INTRODUCTION TO COMMUTATIVE
ALGEBRA AND ALGEBRAIC GEOMETRY.

The purpose of these notes is to give a quick and relatively painless introduction to the language of modern commutative algebra and algebraic geometry. The point of view which we will emphasize is that commutative algebra and algebraic geometry (at least the local theory) are two different languages for talking about the same thing. The algebraic and the geometric aspects of every phenomenon will be introduced and discussed concurrently. The first part of the course will consist of standard material; towards the end we will treat some topics of current interest such as valuation theory and singularities. Due to spacetime limitations, we will omit some important topics, notably cohomology, traditionally present in an introductory course.

Unless otherwise stated, all rings in these notes will be commutative with 1. \( \mathbb{N} \) will denote the set of natural numbers, \( \mathbb{N}_0 \) the set of non-negative integers.

§1. Varieties and ideals.

Let \( k \) be a field and \( x_1, \ldots, x_n \) independent variables. The following are some basic examples of rings appearing in algebraic, analytic and formal geometry. The reader should keep them in mind in order to test and illustrate the general theory.

1. Polynomial rings \( k[x_1, \ldots, x_n] \) and \( D[x_1, \ldots, x_n] \), where \( D = \mathbb{Z} \) or, more generally, \( D \) is the ring of integers in some number field, such as \( \mathbb{Z}[\sqrt{2}] \) or \( \mathbb{Z}^\sqrt{5}i \).
2. Formal power series rings

\[
\begin{align*}
  k[[x_1, \ldots, x_n]] & := \left\{ \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \middle| \alpha = (\alpha_1, \ldots, \alpha_n) \text{ and } c_\alpha \in k \right\} \\
  \mathbb{Z}_p[[x_1, \ldots, x_n]], & \text{ where } p \text{ is a prime number and } \mathbb{Z}_p \text{ is the ring of } p\text{-adic integers.}
\end{align*}
\]

3. Convergent power series rings \( \mathbb{C}\{x_1, \ldots, x_n\} \) and \( \mathbb{Z}_p\{x_1, \ldots, x_n\} \).

The beauty and power of commutative algebra lie in the fact that, it provides a universal language and methods for studying number theory, local algebraic geometry and local questions in complex analysis, as illustrated by the above examples.

Given rings \( R \) and \( S \), a **homomorphism** from \( R \) to \( S \) is a map \( R \to S \) which preserves the ring operations \( + \) and \( \cdot \).
Definition 1.1. Let $R$ be a ring and $I$ a non-empty subset of $R$. $I$ is an **ideal** of $R$ if $I$ is closed under addition and for any $a \in R$, $x \in I$, we have $ax \in I$.

For example, $\{0\}$ is an ideal (usually denoted by $(0)$); the entire ring $R$ is also an ideal, sometimes called the **unit ideal** and denoted by $(1)$.

Let $B = \{e_\lambda\}_{\lambda \in \Lambda}$ be a subset of $R$. Let $BR$ denote the set of all linear combinations of the form

$$BR = \left\{ \sum_{i=1}^n e_\lambda_i b_{\lambda_i} \mid b_{\lambda_i} \in R, e_{\lambda_i} \in B, n \in \mathbb{N} \right\}.$$

**Exercise 1.** If $I = BR$, prove that $I$ is the smallest ideal of $R$ containing $B$.

If $I = BR$, we say that $I$ is the **ideal generated by** $B$, or that $B$ is a set of generators or a **base** of $I$. Of course, a given ideal $I$ may have many different sets of generators. An ideal $I$ is said to be **finitely generated** if it has a finite set of generators.

**Definition 1.2.** A ring $R$ is Noetherian if every ascending chain $I_1 \subset I_2 \subset I_3 \subset \ldots$ of ideals of $R$ stabilizes, that is, there exists $n_0 \in \mathbb{N}$ such that $I_n = I_{n_0}$ for all $n > n_0$.

**Exercise 2.** Prove that a ring $R$ is Noetherian if and only if every ideal of $R$ is finitely generated.

Commutative algebra grew out of number theory and geometric invariant theory at the turn of the century. One of the starting points was Hilbert’s basis theorem:

**Theorem 1.3.** Let $R$ be a Noetherian ring and $x_1, \ldots, x_n$ independent variables. Then $R[x_1, \ldots, x_n]$ is also Noetherian for any $n$.

**Proof.** It is sufficient to consider the case $n = 1$. We want to establish that $R[x]$ is Noetherian, provided $R$ is Noetherian. Let $I$ be an ideal of $R[x]$. Let $J$ denote the ideal of $R$, consisting of all the leading coefficients of elements of $I$ (the reader should check that $J$ is, indeed, an ideal). Since $R$ is Noetherian, $J$ is finitely generated. Hence there exists a finite collection of polynomials $f_1, \ldots, f_m \in R[x]$, whose leading coefficients generate $J$. Let $d = \max_{1 \leq i \leq m} \deg f_i$. Then for every $f \in I$ such that $\deg f \geq d$, there exist $h_1, \ldots, h_m \in R[x]$ such that $\sum_{i=1}^m h_i f_i$ has the same degree and leading coefficient as $f$, in other words,

$$\deg \left( f - \sum_{i=1}^m h_i f_i \right) < \deg f. \quad (1.1)$$

Applying (1.1) repeatedly and using induction on $\deg f$, we can find $g_1, \ldots, g_s \in R[x]$ such that

$$\deg \left( f - \sum_{i=1}^m g_i f_i \right) < d. \quad (1.2)$$
By (1.2), there exists the smallest \( l \in \mathbb{N}_0 \) having the following property. There exist \( r \in \mathbb{N}, f_1, \ldots, f_r \in I \) such that for any \( f \in I \) there are \( g_1, \ldots, g_r \in R[x] \) satisfying

\[
\deg \left( f - \sum_{i=1}^{r} g_i f_i \right) < l
\]

(where, by convention, we take \( \deg 0 \) to be \(-1\)).

Now, suppose \( I \) is not finitely generated. Then \( l > 0 \). Let \( I_l \) denote the set of those elements of \( I \) which have degree exactly \( l - 1 \). Let \( J_l \) denote the ideal of \( R[x] \) consisting of 0 and all the leading coefficients of elements of \( I_l \). Since \( R[x] \) is Noetherian, \( J_l \) is finitely generated. Hence there exist finitely many elements \( f_{r+1}, \ldots, f_s \) of \( I_l \), such that for every \( f \in I_l \) there exist \( g_{r+1}, \ldots, g_s \in R[x] \) satisfying \( \deg \left( f - \sum_{i=r+1}^{s} g_i f_i \right) < l - 1 \). In view of (1.3), this contradicts the minimality of \( l \). \( \square \)

**Corollary 1.4.** Let \( k \) be a field and \( x_1, \ldots, x_n \) independent variables. Then the polynomial ring \( k[x_1, \ldots, x_n] \) is Noetherian. Similarly for \( \mathbb{Z}[x_1, \ldots, x_n] \).

Let \( R \) be a ring and \( I \) an ideal of \( R \). The **quotient** of \( R \) by \( I \) is the set of cosets \( \frac{R}{I} \) (viewed as abelian groups with respect to +), endowed with the obvious ring operations. We have the natural surjective homomorphism \( R \to \frac{R}{I} \), whose kernel is \( I \). We also say that \( \frac{R}{I} \) is a **homomorphic image** of \( R \). Note also that every surjective ring homomorphism \( \pi : R \to S \) is the quotient of \( R \) by some ideal (namely, by \( \text{Ker } \pi \)).

We are now ready to introduce our basic dictionary between algebra and geometry, at first in the classical setting with algebraic varieties on the geometric side and finitely generated algebras over a field on the algebraic side. Soon we will switch to the more general modern setting with arbitrary schemes on the geometric side and arbitrary rings on the algebraic side.

Classically, algebraic geometry studied algebraic subvarieties of \( k^n \) (i.e. subsets of \( k^n \) defined by finitely many polynomial equations), where \( k \) is a field and \( n \in \mathbb{N} \). In fact, \( k \) was usually taken to be \( \mathbb{C} \).

**Definition 1.5.** Let \( k \) be a field and let \( I \) be an ideal of \( k[x_1, \ldots, x_n] \). The **algebraic variety defined by** \( I \) in \( k^n \) is

\[
V(I) = \{ a \in k^n \mid f(a) = 0 \text{ for all } f \in I \}.
\]

Since \( k[x_1, \ldots, x_n] \) is Noetherian, we can choose a finite base \( (f_1, \ldots, f_m) \) for \( I \), so that \( V(I) = \{ a \in k^n \mid f_1(a) = \cdots = f_m(a) = 0 \} \).

Associated to every ideal \( I \) of \( k[x_1, \ldots, x_n] \) we have the algebraic variety \( V(I) \). Conversely, given any set \( V \subset k^n \), we may consider the ideal \( I(V) \) defined by \( I(V) = \{ f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in V \} \). A natural question arises:
what is the relation between $I$ and $I(V(I))$? To answer this question, we need another definition.

**Definition 1.6.** Let $R$ be a ring and $I$ an ideal of $R$. The *radical of $I$*, denoted by $\sqrt{I}$, is defined to be

$$
\sqrt{I} = \{ x \in R \mid \text{there exists } n \in \mathbb{N}_0 \text{ such that } x^n \in I \}.
$$

We say that $I$ is *radical* if $I = \sqrt{I}$.

**Exercise 3.** Prove that $\sqrt{I}$ is an ideal and that $I \subset \sqrt{I}$.

Let $k$ be a field and $I$ an ideal of $k[x_1, \ldots, x_n]$. Clearly, $V(I) = V(\sqrt{I})$. It is also clear that $I \subset I(V(I))$ for any ideal $I \subset k[x_1, \ldots, x_n]$. Hence for any ideal $I$, $\sqrt{I} \subset I(V(\sqrt{I})) = I(V(I))$. It turns out that if $k$ is an algebraically closed field (this means that every non-constant polynomial in $k[x]$ has a root in $k$), we always have $\sqrt{I} = I(V(I))$. This is a non-trivial theorem, called **Hilbert’s Nullstellensatz**. We will state and prove several versions of the Nullstellensatz, all of which are sometimes referred to by this name.

**Theorem 1.7 (The strong form of Hilbert’s Nullstellensatz).** Let $k$ be an algebraically closed field and $I$ an ideal of $R = k[x_1, \ldots, x_n]$. Then $I(V(I)) = \sqrt{I}$. In other words, $\sqrt{I} = \{ f \in R \mid f(a) = 0 \ \forall \ a \in V(I) \}$.

In other words, there is a *one-to-one correspondence* between algebraic subvarieties of $k^n$ and *radical* ideals of $k[x_1, \ldots, x_n]$.

A proof of Hilbert’s Nullstellensatz will be given shortly. First, we would like to advance a little more in our task of constructing a dictionary between algebra and geometry. To do this, we need to define the notions of maximal and prime ideals.

**Definition 1.8.** Let $R$ be a ring and $I \subsetneq R$ an ideal. We say that $I$ is *prime* if for any $x, y \in R$ such that $xy \in I$, we have either $x \in I$ or $y \in I$. We say that $I$ is *maximal* if $I \neq R$ and the only ideal of $R$ properly containing $I$ is $R$ itself. The set of all the maximal ideals of $R$ will be denoted by $Max(R)$, the set of all the prime ideals of $R$ by $\text{Spec } R$.

Associated to the properties of ideals we have encountered so far —radical, prime and maximal — we have the corresponding properties of rings (the precise connection will be explained in a moment).

**Definition 1.9.** Let $R$ be a ring and $x$ an element of $R$. We say that $x$ is *nilpotent* if there exists $n \in \mathbb{N}$ such that $x^n = 0$. We say that $x$ is a *zero divisor* if there exists $y \in R \setminus \{0\}$ such that $xy = 0$. The set of all nilpotent elements of $R$ is called the *nilradical of $R$*, denoted by $\sqrt{(0)}$ or $nil(R)$.

**Remark 1.10.** Since $\sqrt{(0)}$ is the radical of the zero ideal $(0)$, it is itself an ideal. Describing the set of zero divisors of $R$ is more tricky; we will do it somewhat later in the course.
**Definition 1.11.** Let $R$ be a ring. $R$ is said to be **reduced** if it has no non-zero nilpotent elements. $R$ is an integral domain (sometimes abbreviated to “domain”) if $R$ has no non-zero zero divisors.

Every field is an integral domain. If $R$ is a ring, we will denote by $\sqrt{R}$ the ring $\sqrt{R(0)}$; of course, $\sqrt{R}$ is reduced.

**Exercise 4.** Prove that $\sqrt{R}$ equals the intersection of all the prime ideals of $R$ (Hint: to prove one of the two inclusions, you will need Zorn’s lemma).

The intersection of all the maximal ideals of $R$ is called the Jacobson radical of $R$, or simply the radical of $R$, sometimes denoted by $J(R)$.

**Exercise 5.** Prove the following implications:

$I$ is maximal $\iff \frac{R}{I}$ is a field $\iff I$ is prime $\iff \frac{R}{I}$ is an integral domain $\iff I$ is radical $\iff \frac{R}{I}$ is reduced. As a special case of this, we have that $R$ is a field if and only if the zero ideal is maximal, $R$ is a domain if and only (0) is prime and $R$ is reduced if and only if (0) is radical.

By Zorn’s lemma, every ring $R$ (whether Noetherian or not) has at least one maximal ideal, hence, a fortiori, at least one prime ideal. For Noetherian rings the existence of maximal ideals does not require Zorn’s lemma.

**Example 1.12.** Let $k$ be a field, $n \in \mathbb{N}$ and $(a_1, \ldots, a_n) \in k^n$. Then $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal of $k[x_1, \ldots, x_n]$.

**Definition 1.13.** The Zariski topology on $k^n$ is the topology whose open sets are of the form $k^n \setminus V(I)$, where $I$ is an ideal of $k[x_1, \ldots, x_n]$.

**Operations on ideals.** Next, we define the operations on ideals which correspond to the topological operations of union and intersection.

**Definition 1.14.** Let $R$ be a ring, $\{I_\lambda\}_{\lambda \in \Lambda}$ a collection of ideals of $R$. The sum $\sum_{\lambda \in \Lambda} I_\lambda$ is defined by

$$
\sum_{\lambda \in \Lambda} I_\lambda = \left\{ \sum_{i=1}^{r} x_{\lambda_i} \bigg| r \in \mathbb{N}, \lambda_i \in \Lambda, x_{\lambda_i} \in I_{\lambda_i} \text{ for } 1 \leq i \leq r \right\}.
$$

In particular, if $\Lambda = \emptyset$, then $\sum_{\lambda \in \Lambda} I_\lambda = 0$.

The product $IJ$ is defined to be the ideal of $R$ generated by the set $\{xy \mid x \in I, \ y \in J\}$. Of course, $IJ$ can also be thought of as

$$
IJ = \left\{ \sum_{i=1}^{n} x_i y_i \bigg| n \in \mathbb{N}, x_i \in I, y_i \in J \text{ for } 1 \leq i \leq r \right\}.
$$

**Remark 1.15.** Historically, the word “ideal” first appeared in number theory. Kummer’s famous mistake in proving Fermat’s Last Theorem consisted in assuming
that Unique Factorization into prime numbers holds in the ring of integers in any number field. The mistake was soon discovered. For example, in \( \mathbb{Z}[\sqrt{5}i] \), we have \( 6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i) \), and yet 2 is an irreducible element which divides neither \((1 + \sqrt{5}i)\) nor \((1 - \sqrt{5}i)\). It was then realized that a sensible generalization of the Unique Factorization Theorem to rings of integers in number fields is not unique factorization for elements but unique factorization for ideals. This is how the notion of “ideal numbers” or ideals was introduced. For instance, in the above example the ideal \((6)\), generated by 6, has a unique factorization into prime ideals:\[(6) = (2, 1 + \sqrt{5}i)^2(3, 1 + \sqrt{5}i)(3, 1 - \sqrt{5}i).\]

The following properties are obvious from definitions and the Nullstellensatz:

1. \( k^n = V((0)) \)
2. \( \emptyset = V((1)) \)
3. If \( \{I_\lambda\}_{\lambda \in \Lambda} \) is a collection of ideals of \( k[x_1, \ldots, x_n] \), then
   \[ \bigcap_{\lambda \in \Lambda} V(I_\lambda) = V \left( \sum_{\lambda \in \Lambda} I_\lambda \right). \]
4. \( V(I) \cup V(J) = V(IJ) = V(I \cap J) \)
5. \( \sqrt{J} \subset \sqrt{I} \implies V(I) \subset V(J) \) and the converse holds if \( k \) is algebraically closed.

In particular, this shows that Zariski topology is, indeed, a topology.

The starting point for the theory of schemes is the above Example 1.12, and the partial converse to it, known as the weak form of Hilbert’s Nullstellensatz (the connection between the weak and the strong form will become clear in the course of the proof).

**Theorem 1.16 (A weak form of Nullstellensatz).** Let \( k \) be an algebraically closed field. Then \((a_1, \ldots, a_n) \longleftrightarrow (x_1 - a_1, \ldots, x_n - a_n)\) is a one-to-one correspondence between \( k^n \) and \( \text{Max}(k[x_1, \ldots, x_n]) \). In other words, every maximal ideal of \( k[x_1, \ldots, x_n] \) is of the form described in Example 1.12.

Let \( k \) be an algebraically closed field. By Theorem 1.16, we may translate all the geometric definitions and statements about points of \( k^n \) into purely algebraic statements about ideals in the ring \( k[x_1, \ldots, x_n] \). For example, we can define the Zariski topology on \( \text{Max}(k[x_1, \ldots, x_n]) \) as follows: for an ideal \( I \subset k[x_1, \ldots, x_n] \), \( V(I) = \{ m \in \text{Max}(k[x_1, \ldots, x_n]) \mid I \subset m \} \). Thus maximal ideals of \( k[x_1, \ldots, x_n] \) correspond to points of \( k^n \) and radical ideals correspond to algebraic varieties.

Let \( \sigma : A \rightarrow B \) be a homomorphism of rings.

**Definition 1.17.** Let \( I \) be an ideal of \( A \). The extension \( IB \) is the ideal of \( B \) generated by \( \sigma(I) \). If \( J \subset B \) is an ideal of \( B \), the contraction \( J \cap A \) is the ideal \( \sigma^{-1}(J) \).

**Remark 1.18.** The following are immediate from the definition:

1. If \( J \subset B \) is prime then \( J \cap A \) is prime.
2. If \( J \subset B \) is maximal and \( \sigma \) is surjective, then \( J \cap A \) is maximal.
Let $x = (x_1, \ldots, x_n)$. Let $I$ be an ideal of $k[x]$ and consider the natural homomorphism $k[x] \to \frac{k[x]}{I}$. Then the map $m \to m \cap k[x]$ induces a bijection between $\text{Max}(k[x])$ and the set of maximal ideals of $k[x]$, containing $I$. Hence the above correspondence between $k^n$ and $\text{Max}(k[x])$ induces a one-to-one correspondence between $V(I)$ and $\text{Max}(k[x])$. $\frac{k[x]}{I}$ is nothing but the ring of polynomial functions defined on the variety $V(I)$. We say that $\frac{k[x]}{I}$ is the coordinate ring of $V(I)$. For example, $k[x]$ is the coordinate ring of $k^n$. Given two algebraic varieties $X \subset k^n$ and $Y \subset k^l$, defined by ideals $I \subset k[x_1, \ldots, x_n], J \subset k[y_1, \ldots, y_l]$, it makes sense to talk about polynomial maps from $X$ to $Y$. By definition, they are induced by the maps $f : k^n \to k^l$ such that $f^*J \subset I$. In that case, $f^*$ induces a homomorphism of coordinate rings $\frac{k[y]}{J} \to \frac{k[x]}{I}$.

Next, we show that prime ideals of $k[x_1, \ldots, x_n]$ correspond to irreducible subvarieties of $k^n$:

**Definition 1.19.** A closed set $X$ in a topological space is said to be irreducible if whenever $X = X_1 \cup X_2$, we have either $X = X_1$ or $X = X_2$.

Let $P$ be a radical ideal of $k[x_1, \ldots, x_n]$. We want to show that $P$ is prime if and only if $V(P)$ is irreducible. We state the result in a form which works for arbitrary rings (so that we can obtain the same fact for schemes in the next section).

**Proposition 1.20.** A radical ideal $P$ in a ring $R$ is prime if and only if whenever $P = I \cap J$ with $I$ and $J$ ideals of $R$, either $P = I$ or $P = J$.

**Proof.** “If”. First, suppose that $P$ cannot be expressed as $I \cap J$ in a non-trivial way. If $P$ were not prime, there would exist $x, y \in k[x_1, \ldots, x_n] \setminus P$ such that $xy \in P$. Let $I = P + (x), J = P + (y)$. Then $P \not\subset I, P \not\subset J, P \subset I \cap J$. On the other hand, $IJ \subset P$, hence $\sqrt{IJ} \subset P$. Then $I \cap J \subset \sqrt{IJ} \cap \sqrt{IJ} = \sqrt{IJ} \subset P$, so that $I \cap J = P$, a contradiction.

“Only if” is an immediate consequence of the following lemma.

**Lemma 1.21.** Let $P$ be a prime ideal in a ring $R$ and $I_1, \ldots, I_r$ arbitrary ideals of $R$. If $\bigcap_{i=1}^r I_i \subset P$, then $I_i \subset P$ for some $i, 1 \leq i \leq r$.

**Proof.** We give a proof by contradiction. Suppose $I_i \not\subset P$ for any $I$. For each $i$ pick an element $x_i \in I_i \setminus P$. Then $\prod_{i=1}^r x_i \in \bigcap_{i=1}^r I_i \subset P$, but $x_i \notin P$ for any $i$. This contradicts the fact that $P$ is prime. □

§2. Schemes.

In §1 we saw that if $k$ is algebraically closed, points of $k^n$ can be identified with maximal ideals of $k[x_1, \ldots, x_n]$. This suggests generalizing algebraic geometry from $k^n$ to $\text{Max}(R)$, where $R$ is an arbitrary ring, and where we think of maximal ideals as points in our space. The idea of a scheme, developed in the twentieth century,
consists, in addition, in enlarging our notion of a point to include all the prime ideals of $R$.

Let $R$ be a ring. Motivated by the above considerations, we define the **Zariski topology** on Spec $R$ to be the topology whose closed sets are of the form $V(I) = \{ P \in \text{Spec } R \mid I \subset P \}$, where $I$ is an ideal of $R$.

**Definition 2.1.** An **affine scheme** is a pair $(R, \text{Spec } R)$ of a ring and a topological space, where Spec $R$ is endowed with its Zariski topology.

**Remark 2.2.** Note that single point sets need not be closed in Spec $R$. More precisely, we can describe the closure of the set $\{P\}$ for $P \in \text{Spec } R$. Let $Q \in V(P)$, so that $Q$ is a prime ideal containing $P$. For every ideal $I$ such that $P \in V(I)$, we have $I \subset P \subset Q$, so that $Q \in V(I)$. Hence $V(P) \subset \{P\}$. Conversely, $V(P)$ is a closed set containing $P$, hence $\{P\} \subset V(P)$. This proves that $\{P\} = V(P)$. The point $P$ is characterized by being the unique point whose closure is $V(P)$. $P$ is called the **generic point** of the closed set $V(P)$. For example, if $R$ is an integral domain, then $(0)$ is a prime ideal. In this case, $\{(0)\} = \text{Spec } R$, so that $(0)$ is the generic point of the whole space. More generally, the same conclusion holds for $\sqrt{(0)}$ in a ring in which $\sqrt{(0)}$ is prime.

Remark 2.2 proves that, given $P \in \text{Spec } R$, the one-point set $\{P\}$ is closed if and only if $P$ is maximal. In particular, Spec $R$ is not a Hausdorff space, unless every prime ideal of $R$ is maximal.

In the category of algebraic varieties, one had the notion of a morphism between two varieties $X$ and $Y$, which is, by definition, a polynomial map in several variables. We saw that each such morphism $f$ induces a dual homomorphism $f^*$ from the coordinate ring of $Y$ to the coordinate ring of $X$. In scheme theory, the situation is analogous, except, since our basic objects are rings, we start with a homomorphism of rings $A \rightarrow B$ and define the induced morphism Spec $B \rightarrow \text{Spec } A$.

Let $\sigma : A \rightarrow B$ be a homomorphism of rings. Define the map $\sigma^* : \text{Spec } B \rightarrow \text{Spec } A$ by $\sigma^*(P) = P \cap A \equiv \sigma^{-1}(P)$ for $P \in \text{Spec } B$. Maps $\text{Spec } B \rightarrow \text{Spec } A$, which arise in this way are called **morphisms of affine schemes**. It is immediate from definitions that morphisms are continuous with respect to Zariski topology.

Two kinds of morphisms are of particular importance in geometry: open and closed embeddings. Open embeddings correspond to localization of rings, which will be the subject of the next section.

Ring homomorphisms corresponding to closed embeddings are the surjective homomorphisms, which we will discuss right now. Let $I$ be an ideal of $A$. Consider the natural homomorphism $\sigma : A \rightarrow \frac{A}{I}$. Then $\sigma^* : \frac{A}{I} \hookrightarrow \text{Spec } A$ is injective and $\text{Im}(\sigma^*) = V(I)$. Also, $\sigma^*$ is a closed map, for if $J$ is an ideal of $\frac{A}{I}$, then $\sigma^*(V(J)) = V(J \cap A)$. Thus, $\sigma^*$ is a closed embedding from $\frac{A}{I}$ into $\text{Spec } A$, i.e., $\sigma^*$ is a homeomorphism; $\sigma^* : \frac{A}{I} \rightarrow V(I)$ (with the topology on $V(I)$ induced from Spec $A$). This shows that the closed subset $V(I)$ of Spec $A$ itself has the structure of an affine scheme. We say that $V(I)$ is a **closed subscheme**
of Spec $A$. $\frac{I}{A}$ is called the \textbf{coordinate ring} of $V(I)$. As we switch from naive algebraic geometry to this new and more sophisticated view of life, $k^n$ is replaced in our minds by Spec $k[x_1, \ldots, x_n]$ and the algebraic subvariety $V(I)$ by the closed subscheme Spec $\frac{k[x_1, \ldots, x_n]}{I} \subset \text{Spec } k[x_1, \ldots, x_n]$.

Geometrically, prime ideals correspond to irreducible varieties. The point of scheme theory is that we agree to regard irreducible subvarieties themselves as points. One of the advantages of doing so is that it allows to make rigorous all the informal classical arguments of the Italian geometers of the early twentieth century which began with the words “Take a sufficiently general point on the algebraic variety...”. In scheme theory, the canonically defined generic point $P$ takes the place of the intuitive notion of choosing “a generic point” on the irreducible variety $V(P)$.

Apart from rigor, there are other important advantages that the language of schemes has over the classical language of algebraic varieties. The fact that we can do geometry over arbitrary rings, rather than just quotients of $k[x_1, \ldots, x_n]$ means that we can work over fields of positive characteristic and even over $\mathbb{Z}$ itself, which is very important for number theory. In fact, most of the recent advances in number theory would be inconceivable without the use of the geometric language of schemes. For instance, a large part of Faltings’ famous proof of Mordell’s conjecture consists of generalizing the classical theory of algebraic surfaces to arithmetic surfaces, i.e. surfaces of the form Spec $\frac{\mathbb{Z}[x,y]}{(f(x,y))}$. Along with rings over $\mathbb{Z}$, we can consider complex analytic local rings, formal power series rings (which appear naturally in studying local geometry and singularities), rings over the $p$-adic numbers, etc. Scheme theory provides us with a uniform language for doing geometry in all these different contexts, local and global.

Another great advantage of schemes over varieties is the presence of nilpotent structure, which makes the theory much richer. Namely, in classical algebraic geometry, given a non-radical ideal $I \subset k[x_1, \ldots, x_n]$, one did not distinguish between $V(I)$ with $V(\sqrt{I})$; indeed, they are identical as topological spaces. In scheme theory, however, they are regarded as \textit{different} closed subschemes of Spec $k[x_1, \ldots, x_n]$ by definition. More generally, if $R$ is a ring with nilpotent elements, Spec $R$ and Spec $R_{\text{red}}$ are identical as topological spaces, but are different as schemes. This opens interesting \textit{geometric} possibilities. For example, Spec $\frac{k[x,y]}{(x^2)}$ is a double line: it is the $y$-axis counted twice. We also have a completely new notion of embedded points (which will be discussed in more detail later on, in the section on primary decomposition). For instance, the scheme Spec $\frac{k[x,y]}{(x^2, xy)}$ is usually thought of as the union of the $y$-axis with the origin (a meaningless notion in classical algebraic geometry), because $(x^2, xy) = (x) \cap (x, y)^2$. In this case, we say that $(x, y)$ is an \textbf{embedded point} of the scheme Spec $\frac{k[x,y]}{(x^2, xy)}$. Even if one is only interested in the usual, reduced algebraic varieties, such non-reduced objects arise in a natural way as limits of families of varieties under deformations.

