cayley Hamilton. $\square$

Proposition 70. *Let $A \subseteq B$ be domains, A integrally closed in its fraction field k, I an ideal of A and $x \in B$ integral over I. Let*

$$f(t) = t^n + a_t^{n-1} + \cdots + a_n \in k[t]$$

be the minimal polynomial of x over k. Then $a_i \in \sqrt{I}$.

Proof. First, x satisfies $g(x) = 0$ where $g(t) = t^m + b_1 t^{m-1} + \cdots + b_m \in A[t]$, $b_i \in I$. This implies that $f(t)|g(t)$. Next choose a field such that $B \subseteq L$ and $f(t) = (t - x_1)(t - x_2) \cdots (t - x_n)$. Since f divides g, $g(x_i) = 0$ for all i. Hence each x_i is integral over I and thus all $a_i \in k$ are integral over I. That is, $a_i \in \sqrt{I}$ by the previous lemma. $\square$

Lemma 71 ([1], prop 3.16). *Let $A \to B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}$ is the contraction of a prime ideal of B if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. If $\mathfrak{p} = \mathfrak{q}^c$ then $\mathfrak{p}^{ec} = \mathfrak{p}$. Conversely, if $\mathfrak{p}^{ec} = \mathfrak{p}$, let S be the image of $A \smallsetminus \mathfrak{p}$ in B. Then $\mathfrak{p}^e$ does not meet S, therefore its extension in $S^{-1}B$ is a proper ideal and hence is contained in a maximal ideal $\mathfrak{m}$ of $S^{-1}B$. If $\mathfrak{q}$ is the contraction of $\mathfrak{m}$ in B, then $\mathfrak{q}$ is prime, $\mathfrak{q} \supseteq \mathfrak{p}^e$ and $\mathfrak{q} \cap S = \emptyset$ (since $\mathfrak{q}S^{-1}B = \mathfrak{m} \subsetneq S^{-1}B$). Hence $\mathfrak{q}^c = \mathfrak{p}$. $\square$

Theorem 72 (Going-Down). *Let $A \subseteq B$ be domains, A integrally closed, and B integral over A. Given a chain of primes $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n$ in A and a chain of primes $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_m$ in B such that $m < n$ and $Q_i \cap A = \mathfrak{p}_i$ for $i = 1, 2, \ldots, m$, then the chain of primes in B can be extended to $Q_1 \supseteq \ldots \supseteq Q_n$ such that $Q_i \cap A = \mathfrak{p}_i$ for $i = 1, 2, \ldots, n$*

Proof. It is enough to show when $n = 2$ and $m = 1$. Further, by lemma 71 we only need to show $\mathfrak{p}_2 B_{Q_1} \cap A = \mathfrak{p}_2$.

It is easy to see that $\mathfrak{p}_2 B_{Q_1} \cap A \supseteq \mathfrak{p}_2$. Conversely, for $x \in \mathfrak{p}_2 B_{Q_1}$, $x = \frac{y}{s}$ where $y \in \mathfrak{p}_2 B$ and $s \in B - Q_1$. By lemma 69 we have that y is integral over $\mathfrak{p}_2$. Thus by prop 70 the minimal polynomial of y over K (f.f. of A) is

$$f(t) = t^n + a_t^{n-1} + \cdots + a_n \in K[t]$$

with $a_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$. Since $y = sx$, $f(sx) = 0$. Thus s satisfies $g(t) = 0$ where $g(t) = f(tx)$. Let

$$h(t) = \frac{1}{x^n} g(t) = t^n + v_1 t^{n-1} + \cdots + v_n;$$

$h(s) = 0$ and $s = \frac{1}{x} y$. This implies that $h(t)$ is the minimal polynomial of s over K. Hence $v_i \in A$ by previous prop ($I = (1)$). But $v_i = a_i/x^i$. Hence $x^i v_i = a_i \in \mathfrak{p}_2$. If $x \notin \mathfrak{p}_2$ then $v_i \in \mathfrak{p}_2$ implies that s is integral over $\mathfrak{p}_2$. Hence $s \in \sqrt{\mathfrak{p}_2 B} \subseteq \sqrt{Q_1} = Q_1$. A contradiction. So $x \in \mathfrak{p}_2$ and we have equality. $\qquad\square$

Theorem 73 (Dimension of Finitely Generated k-algebras)**.** *Let R be a finitely generated k-algebra (k a field). Let R be integral over a subring $k[y_1, \ldots, y_n]$, y_i algebraically independent over k. Then*

  (1) *every chain of primes in R has length less than or equal to n. In particular, $\dim(R) \leqslant n$;*

  (2) *if R is a domain, then every saturated chain of primes has length n;*

  (3) *in particular, $\dim(k[y_1, \ldots, y_n]) = n$. So $\dim(R) = n$.*

Recall. Polynomial rings are UFD's; every polynomial $f \in k[x_1, x_2, \ldots, x_n]$ is uniquely (up to order and units) a product $f_1^{a_1} f_2^{a_2} \cdots f_k^{a_k}$, where f_i are irreducible polynomials. In particular, if f is irreducible and $f | g \cdot h$ then $f | g$ or $f | h$. I.e. (f) is a prime ideal. Consequently, if R is a polynomial ring and Q is a prime minimal over (0), but $Q \neq (0)$, then $Q = (f)$.

Lemma 74. *Suppose $R = k[x_1, \ldots, x_n]$, $f \in R$ and $f \neq 0$. Then $R/(f)$ is integral over a polynomial ring in $n - 1$ variables.*

Proof. Use a change of variables (lemma 62) so that with out loss of generality,

$$f = x_n^l + x_n^{l-1} g_1(x_1, \ldots, x_{n-1}) + \cdots + g_l(x_1, \ldots, x_{n-1}).$$

Then $R/(f)$ is integral over $k[\overline{x_1}, \ldots, \overline{x_{n-1}}] \subseteq R/(f)$; $\overline{x_i} = x_i + (f)$. To show there are no relations on the $\overline{x_i}$, we need to show there does not exist a non zero $g \in R$ in $n - 1$ variables such that $g(\overline{x_1}, \ldots, \overline{x_{n-1}}) \neq 0$ in $R/(f)$. But $g(\overline{x_1}, \ldots, \overline{x_{n-1}}) = \overline{g(x_1, \ldots, x_{n-1})}$. So the above holds if and only if $g \neq 0$ such that $f | g$ in $k[x_1, \ldots, x_n]$. But for all $h \in R$, $f \cdot h$ always has an x_n^l term. Hence such a g does not exist. $\qquad\square$

Proof of Theorem 73. (1): Induct on n. Consider a chain of primes

$$Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m$$

in R. By incomparability (theorem 57), there is a chain of primes

$$\mathfrak{q}_o \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$$

in $k[x_1, \ldots, x_n]$ where $\mathfrak{q}_i = Q_i \cap k[x_1, \ldots, x_n]$. With out loss of generality, we can assume $\mathfrak{q}_0 = 0$. Further, there exists a non zero element $g \in \mathfrak{q}_1$. If $g = g_1^{a_1} \cdots g_t^{a_t}$, g_j irreducible, then $(0) \neq (g_i) \subseteq \mathfrak{q}_1$ for some i. Thus we may also assume that $\mathfrak{q}_1 = (g)$ for some irreducible element g.

By the lemma, $k[x_1, \ldots, x_n]/(g)$ is integral over a polynomial ring in $n - 1$ variables. Since

$$0 = \mathfrak{q}_1/\mathfrak{q}_1 \subsetneq \mathfrak{q}_2/\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m/\mathfrak{q}_1$$

is chain of primes in $k[x_1, \ldots, x_n]/(g)$, by induction $m - 1 \leqslant n - 1$. Hence $m \leqslant n$.

(2): Again, induct on n. Consider a saturated chain of primes

$$Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m$$

in R. By (1), $m \leqslant n$. As before, if we contracting to $A = k[x_1, \ldots, x_n]$, we get a chain of primes

$$\mathfrak{q}_o \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$$

in $k[x_1, \ldots, x_n]$ where $\mathfrak{q}_i = Q_i \cap A$. Because $k[x_1, \ldots, x_n]$ is integrally closed, going-down holds on $A \subseteq R$.

Therefore there does not exist a prime $\mathfrak{p}$ in A between (0) and $\mathfrak{q}_1$. (This would not allow our original chain to be saturated.) As above, let $\mathfrak{q}_1 = (f)$ for some irreducible $f \in A$. Then, by the above lemma, we have the following integral extensions:

$$k[z_1, \ldots, z_{n-1}] \subseteq k[x_1, \ldots, x_n]/(f) \subseteq R/Q_1$$

where z_i are indeterminants over k. By induction, every saturated chain of primes in R/Q_1 has length $n - 1$. This applies to

$$0 = Q_1/Q_1 \subsetneq Q_2/Q_1 \subsetneq \cdots \subsetneq Q_m/Q_1.$$

Hence $n - 1 = m - 1$, that is, $n = m$.

(3): Combine (1) and (2). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

5   Examples

Example 67. Let $R = k[x, y, z]/(x) \cap (y, z)$. The minimal primes of R are xR and $(y, z)R$. Notice that

$$R/xR \simeq k[x, y, z]/(x) \simeq k[y, z].$$

So saturated chains of primes ending in xR will have length 2. Also,

$$R/(y, z)R \simeq k[x, y, z]/(y, z) \simeq k[x].$$

So saturated chains of primes ending $(y, z)R$ have length 1.

Example 68. Let $R = k[x^3, y^3, z^3, x^2y, x^2z, xyz]$. Notice that R is integral over $k[x, y, z]$, so $\dim(R) = 3$.

Example 69. Let $R = k[x, y, z, xt, yt, zt]$. Notice that the extension $R \subseteq k[x, y, z, t]$ is not integral (there is not integral relation for t). By Noether's normalization lemma (theorem 61), there exists an integral extension $k[y_1, \ldots, y_d] \subseteq R$ where the y_i's are algebraically independent over k. Let $L = k(y_1, \ldots, y_d)$ and $Q(R)$ be the quotient field of R. Since $Q(R)$ is algebraic over L (check this), $y_1, \ldots, y_d$ form a transcendence basis for $Q(R)$. Since all transcendence basis' have the same cardinality, if we can find a transcendence basis for $Q(R)$, we can determine the dimension of R. (For more on transcendence basis', see appendix A1 in [2])

Notice that $Q(R) = k(x, y, z, t)$. Since x, y, z, t are algebraically independent over k, the elements for a transcendence basis and thus $\dim(R) = 4$.

Example 70. Let $R = k[xs, ys, zs, xt, yt, zt]$. Again, $k[x, y, z, s, t]$ is not integral over k. So consider $Q(R) = k(xs, ys, zs, \frac{t}{s})$. So $\dim(R) = 4$.

Example 71. Let $R = k[x^2y, y^2z, xz]$. Notice that

$$\frac{(x^2y)^2(xz)}{y^2z} = x^5, \quad \frac{(y^2z)^2(x^2y)}{(xz)^2} = y^5, \quad \frac{(xz)^4(y^2z)}{(x^2y)^2} = z^5.$$

Since these are algebraically independent elements of $Q(R)$ and the dimension is bounded by 3, $\dim(R) = 3$.

Proposition 75. *Let $A \subseteq B$ be rings and $b \in B$. The following are equivalent:*

(1) b is integral over A;

(2) the image of b in B/P is integral over $A/(P \cap A)$ for all P in $\mathrm{Spec}(B)$;

(3) the image of b in B/P is integral over $A/(P \cap A)$ for all P in $\mathrm{Spec}(B)$ minimal over (0).

Proof. $(1) \Rightarrow (2) \Rightarrow (3)$ is clear. For $(3) \Rightarrow (1)$, assume b is not integral over A. Let $W = \{f(b) \mid f \in A[T], f \text{ monic}\}$. W is multiplicatively closed and 0 is not in W by assumption. Hence there exists a prime ideal $Q \in \mathrm{Spec}(B)$ such that $Q \cap W = \emptyset$. Hence there exists a minimal prime $P \in \mathrm{Spec}(B)$ such that P does not meet W. Then in B/P, $\bar{b}$ is not integral over $A/P \cap A$ since $f(\bar{b}) \neq 0$ for all monic $f \in (A/P \cap A)[T]$. $\square$

Chapter 7

Krull's Theorems and Dedekind Domains

1 Krull's Theorems

Definition. Let R be a ring, $\mathfrak{p} \in \mathrm{Spec}(R)$. Then the *height* of $\mathfrak{p}$, denoted $\mathrm{ht}(\mathfrak{p})$, is:

$$\sup\{n \in \mathbb{N} : \exists\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}.$$

Note that $\mathrm{ht}(\mathfrak{p}) = \dim R/\mathfrak{p}$.

Theorem 76. *Let k be a field and let R be a finitely generated k-algebra. Assume R is a domain, then*

$$\mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p} = \dim R$$

for all $\mathfrak{p} \in \mathrm{Spec}(R)$.