To summarize the nature of the generalization from varieties to schemes, we give
a definition of finitely generated algebras and morphisms of finite type.

Let $A$ be a ring. An $A$-algebra is a ring $B$ together with a fixed homomorphism $\sigma : A \to B$. The homomorphism $\sigma$ is sometimes called the structure homomorphism for the $A$-algebra $B$. An $A$-algebra homomorphism is a ring homomorphism $B \to C$ between two $A$-algebras, which respects the structure homomorphisms.

**Definition 2.3.** Let $B$ be an $A$-algebra and $x = \{x_\lambda\}_{\lambda \in \Lambda}$ a subset of $B$. Let $\bar{A} \subset B$ denote the image of $A$ under the structure homomorphism. The $A$-subalgebra $\bar{A}[x]$ of $B$, generated by $x$, is defined to be the smallest $A$-subalgebra of $B$, containing $x$. In other words, $\bar{A}[x]$ is the set of all elements of $B$ which can be written as multivariable polynomials in the $x_\lambda$ with coefficients in $\bar{A}$. We say that $B$ is a finitely generated $A$-algebra, or that $B$ is of finite type over $A$, if there is a finite subset $x \subset B$ such that $B = \bar{A}[x]$. A morphism $\text{Spec } B \to \text{Spec } A$ is said to be of finite type if $B$ is finitely generated over $A$.

**Remark 2.4.** $B$ is finitely generated over $A$ if and only if $B$ is isomorphic to an $A$-algebra of the form $\frac{A[x_1, \ldots, x_n]}{I}$, where $x_1, \ldots, x_n$ are independent variables, $A[x_1, \ldots, x_n]$ denotes the ring of polynomials in $n$ variables with coefficients in $A$ and $I$ is an ideal of $A[x_1, \ldots, x_n]$.

Coming back to varieties and schemes, we can summarize the situation as follows. Initially, we generalized the naive theory of algebraic varieties in two ways. First, we enlarged our notion of points by agreeing to consider irreducible subvarieties themselves as points. Secondly, we agreed to distinguish between two varieties having different nilpotent structures, even though they may be identical as topological spaces. The effect of these two generalizations is that of replacing the category of algebraic varieties over a field $k$ by the category of affine schemes which are of finite type over $k$. Rings which are of finite type over some field still form a rather restricted class (for instance, none of the rings listed in the beginning of the first lecture are of this type, except $k[x_1, \ldots, x_n]$). Our last generalization consisted in allowing arbitrary rings instead of limiting ourselves to finitely generated algebras over a field.

**Definition 2.5.** An affine scheme $\text{Spec } A$ is said to be reduced if $A$ is reduced.

**Remark 2.6.** Just as in the case of algebraic varieties, prime ideals correspond to irreducible closed subschemes. More precisely, let $A$ be a ring and $I$ a radical ideal. Then by Proposition 1.20, $\text{Spec } \frac{A}{I}$ is irreducible if and only if $I$ is prime. Another way of stating the same fact is that for a reduced ring $A$, $\text{Spec } A$ is an irreducible topological space if and only if $(0)$ is a prime ideal of $A$ if and only if $A$ is an integral domain. In this case, we say that $\text{Spec } A$ is an integral scheme. An important object associated with an integral scheme is its field of rational functions (which is the analogue of the field of meromorphic functions on a complex manifold):

**Definition 2.7** Let $A$ be an integral domain. The field of fractions $K$ of $A$ is
the set of equivalence classes of fractions
\[ K = \left\{ \frac{a}{b} \mid a, b \in A, \ b \neq 0 \right\} / \sim \]
where \( \sim \) is the obvious equivalence relation \( \frac{a}{b} \sim \frac{c}{d} \iff ad = bc \). \( K \) is also called the field of rational functions of the affine scheme \( \text{Spec} \ A \). If \( P \in \text{Spec} \ A \), the field of fractions of \( \frac{A}{P} \) is called the residue field of \( P \), sometimes denoted by \( \kappa(P) \).

We end this section by mentioning the semi-classical precursor of the modern notion of the generic point of an integral subscheme, in order to put things in a historical perspective.

Let \( X \) be an affine subvariety of \( k^n \), where \( k \) is a field. Assume \( X \) is irreducible, so that \( X = V(P) \), where \( P \) is a prime ideal of \( k[x_1, \ldots, x_n] \). Let \( A = \frac{k[x_1, \ldots, x_n]}{P} \) and let \( K \) be the field of fractions of \( A \). We have \( k \subset K \), so that \( k[x_1, \ldots, x_n] \subset K[x_1, \ldots, x_n] \). Let \( P' = PK[x_1, \ldots, x_n] \). Let \( X' = V(P') \subset k^n \). There exists a point \( \xi \in X' \) such that for any \( f \in k[x_1, \ldots, x_n] \), \( f(\xi) = 0 \) implies that \( f \in P \). Such a point \( \xi \) is called a \( k \)-generic point of \( X \) and used to play the role which the modern notion of generic point plays today. One advantage of the modern approach is that the generic point of an irreducible subscheme is canonically defined, while the \( k \)-generic point \( \xi \) above is not, in general, unique.

\section*{§3. Localization.}

By definition, we have a one-to-one correspondence between morphisms of affine schemes and homomorphisms of rings. We saw in §2 that closed embeddings of affine schemes correspond to surjective homomorphisms of rings. In this section, we consider the case of open embeddings, which correspond, appropriately, to the operation of localization in rings.

**Definition 3.1.** Let \( A \) be a ring. A subset \( S \subset A \setminus \{0\} \) is said to be multiplicative if \( 1 \in S \) and \( S \) is closed under multiplication.

**Examples:**

1. Let \( f \in A \setminus \sqrt{(0)} \). Then \( \{1, f, f^2, f^3, \ldots\} \) is multiplicative.
2. If \( P \in \text{Spec} \ A \), then \( A \setminus P \) is a multiplicative set.

**Definition 3.2** Let \( A \) be a ring and \( S \subset A \) a multiplicative subset. The localization of \( A \) at \( S \) is defined to be \( A_S = \{ \frac{a}{s} \mid a \in A, \ s \in S \} / \sim \), where \( \sim \) is the following equivalence relation: \( \frac{a}{s} \sim \frac{b}{t} \) whenever there exists \( u \in S \) such that \( u(at - bs) = 0 \). It is clear that \( A_S \) is a ring with the operations of addition and multiplication, well known from elementary school. \( \frac{0}{1} \) is its zero element and \( \frac{1}{1} \) the unit element.

Let \( A \) be a ring, \( S \subset A \) a multiplicative subset. We have the natural homomorphism \( \sigma : A \to A_S \), given by \( a \mapsto \frac{a}{1} \). \( \sigma \) is injective if \( A \) is an integral domain, but not in general. We have \( \text{Ker} \ \sigma = \{ x \in A \mid sx = 0 \text{ for some } s \in S \} \).
An element $x$ in a ring $A$ is said to be invertible, or a unit, if there exists $y \in A$ such that $xy = 1$. Then every element of $\sigma(S)$ is invertible in $A_S$.

**Examples:**

1. Let $A$ be a ring, $f \in A$. Let $S = \{1, f, f^2, f^3, \ldots\}$. We write $A_f$ for $A_S$. $A_f$ is the ring consisting of all the fractions whose denominator is a power of $f$.

2. Let $A$ be a ring and $P \in \text{Spec } A$. Let $S = A \setminus P$. By abuse of notation, which has become completely standard, we will write $A_P$ for $A_{A \setminus P}$.

**Definition 3.3.** A ring $A$ is local if $A$ has only one maximal ideal.

If $A$ is a local ring with maximal ideal $m$, the field $k = \frac{A}{m}$ is called the residue field of $A$. We will sometimes denote such an $A$ by $(A, m)$ or $(A, m, k)$ to indicate that $m$ is the maximal ideal and $k$ the residue field.

**Remark 3.4.** Let $A$ be a ring and $m \subset A$ an ideal. $A$ is local with the maximal ideal $m$ if and only if every element of $A \setminus m$ is invertible. Indeed, suppose $(A, m)$ is local and let $a \in A \setminus m$. Suppose $a$ is not invertible. Then $(a)$ is a proper ideal of $A$. By Zorn’s lemma, $(a)$ is contained in a maximal ideal, which must be $m$ since $m$ is the only maximal ideal of $A$. This means that $a \in m$, a contradiction. Conversely, suppose every element of $A \setminus m$ is invertible, but $m$ is not maximal. Then there exists $m' \in \text{Max}(A)$ such that $m \subsetneq m' \subsetneq A$. There exists $a \in m' \setminus m$. By assumption $a$ is invertible. Then $(a) = A$ and so $m' \supset (a) = A$, a contradiction.

**Remark 3.5.** Let $A$ be a ring and $P \in \text{Spec } A$. Then $A_P$ is a local ring with the maximal ideal $PA_P$.

**Remark 3.6.** Let $A$ be a ring, $S \subset A$ a multiplicative set, and consider the natural homomorphism

$$\sigma : A \rightarrow A_S.$$ 

Then

$$(3.1) \quad \sigma^*(\text{Spec } A_S) = \{P \in \text{Spec } A \mid P \cap S = \emptyset\}.$$ 

Indeed, let $P \in \text{Spec } A_S$. We must show that $\sigma^*(P) \cap S = \sigma^{-1}(P) \cap S = \emptyset$. If $a \in \sigma^{-1}(P) \cap S$, then $\frac{a}{1} \in P$ and $\frac{1}{a} \in A_S$, hence $1 \in P$ and $P = A_S$, a contradiction because $P$ is a prime ideal of $A_S$.

**Exercise 3.7.** Show the opposite inclusion $\sigma^*(\text{Spec } A_S) \supset \{P \in \text{Spec } A \mid P \cap S = \emptyset\}$ in (3.1). Also, show that $\sigma^*$ is injective and hence induces a bijection between $\text{Spec } A_S$ and $\{P \in \text{Spec } A \mid P \cap S = \emptyset\}$.

$\sigma^*$ is called the restriction map from $\text{Spec } A$ to the subset $\{P \in \text{Spec } A \mid P \cap S = \emptyset\}$. In the case of algebraic varieties, $\sigma^*$ corresponds to restricting a polynomial (i.e., an element of $A$) to the subset where no element of $S$ vanishes.

For example, let $f \in A \setminus \sqrt{(0)}$, $S = \{1, f, f^2, \ldots\}$. Consider $\sigma^* : \text{Spec } A_f \rightarrow \text{Spec } A$. Then $\sigma^*$ induces a bijection between $\text{Spec } A_f$ and $\text{Spec } A \setminus V(f)$. 


Let $I \subseteq A$ be an ideal. Let $\{f_\lambda\}_{\lambda \in \Lambda}$ be a set of generators of $I$. Let $P \in \text{Spec } A$. Then $I \subseteq P$ if and only if $f_\lambda \in P$ for all $\lambda \in \Lambda$.

Let $U_\lambda = \text{Spec } A \setminus V(f_\lambda) \cong \text{Spec } A_{f_\lambda}$. Then $\text{Spec } A \setminus V(I) = \{P \in \text{Spec } A \mid I \not\subseteq P\} = \bigcup_{\lambda \in \Lambda} (\text{Spec } A \setminus V(f_\lambda)) = \bigcup_{\lambda \in \Lambda} U_\lambda$.

Thus the open set Spec $A \setminus V(I)$ is a union of the open sets $U_\lambda = \text{Spec } A \setminus V(f_\lambda) \cong \text{Spec } A_{f_\lambda}$. Since the ideal $I$ was arbitrary, we see that the collection $\{\text{Spec } A \setminus V(f) \mid f \in A\}$ form a basis for the Zariski topology in Spec $A$. We will sometimes refer to the sets Spec $A_f$ as the basic open sets of Spec $A$.

**Remark 3.8.** If $A$ is Noetherian, we may take $\Lambda$ above to be finite. Hence in that case any open set is a finite union of basic open sets.

We end this section by giving another point of view on localizations in terms of inductive limits.

**Definition 3.9.** Let $\Lambda$ be a partially ordered set. We say that $\Lambda$ is a directed set if for any $i, j \in \Lambda$, there exists $l \in \Lambda$ such that $i \leq l$ and $j \leq l$.

**Definition 3.10.** Let $\{A_\lambda\}_{\lambda \in \Lambda}$ be a collection of sets, indexed by a directed set $\Lambda$. Suppose that for any $i, j \in \Lambda$ with $i \leq j$ we are given a map $\mu_{ij} : A_i \to A_j$ such that $\mu_{ii} = \text{id}$ for all $i \in \Lambda$ and $\mu_{ij} \circ \mu_{jl} = \mu_{il}$ for all triples $i, j, l \in \Lambda$ such that $l \geq j \geq i$. $\{A_\lambda\}_{\lambda \in \Lambda}$ is called a **direct system** or an **inductive system**.

Let $\{B_\lambda\}_{\lambda \in \Lambda}$ be another collection of sets indexed by $\Lambda$. Suppose that for any $i, j \in \Lambda$ with $i \geq j$ we are given a map $\phi_{ij} : B_i \to B_j$ such that $\phi_{ii} = \text{id}$ for all $i \in \Lambda$ and $\phi_{jl} \circ \phi_{ij} = \phi_{il}$ for all triples $i, j, l \in \Lambda$ such that $l \leq j \leq i$. $\{B_\lambda\}_{\lambda \in \Lambda}$ is called an **inverse system** or a **projective system**.

**Definition 3.11.** Let $\{A_\lambda\}_{\lambda \in \Lambda}$ be a direct system. The direct limit $\varinjlim A_\lambda$ is defined to be $\varinjlim A_\lambda = \prod_{\lambda \in \Lambda} A_\lambda/\sim$, where $\sim$ is the following equivalence relation. Given $x_\lambda \in A_\lambda$, $x_j \in A_j$, we say that $x_\lambda \sim x_j$ if there exists $l, l \geq i, j$ such that $\mu_{il}(x_\lambda) = \mu_{jl}(x_j)$.

The inverse, or projective limit $\varprojlim B_\lambda$ is defined to be

$$
\varprojlim B_\lambda = \left\{ \{x_\lambda\}_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} B_\lambda \mid \phi_{ij}(x_\lambda) = x_j \text{ for all } i, j \text{ such that } i \geq j \right\}.
$$

**Exercise 3.12.** Show that $\varinjlim A_\lambda$ and $\varprojlim B_\lambda$ are characterized by the following universal mapping properties. Let $A = \varinjlim A_\lambda$. Then there are natural maps $\pi_i : A_i \to A$, $i \in \Lambda$, compatible with all the $\mu_{ij}$. Moreover, given any other set $A'$ and a collection of maps $\pi'_i : A_i \to A'$ compatible with the $\mu_{ij}$, there exists a unique map $A \to A'$, compatible with all the $\pi_i$ and $\pi'_i$.

Similarly, let $B = \varprojlim B_\lambda$. Then there are natural maps $\pi_i : B \to B_i$, $i \in \Lambda$, compatible with all the $\phi_{ij}$. Moreover, given any other set $B'$ and a collection of
maps $\pi'_i : B' \to B_i$ compatible with the $\phi_{ij}$, there exists a unique map $B' \to B$, compatible with all the $\pi_i$ and $\pi'_i$.

If the sets $A_\lambda$ and $B_\lambda$ are endowed with an additional structure (such as rings, groups, etc.), this structure usually extends in an obvious way to projective and inductive limits. We will take this fact for granted without mentioning it explicitly.

**Exercise 3.13.** Let $A$ be a ring, $S \subset A$ a multiplicative subset. Define a partial order in $S$ by saying that $f \leq g$ if there exists $h \in S$ such that $g = fh$. Then $S$ is a directed open set. Show that the localizations $A_f$ form a directed system and that the basic open sets $U_f = \text{Spec } A_f$ form a projective system. Show that

$$\lim_{f \in S} A_f = A_S.$$  

In particular, if $P \in \text{Spec } A$, $A_P = \lim_{f \not\in P} A_f$.

By passing to Specs and reversing all the arrows in (3.2), obtain

$$\lim_{f \in S} \text{Spec } A_f = \text{Spec } A_S$$

(as sets).

§4. A PROOF OF HILBERT’S NULLSTELLENSATZ.

In this section, we give a proof of the various versions of the Nullstellensatz.

An injective ring homomorphism is called a ring extension. Let $\sigma : A \hookrightarrow B$ be an extension of rings. Let $x \in B$.

**Definition 4.1.** We say that $x$ is algebraic over $A$, if it satisfies a polynomial equation of the form

$$(4.1) \quad a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

with $a_i \in A$. $x$ is integral, or finite over $A$ if, in addition, we may take $a_n = 1$ in (4.1). If $x$ is not algebraic, it is said to be transcendental. We say that $\sigma$ is algebraic, or that $B$ is algebraic over $A$, if every $x \in B$ is algebraic. $\sigma$ is integral if every $x \in B$ is integral over $A$. Extensions which are not algebraic are called transcendental.

Note that if $A$ is a field then “integral over $A$” and “algebraic over $A$” are the same thing.

**Proposition 4.2 (an intermediate version of the Nullstellensatz).** Let $k$ be a field and $A$ a finitely generated $k$-algebra. Then $A$ is a domain, algebraic over $k$, if and only if $A$ is a field.
First, let us assume Proposition 4.2 and show that it implies the two other versions of Nullstellensatz which were stated previously.

**Proof of Theorem 1.16.** It is obvious that for every \( a = (a_1, \ldots, a_n) \in k^n \), \((x_1 - a_1, \ldots, x_n - a_n)\) is a maximal ideal of \( k[x_1, \ldots, x_n] \), and that distinct points \( a, a' \in k^n \) give rise to distinct maximal ideals. It remains to show that every maximal ideal is of the form \((x_1 - a_1, \ldots, x_n - a_n)\), \( a \in k^n \). Take any \( m \in \text{Max}(k[x_1, \ldots, x_n]) \). Then \( \frac{k[x_1, \ldots, x_n]}{m} \) is a field, which is a finitely generated \( k \)-algebra (since it is generated by the images of the \( x_i \)). By Proposition 4.2, \( \frac{k[x_1, \ldots, x_n]}{m} \) is algebraic over \( k \), hence equals \( k \) (\( k \) being algebraically closed). Then for each \( i, 1 \leq i \leq n \), there exists \( a_i \in k \) such that \( x_i \equiv a_i \mod m \). Then \( m \supset (x_1 - a_1, \ldots, x_n - a_n) \), hence \( m = (x_1 - a_1, \ldots, x_n - a_n) \), as desired. \( \square \)

To prove Theorem 1.7, we state and prove the following more general result, which holds without the assumption that \( k \) is algebraically closed.

**Proposition 4.3.** Let \( k \) be any field and \( R \) a finitely generated \( k \)-algebra. For an ideal \( I \subset R \), let \( \tilde{V}(I) = \{m \in \text{Max}(R) \mid I \subset m\} \). For a subset \( V \subset \text{Max}(R) \), let \( I(V) = \{f \in R \mid f \not\in m \text{ for all } m \in V\} \). Then for any ideal \( I, I(\tilde{V}(I)) = \sqrt{I} \).

By Theorem 1.16, Proposition 4.3 implies Theorem 1.7.

**Proof of Proposition 4.3 (assuming Proposition 4.2).** Clearly, \( \sqrt{I} \subset I(\tilde{V}(I)) \). We must prove the opposite inclusion.

Take \( f \not\in \sqrt{I} \). We may consider \( B = (\frac{R}{m})_f = \frac{R[f]}{f} \) (where by abuse of notation we identify \( f \) with its natural image in \( \frac{R}{f} \)). We have a natural map \( \sigma : R \rightarrow B \). Take any \( m \in \text{Max}(B) \). Then \( I \subset m \cap R \) and \( f \not\in m \cap R \). If we can show that \( m \cap R \) is maximal, we will have \( m \cap R \in \tilde{V}(I) \) and hence \( f \not\in I(\tilde{V}(I)) \), as desired.

To see that \( m \cap R \) is maximal, apply Proposition 4.2 to \( \frac{B}{m} \) and \( \frac{R}{m \cap R} \). \( B \) is a finitely generated \( k \)-algebra (it is generated by the generators of \( R \) and \( \frac{1}{f} \)). By Proposition 4.2, we have \( m \) maximal \( \implies \frac{B}{m} \) is a field \( \implies \frac{B}{m} \) is algebraic over \( k \) \( \implies \frac{R}{m \cap R} \) is a domain, algebraic over \( k \) (since \( R \cap m \) is prime and \( \frac{R}{m \cap R} \subset \frac{B}{m} \)) \( \implies \frac{R}{m \cap R} \) is a field \( \implies R \cap m \) is a maximal ideal of \( R \). \( \square \)

To complete the proof of Proposition 4.3, and hence of Theorem 1.7, it remains to prove Proposition 4.2.

**Proof of Proposition 4.2.** First, suppose \( A \) is a domain, algebraic over \( k \). Take any \( x \in A \). We must show that \( x \) is invertible in \( A \). Since \( A \) is algebraic, \( x \) satisfies an equation of the form \( a_n x^n + \cdots + a_0 = 0 \), with \( a_i \in k \). Since \( A \) is a domain, we may assume that \( a_0 \neq 0 \). Then \( x(-\frac{1}{a_0}) \sum_{i=0}^{n-1} a_{i+1} x^i = 1 \), which proves that \( x \) is invertible.

Conversely, suppose \( A \) is a field, which is not algebraic over \( k \). Since \( A \) is finitely generated, we may write \( A = k[x_1, \ldots, x_n] \) for some \( x_1, \ldots, x_n \in A \). We can renumber the \( x_i \) such that \( x_1, \ldots, x_r \) are algebraically independent over \( k \) and \( A \) is algebraic over \( k[x_1, \ldots, x_r] \). Replacing \( k \) by the field \( k(x_1, \ldots, x_{r-1}) \) does not change
the problem, so that we may assume \( r = 1 \). For \( 2 \leq i \leq n \), let \( b_i \in k[x_1] \) be the leading coefficient of a polynomial equation over \( k[x_1] \), satisfied by \( x_i \). Then all the \( x_i \) are integral over \( k[x_1]b_2...b_n \). At this point, we need the following basic fact about integral extensions:

**Lemma 4.4.** Let \( A \subset B \) be a finitely generated ring extension. If each of the generators is integral over \( A \), then \( B \) is integral over \( A \).

First, we finish the proof, assuming Lemma 4.4. Since each of the \( x_i \) is integral over \( k[x_1]b_2...b_n \), by Lemma 4.4 \( A \) is integral over \( k[x_1]b_2...b_n \). Since \( A \) is a field, it contains \( k(x_1) \), so that \( k(x_1) \) is integral over \( k[x_1]b_2...b_n \).

**Definition 4.5.** Let \( A \to B \) be a ring extension. The integral closure of \( A \) in \( B \) is the \( A \)-subalgebra \( \bar{A} \) of \( B \) consisting of all the elements of \( B \), integral over \( A \) (the fact that \( \bar{A} \) is a subalgebra follows from Lemma 4.4). \( A \) is said to be integrally closed in \( B \), if \( A = \bar{A} \). If \( A \) is a domain, we will say that it is integrally closed or normal if \( A \) is integrally closed in its field of fractions.

**Definition 4.6.** A domain \( A \) is said to be a unique factorization domain, or UFD, if every element of \( A \) can be written uniquely (up to multiplication by units of \( A \)) as a product of irreducible elements.

Let \( b = x_1b_2...b_n + 1 \), so that \( \deg b \geq 1 \) and \( b \) is relatively prime to \( b_2...b_n \). We have \( k[x_1]b_2...b_n \subseteq k(x_1) \), because \( \frac{1}{b} \in k(x_1) \setminus k[x_1]b_2...b_n \). At the same time, \( k(x_1) \), which is the field of fractions of \( k[x_1]b_2...b_n \), is integral over \( k[x_1]b_2...b_n \). To get a contradiction, it is sufficient to show that \( k[x_1]b_2...b_n \) is normal. Now, it is well known that \( k[x_1] \) is a UFD (this is proved by using Euclidean algorithm, in other words, division with remainder). Thus the normality of \( k[x_1]b_2...b_n \) follows from two facts, which we leave to the reader as easy exercises:

**Exercise 4.7.** If \( B \) is a UFD and \( S \) a multiplicative subset of \( B \), then \( B_S \) is a UFD.

**Exercise 4.8.** Any UFD is normal.

To complete the proofs of all the Nullstellensatizes, it remains to prove Lemma 4.4. To do this, we introduce the concept of a module over a ring.

**Definition 4.9.** Let \( A \) be a ring. An \( A \)-module is an abelian group \( M \) together with an operation \( A \times M \to M \) (multiplication by elements of \( A \)), such that for all \( a, b \in A \), \( x, y \in M \), we have:

1. \( a(bx) = (ab)x \)
2. \( (a + b)x = ax + bx \)
3. \( a(x + y) = ax + ay \)
4. \( 1x = x \).

Any ideal of \( A \) is an \( A \)-module. Any \( A \)-algebra is an \( A \)-module.
**Definition 4.10.** Let $A$ be a ring and $M$ an $A$-module. An $A$-submodule of $M$ is an abelian subgroup of $M$, which is an $A$-module under the operations inherited from $M$.

For example, the $A$-submodules of $A$ are precisely the ideals of $A$.

**Definition 4.11.** Let $M$ be an $A$-module and $x = \{x_\lambda\}_{\lambda \in \Lambda}$ a subset of $M$. The $A$-submodule $B$, generated by $x$ (sometimes denoted by $\sum_{\lambda \in \Lambda} A x_\lambda$), is defined to be the smallest $A$-submodule of $M$, containing $x$. In other words, $\sum_{\lambda \in \Lambda} A x_\lambda$ is the set of all elements of $M$ which can be written as $A$-linear combinations of the $x_\lambda$. We say that $M$ is a **finitely generated** or a **finite** $A$-module if there is a finite subset $\{x_1, \ldots, x_n\} \subset M$ such that $M = \sum_{i=1}^n A x_i$. An $A$-algebra $B$ is said to be **finite** over $A$ if $B$ is a finite $A$-module (of course, this is stronger than saying that $B$ is a finitely generated $A$-algebra).

**Exercise 4.12.** Let $A \subset B \subset C$ be ring extensions. If $B$ is finite over $A$ and $C$ finite over $B$, then $C$ is finite over $A$.

Now we are in the position to prove Lemma 4.4. We prove Lemma 4.4 in the following stronger form.

**Lemma 4.13.** Let $A \hookrightarrow B$ be an extension of rings. The following conditions are equivalent.

1. $B$ is finite over $A$.
2. $B$ is integral and finitely generated over $A$ (as an algebra).
3. $B$ is finitely generated over $A$ as an algebra, and each of the generators is integral over $A$.

**Proof.** (2) $\implies$ (3) is trivial.

(1) $\implies$ (2). Assume that $B$ is finite over $A$. Clearly, $B$ is finitely generated as an $A$-algebra. Let $x_1, \ldots, x_n$ be a set of generators of $B$ as an $A$-module. Take any $y \in B$; we want to show that $y$ is integral over $A$. There exist $a_{ij} \in A$, $1 \leq i, j \leq n$, such that $y x_i = \sum_{j=1}^n a_{ij} x_j$. Let $T$ denote the $n \times n$ matrix with entries $a_{ij}$, $I$ the $n \times n$ identity matrix. Consider the $n \times n$ matrix $y I - T$ with entries in $B$. Let $x$ denote the column $n$-vector with entries $x_i$. By construction, $(y I - T)x = 0$. Hence, by linear algebra, $\det(y I - T)x_i = 0$ for $1 \leq i \leq n$. Since the $x_i$ generate $B$ as an $A$-module, $\det(y I - T)x = 0$ for every $x \in B$, so that $\det(y I - T) = 0$. We have constructed a monic polynomial equation satisfied by $y$ over $A$, which proves that $y$ is integral over $A$.