Proof. Set $n = \dim R$. We proved that all saturated chains of primes have length n. Set $s = \dim R/\mathfrak{p}$ and let

$$\frac{\mathfrak{p}}{\mathfrak{p}} \subsetneq \frac{\mathfrak{p}_1}{\mathfrak{p}} \subsetneq \ldots \subsetneq \frac{\mathfrak{p}_s}{\mathfrak{p}}$$

be a saturated chain in $R/\mathfrak{p}$. Set $t = \mathrm{ht}(\mathfrak{p})$ and let

$$0 = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_t = \mathfrak{p}$$

be saturated. Then:

$$0 = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_t = \mathfrak{p} \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_s$$

is saturated of length $s + t$, and hence $s + t = n$. $\qquad\square$

Example 1. Consider the map

$$\varphi : k[a,b,c,d] \twoheadrightarrow k[x^2y^2, y^3u^3v^3, xy^2uv, x^3y^5u^2v^2].$$

Then $\ker \varphi = \mathfrak{p}$ is prime. What is $\dim k[a,b,c,d]_{\mathfrak{p}}$? By Theorem 76 we have

$$\dim k[a,b,c,d]_{\mathfrak{p}} = \mathrm{ht}(\mathfrak{p}) = \dim k[a,b,c,d] - \frac{\dim k[a,b,c,d]}{\mathfrak{p}} = 4 - 2 = 2.$$

Theorem 77 (Krull's Intersection Theorem)**.** *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Then there exists $i \in I$ such that*

$$(1-i) \bigcap_{n \geq 1} I^n = 0.$$

In particular, if either $I \subseteq \mathrm{Jac}(R)$ or R is a domain,

$$\bigcap_{n \geq 1} I^n = 0.$$

Proof. Set $J := \bigcap_{n \geq 1} I^n$. We have that $JI = J$, in fact let $JI = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a primary decomposition. It is enough to show that $J \subseteq \mathfrak{q}_i$ for all $i = 1, \ldots, n$. There are two cases: if $I \subseteq \sqrt{\mathfrak{q}_i}$, then $I^N \subseteq \mathfrak{q}_i$ for $N >> 0$ and hence $J \subseteq I^N \subseteq \mathfrak{q}_i$. Instead, if $I \not\subseteq \sqrt{\mathfrak{q}_i}$, we have $J \subseteq \mathfrak{q}_i$ since $\mathfrak{q}_i$ is primary. Therefore we conclude by NAK. $\square$

Definition. If $\mathfrak{p} \in \mathrm{Spec}(R)$ is prime, then

$$\mathfrak{p}^{(n)} := \mathfrak{p}^n R_{\mathfrak{p}} \cap R$$

is the $\mathfrak{p}$-primary component of $\mathfrak{p}^n$ and it is called n-th *symbolic power* of $\mathfrak{p}$. In terms of the primary decomposition it is

$$\mathfrak{p}^n = \mathfrak{p}^{(n)} \cap \mathfrak{q}_{i_1} \cap \ldots \cap \mathfrak{q}_{i_n}$$

where $\mathfrak{p} \subsetneq \sqrt{\mathfrak{q}_{i_j}}$.

Theorem 78 (Krull's Principal Ideal Theorem and Height Theorem)**.** *Let R be a Noetherian ring. Then:*

(1) If $\mathfrak{p}$ is a minimal prime over a principal ideal (x), then $\mathrm{ht}(\mathfrak{p}) \leq 1$.

(2) If $\mathfrak{p}$ is minimal over an ideal $(x_1, \ldots, x_n)$, then $\mathrm{ht}(\mathfrak{p}) \leq n$.

Proof. (1) Assume $\mathfrak{p}$ is minimal over (x) but $\mathrm{ht}(\mathfrak{p}) \geq 2$. Replace R with $R_{\mathfrak{p}}$, so that without loss of generality we can assume $\mathfrak{p} = \mathfrak{m}$ the maximal ideal of a local ring R. By minimality over (x) we have that R/xR is Artinian. Since $\mathrm{ht}(\mathfrak{m}) \geq 2$ there exists a prime $\mathfrak{q}$ such that $\mathfrak{q} \subsetneq \mathfrak{m}$ and $\dim R_{\mathfrak{q}} > 0$. Let $\mathfrak{q}^{(n)} = \mathfrak{q}^n R_{\mathfrak{q}} \cap R$ be the n-th symbolic power and note that $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary for every n. Also we have

$$\mathfrak{q} = \mathfrak{q}^{(1)} \supseteq \mathfrak{q}^{(2)} \supseteq \ldots \supseteq \mathfrak{q}^{(n)} \supseteq \mathfrak{q}^{(n+1)} \supseteq \ldots$$

Going modulo (x) we get a descending chain

$$\frac{\mathfrak{q}}{(x)} = \frac{\mathfrak{q}^{(1)}}{(x)} \supseteq \frac{\mathfrak{q}^{(2)} + (x)}{(x)} \supseteq \ldots \supseteq \frac{\mathfrak{q}^{(n)} + (x)}{(x)} \supseteq \frac{\mathfrak{q}^{(n+1)} + (x)}{(x)} \supseteq \ldots$$

that must stabilize. In other words there exists $N >> 0$ such that $(\mathfrak{q}^{(N)} + (x)) = (\mathfrak{q}^{(N+1)} + (x)) = \ldots$ and in particular $\mathfrak{q}^{(N)} \subseteq \mathfrak{q}^{(N+1)} + (x)$. Let $s \in \mathfrak{q}^{(N)}$ and write it as $s = rx + t$, where $t \in \mathfrak{q}^{(N+1)}$. Then $rx = s - t \in \mathfrak{q}^{(N)}$ and, using that $x \notin \mathfrak{q} = \sqrt{\mathfrak{q}^{(N)}}$ because $\mathfrak{m}$ is minimal over (x) and $\mathfrak{q}^{(N)}$ is $\mathfrak{q}$-primary, we get $r \in \mathfrak{q}^{(N)}$. This means $s \in x\mathfrak{q}^{(N)} + \mathfrak{q}^{(N+1)}$ and therefore

$$\mathfrak{q}^{(N)} = x\mathfrak{q}^{(N)} + \mathfrak{q}^{(N+1)}.$$

By NAK we get $\mathfrak{q}^{(N)} = \mathfrak{q}^{(N+1)}$. Now localize at $\mathfrak{q}$:

$$\mathfrak{q}^N R_\mathfrak{q} = \mathfrak{q}^{(N)} R_\mathfrak{q} = \mathfrak{q}^{(N+1)} R_\mathfrak{q} = \mathfrak{q}^{N+1} R_\mathfrak{q}.$$

But now in $R_\mathfrak{q}$ apply NAK to $\mathfrak{q} \cdot \mathfrak{q}^N R_\mathfrak{q} = \mathfrak{q}^N R_\mathfrak{q}$ to get $\mathfrak{q}^N R_\mathfrak{q} = 0$, i.e. $\dim R_\mathfrak{q} = 0$. This is a contradiction, hence $\mathrm{ht}(\mathfrak{m}) \leq 1$.

(2) Induct on n. If $n = 1$ it is just (1). Assume now $n > 1$ and let $\mathfrak{p}$ be minimal over $(x_1, \ldots, x_n)$. We can localize at $\mathfrak{p}$, hence without loss of generality R is local, $\mathfrak{p} = \mathfrak{m}$ and $\sqrt{(x_1, \ldots, x_n)} = \mathfrak{m}$. Choose any prime $\mathfrak{q} \subsetneq \mathfrak{m}$ such that no other prime is between $\mathfrak{q}$ and $\mathfrak{m}$. Note that since R is Noetherian such prime exists unless $\mathrm{ht}(\mathfrak{m}) = 0$, and in this case the theorem is proved. By minimality of $\mathfrak{m}$ there exists $x_i \notin \mathfrak{q}$. Without loss of generality we can assume $x_n \notin \mathfrak{q}$. By choice $\mathfrak{m}$ is minimal over $\mathfrak{q} + (x_n)$, hence $\sqrt{\mathfrak{q} + (x_n)} = \mathfrak{m}$. This means that there exists $N >> 0$ such that

$$x_1^N = r_1 x_n + y_1, \ldots, x_{n-1}^N = r_{n-1} x_n + y_{n-1},$$

where $y_i \in \mathfrak{q}$. Notice that $(y_1, \ldots, y_{n-1}) \subseteq \mathfrak{q}$.

Claim. $\mathfrak{q}$ is minimal over $(y_1, \ldots, y_{n-1})$.

Proof of the Claim. If not there exists a prime $\mathfrak{p}$ such that

$$(y_1, \ldots, y_{n-1}) \subseteq \mathfrak{p} \subsetneq \mathfrak{q} \subsetneq \mathfrak{m},$$

but going modulo $(y_1, \ldots, y_{n-1})$ we get $\mathrm{ht}(\mathfrak{m}/(y_1, \ldots, y_{n-1})) \geq 2$, while $\mathfrak{m}$ is minimal over $(y_1, \ldots, y_{n-1}, x_n)$ since

$$\mathfrak{m} = \sqrt{(x_1, \ldots, x_n)} = \sqrt{(y_1, \ldots, y_{n-1}, x_n)} \subseteq \mathfrak{m}.$$

This picture contradicts (1), hence $\mathfrak{q}$ is minimal over $(y_1, \ldots, y_{n-1})$.

By induction $\mathrm{ht}(\mathfrak{q}) \leq n - 1$. Since $\mathfrak{q}$ was an arbitrary prime below $\mathfrak{m}$ with no other primes in between we have $\mathrm{ht}(\mathfrak{m}) \leq n$. $\qquad\qquad \square$

Corollary 79. *Let R be a Noetherian ring and let $\mathfrak{p} \in \mathrm{Spec}(R)$. Then $\mathrm{ht}(\mathfrak{p}) < \infty$.*

Proof. Since R is Noetherian $\mathfrak{p}$ is finitely generated, say $\mathfrak{p} = (x_1, \ldots, x_n)$. Then $\mathrm{ht}(\mathfrak{p}) \leq n$. $\qquad\qquad \square$

Corollary 80. *Let R be a Noetherian ring. Then $\mathrm{Spec}(R)$ satisfies DCC.*

2   Dedekind Domains

Definition. Let D be a Noetherian integrally closed domain with $\dim D = 1$. Then D is called a *Dedekind domain*.

Example 2.   (1) $\mathbb{Z}$ is a Dedekind domain.

  (2) $k[x]$, where k is a field, is a Dedekind domain.

  (3) $\mathbb{Z}[i]$ is a Dedekind domain.

Proposition 81. *Let D be a Dedekind domain. Then every ideal I can be written uniquely (up to order) as a product $I = \mathfrak{q}_1 \ldots \mathfrak{q}_n$, where all $\mathfrak{q}_i$'s are primary ideals and $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j} = \mathfrak{p}_j$ if $i \neq j$.*

Proof. Without loss of generality we can assume $I \neq (0)$. Let $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a primary decomposition. Since $\dim D = 1$ we have $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ are all maximal ideals, hence $\mathfrak{q}_i + \mathfrak{q}_j = D$ for all $i \neq j$. By Chinese Remainder Theorem we get $I = \mathfrak{q}_1 \ldots \mathfrak{q}_n$. Conversely assume $I = \mathfrak{q}_1 \ldots \mathfrak{q}_n$, with $\mathfrak{q}_i$ primary and $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$. Again by Chinese Remainder Theorem $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ and by Corollary 3 we get $\mathfrak{q}_i = IR_{\mathfrak{p}_i} \cap R$. Hence they are unique. $\qquad\square$

Proposition 82 (Structure of local Dedekind domains)**.** *Let $(D, \mathfrak{m})$ be a local Dedekind domain. Then:*

  (1) There exists $t \in D$ such that $\mathfrak{m} = (t)$.

  (2) Every non zero ideal is of the form $\mathfrak{m}^n$ for some $n \geq 0$ ($\mathfrak{m}^0 = D$).

Proof. (1) Choose any $x \in \mathfrak{m}$, $x \neq 0$. Then $\operatorname{Ass}(D/xD) = \{\mathfrak{m}\}$, therefore there exists an embedding

$$0 \to D/\mathfrak{m} \to D/xD$$
$$1 \mapsto \bar{y}$$

This means $(x : y) = \mathfrak{m}$ and thus $\frac{y}{x}\mathfrak{m} \subseteq D$. But $\frac{y}{x}\mathfrak{m}$ is an ideal, and there are two cases:

- $\frac{y}{x}\mathfrak{m} \subseteq \mathfrak{m}$, in which case $\frac{y}{x}$ is integral over D by the determinant trick. But D is integrally closed, hence $\frac{y}{x} = z \in D$, i.e. $y = zx$. Therefore $1 \in (x : y) = (x : zx) = \mathfrak{m}$, and this is a contradiction.

- $\frac{y}{x}\mathfrak{m} = D$. Then there exists $t \in \mathfrak{m}$ such that $\frac{y}{x}t = 1$, i.e. $x = ty$. This means
$$\mathfrak{m} = (x : y) = (ty : y) = (t).$$

(2) Let I be a non zero ideal. By Krull's Intersection Theorem

$$I \nsubseteq \bigcap_{n \geq 0} \mathfrak{m}^n = (0).$$

Therefore there exists $n \geq 0$ such that $I \subseteq \mathfrak{m}^n = (t^n)$ but $I \not\subseteq \mathfrak{m}^{n+1} = (t^{n+1})$, where t is as in (1). We can write $I = t^n J$, where J is the ideal $I : t^n$. If $J \subseteq \mathfrak{m} = (t)$, then $I \subseteq t^n(t) = (t^{n+1})$, and this is a contradiction. Hence $J = D$ and $I = (t^n)$. $\qquad\square$

Remark. Let R be a ring and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Then $\mathfrak{q}R_\mathfrak{p} \cap R = \mathfrak{q}$. In fact suppose $r \in \mathfrak{q}R_\mathfrak{p} \cap R$, then there exists $s \notin \mathfrak{p}$ such that $sr \in \mathfrak{q}$. This implies $r \in \mathfrak{q}$ since $\mathfrak{q}$ is primary.

Theorem 83. *Let D be a Dedekind domain. Then every ideal can be written uniquely (up to order) in the form*

$$I = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_s^{n_s},$$

where $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ are distinct primes.