(3) $\implies$ (1) Suppose $B$ is finitely generated, with generators integral over $A$. Since a composition of finite extensions is finite (Exercise 4.12), we may assume that, as an algebra, $B$ is generated over $A$ by a single element $x$, integral over $A$. This means that as an $A$-module, $B$ is generated by $1, x, x^2, \ldots, x^n, \ldots$. By assumption, $x$ satisfies a monic equation $x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$ over $A$. Hence $x^n$ belongs to the $A$-submodule of $B$ generated by $1, x^2, \ldots, x^{n-1}$. Then by induction on $l$, any $x^l$ with $l \geq n$ belongs to the $A$-submodule of $B$ generated by $1, x^2, \ldots, x^{n-1}$. Hence
\[ B \] is generated by \( 1, x^2, \ldots, x^{n-1} \) as an \( A \)-module, which proves that \( B \) is finite over \( A \).

This completes the proof of Lemma 4.13, Propositions 4.2 and 4.3 and Theorem 1.7. \( \square \)

\section*{§5. Primary decomposition.}

\textbf{Definition 5.1.} A topological space \( X \) is said to be \textbf{Noetherian} if any descending chain of closed sets in \( X \) stabilizes.

\textbf{Exercise 5.2.} Show that in a Noetherian topological space every closed set can be written uniquely as a finite union of irreducible closed sets.

Clearly, if \( R \) is a Noetherian ring, then the affine scheme \( \text{Spec} \ R \) is Noetherian. Let \( I \) be a \textit{radical} ideal of \( R \). We saw earlier (Proposition 1.20) that the reduced closed subscheme \( V(I) \subset \text{Spec} \ R \) is irreducible if and only if \( I \) is prime. Hence, Exercise 5.2 applied to \( \text{Spec} \ R \) is equivalent to saying that in a Noetherian ring every radical ideal can be written uniquely as an intersection of primes (the uniqueness follows easily from Lemma 1.21).

Since in scheme theory we are interested in including the case of \textit{non-reduced} schemes, we would like to extend this result to ideals of \( R \) which are not necessarily radical. The corresponding result in the non-radical case is called \textbf{primary decomposition}.

First, we note that the elementary argument of Exercise 5.2 applies verbatim to show that every ideal can be written as an intersection (not necessarily unique) of irreducible ideals:

\textbf{Definition 5.3.} Let \( I \) be an ideal of \( A \). \( I \) is \textit{irreducible} if it cannot be written in the form \( I = I_1 \cap I_2 \), where \( I_1 \) and \( I_2 \) properly contain \( I \).

\textbf{Lemma 5.4.} Let \( A \) be a Noetherian ring. Then every ideal of \( A \) can be written as a finite intersection of irreducible ideals in \( A \).

\textit{Proof.} Let \( \Sigma \) denote the collection of all the proper ideals of \( A \) which cannot be expressed as an intersection of finitely many irreducible ideals of \( A \). We want to show that \( \Sigma = \emptyset \). Suppose not. Since \( A \) is Noetherian, \( \Sigma \) contains a maximal element \( I \). Since \( I \in \Sigma \), \( I \) is not irreducible. Then \( I \) can be written as \( I = I_1 \cap I_2 \) for some ideals \( I_1, I_2 \) of \( A \) such that \( I \not\subseteq I_1 \) and \( I \not\subseteq I_2 \). By the maximality of \( I \), we have \( I_1, I_2 \not\in \Sigma \). Hence both \( I_1 \) and \( I_2 \) can be expressed as finite intersections of irreducible ideals of \( A \) and hence so can \( I \). Then \( I \not\in \Sigma \), a contradiction. Therefore \( \Sigma = \emptyset \). \( \square \)

The point of primary decomposition is to give a more explicit description of irreducible ideals and to relate the irreducible ideals appearing in a decomposition of \( I \) to the set of zero divisors in \( \frac{A}{I} \).

\textbf{Definition 5.5.} Let \( A \) be a ring and \( Q \not\subseteq A \) an ideal. \( Q \) is \textit{primary} if for any \( x, y \in A \) such that \( xy \in Q \), either \( x \in Q \) or \( y \in \sqrt{Q} \).
Note that in the above definition we think of \( x, y \) as an ordered pair. The definition is not symmetric in \( x \) and \( y \).

**Remark 5.6.** Let \( Q \) be a primary ideal of \( A \). Then \( P = \sqrt{Q} \) is prime. Indeed, \( xy \in P \implies (xy)^n \in Q \) for some \( n \in \mathbb{N} \implies x^n \in Q \) or \( y^m \in Q \) for some \( m \in \mathbb{N} \). Thus \( x^n \in Q \) or \( y^m \in Q \), so that either \( x \in P \) or \( y \in P \). This proves that \( P \) is prime. We say that \( Q \) is a \( P \)-primary ideal or that it is primary to \( P \).

Let \( Q \) be an ideal such that \( \sqrt{Q} = P \) is prime. Then \( Q \) is primary if and only if \( Q = Q_A P \cap A \). In particular, the intersection of two \( P \)-primary ideals is \( P \)-primary.

Next, we show that every irreducible ideal is primary, so that every ideal in a Noetherian ring is a finite intersection of primary ideals. In the rest of this section, we will discuss to what extent this primary decomposition is unique.

**Exercise 5.7.** Let \( m \in \text{Max}(A) \). Show that an ideal \( Q \) is \( m \)-primary if and only if \( \sqrt{Q} = m \).

**Lemma 5.8.** Let \( A \) be a Noetherian ring, \( I \subset A \) an irreducible ideal. Then \( I \) is primary.

**Proof.** Suppose \( ab \in I \) and \( b \notin I \). Let \( I : a = \{ x \in A \mid ax \in I \} \). \( I : a \) is an ideal. \( I : a \subset I : a^2 \subset (I : a^3) \subset \ldots \) is an ascending sequence of ideals in \( A \). Since \( A \) is Noetherian, there exists \( n \in \mathbb{N} \) such that \( I : a^n = I : a^{n+1} \) for all \( i \geq 1 \).

Now, \( I \subset (I + (a^n)) \cap (I + (b)) \). Conversely, let \( r \in (I + (a^n)) \cap (I + (b)) \). Then \( r = g + ca^n = h + db \) where \( g, h \in I \) and \( c, d \in A \). So \( ra = ga + ca^{n+1} = ha + dab \), so that \( g, h, ab \in I \). Then \( c \in (I : a^{n+1}) = (I : a^n) \), so that \( r = g + ca^n \in I \). We obtain \( I = (I + (a^n)) \cap (I + (b)) \).

Now, \( I \) is irreducible and \( I \not\subseteq I + (b) \) because \( b \notin I \). Hence \( I = I + (a^n) \), so \( a^n \in I \). We have proved that \( a \in \sqrt{I} \). Therefore \( I \) is primary, as desired.

**Corollary 5.9.** Let \( A \) be a Noetherian ring, \( I \subset A \) an ideal. There exists a decomposition

\[
(5.1) \quad I = \bigcap_{i=1}^{n} Q_i,
\]

where each \( Q_i \) is primary.

**Example 5.10.** Primary decomposition is not unique. Let \( A = k[x, y] \). We have \( (x^2, xy) = (x) \cap (y, x^2) = (x) \cap (y, x^2) \), which are two different primary decomposition of the same ideal.

We will now further analyze primary decomposition of a given ideal.

**Definition 5.11.** Let \( A \) be a ring, \( I \subset A \) an ideal. Consider a decomposition \( I = \bigcap_{i=1}^{n} Q_i \) where each \( Q_i \) is primary. Let \( P_i = \sqrt{Q_i} \); by Remark 5.6, the \( P_i \) are prime. The \( P_i \) are called associated primes of \( I \). The minimal ones among the \( P_i \) are called the minimal primes of \( I \). Associated primes which are not minimal are called the embedded components or embedded points of \( I \). Sometimes the
$P_i$ are also referred to as the associated (resp. minimal) primes of the $A$-module $\frac{A}{I}$. In particular, the associated (resp. minimal) primes of $(0)$ are called the associated (resp. minimal) primes of $A$. This terminology seems ambiguous, but usually it causes no confusion.

**Note 5.12.** By Lemma 1.21, the minimal primes of $I$ are precisely the minimal elements of $V(I)$ under inclusion, so that the name is appropriate.

For instance, in Example 5.10, $(x)$ and $(x,y)$ are the associated primes, $(x)$ is the only minimal prime and $(x,y)$ is an embedded point. In this example, we see that the collection of associated primes depends only on the ideal $I$ and not on the choice of the primary decomposition. We will now show that this is true in general by describing the $P_i$ in terms of zero divisors mod $I$.

**Lemma 5.13.** Let $Q \subseteq A$ be a primary ideal, $P = \sqrt{Q}$, $a$ an element of $A$.

1. If $a \in Q$, then $\left(Q : a\right) = A$.
2. If $a \in P \setminus Q$, then $Q \subseteq \left(Q : a\right)$ and $Q : a$ is $P$-primary.
3. If $a \notin P$, then $\left(Q : a\right) = Q$.

**Proof.** (1) is obvious.

We always have $Q \subseteq (Q : a)$ because $Q$ is an ideal.

(2) First, we show that $(Q : a) \subseteq P$. Indeed, take $b \in (Q : a)$; then $ab \in Q$. Since $a \notin Q$ and $Q$ is primary, we have $b \in P$. This proves that $(Q : a) \subseteq P$.

Now, $P = \sqrt{Q} \subseteq \sqrt{(Q : a)} \subseteq \sqrt{P} = P$ (the last equality holds since $P$ is prime), therefore $\sqrt{(Q : a)} = P$.

Now, take $b, c \in A$ such that $bc \in (Q : a)$ and $b \notin \sqrt{(Q : a)} = P$. Then $abc \in Q$. Since $b \notin P = \sqrt{Q}$ and $Q$ is primary, $ac \notin Q$. Hence $c \in (Q : a)$. This proves that $(Q : a)$ is primary.

It remains to show that $Q : a \neq Q$. Indeed, since $a \in P \setminus Q$, there exists a unique $n \in \mathbb{N}$ such that $a^n \notin Q$ but $a^{n+1} \in Q$. Then $a^n \in (Q : a) \setminus Q$. This completes the proof of Lemma 5.13. $\square$

We will now use Lemma 5.13 to interpret primary decomposition in terms of the set of zero divisors mod $I$.

**Theorem 5.14.** Let $I$ be an ideal in a Noetherian ring $A$. Consider a primary decomposition (5.1). Let $P_i = \sqrt{Q_i}$, $1 \leq i \leq n$. Then:

1. $P_1, \ldots, P_n$ are precisely all the prime ideals which are of the form $I : a$ for some $a \in A$.
2. Let $\hat{P}_i = P_i A_T$, $1 \leq i \leq n$. Then the set of zero divisors in the ring $\frac{A}{I}$ is $\bigcup_{i=1}^n \hat{P}_i$.

In particular, the set of zero divisors in $A$ is precisely the union of the associated primes of $A$ (recall that $\text{nil}(A)$ is the intersection of the associated primes of $A$).
Corollary 5.15. The collection \( \{ P_i \}_{1 \leq i \leq n} \) depends only on \( I \) and not on the choice of primary decomposition.

If \( A \) is a ring and \( a \in A \), the annihilator of \( a \) is the ideal \( \text{Ann} \ a = (0) : a \). Thus another way of stating Theorem 5.14 is to say that the associated primes of \( A \) are precisely all the prime ideals of the form \( \text{Ann} \ a \) for \( a \in A \).

Proof of Theorem 5.14. (1) We may assume that for all \( i = 1, 2, \ldots, n \), \( Q_i \not\supset \bigcap_{j=1}^{n} Q_j \). Take any \( i \), \( 1 \leq i \leq n \) and any \( a \in \bigcap_{j=1}^{n} Q_j \setminus Q_i \). We have

\[
(I : a) = \left( \bigcap_{j=1}^{n} Q_j \right) : a = \bigcap_{j=1}^{n} (Q_j : a) = Q_i : a \subset P_i,
\]

where the last two statements hold by Lemma 5.13. Let \( \tilde{P}_i \) denote a maximal element among all the ideals of the form \( I : a \), where \( a \in \bigcap_{j=1}^{n} Q_j \setminus Q_i \). By (5.2) and Lemma 5.13 (2),(3),

\[
(5.3) \quad P_i = \sqrt{\tilde{P}_i}.
\]

We want to show that \( \tilde{P}_i = P_i \), that is, all the \( P_i \) are of the form \( I : a \) for some \( a \in A \). Suppose not. Let \( a \in \bigcap_{j=1}^{n} Q_j \setminus Q_i \) be such that \( \tilde{P}_i = I : a \) and take \( b \in P_i \setminus \tilde{P}_i \).

By (5.3), there exists \( l \in \mathbb{N} \) such that \( b^l \notin \tilde{P}_i \) but \( b^{l+1} \in \tilde{P}_i \). Since \( b^l \notin \tilde{P}_i = I : a \), \( ab^l \notin I \). Since \( a \in \bigcap_{j=1}^{n} Q_j \),

\[
(5.4) \quad ab^l \in \bigcap_{j=1}^{n} Q_j.
\]

Combined with \( ab^l \notin I \), (5.4) gives \( ab^l \in \bigcap_{j=1}^{n} Q_j \setminus Q_i \). On the other hand, \( b^{l+1} a \in I \) by the choice of \( l \). Then \( \tilde{P}_i = I : a \subseteq I : (ab^l) \), where the inclusion is strict because \( b \in I : (ab^l) \setminus \tilde{P}_i \). This contradicts the maximality of \( \tilde{P}_i \). We have proved that all the \( P_i \), \( 1 \leq i \leq n \) are of the form \( I : a \) for some \( a \in A \).

Conversely, let \( P \in \text{Spec} \ A \) be of the form \( P = I : a \) for some \( a \in A \). Then \( P = \bigcap_{j=1}^{n} (Q_j : a) \). Since prime ideals are irreducible (Proposition 1.20), we must have \( P = Q_i : a \) for some \( i \), \( 1 \leq i \leq n \). Hence \( Q_i : a \neq A \), so that, by Lemma 5.13,
\( \sqrt{(Q_i : a)} = P_i \). We obtain \( P = \sqrt{P} = \sqrt{(Q_i : a)} = P_i \). This completes the proof of (1).

(2) We may replace \( A \) by \( A' \), \( I \) by \( (0) \) and \( P_i \) by \( \overline{P}_i \). In particular, we take the \( Q_i \) to be primary components of the zero ideal: \( (0) = \cap_{i=1}^n Q_i \). By (1), each of the \( P_i \) is the annihilator ideal of some \( a \in A \), hence every element in \( \cup_{i=1}^n P_i \) is a zero divisor.

Conversely, take any \( a \in A \setminus \cup_{i=1}^n P_i \). Then by Lemma 5.13 (3), \( Q_i : a = Q_i \) for \( 1 \leq i \leq n \). We have \( \text{Ann} a \equiv (0) : a = \cap_{i=1}^n (Q_i : a) = \cap_{i=1}^n Q_i = (0) \). Thus \( a \in A \setminus \cup_{i=1}^n P_i \) implies that \( a \) is not a zero divisor, as desired. This completes the proof of Theorem 5.14. \( \square \)

§6. Dimension Theory.

Continuing with our dictionary between algebra and geometry, we come to the concept of dimension of an algebraic variety or scheme. Intuitively, we all know what is meant by dimension in geometry; for example, everybody knows that the \( n \)-space \( k^n \) has dimension \( n \). Therefore, it is natural to look for the corresponding definition on the algebraic side: that of the dimension of a ring. There are several alternative ways of thinking about dimension; the purpose of this section is to describe their algebraic interpretation and to prove that all give the same answer.

The first one is the maximal length of a descending chain of irreducible subvarieties. For example, a maximal chain of irreducible subvarieties in \( k^n \) is \( k^n \supset k^{n-1} \supset \cdots \supset k^2 \supset k \supset \{0\} \); it has length \( n \) (not counting \( k^n \) itself). We model our definition of the dimension of a ring on this geometric idea.

The second approach is to consider the number of elements in a local coordinate system on \( X \). More precisely, since we want to include singular varieties, we should consider the smallest number of equations, whose set of common zeroes in \( X \) consists of isolated points. This is the idea behind the integer \( \delta(A) \), associated to a local ring \( A \) later in this section.

A third way of defining dimension, of great importance both in theory and in computations, is the degree of the Hilbert-Samuel polynomial. Finally, in the case of an algebraic variety \( X \) over a field \( k \), the dimension equals the largest transcendence degree of the field of rational functions on an irreducible component of \( X \). We now give precise definitions and prove the equality of all four numbers.

**Definition 6.1.** Let \( A \) be a ring. The **Krull dimension** of \( A \), denoted \( \dim A \), is the maximal length of an ascending chain of prime ideals in \( A \):

\[
(6.1) \quad P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d
\]

not counting the minimal prime \( P_0 \). In other words, if (6.1) is the longest, we say that \( \dim A = d \). If there are arbitrarily long chains of primes in \( A \), we say that \( \dim A = \infty \). For \( P \in \text{Spec} A \), the **height** of \( P \) is defined by \( \text{ht} P = \dim A_P \) (which is the maximal length of a chain of prime ideals contained in \( P \)).
Exercise 6.2. Let $A$ be a ring. Prove that $\dim A = \max\{\dim A_m \mid m \in \text{Max}(A)\}$. (Hint: first, show that for any $P \in \text{Spec} A$, the natural map $\text{Spec} A_P \to \text{Spec} A$ induces a bijection between $\text{Spec} A_P$ and $\{Q \in \text{Spec} A \mid Q \subseteq P\}$.)

Soon we will show that $\dim A < \infty$ if $A$ is a Noetherian local ring.

Problem 6.3. Give an example of an infinite dimensional Noetherian ring.

Exercise 6.2 says that dimension can be computed locally. In other words, in order to study dimension in arbitrary rings, it is sufficient to understand the case of local rings.

Definition 6.4. Let $(A, m, k)$ be a Noetherian local ring. Let $\delta(A)$ denote the smallest number of generators of an $m$-primary ideal in $A$.

Definition 6.5. Let $A$ be a ring and $M$ an $A$-module. The length of $M$ is defined to be the maximal length of a chain of submodules $(0) \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$, not counting $(0)$. If there exist arbitrarily long such chains, we say that $\text{length}(M) = \infty$.

For example, if $V$ is a vector space over a field $k$, $\text{length}(V)$ as a $k$-module is nothing but $\dim_k V$.

A homomorphism of $A$-modules is a homomorphism of abelian groups, which respects multiplication by elements of $A$.

Given $A$-modules $N \subset M$, the quotient $M/N$ of $M$ by $N$ is defined to be the quotient of abelian groups, endowed in the obvious way with the operation of multiplication by elements of $A$. In particular, we may talk about the quotient $I/J$ of two ideals of $A$, $J \subset I$. We may view $I/J$ as an ideal in the ring $A/J$.

Exercise 6.6. Show that length is an additive function, that is, if $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then $\text{length}(M) = \text{length}(M') + \text{length}(M'')$.

Definition 6.7. Let $(A, m, k)$ be a Noetherian local ring. The Hilbert Samuel function of $A$ is the function $H_{A,m} : \mathbb{N} \to \mathbb{N}$, defined by $H_{A,m}(n) = \text{length} \left( \frac{A}{m^{n+1}} \right)$ (considered as an $A$-module). By additivity of length,

\begin{equation}
\text{length} \left( \frac{A}{m^{n+1}} \right) = \sum_{i=0}^{n} \dim_k \frac{m^i}{m^{i+1}},
\end{equation}

where the $\frac{m^i}{m^{i+1}}$ are $k$-modules, that is, $k$-vector spaces.

Note that since $A$ is Noetherian, each of $m^i$ is finitely generated, so that all the quantities in (6.2) are finite.

Theorem 6.8. $H_{A,m}(n)$ is a polynomial for $n \gg 0$. In other words, there exists a polynomial $P(n)$ with rational coefficients, such that $P(n) = H_{A,m}(n)$ for $n \gg 0$. $P(n)$ is sometimes called the Hilbert polynomial of $A$.

A proof of this Theorem 6.8 will be given shortly. First, we finish our list of the different characterizations of $\dim A$. 

Notation 6.9. Let $d(A)$ denote the degree of the Hilbert polynomial of $A$.

Finally, let $A$ be a $k$-algebra. Let $x_1, \ldots, x_n$ be elements of $A$.

Notation. Given $x = (x_1, \ldots, x_n)$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, $x^\alpha$ will denote the monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.

$x_1, \ldots, x_n$ are said to be algebraically independent over $k$ if they satisfy no non-trivial polynomial relations of the form $\sum a_\alpha x^\alpha = 0$, $a_\alpha \in k$. The transcendence degree of $A$ over $k$, denoted $\text{tr. deg}(A/k)$, is defined to be the maximal number of elements of $A$, algebraically independent over $k$. If $A$ is a finitely generated $k$-algebra, then $\text{tr. deg}(A/k) < \infty$.

Example 6.10. Let $k$ be a field, $A = k[x_1, \ldots, x_d]$ the polynomial ring in $d$ variables. $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_d)$ is a chain of prime ideals of length $d$.

Now let $m = (x_1, \ldots, x_d)$ be the maximal ideal corresponding to the origin in $k^d$. Consider the localization $A_m$. $m$ is generated by $d$ elements. The Hilbert-Samuel function of $A_m$ is $H_{A_m, m}(n) = \text{length}(\frac{A}{m^{n+1}}) = (\frac{n+d}{d})$, which is a polynomial in $n$ of degree $d$. In this case, $H_{A_m, m}(d)$ is a polynomial for all $n$, not merely for $n$ sufficiently large.

Thus, in this example, we have

$$tr. \text{deg}(A/k) = d(A_m) = d \geq \dim A \geq \dim A_m \geq \delta(A).$$

We will soon show that all the inequalities in (6.3) are, in fact, equalities.

We now turn to the main purpose of this section, which is to prove that for any Noetherian local ring $A$, $\dim A = d(A) = \delta(A)$. If $A$ is a finitely generated algebra over a field $k$, we will prove that $\dim A = tr. \text{deg}(A/k)$.

The first step is to prove that $d(A)$ is well defined, that is, $H_{A_m, m}(n)$ is, indeed, a polynomial for $n \gg 0$. To this end, we introduce the notion of graded algebras and graded modules.

Definition 6.11. Let $G_0$ be a ring. A graded $G_0$-algebra is a $G_0$-algebra of the form $G = \bigoplus_{n=0}^{\infty} G_n$, such that for all $n, l \in \mathbb{N}_0$, we have $G_n G_l \subset G_{n+l}$ (in particular, each $G_n$ is a $G_0$-module under the ring operations in $G$).

If $G$ is a graded $G_0$-algebra, a graded $G$-module is a $G$-module of the form $M = \bigoplus_{n=0}^{\infty} M_n$ where each $M_n$ is a $G_0$-module and for all $n, l \in \mathbb{N}_0$, we have $G_n M_l \subset M_{n+l}$. For $n \in \mathbb{N}_0$, elements of $M_n$ are called homogeneous of degree $n$.

Example 6.12. Let $A$ be a ring and $I \subset A$ an ideal. Associated to $A$ and $I$ is the graded $\frac{A}{I}$-algebra $\text{gr}_I A = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$. If $I$ is a finitely generated ideal, then $\text{gr}_I A$ is a finitely generated $\frac{A}{I}$-algebra (its generators as an $\frac{A}{I}$-algebra are precisely the
generators of $I$ as an ideal, viewed as elements of $\text{gr}_I A$ of degree 1). By the Hilbert basis theorem, if $A$ is Noetherian then $\text{gr}_I A$ is Noetherian (cf. Exercise 6.13 below). In particular, if $(A, m, k)$ is a local Noetherian ring, $\text{gr}_m A$ is a finitely generated graded $k$-algebra. Moreover, for any $n \in \mathbb{N}_0$, $\dim_k \frac{m^n}{m^{n+1}} < \infty$. In other words, the homogeneous elements of degree $n$ form a finite dimensional vector space. For the moment, this last example of a graded algebra is our main interest for applications. Later in the course, other important examples of graded algebras will appear.

**Exercise 6.13.** Let $G$ be a graded $G_0$-algebra. Prove that $G$ is Noetherian if and only if $G_0$ is Noetherian and $G$ is finitely generated over $G_0$. Now, suppose that this is the case and let $M$ be a finitely generated graded $G$-module. Show that each $M_n$ is a finite $G_0$-module.

The Hilbert-Samuel function of a Noetherian local ring $(A, m, k)$ is

$$H_{A, m}(n) = \sum_{i=0}^{n} \text{length} \frac{m^i}{m^{i+1}}.$$ 

We start our proof of Theorem 6.8 by the following simple observation. Let $P(n)$ be a real valued function of $n$. Let $P^{(1)}(n) = \sum_{i=0}^{n} P(n)$ and let $d \in \mathbb{N}_0$. Then $P$ is a polynomial in $n$ of degree $d$ if and only if $P^{(1)}$ is a polynomial of degree $d + 1$. Hence to prove Theorem 6.8 it is sufficient to prove, for a local Noetherian ring $(A, m, k)$, that for $n \gg 0 \text{length} \frac{m^n}{m^{n+1}}$ is a polynomial in $n$. We can generalize this statement as follows.

Let $G$ be a graded algebra, $M = \bigoplus_{n=0}^{\infty} M_n$ a finite graded $G$-module, as in the Example 6.12 (in particular, each $M_n$ is a finite $G_0$-module). Let $\lambda$ be an additive function from the category of finite $G_0$-modules to $\mathbb{N}_0$. For $n \in \mathbb{N}_0$, we may consider $\lambda(M_n)$ as a function of $n$. To prove Theorem 6.8, it is enough to show that $\lambda(M_n)$ is a polynomial for $n \gg 0$. To this end, we consider the generating function of $M$: $P(M, t) = \sum_{n=0}^{\infty} \lambda(M_n) t^n$, where $t$ is an independent variable.

**Theorem 6.14 (Hilbert, Serre).** Let $x_1, \ldots, x_d$ be a set of homogeneous generators of $M$, $k_i = \deg x_i$. Then $P(M, t) = \frac{f(t)}{\prod_{i=1}^{d} (1-t^{k_i})}$, where $f$ is a polynomial in $t$ with integer coefficients.

**Proof.** Induction on $d$. First, let $d = 0$. Then $A = A_0$, hence $M_n = 0$ for $n \gg 0$, so that $\lambda(M_n) = 0$ for $n \gg 0$ and the result is true in this case.

Next, suppose the result is known for $d - 1$. For each $n \in \mathbb{N}_0$, multiplication by $x_d$ is a $G_0$-module homomorphism from $M_n$ to $M_{n+k_d}$. Let $K_n$ and $L_{n+k_d}$ denote, respectively, the kernel and the cokernel of this homomorphism. For each $n \in \mathbb{N}_0$, we obtain an exact sequence

$$(6.4) \quad 0 \to K_n \to M_n \to M_{n+k_d} \to L_{n+k_d} \to 0.$$
By additivity of \( \lambda \), (6.4) implies that

\[
\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_d}) - \lambda(L_{n+k_d}) = 0. 
\]

Let \( K = \bigoplus_{n=0}^{\infty} K_n, L = \sum_{n=k_d}^{\infty} L_n \). Multiply (6.5) by \( t^{n+k_d} \) and sum over \( n \). We obtain

\[
t^{k_d}P(K,t) - t^{k_d}P(M,t) + P(M,t) - P(L,t) + g(t) = 0, 
\]

where \( g(t) \) is a polynomial in \( t \). Since both \( K \) and \( L \) are annihilated by \( x_d \), both \( K \) and \( L \) are graded \( G_0[x_1, \ldots, x_{d-1}] \)-modules. Hence by the induction assumption, \( \prod_{i=1}^{d-1} (1-t^{ki})P(K,t) \) and \( \prod_{i=1}^{d-1} (1-t^{ki})P(L,t) \) are polynomials in \( t \). By (6.6), we obtain

\[
(1-t^{k_d})P(M,t) = -t^{k_d}P(K,t) + P(L,t) - g(t). 
\]

Hence \( P(M,t) = \frac{f(t)}{\prod_{i=1}^{d-1}(1-t^{ki})} \) for some polynomial \( f(t) \) and the Theorem is proved. \( \square \)

We have the following Corollary, which obviously implies Theorem 6.8.

**Corollary 6.15.** Let \( G = \bigoplus G_n, M = \bigoplus M_n, \lambda, x_i \) be as in Theorem 6.14. Suppose that \( k_i \equiv \deg x_i = 1, 1 \leq i \leq d \). Then, for \( n \gg 0, \lambda(M_n) \) is a polynomial in \( n \) of degree at most \( d-1 \).

**Proof.** By Theorem 6.14, \( P(M,t) = \frac{f(t)}{(1-t)^d} \), where \( f \) is a polynomial in \( t \). Write

\[
f(t) = \sum_{k=0}^{N} a_k t^k. 
\]

Since \( \frac{1}{(1-t)^d} = \sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n \), we have, for \( n \gg 0, \lambda(M_n) = \sum_{k=0}^{N} a_k \binom{n-k+d-1}{d-1} \), which is a polynomial in \( n \) of degree at most \( d-1 \). \( \square \)

**Remark 6.16.** Notice in the above proof that the degree of \( \lambda(M_n) \) for large \( n \) is precisely the order of the pole of \( \frac{f(t)}{(1-t)^d} \) at \( t = 1 \) minus 1.

We now state the main result of this section.

**Theorem 6.17.** Let \((A, m, k)\) be a Noetherian local ring. Then \( \dim A = d(A) = \delta(A) \).

First, we study the case \( \dim A = 0 \).

**Definition 6.18.** A ring \( A \) is said to be **Artinian** if every descending chain of ideals in \( A \) stabilizes.

Despite the apparent similarity of this definition with the Noetherian property, we will now show that the Artinian property is much stronger. Namely, we will show that \( A \) is Artinian if and only if \( A \) is Noetherian and \( \dim A = 0 \).

**Proposition 6.19.** Let \( A \) be an Artinian ring. Then every prime ideal of \( A \) is maximal (in other words, \( \dim A = 0 \)).

**Proof.** Let \( P \subset A \) be a prime ideal. Then \( A/P \) is an Artinian **domain**. We want to show it is a field. Take any \( x \in A/P \). It suffices to show that \( x \) is invertible.
Consider \((x) ⊃ (x^2) ⊃ (x^3) ⊃ \ldots\). This chain of ideals stabilizes, so that \((x^n) = (x^{n+1})\) for some \(n\). Hence there exists \(b ∈ A\) such that \(b x^{n+1} = x^n\). Since \(A\) is a domain, \(bx = 1\), so that \(x\) is invertible. This proves that \(A\) is maximal. \(\square\)

**Corollary 6.20.** Let \(A\) be an Artinian ring. Then \(\text{nil}(A) = J(A)\) (recall that \(J(A)\) stands for the Jacobson radical of \(A\)).

**Proof.** This follows from Exercise 4 of §1. \(\square\)

**Exercise 6.21.** Let \(A\) be any ring, \(m_1, m_2\) two distinct maximal ideals of \(A\). Prove that \(m_1 m_2 = m_1 \cap m_2\).

**Theorem 6.22.** Let \(A\) be an Artinian ring. Then \(A\) has finitely many maximal ideals.

**Proof.** Suppose not. Then there is an infinite set \(m_1, m_2, \ldots, m_n, \ldots\) of distinct maximal ideals of \(A\). Consider the descending chain of ideals \(m_1 ⊃ m_1 \cap m_2 ⊃ m_1 \cap m_2 \cap m_3 ⊃ \ldots\). Since \(A\) is Artinian, we must have \(m_1 \cap m_2 \cap \cdots \cap m_n = m_1 \cap \cdots \cap m_n \cap m_{n+1}\) for some \(n\). By Lemma 1.21, \(m_{n+1} = m_i\) for some \(i \leq n\). This is a contradiction and the Theorem is proved. \(\square\)

**Exercise 6.23.** Let \(A\) be a ring and \(I\) a finitely generated ideal, contained in \(\text{nil}(A)\). Show that there exists \(n ∈ \mathbb{N}\) such that \(I^n = (0)\). More generally, show that if \(I\) is any finitely generated ideal, there exists \(n ∈ \mathbb{N}\) such that \((\sqrt{I})^n \subset I\).

**Theorem 6.24.** Let \(A\) be an Artinian ring. Let \(\operatorname{Max}(A) = \{m_1, \ldots, m_s\}\). Then \((m_1 m_2 \cdots m_s)^n = 0\) for some \(n ∈ \mathbb{N}\).

**Proof.** Let \(I = m_1 m_2 \cdots m_s\). By Exercise 6.21, \(I = J(A)\). By Corollary 6.20, \(I = \sqrt{(0)}\). Now, we cannot apply Exercise 6.23, because we have not yet proved that \(I\) is finitely generated.

Consider the descending chain of ideals \(I ⊃ I^2 ⊃ I^3 ⊃ \cdots ⊃ I^n ⊃ \cdots\). Then \(I^n = I^{n+1}\) for some \(n\). We claim that \(I^n = (0)\). Suppose not. Let \(\Sigma\) denote the collection of all the ideals \(H \subset A\), for which \(HI^n \neq 0\). \(\Sigma \neq \emptyset\) since \(I ∈ \Sigma\). Since \(A\) is Artinian, \(\Sigma\) contains a minimal element \(H\) (in the sense of inclusion). Since \(HI^n \neq 0\), there exists \(x ∈ H\) such that \(x I^n \neq 0\). We have \((x) ⊂ H\), hence \((x) = H\) by the minimality of \(H\). Now, \((x I^n)I^n = x I^{2n} = x I^n \neq (0)\) and \(x I^n ⊂ (x)\), hence \(x I^n = (x)\) by the minimality of \(H\). Then there exists \(y ∈ I^n\) such that \(x = xy\). Then

\[(6.7) \quad x = xy = xy^2 = \cdots = xy^l = \cdots\]

Since \(y ∈ I^n ⊂ I = \sqrt{(0)}\), (6.7) implies that \(x = 0\), which is a contradiction. This proves Theorem 6.24. \(\square\)

**Theorem 6.25.** Let \(A\) be a ring. Then \(A\) is Artinian if and only if \(\text{length}(A) < \infty\) (where we view \(A\) as an \(A\)-module).

**Proof.** \(\Leftarrow\) is obvious.
Let $\text{Max}(A) = \{m_1, \ldots, m_s\}$ and let $I = m_1 \ldots m_s = J(A)$. By the previous theorem, $I^n = 0$ for some $n \in \mathbb{N}$. Then there exists $r \geq s$ and maximal ideals $m_1, \ldots, m_r$, not necessarily all distinct, such that $m_1 m_2 \ldots m_r = 0$. Consider the chain $A \supset m_1 \supset m_1 m_2 \supset \ldots \supset m_1 m_2 \ldots m_{r-1} \supset (0)$ of submodules of $A$. By the additivity of length, it is sufficient to show that $\text{length} \left( \frac{m_1 \ldots m_i}{m_1 m_2 \ldots m_i} \right) < \infty$. Now, $\frac{m_1 \ldots m_i}{m_1 m_2 \ldots m_i m_{i+1}}$ is annihilated by $m_{i+1}$, hence it is an $A_{m_{i+1}}$-module, that is, an $A_{m_{i+1}}$-vector space. In a vector space, a submodule is the same thing as a vector subspace, so that a vector space has finite length if and only if it has finite dimension if and only if every descending chain of submodules stabilizes. This last condition holds by the Artinian property of $A$, hence $\text{dim} \frac{A_{m_{i+1}}}{m_1 m_2 \ldots m_i m_{i+1}} < \infty$. This proves that $\text{length}(A)$ is finite, as desired. \hfill $\square$

**Theorem 6.26.** A ring $A$ is Artinian if and only if $A$ is Noetherian and $\text{dim} \ A = 0$.

**Proof.** Suppose $A$ is Artinian. By the previous theorem, $\text{length}(A) < \infty$, hence $A$ is Noetherian. Since every prime ideal in $A$ is maximal, $\text{dim} \ A = 0$.

Conversely, suppose $A$ is Noetherian and $\text{dim} \ A = 0$. Let $(0) = \bigcap_{i=1}^{s} Q_i$ be a primary decomposition of $(0)$. Let $P_i = \sqrt{Q_i}$ be the associated primes. Since $\text{dim} \ A = 0$, each of the $P_i$ is maximal. Moreover, $\sqrt{(0)} = \cap_{i=1}^{s} P_i$, hence by Exercise 6.23 there exists $n$ such that $(P_1 \ldots P_s)^n = 0$.

Now we can use the same reasoning as in the last theorem. We have $A \supset P_1 \supset P_1 P_2 \supset \ldots \supset P_1 P_2 \ldots P_{r-1} \supset (0)$, where $r > s$ and $P_1, \ldots, P_r$ is a sequence consisting of $P_1, \ldots, P_s$ with some repetitions. Since $A$ is Noetherian, $P_1 \ldots P_s$ is a finitely generated ideal, hence $\frac{P_1 \ldots P_s}{P_1 \ldots P_{s+1}}$ is a finite $A$-module, hence a finite $\frac{A}{P_{s+1}}$-module, i.e. a finite dimensional $\frac{A}{P_{s+1}}$-vector space. Now the reasoning in the proof of the last theorem applies, and we conclude that $\text{length}(A) < \infty$, so that $A$ is Artinian. \hfill $\square$

Now, we shall prove a special case of Theorem 6.17.

**Theorem 6.27.** Let $(A, m, k)$ be a Noetherian local ring. Then $\text{dim} \ A = 0$ if and only if $\delta(A) = 0$ if and only if $d(A) = 0$.

**Proof.** $\text{dim} \ A = 0 \iff m$ is the only prime ideal $\iff m = \sqrt{(0)} \iff (0)$ is $m$-primary $\iff \delta(A) = 0 \iff \exists n_0 \in \mathbb{N}$ such that $A = \frac{A}{m^n}, \forall n \geq n_0 \iff H_{A,m}(n) = \text{const.}$ for $n \gg 0 \iff d(A) = 0$. \hfill $\square$

This takes care of the zero dimensional local rings.

Let $(A, m, k)$ be any Noetherian local ring and $Q \subset A$ an $m$-primary ideal. Next, we show that $d(A) \leq \delta(A)$.

**Proposition 6.28.**

1. $\text{length} \frac{A}{Q^m} < \infty$.

2. $\text{length} \frac{A}{Q^m}$ is a polynomial $H_Q(n)$ for $n \gg 0$ of degree at most $s$ where $s$ is the minimal number of generators of $Q$. 

28. INTRODUCTION TO COMMUTATIVE ALGEBRA AND ALGEBRAIC GEOMETRY.
(3) deg $H_Q$ is independent of $Q$ (hence deg $H_Q = d(A) \leq \delta(A)$).

**Proof.** 1) is clear, since $\frac{A}{Q^n}$ is Artinian.

2) Apply Theorem 6.14 to the $\frac{A}{Q}$-algebra $grA = \bigoplus_{n=0}^{\infty} \frac{Q^n}{Q^{n+1}}$, generated over $\frac{A}{Q}$ by $s$ elements. By Theorem 6.14, $\text{length} \frac{Q^n}{Q^{n+1}}$ is a polynomial in $n$ of degree at most $s - 1$. Since $H_Q(n) = \text{length} \left( \frac{A}{Q^{n+1}} \right) = \sum_{i=0}^{n} \text{length} \left( \frac{Q^i}{Q^{i+1}} \right)$, we have deg $H \leq s$, as desired.

3) It is enough to prove that deg $H_Q = \deg H_m$. Since $Q$ is $m$-primary, there exists $r \in \mathbb{N}$ such that $m^r \subset Q \subset m$. Then $m^r \subset Q^n \subset m^n$ for any $n \in \mathbb{N}$, so that $\text{length} \left( \frac{A}{m^r} \right) \geq \text{length} \left( \frac{A}{Q^n} \right) \geq \text{length} \left( \frac{A}{m^n} \right)$.

Since $H_m(rn) \geq H_Q(n) \geq H_m(n)$ for all $n \in \mathbb{N}$ and since both $H_m$ and $H_Q$ are polynomials in $n$, we have deg $H_Q = \deg H_m$. Q.E.D

To complete the proof of Theorem 6.17, it remains to show that $d(A) \geq \dim A \geq \delta(A)$. We now state a crucial lemma, whose proof will be the subject of the next two sections.

**Lemma 6.29.** Let $x \in A$. Assume that $x$ is not a zero divisor. Then $d \left( \frac{A}{(x)} \right) \leq d(A) - 1$.

The rest of this section is devoted to proving Theorem 6.17, assuming Lemma 6.29.

**Proposition 6.30.** $d(A) \geq \dim A$.

**Proof.** Induction on $d(A)$. If $d(A) = 0$, the Proposition follows from Theorem 6.27.

Suppose $d(A) > 0$.

Let $P_0 \not\subseteq P_1 \not\subseteq \cdots \not\subseteq P_r$ be a chain of prime ideals. We want to show $r \leq d(A)$. Let $\tilde{A} = \frac{A}{P_0}$. Take a non-zero element $x \in \frac{P_1}{P_0}$. Since $\tilde{A}$ is a domain, $x$ is not a zero divisor in $\tilde{A}$. By Lemma 6.29, $d \left( \frac{\tilde{A}}{(x)} \right) \leq d(\tilde{A}) - 1 \leq d(A) - 1$. On the other hand, $\frac{P_1 \tilde{A}}{(x)} \not\subseteq \frac{P_2 \tilde{A}}{(x)} \not\subseteq \cdots \not\subseteq \frac{P_r \tilde{A}}{(x)}$ is a chain of distinct prime ideals of $\frac{\tilde{A}}{(x)}$. Hence $\dim \left( \frac{\tilde{A}}{(x)} \right) \geq r - 1$. Using the induction hypothesis, we obtain $r - 1 \leq \dim \left( \frac{\tilde{A}}{(x)} \right) \leq d \left( \frac{\tilde{A}}{(x)} \right) \leq d(A) - 1$ therefore $r \leq d(A)$, as desired. Q.E.D.

**Corollary 6.31.** If $A$ is a Noetherian local ring, then $\dim A < \infty$. In particular, if $P \in \text{Spec} A$, then $\text{ht} P < \infty$.

It remains to show that $\dim A \geq \delta(A)$.

Given any ideal $I \subset A$, define $\text{ht} I = \min \{ \text{ht} P \mid I \subset P, P \in \text{Spec} A \}$. By Corollary 6.31, $\text{ht} I < \infty$ for any ideal $I$ in a Noetherian ring $A$. 

Lemma 6.32. \( \text{dim } A \geq \delta(A) \).

Proof. Let \( d = \text{dim } A \). We will construct, recursively in \( i \), elements \( x_1, \ldots, x_i \in m \) such that \( \text{ht}(x_1, \ldots, x_i) \geq i \). Assume that \( i \leq d \) and that \( x_1, \ldots, x_{i-1} \) with \( \text{ht}(x_1, \ldots, x_{i-1}) \geq i-1 \) are already constructed. If \( \text{ht}(x_1, \ldots, x_{i-1}) \geq d \), then \( m \) is the only minimal prime of \( (x_1, \ldots, x_{i-1}) \), hence \( (x_1, \ldots, x_{i-1}) \) is \( m \)-primary, hence \( \delta(A) \leq i-1 \leq d \) and the Lemma is proved. Thus we may assume that \( \text{ht}(x_1, \ldots, x_{i-1}) < d \). Let \( P_1, \ldots, P_r \) be the minimal primes of \( (x_1, \ldots, x_{i-1}) \). By assumption, \( \text{ht } P_j < d \), \( 1 \leq j \leq r \), so that \( P_j \neq m \), \( 1 \leq j \leq r \). At this point, we need an elementary lemma about unions of prime ideals.

Lemma 6.33. Let \( I, P_1, \ldots, P_r \) be ideals in a ring \( A \), where all except possibly two of the \( P_j \) are prime. If \( I \subset \bigcup_{j=1}^r P_j \), then \( I \subset P_j \) for some \( j \).

We finish the proof of Lemma 6.32 assuming Lemma 6.33. By Lemma 6.33, \( m \neq \bigcup_{j=1}^r P_j \). Take an element \( x_i \in m \setminus \bigcup_{j=1}^r P_j \). We want to show that \( \text{ht}(x_1, \ldots, x_i) \geq i \). Indeed, take any minimal prime \( P \) of \( (x_1, \ldots, x_i) \). Since \( (x_1, \ldots, x_{i-1}) \subset P \), \( P \supset P_j \) for some \( j \), \( 1 \leq j \leq r \). Since \( x_i \in P \setminus P_j \), \( P_j \subsetneq P \). Since \( \text{ht } P_j \geq \text{ht}(x_1, \ldots, x_{i-1}) \geq i-1 \), we have \( \text{ht } P \geq \text{ht } P_j + 1 = i \). We have constructed the desired elements \( (x_1, \ldots, x_i) \). For some \( i \leq d \), we obtain \( \text{ht}(x_1, \ldots, x_i) \geq d \), hence \( (x_1, \ldots, x_i) \) is \( m \)-primary, hence \( d = \text{ht } m \geq \delta(A) \). It remains to prove Lemma 6.33.

Proof of Lemma 6.33. We may assume that \( P_1, \ldots, P_r \) are prime. The proof is by induction on \( r \). First, suppose \( r = 2 \). Suppose that \( I \not\subset P_1 \) and \( I \not\subset P_2 \). Pick elements \( x_1 \in I \setminus P_1 \) and \( x_2 \in I \setminus P_2 \). Then \( x_1 \in P_2 \) and \( x_2 \in P_1 \), so that \( x_1 + x_2 \in I \setminus (P_1 \cup P_2) \), a contradiction.

Next, suppose the result is known for \( r - 1 \), with \( r \geq 3 \). Suppose \( I \not\subset P_j \) for \( 1 \leq j \leq r \). By the induction assumption, we may assume that \( I \) is not contained in the union of any smaller subcollection of the \( P_j \). For each \( j \), pick \( x_j \in I \setminus \bigcup_{i=1}^{r-1} P_i \).

Now consider the element \( x = x_r + \prod_{j=1}^{r-1} x_j \). Clearly, \( x \in I \setminus \bigcup_{j=1}^{r-1} P_i \). On the other hand, since \( x_j \not\in P_r \) for \( j < r \) and \( P_r \) is prime, we have \( x \not\in P_r \). This contradicts the fact that \( I \subset \bigcup_{i=1}^r P_i \). This completes the proof of Lemma 6.33 and with it Lemma 6.32. \( \square \)

Let \( (A, m, k) \) be a Noetherian local ring of dimension \( d \). Let \( x_1, \ldots, x_d \in m \) be such that \( \sqrt{(x_1, \ldots, x_d)} = m \). The elements \( x_1, \ldots, x_d \) are called a system of parameters of \( A \).

To complete the proof of Theorem 6.17, it remains to prove Lemma 6.29. To do so, we need to study filtrations, ideal-adic topologies and the Artin-Rees lemma. This is the content of the next section.

Let \( A \) be a ring, \( I \) an ideal of \( A \), \( M \) an \( A \)-module. The notion of multiplying \( M \) by an ideal is defined in the obvious way. Namely \( IM \) is the submodule of \( M \) given by \( IM = \{ ax \in M \mid a \in I, x \in M \} \).

**Definition 7.1** An *I*-filtration of \( M \) is a chain of submodules \( M = M_0 \supset M_1 \supset \cdots \supset M_n \) such that \( IM_n \subset M_{n+1} \) for all \( n \in \mathbb{N}_0 \).

A filtration is *stable* if \( IM_n = M_{n+1} \) for \( n \gg 0 \). The *I*-adic topology on \( M \) is the topology whose basic open sets are all the sets of the form \( x + IM \), \( x \in M, n \in \mathbb{N} \).

**Example 7.2.** Let \( A = M = \mathbb{Z} \) and let \( I = (p) \), where \( p \) is a prime number. We have the \( p \)-adic filtration and the \( p \)-adic topology on \( \mathbb{Z} \). Clearly this filtration is stable.

**Remark 7.3.** Let \( \{ M_n \} \) and \( \{ M'_n \} \) be two stable filtrations. Then \( \{ M_n \} \) and \( \{ M'_n \} \) have bounded difference, that is, there exists \( n_0 \in \mathbb{N} \) such that \( M'_{n+n_0} \subset M_n \subset M'_{n-n_0} \) for all \( n \gg 0 \) (this is so because there exists \( n_0 \) such that, for all \( n \in \mathbb{N} \), \( M'_{n+n_0} = I^n M'_{n_0} \subset I^n M \subset M_n \) and similarly in the other direction).

**Lemma 7.4 (the Artin-Rees Lemma).** Let \( A \) be a Noetherian ring, \( M' \subset M \) finitely generated \( A \)-modules. Let \( Q \) be an ideal. Let \( \{ M_n \} \) be a stable \( Q \)-filtration of \( M \). Let \( M'_n = M_n \cap M' \). Then \( \{ M'_n \} \) is a stable \( Q \)-filtration of \( M' \).

**Proof.** Consider the graded \( A \)-algebra \( G = \bigoplus_{n=0}^{\infty} Q^n \) and the graded \( G \)-module

\[
M^* = \bigoplus_{n=0}^{\infty} M_n.
\]

**Lemma 7.5.** \( \{ M_n \} \) is stable if and only if \( M^* \) is a finite \( G \)-module.

**Proof.** For each \( n \), let \( M^*_n \) denote the graded \( G \)-module \( M^*_n = M \oplus M_1 \oplus \cdots \oplus M_n \oplus QM_n \oplus Q^2 M_n \oplus \ldots \). We get a chain of submodules

\[
(7.1) \quad M^*_1 \subset M^*_2 \subset \ldots \subset M^*_n \subset \ldots
\]

of \( M^* \).

By Exercise 6.13, each \( M_n \) is a finite \( A \)-module. Hence since \( G \) is Noetherian, \( M^* \) is finitely generated as a \( G \)-module \( \iff \) it is generated by its homogeneous elements of degree less than some fixed number \( \iff (7.1) \) stabilizes \( \iff \) there exists \( n_0 \in \mathbb{N} \) such that \( M_{n+n_0} = Q^n M_{n_0} \) for all \( n \in \mathbb{N} \) \( \iff \) the filtration is stable. \( \square \)

We return to the proof of the Artin–Rees Lemma. We need the following characterization of finite modules over a Noetherian ring, which we leave to the reader as an easy exercise.

**Exercise 7.6.** Let \( A \) be a Noetherian ring, \( M \) an \( A \)-module. Then \( M \) is finite over \( A \) if and only if it is Noetherian, that is, any ascending chain of submodules \( N_1 \subset N_2 \subset \ldots \subset N_k \subset \ldots \) stabilizes. In particular, if \( A \) is Noetherian, \( M \) a finite
A-module and $M' \subset M$ a submodule, then $M'$ is also a finite $A$-module. (Hint: if $M$ is a finite $A$-module then $M$ can be written as a quotient of a direct sum of finitely many copies of $A$.)

It is easily seen that $\{M_n \cap M'\}$ is a $Q$-filtration.

Let $M'^* = \bigoplus_{n=0}^{\infty} M'_n$. We have $M'^* \subset M^*$. Since $M^*$ is a finite $G$-module, by Exercise 7.6 so is $M'^*$. By Lemma 7.5, this implies the Artin-Rees lemma.

**Corollary 7.7.** Let $A$ be a Noetherian ring, $Q \subset A$ an ideal and $M$ a finite $A$-module. Let $M' \subset M$ be a submodule. Then there exists $n_0 \in \mathbb{N}$ such that $(Q^{n+n_0}M) \cap M' = Q^n(Q^{n_0}M \cap M')$ for all $n \in \mathbb{N}_0$.

**Corollary 7.8.** Keep the above notation. Let $\{M'_n\}$ be a stable $Q$-filtration of $M'$. There exists $n_0 \in \mathbb{N}$ such that $(Q^{n+n_0}M) \cap M' \subset M'_n \subset (Q^{n-n_0}M) \cap M'$ for all $n \geq n_0$.

§8. Dimension theory, continued.

We are now in a position to prove Lemma 6.29. First, we prove the following generalization of Proposition 6.28.

**Proposition 8.1.** Let $(A, m)$ be a Noetherian local ring, $Q \subset A$ an $m$-primary ideal. Let $M$ be a finite $A$-module, $\{M_n\}$ a stable $Q$-filtration of $M$. Let $s$ be the minimal number of generators of $Q$. Then:

1. $\text{length} \left( \frac{M}{M_n} \right) < \infty$ for all $n \in \mathbb{N}_0$.
2. $\text{length} \left( \frac{M}{M_n} \right)$ is a polynomial $H_{M,Q}(n)$ for $n \gg 0$, of degree at most $s$.
3. $\deg H_{M,Q}$ depends only on $M$, not on $Q$ and $\{M_n\}$. The highest coefficient of $H_{M,Q}$ depends only on $M$ and $Q$, not on the filtration $\{M_n\}$.

**Proof.** (1) Since $\{M_n\}$ is a $Q$-filtration, $\frac{M_n}{M_{n+1}}$ is an $A$-module. Since $M_n$ is a finite $A$-module, $\frac{M_n}{M_{n+1}}$ is a finite $A$-module. Hence it is a quotient of the direct sum of finitely many copies of $\frac{A}{Q}$. Now the fact that $\text{length} \frac{A}{Q} < \infty$ implies that $\text{length} \frac{M_n}{M_{n+1}} < \infty$ and hence $\text{length} \frac{M}{M_{n+1}} < \infty$.

(2) Follows immediately from Corollary 6.15 of the Hilbert-Serre Theorem, applied to the graded $\frac{A}{Q}$-algebra $G = \bigoplus_{n=0}^{\infty} \frac{Q^n}{Q^{n+1}}$ and the graded $G$-module $\bigoplus_{n=0}^{\infty} \frac{M_n}{M_{n+1}}$.

(3) Take any other stable $Q$-filtration $\{M'_n\}$. There exists $n_0 \in \mathbb{N}$ such that

\[(8.1) \quad M_{n-n_0} \subset M'_n \subset M_{n+n_0} \quad \text{for all } n \in \mathbb{N}.\]

Let $H'_{M,Q}$ denote the Hilbert polynomial associated to $\{M'_n\}$. By (8.1) $H_{M,Q}(n-n_0) \geq H'_{M,Q}(n) \geq H_{M,Q}(n-n_0)$ for all $n \in \mathbb{N}$, hence $H_{M,Q}$ and $H'_{M,Q}$ have the same degree and highest coefficient. To show that, in addition, $\deg H_{M,Q}$ is independent
of \(Q\), compare \(\deg H_{M,Q}\) with \(\deg H_{M,m}\). Since the degree is independent of the choice of the filtration, we may take the filtrations to be \(Q^n M\) and \(m^n M\), respectively. Since \(Q\) is \(m\)-primary, there exists \(r \in \mathbb{N}\) such that \(m^r \subset Q \subset m\) (Exercise 6.23). Then \(m^r n \subset Q^n \subset m^n\) for any \(n \in \mathbb{N}\). Hence \(H_{M,m}(rn) \geq H_{M,Q}(n) \geq H_{M,m}(n)\) for all \(n \in \mathbb{N}\). This proves that \(\deg H_{M,Q} = \deg H_{M,m}\), as desired. QED

**Notation.** The common degree of the polynomials \(H_{M,Q}\) will be denoted by \(d(M)\).

We now prove Lemma 6.29 in the following stronger form.

**Lemma 8.2.** Let \((A,m)\), \(M\) be as above. Let \(x \in m\). Assume that \(x\) is not a zero divisor for \(M\), that is, \(xa \neq 0\) for any \(a \in M \setminus \{0\}\). Then \(d(MxM) \leq d(M) - 1\).

**Proof.** Let \(N = xM\), \(M' = \frac{M}{N}\). Then \(N \cong M\) since \(x\) is not a zero divisor. Let \(N_n = m^n M \cap N\). We have an exact sequence \(0 \to N \to M \to M' \to 0\), which induces an exact sequence

\[
0 \to \frac{N}{N_n} \to \frac{M}{m^n M} \to \frac{M'}{m^n M'} \to 0.
\]

for each \(n \in \mathbb{N}\). By additivity of length, (8.2) gives

\[
H_{N,m}(n) - H_{M,m}(n) + H_{M',m}(n) = 0.
\]

By the Artin–Rees Lemma, \(\{N_n\}\) is stable. By Proposition 8.1, \(H_{N,m}\) and \(H_{M,m}\) have the same degree and highest coefficient, hence, by (8.3),

\[
\deg H_{M',m} < \deg H_{M,m}.
\]

This proves that \(d(M') \leq d(M) - 1\). QED

This completes the proof of the Dimension Theorem 6.17.

**Exercise 8.3.** Let \(G = \bigoplus_{n=0}^{\infty} G_n\) be a Noetherian graded \(G_0\)-algebra, with \(G_0\) Artinian. Let \(M = \bigoplus_{n=0}^{\infty} M_n\) be a finite graded \(G\)-module and let \(d(M)\) denote the degree of the Hilbert polynomial

\[
H(n) = \sum_{i=0}^{n} \text{length}(M_i)
\]

for \(n \gg 0\). Let \(x \in G_s\) be a homogeneous element of degree \(s\), which is not a zero divisor in \(M\). Show that \(d(\frac{M}{(x)M}) \leq d(M) - 1\).