Proof. By Proposition 81 there exist unique $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ primary ideals, with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$, such that $I = \mathfrak{q}_1 \dots \mathfrak{q}_s$. Furthermore

$$\mathfrak{q}_i = ID_{\mathfrak{p}_i} \cap D = \mathfrak{p}_i^{n_i} D_{\mathfrak{p}_i} \cap D,$$

where the last equality follows from Proposition 82 (2). It is enough to show that $\mathfrak{p}_i^{n_i} = \mathfrak{p}_i^{n_i} D_{\mathfrak{p}_i} \cap D$. But $\sqrt{\mathfrak{p}_i^{n_i}} = \mathfrak{p}_i$ maximal, hence $\mathfrak{p}_i^n$ is primary and the theorem follows by the previous Remark. $\qquad\square$

Chapter 8

Completions and Artin-Rees Lemma

1 Inverse Limits and Completions

Example 3. Let R be a Noetherian ring, let $I \subseteq R$ be an ideal and assume $\bigcap_{n \geq 0} I^n = 0$ (for instance if R is a domain, or $I \subseteq \operatorname{Jac}(R)$). If $x, y \in R$ set $v(x, y) = \sup\{n : x - y \in I^n\}$ and define

$$d(x, y) := \frac{1}{2^{v(x,y)}}.$$

Claim. (R, d) is a metric space.

Proof of the Claim. Clearly $d(x, y) = d(y, x)$ since if J is any ideal, then $x - y \in J$ if and only if $y - x \in J$. Also $d(x, y) = 0$ if and only if $x - y = 0$ since $\bigcap_{n \geq 0} I^n = 0$. Finally assume

$$\frac{1}{2^k} = d(x, y) \quad \text{and} \quad \frac{1}{2^l} = d(y, z).$$

This means $x - y \in I^k \smallsetminus I^{k+1}$ and $y - z \in I^l \smallsetminus I^{l+1}$. Therefore

$$x - z = (x - y) + (y - z) \in I^{\min\{k,l\}}.$$

Therefore

$$d(x, z) \leq \frac{1}{2^{\min\{k,l\}}} \leq \frac{1}{2^k} + \frac{1}{2^l} = d(x, y) + d(y, z).$$

$\square$

Remark. (1) What are the open balls $B_\varepsilon(x)$ in this metric space? Without loss of generality assume $\varepsilon = \frac{1}{2^k}$, then

$$B_{\frac{1}{2^k}}(x) = \{y \in R : d(x, y) < \tfrac{1}{2^k}\} = \{y \in R : d(x, y) \leq \tfrac{1}{2^{k+1}}\} =$$

$$= \{y \in R : x - y \in I^{k+1}\} = x + I^{k+1}.$$

(2) If we put the product topology on $R \times R$, then both

$$+ : R \times R \to R \quad \text{and} \quad \cdot : R \times R \to R$$

are continuous. In fact let $x + I^k$ be a basic open set around $x \in R$ and let $(y, z) \in +^{-1}(x + I^k)$. This means $y + z \in x + I^k$, and therefore

$$(y + I^k) + (z + I^k) \subseteq x + I^k.$$

Hence $+^{-1}(x + I^k)$ contains $(y + I^k) \times (z + I^k)$ around (y, z), i.e. $+$ is continuous. Similarly for the product.

Definition. Let R and $I \subseteq R$ be as above. The metric d defines a topology on R called *I-adic topology*. Also a null Cauchy sequence $\{x_n\}$ is a *Cauchy sequence* (with respect to the metric d) such that for all $\varepsilon > 0$ there exists $k \in \mathbb{N}$ such that for $n \geq k$ $d(x_n, 0) < \varepsilon$. We can now form a new object

$$\widehat{R}^I := \{\text{Cauchy sequences in } R\}/\{\text{null Cauchy sequences in } R\}.$$

We call $\widehat{R}^I$ the *completion* of R with respect to I and it is obtained from R by formally adjoining the "limit points". Also $\widehat{R}^I$ is a ring since R itself is a ring.

Remark. More explicitly, how does a Cauchy sequence in (R, d) look like? For a sequence $\{x_n\}$ in R to be Cauchy means that for all $\varepsilon = \frac{1}{2^l}$ there exists $k \in \mathbb{N}$ such that for all $n, m \geq k$ we get

$$d(x_n, x_m) < \frac{1}{2^l} \iff x_n - x_m \in I^{l+1} \iff x_n + I^{l+1} = x_m + I^{l+1}.$$

So let $y_{l+1} + I^{l+1}$ be the coset which is in the stable value of $x_n + I^{l+1}$ as $n \to \infty$. Note that under the natural map $\pi_l : R/I^{l+1} \twoheadrightarrow R/I^l$ we have

$$\pi_{l+1}(y_{l+1} + I^{l+1}) = y_l + I^l.$$

Algebraically, this is an inverse limit.

Definition. Let R be a ring and $\{M_n\}_{n=1}^{\infty}$ be a collection of R-modules with maps $\varphi_{n+1} : M_{n+1} \to M_n$. Then the *inverse limit* is

$$\varprojlim M_n := \ker \left(D : \prod_n M_n \to \prod_n M_n \right),$$

where D is the R-homomorphism defined as follows:

$$D((m_1, m_2, \ldots)) = (m_1 - \varphi_2(m_2), m_2 - \varphi_3(m_3), \ldots).$$

Remark. Notice that
$$\widehat{R}^I \simeq \varprojlim R/I^n,$$

where $\pi_{n+1} : R/I^{n+1} \to R/I^n$ is the natural projection map. In fact let $\{x_n\}$ be a Cauchy sequence in the I-adic topology and recall that for large m the coset $x_m + I^n$ has a stable value. Choose a representative $y_n + I^n$, so that $y_n + I^n = y_{n+1} + I^n$ for all n. Hence, corresponding to $\{x_n\}$ there is an element in $\varprojlim R/I^n$, i.e. a sequence of cosets

$$\ldots \longrightarrow y_{n+2} + I^{n+2} \xrightarrow{\pi_{n+2}} y_{n+1} + I^{n+1} \xrightarrow{\pi_{n+1}} y_n + I^n \longrightarrow \ldots$$

In this correspondence, null Cauchy sequences correspond to the zero element in $\varprojlim R/I^n$. Moreover, this correspondence preserves the ring operations. Finally, given an element $y \in \varprojlim R/I^n$, we have $y = \{(y_n + I^n)_n\} \in \prod_n R/I^n$ and also

$$y_{n+1} - y_n \in I^n \quad \text{for all } n,$$

i.e. $\{y_n\}$ is a Cauchy sequence.

Definition. Let R and $I \subseteq R$ be as above and let M be a R-module. We can define a pseudo-metric on M using $I^n M$ instead of I^n (it will be a metric if $\bigcap_{n \geq 0} I^n M = 0$). Then the completion of M with respect to I is

$$\widehat{M}^I = \varprojlim M/I^n M.$$

Proposition 84. *Let R be a ring and let $I \subseteq R$ be an ideal such that $\bigcap_{n \geq 0} I^n = 0$. Then*
$$I\widehat{R}^I \subseteq \mathrm{Jac}(\widehat{R}^I).$$

Proof. It is enough to show that $1 - x$ is a unit in $\widehat{R}^I$ for all $x \in I$. Notice that

$$\frac{1}{1 - x} = \sum_{i \geq 0} x^i$$

and define $s_n = \sum_{i=0}^n x^i$. Then $\{s_n\}$ is a Cauchy sequence since $s_{n+1} - s_n = x^{n+1} \in I^{n+1}$, hence there exists $s \in \widehat{R}^I$ which is the limit of s_n, i.e. $s - s_n \in I^n \widehat{R}^I$. Therefore

$$(1 - x)s - (1 - x)s_n = (1 - x)s - (1 - x^{n+1}) \in I^n \widehat{R}^I.$$

Since $x^{n+1} \in I^{n+1}$ we get

$$(1 - x)s - 1 \in I^n \widehat{R}^I \quad \text{for all } n$$

and hence

$$(1 - x)s = 1 \quad \text{in } \widehat{R}^I.$$

$\square$

2 Artin-Rees Lemma

Definition. A ring S is (non-negatively) *graded* if $S = \bigoplus_{i \geq 0} S_i$ as an abelian group, and $S_i \cdot S_j \subseteq S_{i+j}$ for all $i, j \geq 0$. In particular S_0 is a ring and each graded piece S_j is an S_0-module. An S-module M is graded if it can be written in the form $M = \bigoplus_j M_j$, with $S_i M_j \subseteq M_{i+j}$.

Example 4. (1) $S = A[x_1, \ldots, x_n]$ is a graded ring with S_j the A-module spanned by the homogeneous polynomials of degree j.

(2) If R is a ring and $I \subseteq R$ is an ideal we define

$$\mathcal{R}(I) := R \oplus I \oplus I^2 \oplus \cdots$$

the *Rees Ring* of I. One can artificially put a variable t in to keep track of the grading. In this way:

$$\mathcal{R}(I) \simeq R \oplus It \oplus I^2 t^2 \oplus \ldots = R[It] \subseteq R[t].$$

Remark. Let R be a ring and let $I \subseteq R$ be an ideal. If R is Noetherian, so is $\mathcal{R}(I)$.

Proof. By assumption I is finitely generated, say $I = (x_1, \ldots, x_n)$. Then

$$\mathcal{R}(I) = R[x_1 t, \ldots, x_n t] \subseteq R[t].$$

Hence there exists a surjection

$$R[T_1, \ldots, T_n] \twoheadrightarrow \mathcal{R}(I)$$
$$T_i \mapsto x_i t$$

By the Hilbert Basis Theorem 37 $R[T_1, \ldots, T_n]$ is Noetherian, and so is $\mathcal{R}(I)$. $\square$

Definition. Let R be a ring and let M be a finitely generated R-module. Define

$$\mathcal{M}(I) := M \oplus IM \oplus I^2 M \oplus \ldots$$

Then $\mathcal{M}(I)$ has the structure of a graded $\mathcal{R}(I)$-module if, given $it^n \in I^n t^n \subseteq \mathcal{R}(I)$ and $m \in I^j M$, we set

$$(it^n)m = im \in I^{n+j} M.$$

Remark. Notice that if $M = Rm_1 + \ldots + Rm_k$, then

$$\mathcal{M}(I) = \mathcal{R}(I)m_1 + \ldots + \mathcal{R}(I)m_k.$$

Theorem 85 (Artin-Rees Lemma). *Let R be a Noetherian ring, let $I \subseteq R$ be an ideal and let $N \subseteq M$ be finitely generated R-modules. Then there exists $k \in \mathbb{N}$ such that for all $n \geq K$*

$$I^n M \cap N = I^{n-k}(I^k M \cap N).$$

Proof. Consider $\mathcal{R}(I) = R[It]$ and $\mathcal{M}(I) = \bigoplus_{j \geq 0} I^j M$ as above. Define $\mathcal{N}$ to be the following $\mathcal{R}(I)$ submodule of $\mathcal{M}(I)$:

$$\mathcal{N} = N \oplus (IM \cap N) \oplus (I^2 M \cap N) \oplus \dots$$

Notice that $I(I^n M \cap N) \subseteq I^{n+1} M \cap N$, so that $\mathcal{M}$ is a $\mathcal{R}(I)$-module. Since $\mathcal{R}(I)$ is Noetherian (by Remark 2) and $\mathcal{M}(I)$ is finitely generated, so is $\mathcal{N}$. Say $\mathcal{N} = \mathcal{R}(I)x_i + \dots + \mathcal{R}(I)x_l$, with $x_i \in \mathcal{N}$, and $x_i = \sum_j x_{ij}$, where $x_{ij} \in I^j M \cap N$, and all but finitely many are zero. So $\mathcal{N} = \sum_{i,j} \mathcal{R}(I)x_{ij}$, and without loss of generality we can assume $x_1, \dots, x_l$ are homogeneous, say $\deg x_i = n_i$, i.e. $x_i \in I^{n_i} M \cap N$. Let $k = \max\{n_1, \dots, n_l\}$.

Claim. With this choice of k we have $I^n M \cap N = I^{n-k}(I^k M \cap N)$ for all $n \geq k$.

Proof of the Claim. Notice that $I^{n-k}(I^k M \cap N) \subseteq I^n M \cap N$ for all $n \geq k$. Conversely let $n \geq k$ and let $u \in I^n M \cap N$. Write it as

$$u = \sum_{i=1}^{l} r_i x_i,$$

where $r_i \in \mathcal{R}(I)$, and without loss of generality they can be chosen homogeneous. Hence $\deg r_i = n - n_i$, that is

$$r_i \in \mathcal{R}(I)_{n-n_i} = I^{n-n_i} t^{n-n_i}.$$

This means that

$$u \in \sum_{i=1}^{l} I^{n-n_i} x_i \subseteq \sum_{i=1}^{l} I^{n-n_i}(I_i^n M \cap N) \subseteq I^{n-k}(I^k M \cap N).$$

$\square$

3   Properties of Completions

Definition. Let R be a ring and let $\{A_n\}$ and $\{B_n\}$ be inverse limit systems of R-modules. We say that $\alpha : \{A_n\} \to \{B_n\}$ is a *morphism of inverse limits* ($\alpha = \{\alpha_n\}$) if:

$$
\begin{array}{ccc}
A_{n+1} & \xrightarrow{\alpha_{n+1}} & B_{n+1} \\
\downarrow & & \downarrow \\
A_n & \xrightarrow{\alpha_n} & B_n
\end{array}
$$

where each α_i is a R-homomorphism. In this case α induces a homomorphism

$$\varprojlim A_n \xrightarrow{\alpha} \varprojlim B_n.$$

Lemma 86 (Snake Lemma). *Let R be a ring and suppose we have the following exact diagram of R-modules:*

$$
\begin{array}{ccccccc}
A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' &
\end{array}
$$

Then there exists a morphism $\delta : \ker h \to \operatorname{coker} f$ such that

$$
\ker f \xrightarrow{\alpha} \ker g \xrightarrow{\beta} \ker h \xrightarrow{\delta} \operatorname{coker} f \xrightarrow{\alpha'} \operatorname{coker} g \xrightarrow{\beta'} \operatorname{coker} h
$$

is exact. Furthermore, if α is one-to one, then so is $(\ker f \xrightarrow{\alpha} \ker g)$. Similarly, if β' is surjective so is $(\operatorname{coker} g \xrightarrow{\beta'} \operatorname{coker} h)$.