Now we can relax and derive several important corollaries from Theorem 6.17.
Corollary 8.4. Let \((A, m, k)\) be a Noetherian local ring. Then \(\dim A \leq \dim_k \frac{m}{m^2}\).

Proof. Let \(x_1, \ldots, x_s\) be elements of \(m\) whose images in \(\frac{m}{m^2}\) generate \(\frac{m}{m^2}\). Then

\[
(8.4) \quad m = (x_1, \ldots, x_s) + m^2.
\]

We now invoke one of the most famous lemmas in all of commutative algebra—the Lemma of Nakayama—to conclude that (8.4) implies \(m = (x_1, \ldots, x_s)\). This will show that \(\dim A = \delta(A) \leq s\), as desired.

It remains to state and prove Nakayama’s Lemma.

Lemma 8.5 (Nakayama’s Lemma). Let \(A\) be a ring, \(I\) an ideal of \(A\), \(M\) an \(A\)-module, \(N \subseteq M\) a submodule. Assume either that \(M\) is finite or that \(I\) is nilpotent (that is, \(I^n = (0)\) for some \(n \in \mathbb{N}\)). Suppose that \(M = IM + N\). Then there exists \(x \in I\) such that \((1 + x)M = N\). If, in addition, \(I \subset J(A)\), then \(M = N\).

Applied to (8.4) with \(I = M = m\), \((x_1, \ldots, x_s) = N\), Nakayama’s Lemma implies that \(m = (x_1, \ldots, x_s)\).

Proof of Nakayama’s Lemma. If \(I\) is nilpotent, we have \(I^n = (0)\) for some \(n \in \mathbb{N}\). Substituting \(IM\) for \(M\) recursively in the expressions \(I^iM + N\), we obtain \(M = IM + N = I^2M + N = \cdots = I^nM + N = N\), and the Lemma is true in this case.

Next, suppose \(M\) is finite over \(A\). Let \(w_1, \ldots, w_n\) be the generators of \(M\). Replacing \(M\) by \(\frac{M}{N}\), we may assume that \(N = (0)\). Then \(M = IM\), hence \(w_1, \ldots, w_n \in IM\).

Then there exist \(a_{ij} \in I, 1 \leq i, j \leq n\), such that

\[
\begin{align*}
w_1 &= a_{11}w_1 + a_{12}w_2 + \cdots + a_{1n}w_n \\
w_2 &= a_{21}w_1 + a_{22}w_2 + \cdots + a_{2n}w_n \\
&\vdots \\
w_n &= a_{n1}w_1 + a_{n2}w_2 + \cdots + a_{nn}w_n
\end{align*}
\]

(8.5)

Let

\[
T = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
& \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}.
\]

By (8.5),

\[
\begin{pmatrix}
w_1 \\
w_2 \\
& \vdots \\
w_n
\end{pmatrix} = \begin{pmatrix}
a_{11}w_1 & a_{12}w_2 & \cdots & a_{1n}w_n \\
a_{21}w_1 & a_{22}w_2 & \cdots & a_{2n}w_n \\
& \vdots & \ddots & \vdots \\
a_{n1}w_1 & a_{n2}w_2 & \cdots & a_{nn}w_n
\end{pmatrix} \begin{pmatrix}
0 \\
0 \\
& \vdots \\
0
\end{pmatrix}.
\]

(8.6)
Let $1_n$ denote the $n \times n$ identity matrix. (8.6) says $(1_n - T) \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Since

$$\det(1_n - T)1_n = \text{adj}(1_n - T)(1_n - T),$$

we have $\det(1_n - T)w_i = 0$, $i = 1, 2, \ldots, n$.

Since all the $a_{ij} \in I$, $\det(1_n - T) = 1 + x$ for some $x \in I$. We have

$$(8.7) \quad (1 + x)w_i = 0, \quad 1 \leq i \leq n.$$ 

Since $M = \sum_{i=1}^n Aw_i$, (8.7) implies $(1 + x)M = (0)$. If, in addition, $x \in J(A)$, then $1 + x$ is not in any maximal ideal of $A$, hence $1 + x$ is invertible. Then $M = (0)$, as desired. □

$\dim_k \frac{m}{m^2}$ is called the embedding dimension, $\frac{m}{m^2}$ is called the Zariski cotangent space of $A$. Its dual $\text{Hom}_k \left( \frac{m}{m^2}, k \right)$ is called the Zariski tangent space.

We continue with Corollaries of Theorem 6.17.

**Corollary 8.6.** Let $A$ be a Noetherian ring and let $x_1, \ldots, x_r$ be elements of $A$, such that $(x_1, \ldots, x_r) \neq A$ (in other words, there exists $m \in \text{Max}(A)$, containing all the $x_i$). Then for any minimal prime $P$ of $(x_1, \ldots, x_r)$, we have $\text{ht} P \leq r$ (in particular, $\text{ht}(x_1, \ldots, x_r) \leq r$).

**Proof.** Let $P$ be any minimal prime of $(x_1, \ldots, x_r)$.

**Exercise 8.7.** Let $I$ be an ideal in a Noetherian ring $A$, $P$ a minimal prime of $I$. Show that $\sqrt{IA_P} = PA_P$.

By Exercise 8.7, $\sqrt{(x_1, \ldots, x_r)A_P} = PA_P$, hence $\text{ht} P \equiv \dim A_P = \delta(A_P) \leq r$.

**Theorem 8.8 (Krull’s Principal Ideal Theorem).** Let $A$ be a Noetherian ring, $x$ an element of $A$, which is neither a unit nor a zero divisor. Then every minimal prime ideal of $(x)$ has height 1.

**Proof.** Let $P$ be a minimal prime of $(x)$. By Corollary 8.6, $\text{ht} P \leq 1$. It remains to show that $\text{ht} P \neq 0$. Indeed, suppose $\text{ht} P = 0$. Then $P$ is a minimal prime of $A$. By Theorem 5.14, every element of $P$ is a zero divisor, which contradicts the fact that $x \in P$.

**Exercise 8.9.** Let $A$ be a ring, $S \subset A$ a multiplicative set and $P$ a prime ideal such that $P \cap S = \emptyset$. Show that $\text{ht} P = \text{ht}(PA_S)$.

**Exercise 8.10.** For any $n \in \mathbb{N}$, give an example of a Noetherian local ring $A$ and $x \in A$ which is not a zero divisor, such that $(x)$ has an associated prime of height $n$.

Let $(A, m)$ be a Noetherian local ring, $x$ an element of $m$ which is not a zero divisor. From Lemma 6.29 and the Dimension Theorem we know that

$$(8.8) \quad \dim \frac{A}{(x)} \leq \dim A - 1.$$ 

The next Corollary says that the inequality is, in fact, an equality.
Corollary 8.11. In this situation, we have \( \dim \frac{A}{(x)} = \dim A - 1 \).

Proof. Let \( d' = \dim \frac{A}{(x)} = \delta \left( \frac{A}{(x)} \right) \). Let \( x_1, \ldots, x_{d'} \) be elements of \( A \) whose images in \( \frac{A}{(x)} \) generate an \( \frac{m}{(x)} \)-primary ideal. Then \( x_1, \ldots, x_{d'}, x \) generate an \( m \)-primary ideal in \( A \). Then \( \dim A = \delta(A) \leq d' + 1 = \dim \frac{A}{(x)} + 1 \), which proves the opposite inequality of (8.8). Hence the Corollary is proved.

§9. Dimension and transcendence degree in finitely generated algebras over a field.

Notation. If \( P \in \text{Spec} A \) for a ring \( A \), let \( \kappa(P) = \frac{A_P}{P_A} \) denote the residue field of the local ring \( A_P \).

Let \( k \) be a field and \( A \) a finitely generated \( k \)-algebra. If \( x_1, \ldots, x_n \) are the generators of \( A \) over \( k \), we can be written as the quotient of the polynomial ring \( k[x_1, \ldots, x_n] \) by an ideal \( I \subset k[x_1, \ldots, x_n] \); that is, \( A = \frac{k[x_1, \ldots, x_n]}{I} \).

Theorem 9.1.

1. \( \dim A = \text{tr.deg}(A/k) \).
2. If \( P \in \text{Spec} A \) and \( K \) is the field of rational functions of some irreducible component of \( \text{Spec} A \) containing \( P \) (in other words, \( K = \kappa(P_0) \) for some minimal prime \( P_0 \) of \( A \), contained in \( P \)), we have \( \dim \frac{A_P}{P_0A_P} + \text{tr.deg}(\kappa(P)/k) = \text{tr.deg}(K/k) \).

Proof. By the following exercise, we may assume that \( A \) is a domain in (1):

Exercise 9.2. Let \( A \) be a finitely generated \( k \)-algebra and \( P_1, \ldots, P_r \) the minimal primes of \( A \). Show that

1. \( \dim A = \max_{1 \leq i \leq r} \{ \dim \frac{A}{P_i} \} \)
2. \( \text{tr.deg}(A/k) = \max_{1 \leq i \leq r} \{ \text{tr.deg}(\frac{A}{P_i}/k) \} \).

In (2) of Theorem 9.1, we may replace \( A \) by \( A_{P_0} \). From now on, we will assume that \( A \) is a domain.

Let \( d = \dim A \) and let \( (0) \not\subset P_1 \not\subset \cdots \not\subset P_d \) be a maximal chain of prime ideals. Then \( \dim A_{P_d} = d \). Moreover, \( P_d \) is maximal, hence by Proposition 4.2, \( \text{tr.deg}(\frac{A_{P_d}}{k}) = 0 \). Since \( \text{tr.deg}(A/k) \) is obviously unaffected by localization (here we are using the fact that \( A \) is a domain), we have (2) \(\implies\) (1) in Theorem 9.1.

It remains to prove (2). Let \( P \in \text{Spec} A \). Let \( t = \text{tr.deg} \left( \frac{A_P}{P_A}/k \right) \). Replacing the \( x_i \), we may assume that the images of \( x_1, \ldots, x_t \) in \( A \) form a transcendence base of \( \frac{A_P}{P_A} \) over \( k \). Let \( L = k(x_1, \ldots, x_t) \) (this is where we are using the fact that \( A \) is a domain: the natural map \( A \to A_P \) is injective). We have a natural map \( \phi : L[x_{t+1}, \ldots, x_n] \to A_P \); by definition, \( A_P = L[x_{t+1}, \ldots, x_n]_{\phi^{-1}(P)} \). Let \( K \) be the field of fractions of \( A \). Since transcendence degree is additive in field extensions, we have \( \text{tr.deg}(A/k) = \)
tr. deg(\(A_P/k\)) = tr. deg(K/k) = t + tr. deg(K/L). Therefore we may replace \(k\) by 
\(L\) and \(A\) by \(L[x_{t+1}, \ldots, x_n]\). In other words, we may assume that \(P\) is maximal and 
\(t = 0\). It remains to prove that under these assumptions, \(\dim A_P = \text{tr. deg}(A/k)\).

**Lemma 9.3.** Let \((A, m, k)\) be a Noetherian local ring of dimension \(d\). Let \(x_1, \ldots, x_d\) be a system of parameters of \(A\) and let \(Q = (x_1, \ldots, x_d)\). Let \(f \in A[t_1, \ldots, t_d]\) be a homogeneous polynomial of degree \(s\) in \(d\) variables \(t_1, \ldots, t_d\). If \(f(x_1, \ldots, x_d) \in Q^{s+1}\), then \(f \in mA[t_1, \ldots, t_d]\).

**Proof.** Let \(\bar{f}\) denote the natural image of \(f\) in \(\frac{A}{Q}[t_1, \ldots, t_d]\). Consider the map

\[
\alpha : \frac{A}{Q}[t_1, \ldots, t_d] \to \bigoplus_{i=0}^{\infty} \frac{Q^i}{Q^{i+1}},
\]

defined by \(\alpha(t_i) = x_i, 1 \leq i \leq d\). By Proposition 6.28, \(d \left( \bigoplus_{i=0}^{\infty} \frac{Q^i}{Q^{i+1}} \right) = \dim A = d\).

Also \(\text{length} \left( \frac{(t_1, \ldots, t_d)^s}{(t_1, \ldots, t_d)^{s+1}} \right) = \text{length} \left( \frac{A}{Q} \right) \cdot \left( \frac{d+s-1}{d-1} \right)\), so that \(d \left( \frac{A}{Q}[t_1, \ldots, t_d] \right) = d\).

By assumption, \(f \in \ker \alpha\). Since both algebras in (9.1) have the same degree of Hilbert polynomial, by Exercise 8.3 \(\bar{f}\) is a zero divisor in \(\frac{A}{Q}[t_1, \ldots, t_n]\). We leave it as an Exercise to finish the proof:

**Exercise 9.4.** Show that \((0)\) is a primary ideal in \(\frac{A}{Q}[t_1, \ldots, t_d]\) and that

\[m \frac{A}{Q}[t_1, \ldots, t_d] = \text{nil} \left( \frac{A}{Q}[t_1, \ldots, t_d] \right)\]

is the only associated prime of \(\frac{A}{Q}[t_1, \ldots, t_d]\). In particular, every zero divisor in \(\frac{A}{Q}[t_1, \ldots, t_d]\) belongs to \(m \frac{A}{Q}[t_1, \ldots, t_d]\).

Q.E.D.

**Corollary 9.5.** Let \((A, m)\) be a Noetherian local ring of dimension \(d\), \(x_1, \ldots, x_d\) a system of parameters of \(A\). Suppose \(A\) contains a field \(k_0\). Then \(x_1, \ldots, x_d\) are algebraically independent over \(k_0\).

**Proof.** Let \(f(x_1, \ldots, x_d) = 0\) be an algebraic relation among the \(x_i\) over \(k_0\). Write \(f = f_s + f_{s+1} + \cdots + f_t\) where each \(f_i\) is homogeneous of degree \(i\). Then \(f_s(x_1, \ldots, x_d) \in Q^{s+1}\), hence by Lemma 9.3 \(f \in mA[t_1, \ldots, t_d]\), which implies \(f \equiv 0\) since \(f\) is a polynomial with coefficients in \(k_0\).

Corollary 9.5 proves that \(\dim A_P \leq \text{tr. deg}(A/k)\). For the opposite inequality, we need the Noether Normalization Lemma.

**Lemma 9.6 (Noether Normalization Lemma).** Let \(k\) be a field and \(A = k[x_1, \ldots, x_n]\) a finitely generated \(k\)-algebra. Then there exist \(y_1, y_2, \ldots, y_d \in A\), algebraically independent over \(k\), such that \(A\) is integral over \(k[y_1, \ldots, y_d]\).

**Proof.** We may assume that \(x_1, \ldots, x_d\) are algebraically independent over \(k\) and \(x_{d+1}, \ldots, x_n\) are algebraic over \(k[x_1, \ldots, x_d]\). We will prove, by induction on \(i\),
that there exists a choice of generators $x_j$ such that $x_{d+1}, \ldots, x_i$ are integral over $k[x_1, \ldots, x_d]$. Suppose this is known for $i, d \leq i < n$. We must prove the same statement for $i + 1$. We will make a change of variables of the form

$$\tilde{x}_j = x_j + x_{i+1}^{\lambda_j},$$

$1 \leq j \leq d$. By assumptions, there is an algebraic dependence relation

$$F(x_{i+1}) = a_0 x_{i+1}^l + a_1 x_{i+1}^{l-1} + \cdots + a_l = 0,$$

$a_j \in k[x_1, \ldots, x_d]$. It is enough to find $\lambda_j \in \mathbb{N}, 1 \leq j \leq d$, such that after the substitution (9.2), (9.3) becomes an integral equation for $x_{i+1}$ over $k[\tilde{x}_1, \ldots, \tilde{x}_d]$. Then $x_{i+1}$ will be integral over $k[\tilde{x}_1, \ldots, \tilde{x}_d]$ and $x_{d+1}, \ldots, x_i$ over $k[\tilde{x}_1, \ldots, \tilde{x}_d, x_{i+1}]$, hence also over $k[\tilde{x}_1, \ldots, \tilde{x}_d]$.

Let $\bar{x} = (x_1, \ldots, x_d)$, $\bar{x}^\alpha = x_1^{\alpha_1} \ldots x_d^{\alpha_d}$. Write

$$F(x_{i+1}) = \sum_{\alpha j} a_\alpha \bar{x}^\alpha x_{i+1}^j.$$

Choose $\lambda_1 \gg \lambda_2 \gg \cdots \gg \lambda_d \gg 2$ such that $\sum_{s=1}^d \alpha_s \lambda_s + j \neq \sum_{s=1}^d \alpha'_s \lambda_s + j'$ for any two monomials $\bar{x}^\alpha x_{i+1}^j \neq \bar{x}^\alpha' x_{i+1}^{j'}$ appearing in (9.4) with non-zero coefficients (the existence of such $\lambda_j$ is easy to see by induction on $d$).

Substituting (9.2) into (9.3), the coefficient of the highest order term in $x_{i+1}$ is a non-zero element of $k$ by the choice of $\lambda_j$. Hence after the substitution (9.2), (9.3) becomes an integral dependence relation of $x_{i+1}$ over $k[\tilde{x}_1, \ldots, \tilde{x}_d]$, as desired.

By induction in $i$, we find a choice of generators $x_i$ such that $k[x_1, \ldots, x_n]$ is integral over $k[x_1, \ldots, x_d]$. QED

**Remark 9.7.** If $k$ is infinite, we can achieve the same result by a transformation of the form $\tilde{x}_j = x_j + c_j x_{i+1}$, $1 \leq j \leq d$, where $c_j$ are sufficiently general constants in $k$.

It is also worth mentioning that the analogue of Noether normalization for formal or convergent power series ring is stronger. Namely, we have

**Theorem 9.8.** Let $(A, m, k)$ be a formal (resp. convergent) power series ring over $k$ (resp. $\mathbb{C}$). Let $y_1, \ldots, y_d$ be a system of parameters of $A$. Then $A$ is finitely generated as a module over $k[[y_1, \ldots, y_d]]$ (resp. $\mathbb{C}\{y_1, \ldots, y_d\}$) (it is easy to see that there are no formal or convergent relations among the $y_i$, that is, no formal or convergent power series in the $y_i$ is equal to 0 in $A$).

Thus in the formal and convergent cases it is much easier to choose $y_1, \ldots, y_d$: any system of parameters will do.

Theorem 9.8 can be proved rather easily using the Weierstrass preparation theorem, but we will not do it here (see [4, Chapter V, (31.6) and Chapter VII, (45.3) and (45.5)]).
Let $A, y_1, \ldots, y_d$ be as in Noether Normalization Lemma. Clearly,

$$d = \text{tr. deg}(A/k).$$

To prove Theorem 9.1, it remains to prove that $\dim A_m = d$ for every $m \in \text{Max}(A)$. It is a little easier to prove that $\dim A_m = d$ for some $m \in \text{Max}(A)$; this is already enough for Theorem 9.1 (1). We prove this weaker result first in order to warm up.

The plan is to show that $\dim k[y_1, \ldots, y_d] = d$ and then analyze the behaviour of dimension under integral extensions and show that it is preserved by such extensions.

**Lemma 9.9.** Let $m \in \text{Max}(k[y_1, \ldots, y_d])$. Then $\text{ht} m = d$. In particular,

$$\dim k[y_1, \ldots, y_d] = d.$$

**Proof.** Take any $m \in \text{Max}(k[y_1, \ldots, y_d])$ and let $k' = \kappa(m) = k[y_1, \ldots, y_d]$. By Proposition 4.2, $k'$ is a finite algebraic extension of $k$. Let $\bar{y}_i = y_i \mod m$ be the natural image of $y_i$ in $k'$; then $k'$ is generated by $\bar{y}_1, \ldots, \bar{y}_d$ as a $k$-algebra. For $1 \leq i \leq d$, let $f_i$ denote the minimal polynomial of $\bar{y}_i$ over the field $k[\bar{y}_1, \ldots, \bar{y}_{i-1}]$. For each $i$, pick and fix a polynomial $f_i \in k[y_1, \ldots, y_i]$ whose natural image in $k[\bar{y}_1, \ldots, \bar{y}_{i-1}, \bar{y}_i]$ is $\bar{f}_i$. Then, by induction on $i$, $k' = \frac{k[y_1, \ldots, y_d]}{(f_1, \ldots, f_d)}$. Hence $m = (f_1, \ldots, f_d)$; in particular, $\dim A_m = d(m) \leq d$. On the other hand, let $P_i \subset k[y_1, \ldots, y_i]$ denote the kernel of the natural map $k[y_1, \ldots, y_i] \to k[\bar{y}_1, \ldots, \bar{y}_i]$. It is easy to see that $(0) \subset P_1 k[y_1, \ldots, y_d] \subset \cdots \subset P_d = m$ is a chain of $d$ distinct prime ideals, so that $\dim A_m = d$. □

To complete the proof of Theorem 9.1, it remains to analyze the behaviour of dimension in integral ring extensions.

**Proposition 9.10.** Let $A \subset B$ be an integral ring extension. Then $\dim A = \dim B$.

**Lemma 9.11.** Let $A \subset B$ be an integral ring extension and $P \in \text{Spec} A$, $Q \in \text{Spec} B$ such that $Q \cap A = P$. Then $P$ is maximal if and only if $Q$ is maximal.

**Proof.** $A/P \hookrightarrow B/Q$ is an integral extension of integral domains. Thus we can further reduce Lemma 9.11 to

**Lemma 9.12.** Let $A \subset B$ be an integral extension of integral domains. Then $A$ is a field if and only if $B$ is a field.

**Proof.** $\implies$ is proved by the same argument as $\implies$ in Proposition 4.2.

($\impliedby$) Assume that $B$ is a field. Let $x \in A$. Then $\frac{1}{x} \in B$. Since $B$ is a domain, integral over $A$, $\frac{1}{x}$ satisfies an integral dependence relation $x^{-m} + b_1x^{-m+1} + \cdots + b_m = 0$, where $b_i \in A$. Then $\frac{1}{x} = -b_1 - b_2x - \cdots - b_mx^{m-1} \in A$, which proves that $A$ is a field. QED

**Corollary 9.13.** Let $A \subset B$ be an integral ring extension, $P \in \text{Spec} A$. Then

1. There exists $Q \in \text{Spec} B$ such that $Q \cap A = P$
2. There are no inclusion relations between primes $Q \subset B$, satisfying (1).
Proof. (1) Localize both $A$ and $B$ by the multiplicative set $S = A \setminus P$. Then $A_P \hookrightarrow B_S$, is an integral ring extension. Let $Q$ be any maximal ideal of $B$. Then $Q \cap A_P$ must be maximal by Lemma 9.11, hence $Q \cap A_P = PA_P$.

Then $Q \cap B$ lies over $P$: $(Q \cap B) \cap A = Q \cap A = (Q \cap A_P) \cap A = PA_P \cap A = P$. 

2) Suppose $Q_1 \subset Q_2$ are two primes of $B$ such that $Q_1 \cap A = Q_2 \cap A = P$. Then $Q_1B_S$ and $Q_2B_S$ are both maximal in $B_S$ which contradicts the fact that $Q_1 \not\subset Q_2$.

Corollary 9.14 (The going up theorem). Let $A \subset B$ be an integral extension of integral domains. Let $P \subset P' \subset A$ be prime ideals. Let $Q \subset B$ be a prime ideal such that $Q \cap A = P$. Then there exists a prime $Q'$ of $B$, such that $Q \subseteq Q'$ and $P' = Q' \cap A$.

Proof. Apply Corollary 9.13 (1) to the extension $\frac{A}{P} \hookrightarrow \frac{B}{Q}$ and the ideal $\frac{P'}{P'}$. There exists $Q'' \in \text{Spec} \frac{B}{Q}$ such that $Q'' \cap \frac{A}{P} = \frac{P'}{P'}$. Put $Q' = Q'' \cap B$.

Proof of Proposition 9.10. Let $A \subset B$ be an integral ring extension. Let $Q_0 \subset \cdots \subset Q_n$ be a chain of prime ideals of $B$. By Corollary 9.13 (2), $Q_0 \cap A \subset \cdots \subset Q_n \cap A$ is a chain of distinct prime ideals of $A$. This proves that $\dim B \leq \dim A$. Conversely, let $P_0 \subset \cdots \subset P_n$ be a chain of prime ideals of $A$. By Corollary 9.13 (1), there exists $Q_0 \in \text{Spec} B$ lying over $P_0$. By the going up theorem and induction on $i$, we can successively construct a chain of prime ideals $Q_0 \subset \cdots \subset Q_n$ of $B$ such that $Q_i \cap A = P_i$. This proves that $\dim A \leq \dim B$, so that $\dim B = \dim A$. □

We come back to the proof of Theorem 9.1. We have an integral domain $A$ of finite type over $k$. By Noether Normalization Lemma, there exist $y_1, \ldots, y_d$, algebraically independent over $k$, such that $A$ is finite over $k[y_1, \ldots, y_d]$. By Lemma 9.9 and Proposition 9.10, $\dim A = \dim k[y_1, \ldots, y_d] = d$. In other words, the largest height of a maximal ideal in $A$ is $d$. This proves (1) of Theorem 9.1. To prove (2) of Theorem 9.1, we need a stronger result: every maximal ideal in $A$ has height exactly $d$. The existence of a maximal ideal of height $d$ was proved by starting with a maximal chain of primes in $k[y_1, \ldots, y_d]$ and constructing a chain of primes in $A$ lying above it recursively, using the going up theorem at each step. Now, we would like to start with a fixed maximal ideal $m$ of $A$. Since $m \cap k[y_1, \ldots, y_d]$ is maximal by Lemma 9.11, we can consider a chain of $d$ primes $(0) \subset P_1 \subset \cdots \subset P_d = m \cap k[y_1, \ldots, y_d]$ in $k[y_1, \ldots, y_d]$. To imitate the procedure in the proof of Proposition 9.10 and construct a chain of primes in $A$ lying over the $P_i$, we now need a going down theorem. The fact that the going down theorem holds in our context is a somewhat more delicate result; it depends not only on the fact that $A$ is integral over $k[y_1, \ldots, y_d]$ but also on the fact that $k[y_1, \ldots, y_d]$ is normal. Thus to complete the proof of Theorem 9.1, it remains to prove two things:

Proposition 9.15 (The going down theorem). Let $\phi : A \hookrightarrow B$ be an integral extension of integral domains, such that $A$ is normal. Let $P, P' \in \text{Spec} A$, $Q' \in \text{Spec} B$ be such that $P \subset P'$ and $P' = Q' \cap A$. Then there exists $Q \in \text{Spec} B$ such that $Q \subset Q'$ and $P = Q \cap A$. 

Lemma 9.16. \( k[y_1, \ldots, y_d] \) is normal.

Once the going down theorem and the normality of \( k[y_1, \ldots, y_d] \) are established, Theorem 9.2 (2) will follow from the following result, proved by imitating the proof of Proposition 9.10.

Exercise 9.17. Let \( A \subset B \) be a ring extension. Let \( Q \in \text{Spec } A, P = Q \cap A \). Show that:

1. If \( A \subset B \) has the going down property, then \( \text{ht } Q \geq \text{ht } P \).
2. If for any prime \( P' \subset P \), there are no inclusion relations among the primes of \( B \) contracting to \( P' \), then \( \text{ht } Q \leq \text{ht } P \).

Proof of the going down theorem. Let \( K \) and \( L \) denote, respectively, the fields of fractions of \( A \) and \( B \). Replacing \( B \) by its integral closure in \( L \) and \( Q' \) by a prime ideal of the integral closure lying over \( Q' \) does not change the problem. Furthermore, we may replace \( L \) by a normal extension of \( K \) and \( B \) by the integral closure of \( A \) in \( L \). Thus we will assume that \( L \) is a normal extension of \( K \) and \( B \) is integrally closed in \( L \) (in particular, any automorphism of \( L \) over \( K \) maps \( B \) to itself).

By Corollary 9.13 (1), there exists \( Q' \in \text{Spec } B \) such that \( Q' \cap A = P \). By the going up theorem there exists a prime \( Q' \cap Q \) in \( B \) such that \( Q' \cap A = P' \). Hence to prove the going down theorem, it is sufficient to prove the following lemma.

Lemma 9.18. Let \( A, B, K \) and \( L \) be as in Proposition 9.15. Assume that \( L \) is a normal extension of \( K \) and that \( B \) is integrally closed in \( L \). Let \( P \in \text{Spec } A, Q_1, Q_2 \in \text{Spec } B \) be such that \( Q_1 \cap A = Q_2 \cap A = P \). Then there exists an automorphism \( \sigma \) of \( L \) over \( K \) such that \( \sigma(Q_1) = Q_2 \).