Proof. Diagram chasing. $\qquad\square$

Lemma 87. *Let $\{A_n\}, \{B_n\}$ and $\{C_n\}$ be inverse limit systems and assume that $\{A_n\} \xrightarrow{\alpha} \{B_n\} \xrightarrow{\beta} \{C_n\}$ are such that*

$$
0 \longrightarrow A_n \xrightarrow{\alpha_n} B_n \xrightarrow{\beta_n} C_n \longrightarrow 0
$$

are all short exact sequences. Then

(1) The following sequence is exact

$$
0 \longrightarrow \varprojlim A_n \xrightarrow{\alpha} \varprojlim B_n \xrightarrow{\beta} \varprojlim C_n
$$

(2) If $A_{n+1} \to A_n$ is surjective for all n, then β is surjective.

Proof. Let $d_A : \prod A_n \to \prod A_n$ be the map such that

$$
\varprojlim A_n = \ker d_A.
$$

Similarly define d_B and d_C for $\{B_n\}$ and $\{C_n\}$. We have the following row-exact diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \prod A_n & \xrightarrow{\alpha_n} & \prod B_n & \xrightarrow{\beta_n} & \prod C_n & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle d_A} & & \downarrow{\scriptstyle d_B} & & \downarrow{\scriptstyle d_C} & & \\
0 & \longrightarrow & \prod A_n & \xrightarrow{\alpha_n} & \prod B_n & \xrightarrow{\beta_n} & \prod C_n & \longrightarrow & 0
\end{array}
$$

By Snake Lemma we get an exact sequence

$$
0 \longrightarrow \varprojlim A_n \xrightarrow{\alpha} \varprojlim B_n \xrightarrow{\beta} \varprojlim C_n \longrightarrow \operatorname{coker} d_A.
$$

This proves (1). Also, if $A_{n+1} \to A_n$ is surjective for all n, we have $\operatorname{coker} d_A = 0$, and hence (2) follows. $\qquad\square$

Definition. Let R be a ring and let $I \subseteq R$ be an ideal. A sequence $\{I_n\}$ of ideals $I_1 \supseteq I_2 \supseteq \ldots$ is said to be *cofinal* with $\{I^n\}$ if for all n there exists k such that $I_k \subseteq I^n$, and conversely for all n there exists k such that $I^k \subseteq I_n$.

Remark. If $\{I_n\}$ is cofinal with $\{I^n\}$, the I-adic topology $\{x + I^n\}$ is the same as the topology determined by taking neighborhood basis of x to be $\{x + I_n\}$. So the completions are isomorphic, i.e.

$$\widehat{R}^I = \varprojlim R/I^n \simeq \varprojlim R/I_n.$$

Likewise, for any chain $M_1 \supseteq M_2 \supseteq \ldots$ of R-modules cofinal with $\{I^n M\}$, we get

$$\widehat{M}^I = \varprojlim M/I^n M \simeq \varprojlim M/M_n.$$

Lemma 88. *Let $R \to S$ be a ring homomorphism. Then S is flat over R if and only if, given finitely generated R modules M and N and an injection $0 \to N \xrightarrow{i} M$, then $0 \to N \otimes_R S \xrightarrow{i \otimes 1} M \otimes_R S$ is exact.*

Proof. If S is flat, then by definition $0 \to N \otimes_R S \xrightarrow{i \otimes 1} M \otimes_R S$ is exact for all injections $0 \to N \xrightarrow{i} M$, with M and N finitely generated R-modules. Conversely, assume S is not flat. Then there exists an injection $0 \to N \xrightarrow{i} M$ such that $0 \to N \otimes_R S \xrightarrow{i \otimes 1} M \otimes_R S$ is not exact. Suppose $i \otimes 1 \left(\sum_{i=1}^{l} n_i \otimes s_i \right) = 0$ and let $N_0 := Rn_1 + \ldots Rn_l \subseteq N$. Then $0 \to N_0 \xrightarrow{i'} M$ is exact and $i' \otimes 1 \left(\sum_{i=1}^{l} n_i \otimes s_i \right) = 0$. By definition, $M \otimes_R S = R[m, s : m \in M, s \in S]/Z$, where $Z \subseteq R[m, s : m \in M, s \in S]$ is a submodule. Therefore

$$i' \otimes 1 \left(\sum_{i=1}^{l} n_i \otimes s_i \right) = 0 \iff \sum_{i=1}^{l} i'(n_i) \otimes s_i = 0 \iff \sum_{i=1}^{l} [i'(n_i), s_i] \in Z.$$

Hence there exist $r_j \in R$ and $z_j \in Z$ such that $\sum_{i=1}^{l}[i'(n_i), s_i] = \sum_j r_j z_j$. Let $M_0 \subseteq M$ be the submodule generated over R by $i'(n_i)$ and all elements of M appearing in the z_j's. Then

$$0 \longrightarrow N_0 \longrightarrow M_0$$

is exact, and N_0 and M_0 are finitely generated R-modules. By assumption, since $i' \otimes 1 \left(\sum_{i=1}^{l} n_i \otimes s_i \right) = 0$, we have $\sum_{i=1}^{l} n_i \otimes s_i = 0$ in $N_0 \otimes_R S$, and hence it is zero in $N \otimes_R S$. $\qquad\square$

Theorem 89. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal such that $\bigcap_{n \geq 0} I^n = 0$. Then*

(1) If we have a short exact sequence of R-modules

$$0 \longrightarrow N \xrightarrow{\alpha} M \xrightarrow{\beta} L \longrightarrow 0,$$

the following sequence

$$0 \longrightarrow \widehat{N}^I \stackrel{\alpha}{\longrightarrow} \widehat{M}^I \stackrel{\beta}{\longrightarrow} \widehat{L}^I \longrightarrow 0$$

is also exact.

(2) If M is finitely generated, then

$$\widehat{M}^I \simeq M \otimes_R \widehat{R}^I.$$

(3) The map $R \to \widehat{R}^I$ is flat.