By Lemma 9.18 there exists an automorphism \( \sigma \) such that \( \sigma(Q') = Q' \). Then \( Q = \sigma(Q') \) is the desired prime ideal. It remains to prove Lemma 9.18 (note that for Theorem 9.1 we only need it in the case when \( L \) is finite over \( K \)).

Proof of Lemma 9.18. First, assume that \( L \) is finite over \( K \), so that the group \( G \) of automorphisms is finite: \( G = \{ \sigma_1, \ldots, \sigma_s \} \). Suppose \( Q_2 \neq \sigma_i(Q_1) \) for any \( i \). Since \( Q_1 \neq \sigma_i(Q_2) \) for any \( i, \), \( Q_1 \not\subset \bigcup_{i=1}^{s} \sigma_i(Q_2) \) by Lemma 6.33. Take \( x \in Q_1 \setminus \bigcup_{i=1}^{s} \sigma_i(Q_2) \). Then \( \sigma_i(x) \notin Q_2 \) for any \( i \), hence

\[
(9.5) \quad y = \prod_{i=1}^{s} \sigma_i(x) \notin Q_2.
\]

But \( y \) is invariant under all the automorphisms of \( L \) over \( K \), hence there is \( r \in \mathbb{N} \) such that \( y^r \in K \). Since \( y \) is integral over \( A \), we have \( y^r \in A \). Then \( y \in A \cap Q_1 = P \subset Q_2 \), which contradicts (9.5). This proves Lemma 9.18 in case \( L \) is finite over \( K \).

Next, suppose \( L \) is not finite over \( K \). Let \( K' \) denote the maximal purely inseparable extension of \( K \) contained in \( L \) (\( K' \) is nothing but the invariant field of the group \( G \) of automorphisms). Then \( L \) is Galois over \( K' \). Let \( A' \) denote the integral closure of \( A \) in \( K' \).
**Exercise 9.19.** Show that the natural map \( \text{Spec } A' \rightarrow \text{Spec } A \) is a bijection.

By Exercise 9.19, we may replace \( A \) by \( A' \) and \( K \) by \( K' \); that is, we may assume that \( L \) is Galois over \( K \). Let \( L' \) be a finite Galois extension of \( K \) contained in \( L \), and let

\[
F(L') = \{ \sigma \in G \mid \sigma(Q_1 \cap L') = Q_2 \cap L' \}.
\]

Since \( K \subset L' \) is a finite field extension, Lemma 9.18 holds with \( B \) replaced by the integral closure of \( A \) in \( L' \). Hence \( F(L') \) is not empty.

The Krull topology on \( G \) is defined to be the topology whose basis consists of all the cosets of the form \( \sigma H \), where \( \sigma \in G \) and \( H \) is a normal subgroup of \( G \) of finite index.

**Exercise 9.20.** Show that \( F(L') \) is closed in the Krull topology.

Now, the set of finite groups which are homomorphic images of \( G \) form a projective system, whose maps are the natural surjective homomorphisms: whenever \( H_i \subset H_j \) are two normal subgroups of finite index, we have a natural surjective map \( \frac{G}{H_i} \rightarrow \frac{G}{H_j} \). Since an automorphism \( \sigma \in G \) is completely determined by the collection of all of its restrictions to finite subextensions \( K \subset L' \) of \( K \) contained in \( L \), we have \( G = \lim \frac{G}{H} \). Moreover, the Krull topology on \( G \) is, by definition, nothing but the inverse limit of the discrete topologies on \( \frac{G}{H} \) (that is, it is the topology whose basis is formed by all the inverse limits of all the sets in \( \frac{G}{H} \) or, equivalently, the coarsest topology which makes all the natural maps \( G \rightarrow \frac{G}{H} \) of Exercise 3.12 continuous).

Since we are considering only normal subgroups of finite index, \( \frac{G}{H} \) is finite, so that the discrete topology on \( \frac{G}{H} \) is compact and Hausdorff.

Now, the inverse limit of compact Hausdorff spaces \( X_i \) is compact. Indeed, by definition \( \lim \frac{G}{H} \subset \prod_i X_i \). \( \prod_i X_i \) is compact by Tychonoff’s theorem and one checks easily that \( \lim \frac{G}{H} \) is closed in \( \prod_i X_i \) using the Hausdorff property of the \( X_i \).

Hence \( G \) is compact in the Krull topology. Now, any finite collection of finite Galois subextensions of \( L \) is contained in another finite Galois subextension. Hence any finite collection the closed sets \( F(L') \) has a non-empty intersection. Since \( G \) is compact, this implies that \( \bigcap_{L'} F(L') \neq \emptyset \). Any element \( \sigma \in \bigcap_{L'} F(L') \) satisfies the conclusion of Lemma 9.18. □

□

This completes the proof of the going down theorem. To finish proving Theorem 9.1, it remains to prove the normality of \( k[y_1, \ldots, y_d] \) (Lemma 9.15). By Exercise 4.8, it is sufficient to prove that \( k[y_1, \ldots, y_d] \) is a UFD. This follows by induction on \( d \) from the Gauss lemma:

**Exercise 9.21 (the Gauss lemma).** Let \( A \) be a UFD and \( y \) an independent variable. Then \( A[y] \) is a UFD. (Hint: let \( K \) be the field of fractions of \( A \). Since \( K[y] \)
is a UFD, the question is reduced to the following: given polynomials \( f, g, h \in A[y] \) and an irreducible element \( a \in A \) such that \( a \mid fg \), either \( a \mid f \) or \( a \mid g \).

This completes the proof of Theorem 9.1. □

We end this section by giving an alternative proof of Lemma 9.9 using 9.15–9.17.

A second proof of Lemma 9.9. Take any \( m \in \text{Max}(k[y_1, \ldots, y_d]) \). We want to prove that \( \text{ht} \ m = d \). Let \( k' = \frac{k[y_1, \ldots, y_d]}{m} \). Then \( k' \) is a finite extension of \( k \), so that \( k[y_1, \ldots, y_d] \subset k'[y_1, \ldots, y_d] \) is a finite ring extension. Let \( a_1, \ldots, a_d \) denote the natural images of \( y_1, \ldots, y_d \) in \( k' \). Then \( (y_1 - a_1, \ldots, y_d - a_d) \) is a maximal ideal of \( k'[y_1, \ldots, y_d] \) of height \( d \) by Example 6.10. Since \( (y_1 - a_1, \ldots, y_d - a_d) \cap k[y_1, \ldots, y_d] = m \), we have \( \text{ht} \ m = d \) by Exercise 9.17. □

§10. Regular Rings.

Regular rings are those rings which correspond to complex manifolds in classical algebraic geometry. In other words, they correspond to algebraic varieties which are locally diffeomorphic to \( \mathbb{C}^n \) at every point. Yet another way of saying this is that regular varieties do not have self-intersections, corners or cusps (these latter kinds of points are called singularities). Algebraically, we express this intuitive idea by saying that locally at every point there is a local coordinate system with \( d \) coordinates, where \( d \) is equal to the dimension. In other words, a point \( \xi \) on a \( d \)-dimensional variety or scheme is regular if there exist \( d \) equations locally at \( \xi \) whose common set of zeroes is \( \xi \) with its reduced structure. Now for precise definitions.

Let \((A, m, k)\) be a Noetherian local ring of dimension \( d \).

**Definition 10.1.** \( A \) is regular if \( m \) can be generated by exactly \( d \) elements ( \( \iff \dim_k \frac{m}{m^2} = d \iff \bigoplus_{n=0}^{\infty} \frac{m^n}{m^{n+1}} \cong k[t_1, \ldots, t_d] \)).

**Definition 10.2.** If \( A \) is regular of dimension \( d \), a set \( \{x_1, \ldots, x_d\} \) of \( d \) generators of \( m \) is called a regular system of parameters for \( A \) (this is equivalent to saying that \( x_1, \ldots, x_d \) are linearly independent mod \( m^2 \)).

**Definition 10.3.** Let \( A \) be any Noetherian ring. We say that \( A \) is regular if \( A_m \) is regular for all \( m \in \text{Max}(A) \).

Properties of regular local rings:

1) A regular local ring is a domain. This follows from the graded algebra description appearing in Definition 10.1 and the following two exercises:

**Exercise 10.4.** Let \( A \) be a ring, \( I \subset A \) an ideal such that

\[
\bigcap_{n=1}^{\infty} I^n = 0.
\]

If \( \text{gr}_IA \) is a domain then \( A \) is a domain.
Exercise 10.5. Let $A$ be a Noetherian ring, $m \subsetneq A$ an ideal. Assume either that $m \subset J(A)$ or that $A$ is a domain. Then $\bigcap_{n=1}^{\infty} m^n = (0)$.

Problem 10.6. Prove that a regular local ring is normal. (Hint: prove that if $\text{gr}_1 A$ is normal, then $A$ is normal, provided that $A$ is Noetherian and $I \subset J(A)$ (in particular, $I$ satisfies (10.1)).)

More generally, it is known that a regular local ring is a UFD (this is a non-trivial theorem of Auslander and Buchsbaum).

Example 10.7. Let $k$ be a field. Then the polynomial ring $k[x_1, \ldots, x_d]$ is regular.

Indeed, let $m \subset k[x_1, \ldots, x_d]$ be a maximal ideal. In the first proof of Lemma 9.9, we explicitly constructed a set of $d$ generators for $m$. More generally, it is easy to see that if $A$ is a regular ring, then so are $A[x_1, \ldots, x_n]$ and $A[[x_1, \ldots, x_n]]$, where $x_1, \ldots, x_n$ are independent variables.

Proposition 10.8. Let $(A, m, k)$ be a regular local ring of dimension $d$. Let $l \leq d$. Let $x_1, \ldots, x_l$ be elements of $m$, none of which belongs to the ideal generated by the others. The following are equivalent:

1) $x_1, \ldots, x_l$ are linearly independent mod $m^2$.
2) $x_1, \ldots, x_l$ can be extended to a regular system of parameters of $A$.
3) $A/(x_1, \ldots, x_l)$ is a regular local ring.

If (1)–(3) hold, we have $\text{ht}(x_1, \ldots, x_l) = l$.

Proof. 1) $\iff$ 2). By Nakayama’s Lemma, $x_1, \ldots, x_d$ is a regular system of parameters if and only if $x_i \mod m^2$ form a basis for $m/m^2$. Hence 2) follows from the fact that a collection of linearly independent elements in a vector space can be extended to a basis.

2) $\implies$ 3). Extend $x_1, \ldots, x_l$ to a system of parameters $x_1, \ldots, x_d$. Let $A' = A/(x_1, \ldots, x_l)$, $m' = m/(x_1, \ldots, x_l)$. Then $\dim A' \geq d - l$, for if an $m'$-primary ideal was generated by fewer than $d - l$ elements, together with $x_1, \ldots, x_l$ we would obtain a set of fewer than $d$ generators for an $m$-primary ideal in $A$. On the other hand, $m'$ is generated by $x_{l+1}, \ldots, x_d$. Hence $\dim A' = d - l$ and $A'$ is regular.

3) $\implies$ 1). Let $x_1, \ldots, x_r$ be the largest subset of $x_1 \ldots x_l$ which are linearly independent mod $m^2$. Suppose $r < l$. Then by (1)$\implies$(3), $A/(x_1, \ldots, x_r)$ is a regular local ring of dimension $d - r$, in particular, a domain. Then $x_{r+1}$ is not a zero divisor in $A/(x_1, \ldots, x_r)$, hence by Lemma 6.29 $\dim A/(x_1, \ldots, x_{r+1}) < \dim A/(x_1, \ldots, x_r) = d - r$. On the other hand, let $m'$ be as above. Then $\dim_k m'/m'^2 = d - r$ by definition of $r$. This contradicts the regularity of $A/(x_1, \ldots, x_r)$.

Finally, suppose (1)–(3) hold. Then $\text{ht}(x_1, \ldots, x_l) \leq l$ by Corollary 8.6. By (3), $A/(x_1, \ldots, x_i)$ is a domain for all $i \leq d$; in other words, $(x_1, \ldots, x_i)$ is a prime ideal for $i \leq d$. Then $0 \subseteq (x_1) \subseteq (x_1, x_2) \subseteq \cdots \subseteq (x_1, \ldots, x_l)$. This proves that $\text{ht}(x_1, \ldots, x_l) = l$. $\square$
Definition 10.9. Let $k$ be a field. $k$ is **perfect** if either char $k = 0$ or char $k = p > 0$ and $k^p = k$.

Definition 10.10. Let $\sigma : k \hookrightarrow k'$ be a field extension. We say that $k'$ is **separably generated** over $k$ if $\sigma$ can be decomposed into a purely transcendental extension and a separable algebraic extension. If $k(x_1, \ldots, x_t)$ is a purely transcendental subextension of $k'$ over which $k'$ is separable algebraic, $x_1, \ldots, x_t$ is called a **separating transcendence base**.

Exercise 10.11.

1. Any finite field is perfect.
2. If $k$ is perfect, then any algebraic extension of $k$ is separable.
3. More generally, if $k$ is perfect, any finitely generated field extension of $k$ is separably generated.

Exercise 10.12. Let $k \hookrightarrow k'$ be a finitely generated, separably generated extension of transcendence degree $t$. Let $x_1, \ldots, x_n$ be a set of generators of $k'$ over $k$ (as a field). Show that there exists a subset of $x_1, \ldots, x_n$ which is a separating transcendence base.

Theorem 10.13. Let $k$ be a field. Let $A = \frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_l)}$, $P \in \text{Spec } A$. Let $Q$ be the inverse image of $P$ in $k[x_1, \ldots, x_n]$. Then:

1. $\text{ht}(f_1, \ldots, f_l)k[x_1, \ldots, x_n]_Q \geq \text{rk} \left( \frac{\partial f_i}{\partial x_j} \right) \text{ mod } P$.
2. If equality holds in (1), then $A_P$ is regular.
3. If $\kappa(P)$ is separably generated over $k$ and $A_P$ is regular, then equality holds in (1).

Note that by Exercise 10.11 $\kappa(P)$ is always separably generated over $k$ in the case when $k$ is perfect.

**Proof.** First, assume $P$ is maximal. Let $k' = \frac{A}{I}$. Then $k \to k'$ is a finite field extension and $k[x_1, \ldots, x_n] \to k'[x_1, \ldots, x_n]$ a finite ring extension. Let $a_i$ be the natural image of $x_i$ in $k'$ and consider the ideal $Q' = (x_1 - a_1, \ldots, x_n - a_n) \subset k'[x_1, \ldots, x_n]$. Then $Q' \cap k[x_1, \ldots, x_n] = Q$. The homomorphism $k[x_1, \ldots, x_n] \to k'[x_1, \ldots, x_n]$ induces a map $\varphi : \frac{Q}{Q'} \to \frac{Q'}{Q''}$ between two $k'$-vector spaces of dimension $n$.

Lemma 10.14. $\varphi$ is an isomorphism if and only if $k'$ is separable over $k$.

**Proof.** Let $\bar{g}_i$ denote the minimal polynomial of $a_i$ over $k(a_1, \ldots, a_{i-1}) \subset k'$, $1 \leq i \leq n$ and let $g_i$ an arbitrary inverse image of $\bar{g}_i$ in $k[x_1, \ldots, x_i]$. Then, as in the proof of Lemma 9.9, $g_1(x_1), \ldots, g_n(x_1, \ldots, x_n)$ generate $Q$. Therefore $\phi(Q)$ is the vector space generated by the linear forms of $g_1, \ldots, g_n$. Hence $\phi$ is an isomorphism if and only if $\det \left| \frac{\partial g_i}{\partial x_j} \right| \notin Q$. Now, the extension $k \subset k'$ is separable $\iff$ each of the $g_i$ is separable $\iff \frac{\partial g_i}{\partial x_i} \notin Q$ for all $i \iff \det \left| \frac{\partial g_i}{\partial x_j} \right| = \prod_{i=1}^{n} \frac{\partial g_i}{\partial x_i} \notin Q$, as desired. □
Now, let \( r = \text{rk} \left( \frac{\partial f_i}{\partial x_j} \Big|_Q \right) \). Say, \( f_1, \ldots, f_r \) are such that \( \text{rk} \left( \frac{\partial f_i}{\partial x_j} \Big|_Q \right)_{1 \leq i, j \leq r} = r \).

This means that the natural images of \( f_1, \ldots, f_r \) in \( Q' \) are linearly independent, hence they are linearly independent in \( Q'_{Q''} = \frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_r)} \) is a regular local ring by Proposition 10.8 (in particular, it is a domain).

Then \( r = \text{ht}(f_1, \ldots, f_r)k[x_1, \ldots, x_n]Q \leq \text{ht}(f_1, \ldots, f_r) \), which proves (1). Now, suppose \( r = \text{ht}(f_1, \ldots, f_r)k[x_1, \ldots, x_n]Q \). Since \((f_1, \ldots, f_r)k[x_1, \ldots, x_n]Q \) is prime, this equality of heights implies that

\[
(f_1, \ldots, f_r)k[x_1, \ldots, x_n]Q = (f_1, \ldots, f_r)k[x_1, \ldots, x_n]Q,
\]

which shows that \( A_P = \frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_r)} \) is regular.

Next, assume that \( k' \) is separable over \( k \) and \( A_P \) is regular. Then \( \varphi \) is an isomorphism. Since \( A_P \) is regular, \((f_1, \ldots, f_r) = (f_1, \ldots, f_r) \) by Proposition 10.8.

\[
\text{rk} \left( \frac{\partial f_i}{\partial x_j} \Big|_Q \right)_{1 \leq i, j \leq r}
\]

is equal to the dimension of the \( k' \)-vector subspace of \( Q'_{Q''} \), spanned by the images of \( f_1, \ldots, f_r \). Since \( \phi \) is an isomorphism and since \( f_1, \ldots, f_r \) are linearly independent mod \( Q^2 \), we have \( \text{rk} \left( \frac{\partial f_i}{\partial x_j} \Big|_Q \right)_{1 \leq i, j \leq r} = r \), as desired.

Finally, suppose \( P \) is not maximal. Let \( r = \text{rk} \left( \frac{\partial f_i}{\partial x_j} \right) \mod P \). Say,

\[
\text{rk} \left( \frac{\partial f_i}{\partial x_j} \Big|_Q \right)_{1 \leq i, j \leq r} = r.
\]

Let \( \bar{x}_i \) denote the natural image of \( x_i \) in \( \kappa(P) \). Renumbering the \( x_i \), we may assume that \( \bar{x}_{r+1}, \ldots, \bar{x}_{r+t} \) are algebraically independent over \( k \) and \( \bar{x}_{r+t+1}, \ldots, \bar{x}_n \) are algebraic over \( k(\bar{x}_{r+1}, \ldots, \bar{x}_{r+t}) \). Let

\[
k' = \frac{k[x_{r+1}, \ldots, x_n]P \cap k[x_{r+1}, \ldots, x_n]}{P \cap k[x_{r+1}, \ldots, x_n]} = k(\bar{x}_{r+1}, \ldots, \bar{x}_n),
\]

\[
k'' = k(\bar{x}_{r+1}, \ldots, \bar{x}_{r+t}).
\]

By the choice of \( t \), \( k' \) is algebraic over \( k'' \) and \( k'' \subset A_P \). Since \( k''[x_1, \ldots, x_r, x_{r+t+1}, \ldots, x_n] \) is obtained from \( k[x_1, \ldots, x_n] \) by localizing with respect to the multiplicative system \( k[x_{r+1}, \ldots, x_{r+t}] \), disjoint from \( P \), replacing \( k \) by \( k'' \) in the Theorem does not change the problem. In other words, we may assume that \( t = 0 \) and \( k' \) is algebraic over \( k \). Then \( k[x_1, \ldots, x_n] \rightarrow k'[x_1, \ldots, x_n] \) is a finite ring extension. Let \( P_0 = (x_{r+1} - \bar{x}_{r+1}, \ldots, x_n - \bar{x}_n) \cap k[x_1, \ldots, x_n] \). By the going up theorem, there exists an ideal \( Q' \subset k'[x_1, \ldots, x_n] \) lying over \( Q \) containing \( (x_{r+1} - \bar{x}_{r+1}, \ldots, x_n - \bar{x}_n) \). Since height of ideals is preserved by finite extensions, none of the statements in Theorem 10.13 are affected by replacing \( k \) by \( k' \), \( A \) by \( \frac{k'[x_1, \ldots, x_n]}{(f_1, \ldots, f_r)} \), \( Q \) by \( Q' \), etc. For (3) in Theorem 10.13, note that if \( \kappa(P) \) is separably
generated over $k$ then by Exercise 10.12 we may choose $k'$ so that $\kappa(P)$ is separably generated over $k'$.

To complete the proof of Theorem 10.13, it is sufficient to show that, under the assumption $t = 0$, $Q$ is a maximal ideal of $k[x_1, \ldots, x_n]$, since the theorem has already been proved in this case. By Proposition 4.2, this is equivalent to proving that $\kappa(P)$ is algebraic over $k$. The assumption $t = 0$ means that $\bar{x}_{r+1}, \ldots, \bar{x}_n$ are algebraic over $k$. Thus it remains to prove that $\bar{x}_1, \ldots, \bar{x}_r$ are algebraic over $k(\bar{x}_{r+1}, \ldots, \bar{x}_n)$. Since $k'$ is a quotient of $\frac{k(\bar{x}_{r+1}, \ldots, \bar{x}_n)}{(f_1, \ldots, f_t)k(\bar{x}_{r+1}, \ldots, \bar{x}_n)}$, everything is reduced to the following lemma.

**Lemma 10.15.** Consider elements $f_1, \ldots, f_r$ in $k[x_1, \ldots, x_r]$ and a prime ideal $Q \in V(f_1, \ldots, f_r)$, such that $\det \left( \frac{\partial f_i}{\partial x_j} \right) \notin Q$. Then $Q \in \text{Max}(k[x_1, \ldots, x_r])$.

Note: When we apply the Lemma to finish the proof of Theorem 10.13, the field $k$ of the Lemma plays the role of $k' = k(\bar{x}_{r+1}, \ldots, \bar{x}_n)$ in the Theorem; the ideal $Q$ of the Lemma corresponds to the kernel of the natural homomorphism $\psi : k'[x_1, \ldots, x_r] \to \kappa(P)$. Thus the Lemma will imply that $\kappa(P)$ is the quotient of $k'[x_1, \ldots, x_r]$ by a maximal ideal, hence is algebraic over $k'$ by Proposition 4.2, as desired.

**First proof of Lemma 10.15.** By Nullstellensatz, there exists $m \in V(Q)$ such that $\det \left( \frac{\partial f_i}{\partial x_j} \right) \notin m$. By Theorem 10.13, applied to the maximal ideal $m \subset k[x_1, \ldots, x_r]$, $\text{ht}(f_1, \ldots, f_r)k[x_1, \ldots, x_r]_m = r$. Since $k[x_1, \ldots, x_r]Q = (k[x_1, \ldots, x_r]_m)Q$ and height is preserved under localization (Exercise 8.9), $\text{ht}(f_1, \ldots, f_r)k[x_1, \ldots, x_r]Q = r \geq \dim k[x_1, \ldots, x_r]$. Hence $\text{ht}(f_1, \ldots, f_r)k[x_1, \ldots, x_r]Q = r$, which proves that every ideal containing $(f_1, \ldots, f_r)$ is maximal. □

**Second proof of Lemma 10.15, not using Nullstellensatz.** We use induction on $r$. Let $k' = \kappa(Q)$. If $r = 1$, $f_1$ is a polynomial in one variable with non-zero derivative, hence $Q$ is generated by one of the irreducible factors of $f_1$ and the result is immediate.

Suppose $r > 1$ and the Lemma is known for $r - 1$. Let

$$\bar{k} = \frac{k[x_1, \ldots, x_{r-1}]Q \cap k[x_1, \ldots, x_{r-1}]}{(Q \cap k[x_1, \ldots, x_{r-1}])}.$$  

We may assume that $\frac{\partial f_r}{\partial x_r} \notin Q$. Then $\text{ht}(f_r)\bar{k}[x_r] = 1$ and

$$Q\bar{k}[x_r]Q \cap \bar{k}[x_r] = (f_r)\bar{k}[x_r]Q \cap \bar{k}[x_r].$$

Hence

$$(f_1, \ldots, f_r)k[x_1, \ldots, x_r]Q = ((f_r) + Q \cap k[x_1, \ldots, x_{r-1}])k[x_1, \ldots, x_r]Q.$$
Since the rank of the matrix \( \left( \frac{\partial f_i}{\partial x_j} \right) \) is clearly independent of the choice of the base of the ideal \((f_1, \ldots, f_r)\), (10.2) implies that there exist \( \tilde{f}_1, \ldots, \tilde{f}_{r-1} \in Q \cap k[x_1, \ldots, x_{r-1}] \) such that \( \det \left| \frac{\partial \tilde{f}_i}{\partial x_j} \right|_{1 \leq i, j \leq r-1} \notin Q \). By the induction assumption,

\[ \text{ht}(Q \cap k[x_1, \ldots, x_{r-1}]) = r - 1, \]

hence \( \text{ht}Q = r = \dim k[x_1, \ldots, x_r] \), which proves that \( Q \) is maximal. \( \square \)

This completes the proof of Theorem 10.13. \( \square \)

**Corollary 10.16.** Let \( k \) be a perfect field, \( A \) a regular ring, which is a localization of a finitely generated \( k \)-algebra, \( P \) a prime ideal of \( A \). Then \( A_P \) is regular.

**Remark 10.17.** Corollary 10.16 is true for any regular local ring, whether or not it is a localization of a finitely generated \( k \)-algebra, but we will not prove it here. See [3, (19.B), Theorem 48, p. 142] for a proof.

**Example 10.18.** Let \( k \) be an imperfect field, \( a \in k \setminus kp \). Let \( x \) be an independent variable and put \( K = \frac{k[x]}{(x^p - a)} \). Then \( K \) is a field (Proposition 4.2 and Lemma 4.4), that is, a regular local ring of dimension 0. At the same time, \( \frac{\partial (x^p - a)}{\partial x} \equiv 0 \). We have \( K = \kappa(0) \) for \( (0) \in \text{Spec}K \). This shows that the hypothesis that \( \kappa(P) \) be separably generated over \( k \) is necessary in Theorem 10.13 (3).

Of course, a zero dimensional local ring is regular if and only if it is a field. We end this section by considering the case of regular one-dimensional local rings. Problem 10.6 says that any regular local ring is normal. We will now show that the converse is true for one-dimensional local rings.

**Theorem 10.19.** Let \( A \) be a one-dimensional Noetherian local ring. Then \( A \) is regular if and only if \( A \) is normal.

**Proof.** Although “only if” is a special case of Problem 10.6, we will prove it directly. Suppose \( A \) is regular. Then the maximal ideal \( m \) of \( A \) is principal, that is, generated by a single element \( x \). Let \( y \) be any non-zero element of \( m \). Since \( \bigcap_{n=0}^{\infty} m^n = (0) \) in any Noetherian local ring (Exercise 10.5 or use Nakayama’s Lemma), there exists \( N \in \mathbb{N} \) such that \( y \notin m^N \). \( y \) can be written in the form \( y = x^N z \), where \( z \notin (x) = m \). Of course, this representation is unique. This implies that \( A \) is a UFD, hence normal.

“If” is more subtle. We assume that \( A \) is normal and want to prove that \( m \) is principal. We define the notion of \( I^{-1} \) for an ideal \( I \) in a domain \( A \).

**Notation.** Let \( A \) be a domain, \( K \) the field of fractions of \( A \), \( I \) an ideal of \( A \). We define \( I^{-1} = \{ x \in K \mid xa \in A \text{ for all } a \in I \} \).

\( I^{-1} \) is an \( A \)-submodule of \( K \). Of course, \( II^{-1} \) is an ideal of \( A \).

**Lemma 10.20.** Assume that \((A, m)\) is local. Then \( I \) is principal if and only if \( II^{-1} = A \).

**Proof.** If \( I = (x) \) is principal, then \( I^{-1} = Ax^{-1} \subset K \). Hence \( II^{-1} = A \).
Conversely, suppose $II^{-1} = A$. Then

\[(10.2) \quad 1 = \sum_{i=1}^{n} a_i x_i,\]

where $a_i \in I$, $x_i \in I^{-1}$. Since $a_i x_i \in A$ for all $i$, (10.2) implies that $a_i x_i \notin m$ for some $i$. Say, $x_1 a_1 \notin m$. This means that $a_1 x_1$ is invertible, so that $\frac{1}{x_1} \in I^{-1}$. Now take any other $b \in I$. Since $\frac{1}{x_1} \in I^{-1}$, $\frac{b}{x_1} \in A$, hence $b \in (x_1)$. This proves that $I = (x_1)$, so that $I$ is principal. □

**Exercise 10.21.** Let $A$ be any domain (i.e. not necessarily local), $I \subset A$ and ideal. Prove that $II^{-1} = A$ if and only if $I$ is locally principal, that is, $IA_P$ is principal for any $P \in \text{Spec } A$. Locally principal ideals together with their inverses generate a group (under the operation of multiplication). In geometry, elements of this group are called line bundles on $\text{Spec } A$.