Proof. (1) Tensor the short exact sequence with R/I^n:

$$\frac{N}{I^n N} \stackrel{\alpha_n}{\longrightarrow} \frac{M}{I^n M} \stackrel{\beta_n}{\longrightarrow} \frac{L}{I^n L} \longrightarrow 0.$$

This sequence is exact since tensor product is right exact. Starting from this sequence we get the following exact diagram (considering the kernels of the two surjections)

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{N}{I^n M \cap N} & \stackrel{\alpha_n}{\longrightarrow} & \dfrac{M}{I^n M} & \stackrel{\beta_n}{\longrightarrow} & \dfrac{L}{I^n L} & \longrightarrow & 0 \\
& & \big\uparrow{\scriptstyle \pi_n} & & \big\uparrow{\scriptstyle \pi_n} & & \big\uparrow{\scriptstyle \pi_n} & & \\
0 & \longrightarrow & \dfrac{N}{I^{n+1} M \cap N} & \stackrel{\alpha_n}{\longrightarrow} & \dfrac{M}{I^{n+1} M} & \stackrel{\beta_n}{\longrightarrow} & \dfrac{L}{I^n L} & \longrightarrow & 0
\end{array}
$$

This gives a short exact sequence of inverse limits and, moreover, the natural maps π_n are all surjective, therefore, from Lemma 1, we get the following short exact sequence

$$0 \longrightarrow \varprojlim \frac{N}{I^n M \cap N} \longrightarrow \widehat{M}^I \longrightarrow \widehat{L}^I \longrightarrow 0.$$

Clearly, for all $n \in \mathbb{N}$, $I^n N \subseteq I^n M \cap N$. Finally, by Artin-Rees Lemma, there exists k such that $I^n M \cap N \subseteq I^{n-k} N$ for all $n \geq k$. Therefore $\{I^n M \cap N\}$ is cofinal with $\{I^n N\}$ and hence

$$\varprojlim \frac{N}{I^n M \cap N} \simeq \varprojlim \frac{N}{I^n N} = \widehat{N}^I.$$

(2) Notice that we have always a map

$$M \otimes_R \widehat{R}^I \to \widehat{M}^I,$$

and if M is free it is clearly an isomorphism. Since M is finitely generated there exists a short exact sequence

$$0 \longrightarrow K \longrightarrow R^n \stackrel{\pi}{\longrightarrow} M \longrightarrow 0,$$

where $K = \ker \pi$. Since R is Noetherian, K is finitely generated, therefore there exists an exact sequence

$$R^m \xrightarrow{\ \alpha\ } R^n \xrightarrow{\ \pi\ } M \longrightarrow 0.$$

By (1) we get the following exact sequence

$$
\begin{array}{ccccccc}
(\widehat{R}^I)^m & \xrightarrow{\ \widehat{\alpha}\ } & (\widehat{R}^I)^n & \xrightarrow{\ \widehat{\pi}\ } & \widehat{M}^I & \longrightarrow & 0 \\
\big\uparrow{\simeq} & & \big\uparrow{\simeq} & & \big\uparrow & & \\
R^m \otimes_R \widehat{R}^I & \longrightarrow & R^n \otimes_R \widehat{R}^I & \longrightarrow & M \otimes_R \widehat{R}^I & \longrightarrow & 0
\end{array}
$$

and (2) follows by Five Lemma.

(3) Assume $0 \to N \to M$ is an exact sequence of finitely generated R-modules. Then, by (1) and (2), we get

$$0 \longrightarrow \widehat{N}^I \longrightarrow \widehat{M}^I$$

is exact, and therefore the map $R \to \widehat{R}^I$ is flat by Lemma 88. $\qquad\square$

Theorem 90. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal such that $\bigcap_{n \geq 1} I^n = 0$. Then $\widehat{R}^I$ is Noetherian.*

Proof. One can prove that, if $I = (a_1, \ldots, a_l)$, then

$$\widehat{R}^I \simeq \frac{R[[x_1, \ldots, x_l]]}{(x_1 - a_1, \ldots, x_l - a_l)}.$$

Then it suffices to prove that $R[[x_1, \ldots, x_l]]$ is Noetherian. Induct on l, so that it is enough to show that $R[[x]]$ is Noetherian. We will show that every prime $\mathfrak{p} \in \mathrm{Spec}(R[[x]])$ is finitely generated. Define $\mathfrak{p}_0 \subseteq R$ as $\mathfrak{p}_0 := \{g(0) : g \in \mathfrak{p}\}$ (the constant terms). Then $\mathfrak{p}_0 \subseteq R$ is finitely generated, say $\mathfrak{p}_0 = (a_1, \ldots, a_n)$. Then there exists $f_i \in \mathfrak{p}$ such that $f_i(0) = a_i$ for all i. Two cases are possible:

- If $x \notin \mathfrak{p}$. In this case we claim that $\mathfrak{p} = (f_1, \ldots, f_n)$, so that $\mathfrak{p}$ is finitely generated. Let $g \in \mathfrak{p}$, so that $g(0) \in \mathfrak{p}_0$ and hence

$$g(0) = \sum_{i=1}^{n} r_{i0} a_i,$$

for some $r_{10}, \ldots, r_{n0} \in R$. Then

$$g(x) - \sum_{i=1}^{n} r_{i0} f_i(x) = x g_1(x).$$

But $\mathfrak{p}$ is prime and $x \notin \mathfrak{p}$, hence $g_1 \in \mathfrak{p}$. Repeat the process to get

$$g_1(x) - \sum_{i=1}^{n} r_{i1} f_i(x) = x g_2(x),$$

so that

$$g(x) - \sum_{i=1}^{n}(r_{i0} + r_{i1}x)f_i(x) = x^2 g_2(x).$$

Inductively, there exist $r_{ij} \in R$ such that

$$g(x) - \sum_{i=1}^{n}(r_{i0} + r_{i1}x + \ldots + x^j r_{ij})f_i(x) = x^{j+1}g_{j+1}(x) \quad \text{for all } j.$$

Therefore

$$g(x) - \sum_{i=1}^{n}(\sum_{j=1}^{\infty}x^j r_{ij})f_i(x) \in \bigcap_{j\geq 0}(j^n) = 0,$$

that is $g \in \mathfrak{p}$.

- If $x \in \mathfrak{p}$, then for $g(x) \in \mathfrak{p}$ write $g(x) = g(0) + xh(x)$, for some $h(x) \in R[[x]]$. This implies $g(0) \in \mathfrak{p}$. But then

$$(\mathfrak{p}_0, x) \subseteq \mathfrak{p} \subseteq (\mathfrak{p}_0, x),$$

i.e. $\mathfrak{p} = (\mathfrak{p}_0, x) = (a_1, \ldots, a_n, x)$ is finitely generated. $\qquad\square$

Bibliography

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[3] Christian Peskine. *An algebraic introduction to complex projective geometry. 1*, volume 47 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1996. Commutative algebra.

Index