We continue with the proof of Theorem 10.19. By Lemma 10.20, it remains to prove that $mm^{-1} = A$ for a local 1-dimensional normal Noetherian ring $(A,m)$. Suppose $mm^{-1} \subsetneq A$. Since $mm^{-1}$ is an ideal, we have $mm^{-1} \subset m$. Since $1 \in m^{-1}$, $mm^{-1} = m$. By induction on $n$, $m(m^{-1})^n = m$ for any $n \in \mathbb{N}$.

**Lemma 10.22.** Let $A$ be a domain with field of fractions $K$. Take $x \in K$. Let $A : x = \{a \in A \mid ax \in A\}$. If $x$ is integral over $A$, then $\bigcap_{n=1}^{\infty} (A : x^n) \neq (0)$. The converse holds if $A$ is Noetherian.

**Proof.** If $x$ is integral over $A$, then $x^n \in \sum_{i=0}^{n-1} Ax^i$ for some $n \in \mathbb{N}$. Then $x^l \in \sum_{i=0}^{n-1} Ax^i$ for all $l \geq n$ by induction on $l$. Then $A : x^l \supset \bigcap_{i=1}^{n-1} (A : x^i)$ for all $l \geq n$. This proves the first statement.

Conversely, assume that $A$ is Noetherian and take a non-zero element

$$y \in \bigcap_{n=1}^{\infty} (A : x^n).$$

Then $Ay^{-1}$ is isomorphic to $A$ as an $A$-module, hence is Noetherian. $\sum_{i=0}^{n} Ax^n$ form an ascending chain of submodules of $Ay^{-1}$. By the Noetherian property this chain must stabilize. Hence for some $n$, $x^n \in \sum_{i=0}^{n-1} Ax^i$, which implies that $x$ satisfies an integral equation of degree $n$ over $A$. □

Coming back to the proof of Theorem 10.19, take any $x \in m^{-1}$. Since $m(m^{-1})^n = m$ for all $n \in \mathbb{N}$,
we have $A : x^n \supset m$ for all $n \in \mathbb{N}$. By Lemma 10.22, $x$ is integral over $A$, hence $x \in A$ by normality of $A$. This proves that

$$m^{-1} = A.$$  

We now use the fact that $A$ is one dimensional to derive a contradiction. Take a non-zero element $x \in m$. Since $A$ is a domain, $x$ is not a zero divisor, hence $\text{ht}(x) = 1$. Since $\dim A = 1$, this means that $(x)$ is $m$-primary, so that $m = \sqrt{(x)}$. Then there exists $n \in \mathbb{N}$ such that $mn^{-1} \not\subset (x)$ but $m^n \not\subset (x)$. Take any $y \in mn^{-1} \setminus (x)$. Then $\frac{y}{x} \in m^{-1} \setminus A$, which contradicts (10.3). This completes the proof. □

Let $A$ be an integral domain with field of fractions $K$. We may consider the integral closure $\bar{A}$ of $A$ in $K$. The inclusion $A \hookrightarrow \bar{A}$ gives rise to the natural morphism of integral schemes $\pi : \text{Spec } \bar{A} \to \text{Spec } A$. If $A$ is Noetherian and satisfies certain mild additional conditions (they will be specified later, but they hold for any algebra of finite type over a field and any quotient or localization of a formal or convergent power series ring), $\bar{A}$ is also Noetherian. The canonical morphism $\pi$ is called normalization of the scheme $\text{Spec } A$. It was defined (surprisingly late—in the nineteen forties) by Oscar Zariski. This is an example of the usefulness of the algebraic language in geometry: this notion, extremely important as it turned out to be, did not occur to anyone until the algebraic language was developed. Normalization will be of interest to us when we discuss resolution of singularities. Geometrically, Theorem 10.19 says that normalization resolves the singularities of curves. More generally, it says that for an arbitrary Noetherian scheme normalization resolves the singularities in codimension 1. When normalization was defined, the theorem of resolution of singularities was known for almost a century, yet it was quite a surprise that it had such a simple and elegant proof and that the procedure for desingularization had such a simple description.

§11. Sheaves.

Until now, we only considered affine schemes. However, inasmuch as we are interested in studying global questions in algebraic geometry (for instance, if we want to define the analogue of compact complex manifolds), we are led to consider more general schemes, for which affine schemes are basic building blocks. Arbitrary schemes are glued from affine ones in the same way that manifolds are glued from open subsets of $\mathbb{R}^n$. The notion which expresses the idea of glueing global objects from local data in modern algebraic geometry is that of a sheaf. The definition of sheaves is the subject of this section.

Before making the general definitions, we consider the case of an affine scheme $\text{Spec } A$, where $A$ is a domain (as we will see, the absence of zero divisors makes life easier). We saw that open affine subschemes of $\text{Spec } A$ of the special form $\text{Spec } A_f$, $f \in A$, form a basis for the Zariski topology. It is natural to regard the ring $A_f$ as the “coordinate ring” or the “ring of regular functions” on the affine open scheme $\text{Spec } A_f$. However, these basic affine open sets do not, in general, exhaust all the
open subsets of Spec $A$. For the purposes of glueing affine schemes together, we are forced to consider these more general affine open subsets. In particular, we must define what we mean by the ring of regular functions on an arbitrary open set $U$. The main ideas are illustrated by the following exercises.

**Exercise 11.1.** Let $A$ be a domain. Prove that $A = \bigcap_{P \in \text{Spec } A} A_P = \bigcap_{m \in \text{Max}(A)} A_m$, where we view all the $A_P$ as subsets of the field of fractions of $A$.

The point of this exercise is that an affine scheme can be reconstructed in a straightforward way from the collection of all its local rings.

**Exercise 11.2.** Let $A$ be a domain and let $U \subset \text{Spec } A$ be an open set. Let

\[(11.1) \quad \mathcal{O}_U = \bigcap_{P \in U} A_P.\]

Prove that:

1. For every $P \in U$, $(\mathcal{O}_U)_{P \cap \mathcal{O}_U} = A_P$.
2. There are natural inclusions

\[(11.2) \quad U \xrightarrow{i} \text{Spec } \mathcal{O}_U \hookrightarrow \text{Spec } A.\]

3. If $A$ is noetherian then so is $\mathcal{O}_U$.

If $\iota$ of (11.2) is a set theoretic bijection then it is natural to regard $U = \text{Spec } \mathcal{O}_U$ as an affine open subscheme of Spec $A$. Of course, it may happen that $\iota$ is not surjective, in which case $U$ is open but not affine. An example of that is provided by letting $U$ be the plane without the origin. In other words, let $A = k[x, y]$, $U = \text{Spec } A \setminus \{(x, y)\}$. Then $\mathcal{O}_U = A$. The conclusion we can draw from all of the above is that it is natural to think of $\mathcal{O}_U$ as the ring of regular functions on the set $U$.

It is not immediately obvious how to generalize the above definitions to the case when $A$ is not a domain, because it is not clear what should replace $\bigcap_{P \in U} A_P$ (if $A$ is not a domain, the different local rings $A_P$ are not naturally subrings of any single ring of fractions. To overcome this difficulty, we will develop the powerful machine of sheaf theory. Now for the general definitions.

Let $X$ be a topological space.

**Definition 11.3.** A pre-sheaf $\mathcal{F}$ of sets on $X$ is the data consisting of a set $\mathcal{F}_U$ for each open set $U \subset X$ and a map $\rho_{UV} : \mathcal{F}_U \to \mathcal{F}_V$ for each pair $U, V$ of open sets such that $V \subset U$, satisfying the following conditions:

1. $\mathcal{F}_\emptyset$ is a one-element set.
2. $\rho_{UU}$ is the identity map for all $U$.
3. Given any three open sets $W \subset V \subset U$, we have $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$. 


The set $\mathcal{F}_U$ is called the set of sections of $\mathcal{F}$ over $U$; the maps $\rho_{UV}$ are called restriction maps.

If the sets $\mathcal{F}_U$ have some additional structure, such as rings or groups, we may talk about a presheaf of ring (resp. groups). In this case, we require, in addition, that the maps $\rho_{UV}$ be homomorphisms of the structure in question. Also, Definition 11.3 (1) has to be modified to say that $\mathcal{F}_\emptyset$ is the zero ring (resp. the trivial group).

Let $\mathcal{F}$ be a presheaf.

**Definition 11.4.** We say that $\mathcal{F}$ is a sheaf if the following two conditions (identity and gluability) are satisfied for any open set $U$ and any open covering $U = \bigcup_{\lambda \in \Lambda} U_\lambda$.

For $\lambda, \mu \in \Lambda$, let us write $U_{\lambda\mu}$ for $U_\lambda \cap U_\mu$, $\rho_\lambda$ for $\rho_{U_\lambda}$ and $\rho_{\lambda\mu}$ for $\rho_{U_\lambda U_\mu}$.

We require

1. Identity: for $f, g \in \mathcal{F}_U$, if $\rho_\lambda(f) = \rho_\lambda(g)$ for all $\lambda \in \Lambda$ then $f = g$.
2. Gluability: given sections $f_\lambda \in \mathcal{F}_{U_\lambda}$, $\lambda \in \Lambda$ such that $\rho_{\lambda\mu}(f_\lambda) = \rho_{\mu\lambda}(f_\mu)$ for all $\lambda, \mu \in \Lambda$, there exists $f \in \mathcal{F}_U$ such that $f_\lambda = \rho_\lambda(f)$ for all $\lambda$.

**Remark 11.5.** The meaning of Definition 11.4 is that $\mathcal{F}$ is a sheaf if and only if each $\mathcal{F}_U$ can be completely recovered from local information. Indeed, Definition 11.4 amounts to saying that for any open covering $U = \bigcup_{\lambda \in \Lambda} U_\lambda$,

$$
\mathcal{F}_U \cong \left\{ \{f_\lambda\}_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} \mathcal{F}_{U_\lambda} \mid \rho_{\lambda\mu}(f_\lambda) = \rho_{\mu\lambda}(f_\mu) \text{ for all } \lambda, \mu \in \Lambda \right\}.
$$

**Examples 11.6.** I. The constant sheaf $F$ on $X$. Let $F$ be a set, put $\mathcal{F}_U = F$ for all $U$ and let $\rho_{UV} : F \to F$ be the identity map for all $V \subset U$.

II. Let $X$ be a topological (resp. smooth) manifold and let $\mathcal{F}_U$ be the ring of continuous (resp. $C^\infty$) functions on $U$. Given two open sets $V \subset U$ and $f \in \mathcal{F}_U$, define $\rho_{UV}(f)$ to be the restriction of $f$ to $V$ (this motivates the name restriction maps). Then $\mathcal{F}_U$ together with the maps $\rho_{UV}$ define a sheaf of rings.

**Exercise 11.7.** Let $X = \text{Spec } A$ be an integral affine scheme (in other words, $A$ is a domain). For each open set $U \subset X$, let $\mathcal{O}_U$ denote the ring defined above. For a pair of open sets $V \subset U$, we have the obvious inclusion $\mathcal{O}_U \cong \bigcap_{P \in U} A_P \subset \bigcap_{P \in V} A_P \cong \mathcal{O}_V$.

The natural projection $\prod_{P \in U} A_P \to \prod_{P \in V} A_P$ induces a ring homomorphism $\rho_{UV} : \mathcal{O}_U \to \mathcal{O}_V$. Prove that the rings $\mathcal{O}_U$, together with the maps $\rho_{UV}$, form a sheaf of rings on $X$. This sheaf is called the structure sheaf of $X$.

Now let $X = \text{Spec } A$ be any affine scheme (i.e. we no longer require $A$ to be a domain). Let $U$ be an open subset of $X$. We define $\mathcal{O}_U$ to be the following subset of $\bigcap_{P \in U} A_P$. For a $Q \in \text{Spec } A$, $g \notin Q$, let $\rho_{gQ}$ denote the natural localization map $\rho_{gQ} : A_g \to A_Q$. We define

$$
\mathcal{O}_U = \{ \{f_P \in A_P\}_{P \in U} \mid \forall P \in U \ \exists g \in A \setminus P, f \in A_g \ s.t. \forall Q \ni g, f_Q = \rho_{gQ}(f) \}.
$$
Expressing (11.3) in words, \( \mathcal{O}_U \) consists of those elements \( \{ f_P \in A_P \}_{P \in U} \) \( \prod_{P \in U} A_P \) such that every point \( P \) is contained in some basic open set Spec \( A_g \) such that all the \( f_Q, Q \in A_g \), are images of a single element \( f \in A_g \).

**Exercise 11.8.** (a) Prove that if \( A \) is a domain, (11.3) agrees with the definition of \( \mathcal{O}_U \) given earlier in (11.1).

(b) Keep the above notation. Let \( V \) be an open subset of \( U \). Show that the natural projection \( \prod_{P \in U} A_P \to \prod_{P \in V} A_P \) induces a map \( \rho_{UV} : \mathcal{O}_U \to \mathcal{O}_V \).

(c) Prove that \( \{ \mathcal{O}_U \} \) with the restriction maps \( \rho_{UV} \) form a sheaf of rings on \( X \).

(d) Prove that if \( A \) is noetherian then \( \mathcal{O}_U \) is noetherian for each open set \( U \).

(e) Prove that \( \mathcal{O}_X = A \) (and hence \( \mathcal{O}_{X \setminus V(f)} = A_f \) for each \( f \in A \)).

**Definition 11.9.** \( \mathcal{O}_U \) is called the **structure sheaf** of \( X \).

We now give an alternative definition of \( \mathcal{O}_U \). The reader will appreciate, however, that all these definitions revolve around one basic idea: gluing global sections from local data. More precisely, (11.3) defines sections over \( U \) by gluing them from the infinitesimal data of \( f_P, P \in U \), while in the following definition we consider an open cover \( U = \bigcup_{\lambda \in \Lambda} U_{\lambda} \) and glue sections over \( U \) from sections over the \( U_{\lambda} \).

Again, let \( X = \text{Spec} \ A \) be any affine scheme, and let \( U \) be an open subset of \( X \). Consider an open covering of the form \( U = \bigcup_{\lambda \in \Lambda} U_{\lambda} \), where each \( U_{\lambda} = \text{Spec} \ A_{g_{\lambda}} \) is a basic affine open subset. Then for each \( \lambda, \mu \in \Lambda, U_{\lambda} \cap U_{\mu} = \text{Spec} \ A_{g_{\lambda} g_{\mu}} \). For each \( \lambda, \mu \in \Lambda \), let \( \rho_{\lambda \mu} : A_{g_{\lambda}} \to A_{g_{\lambda} g_{\mu}} \) denote the localization by \( g_{\mu} \) (\( \rho_{\lambda \mu} \) is nothing but the restriction map of the structure sheaf of \( \text{Spec} \ A \)).

**Exercise 11.10.** (a) Prove that the ring \( \mathcal{O}_U \) is naturally isomorphic to the following subring of \( \prod_{\lambda \in \Lambda} A_{g_{\lambda}} \):

\[
\mathcal{O}_U \cong \{ \{ f_\lambda \in A_{g_\lambda} \}_{\lambda \in \Lambda} \mid \forall \lambda, \mu \in \Lambda, \rho_{\lambda \mu}(f_\lambda) = \rho_{\mu \lambda}(f_\mu) \}.
\]

(b) Given two open subsets of \( X, V \subset U \), show the restriction map \( \rho_{UV} \) can be described as follows in terms of (11.4). Choose an open cover of \( V \) by basic affine open sets: \( V = \bigcup_{\psi \in \Psi} V_\psi \), where \( V_\psi = \text{Spec} \ A_{h_\psi} \), and where for each \( \psi \in \Psi \) there exists \( \lambda(\psi) \in \Lambda \) satisfying \( g_{\lambda(\psi)} \mid h_\psi \) (in particular, \( V_\psi \subset U_{\lambda(\psi)} \)). Let \( \rho_{\lambda(\psi), \psi} : A_{g_{\lambda(\psi)}} \to A_{h_\psi} \) be the localization by \( h_\psi \). For \( f \in \mathcal{O}_U \), represent \( f \) by \( \{ f_\lambda \in A_{g_{\lambda}} \}_{\lambda \in \Lambda} \), as in (11.4). Show that \( \rho_{UV}(f) \) is the element of \( \mathcal{O}_V \), described by \( \{ \rho_{\lambda(\psi), \psi}(f_{\lambda(\psi)}) \}_{\psi \in \Psi} \).

**Exercise 11.11.** Show that there are natural maps \( U \hookrightarrow \text{Spec} \mathcal{O}_U \hookrightarrow \text{Spec} \ A \). Show also that for any \( P \in U \), \( (\mathcal{O}_U)_{P \cap \mathcal{O}_U} \cong A_P \), so that we have a natural map \( \mathcal{O}_U \to A_P \) for each \( P \in U \).

If \( \iota \) is a set theoretic bijection, then we say that \( U = \text{Spec} \mathcal{O}_U \) is an affine open subscheme of \( \text{Spec} \ A \).
Stalks and germs. Let \( X \) be a topological space and \( F \) a presheaf of sets on \( X \). Let \( P \) be a point of \( X \). Open sets containing \( P \), together with the inclusion maps \( V \subset U \), form an inverse system. Since, by definition, the correspondence \( U \to \mathcal{F}_U \) is a contravariant functor from the open sets of \( X \) to sets, the sets \( \mathcal{F}_U \) form a direct system.

**Definition 11.12.** The **stalk** of \( F \) at \( P \) is \( F_P := \varprojlim_{U \ni P} \mathcal{F}_U \). For an open set \( U \ni P \) and a section \( f \in \mathcal{F}_U \), the natural image of \( f \) in \( F_P \), which we will sometimes denote by \( f_P \), is called the **germ** of \( f \) at \( P \).

**Exercise 11.13.** Describe the stalk at a point \( P \) in each of the three examples of sheaves above.

Sheafication. The following three exercises describe how, given a presheaf \( F \), one can canonically associate to it a sheaf \( \tilde{F} \).

**Exercise 11.14.** Let \( F \) be a presheaf of sets (resp. rings, resp. groups). For an open set \( U \subset X \), define \( \tilde{F}_U \) to be the following subset of \( \prod_{P \in U} F_P \):

\[
\tilde{F}_U = \{ \{ f_P \in F_P \}_{P \in U} \mid \forall P \in U \exists \text{ open } V, P \in V \subset U \text{ and } g \in \mathcal{F}_V \text{ such that } \forall Q \in V, f_Q = g_Q \}.
\]

Show that \( F \) is a sheaf if and only if for each open set \( U \subset X \), \( \mathcal{F}_U = \tilde{F}_U \).

**Exercise 11.15.** Let \( F \) be a presheaf. For each open set \( U \subset X \), let \( \tilde{F}_U \) be defined as in (11.5). Given two open set \( V \subset U \), the natural projection \( \prod_{P \in U} \mathcal{F}_P \to \prod_{P \in V} \mathcal{F}_P \) induces a map \( \tilde{\rho}_{UV} : \tilde{F}_U \to \tilde{F}_V \). Show that the sets \( \tilde{F}_U \), together with the maps \( \tilde{\rho}_{UV} \), form a sheaf. The resulting sheaf \( \tilde{F} \) is called the **sheafification** of \( F \).

**Exercise 11.16.** Let \( X = \text{Spec } A \) be an affine scheme and \( X = \bigcup_{\lambda \in \Lambda} U_\lambda \), with \( U_\lambda = \text{Spec } A_{g_\lambda} \) a covering of \( X \) by basic affine open sets. Show that the structure sheaf of \( X \) is the sheafification of the presheaf \( A \), defined as follows:

\[
A_U = \mathcal{O}_U, \text{ if } U \text{ is contained in one of the } U_\lambda
= \text{ the zero ring otherwise}
\]

Given open set \( V \subset U \), the restriction map is defined to be the restriction map of the structure sheaf of \( U_\lambda \) if \( U \) is contained in one of the \( U_\lambda \) and the zero map otherwise.

§12. Schemes.

Let \( A \) be a ring. The **\( n \)**-dimensional affine space over \( A \) is, by definition, \( \mathbb{A}^n_A = \text{Spec } A[t_1, \ldots, t_n] \). The natural inclusion \( A \subset A[t_1, \ldots, t_n] \) gives rise to the
natural projection \( A^n_A \rightarrow \text{Spec } A \). Intuitively, one should think of \( A^n_A \) as the direct product of \( \text{Spec } A \) with the usual \( n \)-dimensional affine space. Of course, this is strictly heuristic. If one tried to make this last statement precise, one would run into trouble with the definition of “the usual affine space” (affine space over what field? and why over a field? remember that \( A \) might be something like \( \mathbb{Z} \)). The heuristic picture is precise only if \( A \) is of finite type over a field \( k \).

The example of the \( n \)-dimensional affine space points to another feature of scheme theory and algebraic geometry as a whole: the built in capacity for talking about families of varieties or schemes (or deformations of a variety or a scheme), which is such a central notion in the subject. Namely, if \( \text{Spec } B \rightarrow \text{Spec } A \) is a morphism of affine schemes, we may regard \( \text{Spec } B \) as a family of affine schemes over \( \text{Spec } A \). \( \text{Spec } A \) is the base of the family, while the fibers \( V(PB), P \in \text{Spec } A \) are individual members of the family. For example, \( A^n_A \) can be regarded as the trivial family of affine spaces over \( \text{Spec } A \). The fiber over \( P \in \text{Spec } A \) is the affine space \( A^n_{\kappa(P)} \), which is the scheme-theoretic version of the algebraic variety \( \kappa(P)^n \).

Now that we have developed the theory of sheaves, we are ready for a definition of a scheme.

**Definition 12.1.** A scheme is a topological space \( X \) together with a sheaf of rings \( \mathcal{O} \), such that there exists an open covering \( X = \bigcup_{\lambda \in \Lambda} U_\lambda \), where each \( U_\lambda \) is of the form \( U_\lambda = \text{Spec } A_\lambda \) for some ring \( A_\lambda \), such that for each \( \lambda \in \Lambda \), the restriction of \( \mathcal{O} \) to \( U_\lambda \) is the structure sheaf of \( \text{Spec } A_\lambda \). The sheaf \( \mathcal{O} \) is called the structure sheaf of \( X \).

We now give a more explicit description of \( \mathcal{O} \) in terms of the structure sheaves of the \( U_\lambda \).

Let \( X \) be a scheme, and let \( V \) be an open subset of \( X \). Consider an open covering of \( V \) of the form \( V = \bigcup_{\psi \in \Psi} V_\psi \), where each \( V_\psi = \text{Spec } B_\psi \) is an affine open subset. Moreover, for each \( \psi, \mu \in \Psi \), \( V_\psi \cap V_\mu \) is an open subset of \( X \) and therefore can be covered by open affine subschemes: \( V_\psi \cap V_\mu = \bigcup_{\phi \in \Phi_{\psi \mu}} V_{\psi \mu \phi} \), where \( V_{\psi \mu \phi} = \text{Spec } B_{\psi \mu \phi} \).

For each \( \psi, \mu \in \Psi \) and \( \phi \in \Phi_{\psi \mu} \), let \( \rho_{\psi \mu \phi} : B_\psi \rightarrow B_{\psi \mu \phi} \) denote the restriction map of the structure sheaf of \( \text{Spec } B_\psi \).

**Exercise 12.2.** (a) Show that \( \mathcal{O}_V \) is naturally isomorphic to the following subring of \( \prod_{\psi \in \Psi} B_\psi \):

\[
(12.1) \quad \mathcal{O}_V = \{ \{ f_\psi \}_{\psi \in \Psi} \mid \forall \psi, \mu \in \Psi, \phi \in \Phi_{\psi \mu}, \rho_{\psi \mu \phi}(f_\psi) = \rho_{\psi \mu \phi}(f_\mu) \}.
\]

(b) Given two open subsets of \( X \), \( W \subset V \), we can choose an affine open cover \( W = \bigcup_{\delta \in \Delta} W_\delta \), such that for each \( \delta \in \Delta \) there exists \( \psi(\delta) \in \Psi \) satisfying \( W_\delta \subset V_{\psi(\delta)} \).

For \( f \in \mathcal{O}_V \), represent \( f \) by \( \{ f_\psi \}_{\psi \in \Psi} \), as in (12.1). Show that \( \rho_{VW}(f) \) is the element of \( \mathcal{O}_W \), described by \( \{ \rho_{U_{\psi(\delta)}V_\delta}(f_{\psi(\delta)}) \}_{\delta \in \Delta} \).
Definition 12.3. Let $X$, $Y$ be schemes. A morphism from $X$ to $Y$ is a map of topological spaces $X \to Y$, together with affine open coverings $Y = \bigcup_{\lambda \in \Lambda} V_\lambda$, $X = \bigcup_{\lambda \in \Lambda, \phi \in \Phi_\lambda} U_{\lambda \phi}$ such that $\pi^{-1}(V_\lambda) = \bigcup_{\phi \in \Phi_\lambda} U_{\lambda \phi}$ and such that for each $\lambda, \phi$ the map $\pi|_{U_{\lambda \phi}} : U_{\lambda \phi} \to V_\lambda$ is induced by a morphism of affine schemes.

We now define the projective space $\mathbb{P}^n_A$ over $\text{Spec } A$. By definition, $\mathbb{P}^n_A$ is glued from $n + 1$ affine pieces, each of which is isomorphic to $\mathbb{A}^n_A$.

Define $\mathbb{P}^n_A = \bigcup_{i=0}^n U_i$, where $U_i = \text{Spec } A \left[ \frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right]$. The meaning of this notation is that, in addition to saying that each $U_i$ is isomorphic to $\mathbb{A}^n_A$, it also describes the gluing of $U_i$ with $U_j$ along $U_i \cap U_j$. Namely, if we write $U_i = \text{Spec } A[y_1, \ldots, y_n]$, $U_j = \text{Spec } A[z_1, \ldots, z_n]$, with $i < j$ and the variables listed in the same order as above, our notation is a concise way of writing the change of coordinates on $U_i \cap U_j$:

$$y_l = \frac{z_l}{z_{i+1}}, \quad 0 \leq l \leq i \text{ or } j < l \leq n$$
$$= \frac{z_{l+1}}{z_{i+1}}, \quad i < l < j$$
$$= \frac{1}{z_{i+1}}, \quad l = j.$$

To restate the same definition in yet another way, $U_i \cap U_j$ is a basic affine open set of both

$$U_i = \text{Spec } A \left[ \frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right]$$
$$U_j = \text{Spec } A \left[ \frac{x_0}{x_j}, \ldots, \frac{x_{j-1}}{x_j}, \frac{x_{j+1}}{x_j}, \ldots, \frac{x_n}{x_j} \right];$$

we have $U_i \cap U_j = U_i \setminus V(\frac{x_i}{x_j}) = U_j \setminus V(\frac{x_i}{x_j})$, where the last equality is described algebraically by the identification of the localizations

$$\left( A \left[ \frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right] \right)_{x_i} \cong \left( A \left[ \frac{x_0}{x_j}, \ldots, \frac{x_{j-1}}{x_j}, \frac{x_{j+1}}{x_j}, \ldots, \frac{x_n}{x_j} \right] \right)_{x_j}.$$

We have a natural projection $\mathbb{P}^n_A \to \text{Spec } A$, defined to be, in each coordinate chart, the natural projection $\mathbb{A}^n_A \to \text{Spec } A$: the maps

$$A \to A \left[ \frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i} \right]$$
$$\text{Spec } A \leftarrow \text{Spec } \mathbb{A}^n_A.$$
patch together to give a morphism \( \text{Spec } A \leftarrow \mathbb{P}_A^n \). The ring \( A[x_0, \ldots, x_n] \) is sometimes called the **homogeneous coordinate ring** of \( \mathbb{P}_A^n \).

We now give another, more canonical description of \( \mathbb{P}_A^n \), independent of our choice of coordinate system and the covering by charts, directly in terms of the graded \( A \)-algebra \( A[\![x_0, \ldots, x_n]\!] \).

Let \( G = \bigoplus_{n=0}^{\infty} G_n \) be a graded algebra. An ideal \( I \subset G \) is said to be **homogeneous** if it can be generated by homogeneous elements \( \iff \text{given } x = \sum_{i=0}^{n} x_i \in I, \text{ with } x_i \in G_i, \text{ we have } x_i \in I \text{ for all } i, 0 \leq i \leq n \). For example, \( \bigoplus_{n=1}^{\infty} G_n \) is a homogeneous ideal of \( G \).

**Definition 12.4.** \( \text{Proj } G \) is defined to be the set of all the homogeneous prime ideals of \( G \), not containing \( \bigoplus_{n=0}^{\infty} G_n \), endowed with the Zariski topology: the closed sets are all the sets of the form \( V(I) = \{ P \in \text{Proj } G \mid I \subset P \} \), where \( I \) ranges over the homogeneous ideals of \( G \).

**Remark 12.5.** To see that \( \text{Proj } G \) is a scheme, we can cover it by affine charts as follows. Let \( G = G_0[\![x_\lambda]_{\lambda \in \Lambda}\!] \), with \( x_\lambda \) homogenous of degree \( k_\lambda > 0 \). Then \( \text{Proj } G = \bigcup_{\lambda \in \Lambda} U_\lambda \) where \( U_\lambda = \text{Spec } (G_{x_\lambda})_0 \). Here \( G_{x_\lambda} \) has the obvious structure of a graded algebra and the subscript \( 0 \) denotes its degree 0 part.

In other words, there is a 1-1 correspondence between homogeneous prime ideals \( P \subset G \), not containing \( x_\lambda \), and prime ideals of \( (G_{x_\lambda})_0 \). This correspondence is given by \( P \rightarrow PG_{x_\lambda} \cap (G_{x_\lambda})_0 \). Conversely, given \( Q \in \text{Spec } (G_{x_\lambda})_0 \), it is easy to show that \( \sqrt{QG_{x_\lambda}} \) is a homogeneous prime ideal, whose contraction to \( G \) is the element of \( \text{Proj } G \) corresponding to \( Q \). Verifying the details is left as an exercise.

Take \( \lambda, \mu \in \Lambda \). The coordinate transformations on \( U_\lambda \cap U_\mu \) is described by

\[
\left( (G_{x_\lambda})_0 \right)_{x_\lambda^{k_\lambda}}^{x_\mu^{k_\mu}} = \left( (G_{x_\mu})_0 \right)_{x_\mu^{k_\mu}}^{x_\lambda^{k_\lambda}} = \left( G_{x_\lambda x_\mu} \right)_0
\]

The construction globalizes naturally. Namely, if \( X = \bigcup_i \text{Spec } A_i \), we can define \( \mathbb{P}^n_X = \bigcup_i \mathbb{P}^n_{A_i} \), where the \( \mathbb{P}^n_{A_i} \) are glued together in the obvious way. The canonical morphisms \( \mathbb{P}^n_{A_i} \rightarrow \text{Spec } A_i \) are also glued together to give the natural map \( \mathbb{P}^n_X \rightarrow X \).

One of the main subjects of study in the rest of this course, and in algebraic geometry at large, are birational projective morphisms, or **blowings up**. We end this section by defining birational and projective. In the next section we will give a more constructive definition of blowing up, rather than characterizing it by its abstract properties of being birational and projective.

**Definition 12.6.** Let \( \pi : Y \rightarrow X \) be a morphism of schemes. We say that \( \pi \) is projective, or that \( Y \) is **projective over** \( X \), if there exists an open affine cover \( X = \bigcup_i \text{Spec } A_i \) and \( n \in \mathbb{N} \) with the following property. Let \( V_i = \pi^{-1}(\text{Spec } A_i) \)
and let $\pi_i = \pi|_{V_i}$. Then we require that for each $i$, $\pi_i$ have a factorization of the form $V_i \xrightarrow{\iota_i} \mathbb{P}^n_{A_i} \xrightarrow{\alpha_i} \text{Spec } A_i$, where $\iota_i$ is a closed embedding and $\alpha_i$ is the natural projection. To say that $\pi$ is projective is a little weaker than saying that $\pi$ has a factorization of the form

\[(12.2)\quad Y \hookrightarrow \mathbb{P}^n_X \to X,\]

since the definition of projective requires that a factorization of type (12.2) exist locally on $X$.

**Definition 12.7.** Let $X$ be a scheme, $\xi \in X$ a point. Let $\text{Spec } A \subset X$ be an open affine chart of $X$ containing $\xi$ and let $P$ be the prime ideal of $A$ corresponding to $\xi$. The ring $A_P$ is called the local ring of $\xi$ in $X$ and is denoted by $\mathcal{O}_{X,\xi}$. Of course, $\mathcal{O}_{X,\xi}$ is independent of the choice of the affine open chart $\text{Spec } A$.

**Definition 12.8.**

1. A scheme $X = \bigcup \text{Spec } A_i$ is said to be **reduced** if all the $A_i$ are reduced.

2. $X$ is said to be **integral** if it is reduced and irreducible as a topological space (i.e. is not a union of two non-trivial closed sets).

**Remark 12.9.** If $X$ is integral, then each $\text{Spec } A_i$ is a dense open set (otherwise its closure and its complement would express $X$ as a union of two closed sets). Hence each $A_i$ is a domain, otherwise there would exist a non-trivial decomposition of $\text{Spec } A_i$ into closed sets, which could be extended to a non-trivial decomposition of $X$ by passing to closures. We also have that $\text{Spec } A_i \cap \text{Spec } A_j \neq \emptyset$ for any $i$ and $j$, otherwise we would have $X = (X \setminus \text{Spec } A_i) \cup (X \setminus \text{Spec } A_j)$. Then the $(0)$ ideal is common to both $\text{Spec } A_i$ and $\text{Spec } A_j$. Let $\xi$ denote the common point of all the $\text{Spec } A_i$ which corresponds to the $(0)$ ideal in $A_i$. Since $\{\xi\} \cap \text{Spec } A_i = \text{Spec } A_i$, we have $\{\xi\} = X$. This point $\xi$ is called the **generic point** of $X$.

**Definition 12.10.** Let $X$ be an integral scheme and $\xi$ its generic point. Then $\mathcal{O}_{X,\xi} = K(X)$ is a field, called the **field of rational functions** on $X$ or the **function field** of $X$. $K(X)$ is nothing but the common field of fractions of all of the $A_i$.

Let $\pi : X \to Y$ be a morphism of schemes. Let $\xi \in X$ and $\eta = \pi(\xi) \in Y$. Then $\pi$ induces a map $\pi^* : \mathcal{O}_{Y,\eta} \to \mathcal{O}_{X,\xi}$. We have $m_{Y,\eta} = m_{X,\xi} \cap \mathcal{O}_{Y,\eta}$.

**Exercise 12.11.** Let $\sigma : A \to B$ be a ring homomorphism and $\sigma^* : \text{Spec } B \to \text{Spec } A$ the corresponding morphism of affine schemes. Show that $\ker \sigma$ is nilpotent if and only if $\sigma^*$ is dominant, that is, $\sigma^*(\text{Spec } B) = \text{Spec } A$.

Now, suppose $X$ and $Y$ are integral and let $\xi$ and $\eta$ be the respective generic points of $X$ and $Y$. Let $\pi : X \to Y$ be a dominant morphism. This is equivalent to saying that $\pi$ maps the generic point of $X$ to the generic point of $Y$. Hence in this case we get a field extension $\pi^* : K(Y) \hookrightarrow K(X)$. 


Definition 12.12. \( \pi \) is birational if \( \pi^* : K(Y) \xrightarrow{\sim} K(X) \) is an isomorphism.

Definition 12.13. A morphism of affine schemes \( \pi : \text{Spec } B \to \text{Spec } A \) is said to be of finite type if \( B \) is a finitely generated \( A \)-algebra. Let \( \pi : X \to Y \) be a morphism of arbitrary schemes. \( \pi \) is said to be locally of finite type if the affine open coverings \( \{V_\lambda\} \) and \( \{U_{\lambda \phi}\} \) can be chosen so that for all \( \lambda \in \Lambda, \phi \in \Phi_\lambda \), the map \( \pi|_{U_{\lambda \phi}} \) is a morphism of finite type of affine schemes. \( \pi \) is said to be of finite type if, in addition, the set \( \Phi_\lambda \) is finite for each \( \lambda \in \Lambda \) (that is, there are finitely many \( U_{\lambda \phi} \) over each \( V_\lambda \)).

For example, any projective morphism is of finite type.

Remark 12.14. Let \( \pi : X \to Y \) be a morphism of finite type between integral schemes. Then \( \pi \) is birational \( \iff \) there exist open subsets \( U \subset X, V \subset Y \), such that \( \pi \) induces an isomorphism \( U \cong V \).

Proof. Suppose \( \pi \) is birational. Take an affine open set \( V \subset Y \) and an affine open subset \( U \subset \pi^{-1}(V) \), of finite type over \( V \). Let \( U = \text{Spec } A, V = \text{Spec } B \). Clearly, replacing \( X \) by \( U \) and \( Y \) by \( V \) does not change the problem. Since \( \pi \) is birational and of finite type, we may write \( A = B \left[ \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \right] \), where \( a_i, b_i \in A \). Then \( \pi^* \) induces an isomorphisms of \( V \setminus V(b_1, \ldots, b_n) \) with its pre-image.

§13. Blowing up.

Let \( A \) be a ring, \( X = \text{Spec } A, I = (f_1, \ldots, f_n) \) a finitely generated ideal of \( A \).

Definition 13.1. The blowing up of \( X \) along \( I \) is the birational projective morphism \( \pi : \tilde{X} \to X \), defined as follows. Consider the morphism \( \varphi : X \setminus V(I) \to \mathbb{P}^{n-1}_X \), which is defined precisely below, but which should intuitively be thought of as the map which sends every \( \xi \in X \setminus V(I) \) to \( (\xi, (f_1(\xi) : \cdots : f_n(\xi))) \in \mathbb{P}^{n-1}_X \). \( \tilde{X} \) is defined to be the closure \( \varphi(X \setminus V(I)) \subset \mathbb{P}^{n-1}_X \) in the Zariski topology. More precisely, the map \( \varphi \) is described as follows. Write \( X \setminus V(I) = \bigcup_{i=1}^n \text{Spec } A_{f_i}, \mathbb{P}^{n-1}_X = \bigcup_{i=1}^n \text{Spec } A \left[ \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right] \). Then in each of the \( n \) affine charts \( \varphi \) is defined by

\[
A_{f_i} \leftarrow A \left[ \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right]
\]

\[
\frac{f_j}{f_i} \leftarrow \frac{x_j}{x_i}
\]

It is easy to check that those \( n \) maps glue together to give a morphism \( X \setminus V(I) \to \mathbb{P}^{n-1}_X \).

Remark 13.2.

(1) Since the blowing up \( \tilde{X} = \varphi(X \setminus V(I)) \subset \mathbb{P}^{n-1}_X \), the natural projection \( \mathbb{P}^{n-1}_X \to \text{Spec } A \) induces a map \( \tilde{X} \to \text{Spec } A \). In particular, \( \tilde{X} \) is projective over \( \text{Spec } A \).
(2) The natural map \( \pi : \tilde{X} \rightarrow \text{Spec } A \) is an isomorphism away from \( V(I) \) (the inverse mapping is given by \( \varphi \)). This means that the map \( \pi : \tilde{X} \rightarrow X \) is birational.

As we will see later, blowing up is characterized by the properties of being birational and projective.

**Remark 13.3.** For all \( 1 \leq i, j \leq n \), the equation \( f_i x_j - f_j x_i \in A[x_1, \ldots, x_n] \) vanishes on \( \tilde{X} \). This describes the full set of defining equations of \( \tilde{X} \) in \( \mathbb{P}^{n-1}_X \) in the case when \( A \) is Noetherian and \( V(I) \) is a complete intersection (which means ht \( I = n \)), but not in general (a proof of this assertion is postponed). In general, the defining equations \( f \tilde{X} \) in \( \mathbb{P}^{n-1}_X = \text{Proj } A[x_1, \ldots, x_n] \) are not easy to describe.

If \( A \) is an integral domain, we can think of \( \tilde{X} \) as

\[
\tilde{X} = \bigcup_{i=1}^{n} \left( \text{Spec } A \left[ \frac{f_1}{f_i}, \ldots, \frac{f_n}{f_i} \right] \right).
\]  

If fact, even if \( A \) is not a domain, we can still make sense of the description (13.1) (see Example 13.13 below).

**Example 13.4.** 1) Blowing up the plane at a point. Let \( A = k[x, y], I = (x, y) \), so that Spec \( A \) is the affine plane and \( I \) is the origin. Then \( \mathbb{P}^1_A = \text{Proj } A[u_1, u_2] \) should intuitively be thought of as the direct product of \( \mathbb{P}^1_k \) with the plane. We have the map Spec \( A \setminus \{0\} \rightarrow \mathbb{P}^1_A \), described locally in each of the two coordinate charts by \( A[u_1, u_2] \rightarrow A_y, \frac{u_1}{u_2} \rightarrow \frac{x}{y} \) and \( A[u_2] \rightarrow A_x, \frac{u_2}{u_1} \rightarrow \frac{y}{x} \).

\( \tilde{X} \) is defined in \( \mathbb{P}^1_A \) by the equation \( xu_2 - yu_1 = 0 \). For example, if \( k = \mathbb{R} \), then \( \tilde{X} \) is nothing but the Möbius band.

Perhaps the most useful way of thinking about the blowing up \( \tilde{X} \) is that it is a scheme glued together from two coordinate charts

\[
\tilde{X} = \text{Spec } k \left[ u_1, \frac{u_2}{u_1} \right] \cup \text{Spec } k \left[ u_2, \frac{u_1}{u_2} \right],
\]

where the glueing is implicit in the notation.

2) Similarly, we can blow up the affine \( n \)-space at the origin. Let

\[
A = k[x_1, \ldots, x_n], \quad I = (x_1, \ldots, x_n).
\]

Then \( \mathbb{P}^{n-1}_X = \text{Proj } A[u_1, \ldots, u_n] \). \( \tilde{X} \subset \mathbb{P}^{n-1}_X \) is the subscheme defined by the equations \( x_iu_j - x_ju_i, 1 \leq i, j \leq n \). Again, \( \tilde{X} \) is covered by \( n \) coordinate charts of the form Spec \( k \left[ \frac{u_i}{u_1}, \ldots, \frac{u_{i-1}}{u_1}, u_1, \frac{u_i}{u_1}, \ldots, \frac{u_n}{u_1} \right] \).

3) Finally, the blowing up of Spec \( k[x_1, \ldots, x_n] \) along \( (x_1, \ldots, x_l) \) for \( l < n \) is the subset of \( \mathbb{P}^{l-1}_A \) defined by the equations \( x_iu_j - x_ju_i, 1 \leq i, j \leq l \). \( \tilde{X} \) is covered by \( l \) coordinate charts of the form Spec \( k \left[ \frac{u_1}{u_i}, \ldots, \frac{u_{i-1}}{u_i}, u_i, \frac{u_{i+1}}{u_i}, \ldots, \frac{u_l}{u_i}, u_{l+1}, \ldots, u_n \right] \).
Intuitively, we may think of this last construction as first blowing up the origin in $\text{Spec } k[x_1, \ldots, x_l]$ and then taking the direct product of the whole situation with $\text{Spec } k[x_{l+1}, \ldots, x_n]$.

**Another characterization of blowing up.** We now give yet another description of the blowing up of $\text{Spec } A$ along an ideal $I$, equivalent to the above, but without reference to any particular ideal base $(f_1, \ldots, f_n)$.

First, we need a general fact about closed subschemes of $\text{Proj } G$ for a graded algebra $G$. As mentioned earlier, such closed subschemes are defined by homogeneous ideals of $G$. Surprisingly, while for any ring $A$, by definition, distinct ideals of $A$ define distinct closed subschemes of $\text{Spec } A$, it is possible for two distinct homogeneous ideals of $G$ to define the same closed subscheme of $\text{Proj } G$. The next exercise gives an exact characterization of pairs of homogeneous ideals of $G$ define the same closed subscheme of $\text{Proj } G$.

Let $G$ be a graded algebra. Let $\{x_\lambda\}_{\lambda \in \Lambda}$ be a set of homogeneous, positive degree generators of $G$ over $G_0$. Let $I$ be a homogeneous ideal of $G$.

**Definition 13.5.** The saturation of $I$ is the homogeneous ideal of $G$, defined by

$$\bar{I} = \{ y \in G \mid \forall \lambda \in \Lambda \exists n_\lambda \in \mathbb{N} \text{ s.t. } yx_\lambda^{n_\lambda} \in I \}.$$  

$I$ is said to be saturated if $I = \bar{I}$.

**Exercise 13.6.**

1. Show that the definition of $\bar{I}$ does not depend on the choice of the set of generators $\{x_\lambda\}_{\lambda \in \Lambda}$.
2. Show that $\bar{I}$ is saturated.
3. Show that for any homogeneous ideal $I$, $\sqrt{I} = \bar{I}$ (this shows that at least $I$ and $\bar{I}$ define the same closed subset of $\text{Proj } G$).
4. Let $I$ and $J$ be two homogeneous ideals of $G$. Show that the closed subschemes $V(I)$ and $V(J)$ of $\text{Proj } G$ coincide if and only if $\bar{I} = \bar{J}$. In particular, $\bar{I}$ is the greatest homogeneous ideal of $G$ which defines the same closed subscheme as $I$.

We come back to our invariant characterization of blowing up. Let $A$ be a ring, $I$ a finitely generated ideal, as above. Then $\tilde{X} \cong \text{Proj } Gr_I A$.

Indeed, let $I = (f_1, \ldots, f_n)$. We have the obvious surjective homomorphism $\phi : A[u_1, \ldots, u_n] \to Gr_I A$, given by $u_i \mapsto f_i$, so that $\text{Proj } Gr_I A$ is a closed subscheme of $\mathbb{P}^{n-1}_A$. Furthermore, let $J = \text{Ker } \phi$. Then

$$J = \left\{ g(u) = \sum a_\alpha u^\alpha \mid \text{homogeneous polynomials such that } g(f_1, \ldots, f_m) = 0 \right\}.$$  

Let $J'$ denote the greatest homogeneous ideal having the property $\varphi(\text{Spec } A \setminus V(I)) \subset V(J')$ (by definition, $\tilde{X} = V(J')$).
Exercise 13.7. Show that $J' = \bar{J}$, so that $\text{Proj} \ Gr_1 A = \bar{X}$.

Now let $X$ be any scheme, not necessarily affine. We would like to define the notion of blowing up $X$ along an ideal. However, we run into a difficulty: it is not clear what “ideal” means in this context. The natural thing to do is to think about sheaves of ideals (which are a special case of sheaves of modules). This brings us to another central notion in the theory of schemes — that of quasi-coherent and coherent sheaves of modules.

Sheaves of modules. Coherence and quasi-coherence. Roughly speaking, quasi-coherent sheaves can be thought of as a generalization of vector bundles in topology and complex analysis, with coherent sheaves corresponding to vector bundles of finite rank.

First, we need to define tensor product for modules over a ring. For a ring $A$, a free $A$-module is a module which is isomorphic to a (possibly infinite) direct sum of copies of $A$.

Definition 13.8. Let $A$ be a ring and $M_1, M_2$ $A$-modules. The tensor product $M_1 \otimes_A M_2$ is defined to be the free module generated by the symbols $x_1 \otimes x_2$ modulo the submodule generated by all the relations of the form $(a_1 x_1 + a'_1 x'_1) \otimes x_2 - a_1 (x_1 \otimes x_2) - a'_1 (x'_1 \otimes x_2)$ and $x_1 \otimes (a_2 x_2 + a'_2 x'_2) - a_2 (x_1 \otimes x_2) - a'_2 (x_1 \otimes x'_2)$.

Note that if $M$ is an $A$-module and $B$ an $A$-algebra, then $M \otimes_A B$ has a natural structure of a $B$-module. Note also that if $\phi : M_1 \rightarrow M_2$ is a homomorphism of $A$-modules, it makes sense to talk about the induced homomorphism $\phi \otimes_A B : M_1 \otimes_A B \rightarrow M_2 \otimes_A B$.

Definition 13.9. Let $A$ be a ring, $M$ an $A$-module and $S \subset A$ a multiplicative set. The localization $M_S$ of $M$ by $S$ is defined to be $M_S = \{ \frac{x}{s} \mid x \in M, s \in S \}/\sim$, where $\sim$ is the usual equivalence relation: $\frac{u}{v} \sim \frac{u'}{v'}$ whenever there exists $u \in S$ such that $u(xt - ys) = 0$. $M_S$ has a natural structure of an $A_S$-module (hence also of an $A$-module).

Exercise 13.10. Keep the notation of Definition 12.6. Show that $M_S = M \otimes_A A_S$.

Let $X$ be a topological space. Let $\mathcal{O}$ be a sheaf of rings on $X$.

Definition 13.11. A sheaf of $\mathcal{O}$-modules is a sheaf $\mathcal{F}$ of abelian groups on $X$, such that for each open set $U \subset X$, $\mathcal{F}_U$ has the structure of an $\mathcal{O}_U$-module, and for any two open sets $V \subset U$, the restriction map $\mathcal{F}_U \rightarrow \mathcal{F}_V$ is a homomorphism of $\mathcal{O}_U$-modules (note that $\mathcal{O}_V$, and hence also $\mathcal{F}_V$ are naturally $\mathcal{O}_U$-modules via the restriction map $\mathcal{O}_U \rightarrow \mathcal{O}_V$).

Example 13.12. Let $X = \text{Spec} A$ be an affine scheme. As usual, we denote by $\mathcal{O}$ the structure sheaf of $X$. Let $M$ be an $A$-module. We define a sheaf $\mathcal{M}$ of $\mathcal{O}$-modules as follows: for each open set $U$, put $\mathcal{M}_U = M \otimes_A \mathcal{O}_U$. The restriction maps $\mathcal{M}_U \rightarrow \mathcal{M}_V$ are induced in the obvious way from the restriction maps of $\mathcal{O}$.
Definition 13.13. Let $X$ be a scheme and let $\mathcal{O}$ denote the structure sheaf of $X$. A sheaf $\mathcal{F}$ of $\mathcal{O}$-modules is said to be quasi-coherent if there exists an affine open covering $X = \bigcup_{\lambda \in A} U_{\lambda}$ such that the restriction of $\mathcal{F}$ to each $U_{\lambda}$ is of the form described in Example 13.12. $\mathcal{F}$ is said to be coherent if, in addition, $\mathcal{F}_{U}$ is a finitely generated $\mathcal{O}_{U}$-module for each open set $U$.

Example 13.14. The structure sheaf $\mathcal{O}$ of $X$ itself is a coherent sheaf of modules.

Remark 13.15. Let $X$ be a scheme. There is a natural 1-1 correspondence between quasi-coherent ideal sheaves on $X$ and closed subschemes of $X$. Namely, let $\mathcal{I}$ be a quasi-coherent ideal sheaf. Let $X = \bigcup U_{\lambda}$ be the affine open covering of Definition 13.13. Then $V(\mathcal{I}_{U_{\lambda}})$ defines a closed subscheme of $Y_{\lambda} \subset U_{\lambda}$. $\bigcup_{\lambda} Y_{\lambda}$ is a closed subscheme of $X$, which we will denote by $V(\mathcal{I})$.

Let $X = \bigcup_{i} \text{Spec } A_{i}$ be a scheme, $\mathcal{I}$ a coherent ideal sheaf on $X$. We can now define the blowing up $\pi : \widetilde{X} \rightarrow X$ of $X$ along $\mathcal{I}$. Namely, let $I_{i}$ denote the ideal of sections of $\mathcal{I}$ on $\text{Spec } A_{i}$; $I_{i}$ is an ideal of $A_{i}$. Let $\widetilde{X}_{i} \rightarrow \text{Spec } A_{i}$ denote the blowing up of $\text{Spec } A_{i}$ along $I_{i}$. It is a routine matter to show that all the $\widetilde{X}_{i}$ can be glued together in a natural way to give the blowing up $\pi : \widetilde{X} \rightarrow X$ of $X$ along $\mathcal{I}$. Note that there is no reason to expect $\pi$ to factor through the projective space $\mathbb{P}^{n}_{X}$ for any $n$; we only know that such a factorization exists locally on $X$.

We will now give yet another characterization of blowing up, this time by a universal mapping property.

Let $\pi : X \rightarrow Y$ be a morphism of schemes and $\mathcal{I}$ a quasi-coherent ideal sheaf on $Y$. Let $X = \bigcup_{i,j \in \Phi} \text{Spec } B_{ij}$ and $Y = \bigcup_{i} \text{Spec } A_{i}$ be the open coverings appearing in the definition of morphism (Definition 12.3). For each $i$ and each $j \in \Phi$, we have a homomorphism $A_{i} \rightarrow B_{ij}$. Let $\pi^{*} \mathcal{I}$ denote the ideal sheaf on $X$ whose ideal sections over $\text{Spec } B_{ij}$ is $I_{i}B_{ij}$. $\pi^{*} \mathcal{I}$ is a quasi-coherent ideal sheaf on $X$.

Let $X$ be a scheme and $\mathcal{I}$ a coherent ideal sheaf on $X$. The idea, which we now explain in detail, is that the blowing up $\pi : \widetilde{X} \rightarrow X$ of $X$ along $\mathcal{I}$ is characterized by the universal mapping property with respect to making $\mathcal{I}$ invertible (Definition 13.19 below).

If $I = (x)$ is a principal ideal in a ring $A$, then $I \cong \frac{A}{\text{Ann } x}$ as $A$-modules. If, in addition, $x$ is not a zero divisor in $A$, then $I \cong A$ as $A$-modules. Recall that an ideal $I$ is said to be locally principal if it is principal in every local ring $A_{P}$, $P \in \text{Spec } A$. The next Lemma and its Corollary show that given a locally principal ideal in a ring $A$ (not necessarily Noetherian), Spec $A$ can be covered by finitely many affine open charts of the form $\text{Spec } A_{g}$, such that $IA_{g}$ is principal for each $g$.

Example 13.16. Let $A$ be a Dedekind domain (that is, a one-dimensional regular ring, such as $\mathbb{Z}[\sqrt{5}]$), and $I$ an ideal of $A$ of height 1. Then $I$ is locally principal (since $A$ is a regular 1-dimensional ring), but it need not be principal (Remark
Lemma 13.17. Let $I$ be a locally principal ideal in a ring $A$. Let $\mathbf{f} = \{f_\lambda\}_{\lambda \in \Lambda}$ be a set of generators of $I$. Then for every $P \in \text{Spec } A$, $IA_P = (f_\lambda)A_P$ for some $\lambda$.

Proof. Replacing $A$ by $A_P$, we may assume that $A$ is local with maximal ideal $P$ and that $I$ is principal. Let $x$ be a generator of $I$. Then for every $\lambda \in \Lambda$ there exists $a_\lambda \in A$ such that $f_\lambda = a_\lambda x$. If $a_\lambda \in P$ for all $\lambda \in \Lambda$, then $x \in I = fA \subset P(x)$, hence $x = yx$ for some $y \in P \implies (1-y)x = 0 \implies x = 0 \implies I = (0)$ and there is nothing to prove. Hence we may assume that one of the $a_\lambda$ is a unit in $A$. Then $x = a_\lambda^{-1}f_\lambda$ and $J = (f_\lambda)$, as desired. \hfill \Box

Corollary 13.18. Let $I$ be a locally principal ideal in a ring $A$ and let $\mathbf{f} = \{f_\lambda\}_{\lambda \in \Lambda}$ be a set of generators of $I$. Then there exists a finite subset $\{f_1, \ldots, f_n\} \subset \mathbf{f}$ and a finite open affine cover $\text{Spec } A = \bigcup_{i=1}^n \text{Spec } A_{g_i}$ such that $IA_{g_i} = (f_i)A_{g_i}$, $1 \leq i \leq n$.

Proof. By Lemma 13.17,

\begin{equation}
\sum_{\lambda \in \Lambda} ((f_\lambda) : I) = A
\end{equation}

(otherswise, localizing at a maximal ideal containing $\sum_{\lambda \in \Lambda} ((f_\lambda) : I)$, we would find a localization $A_P$ of $A$ such that $((f_\lambda) : I)A_P \neq A_P$ for any $\lambda$, that is, $I$ is not generated by any of the $f_\lambda$). By (13.2), 1 belongs to some finite sum of ideals of the form $(f_\lambda) : I$, $\lambda \in \Lambda$. Hence there exists a finite subset $\{f_1, \ldots, f_n\} \subset \mathbf{f}$ and $g_i \in (f_i) : I$, $1 \leq i \leq n$, such that $\sum_{i=1}^n g_i = 1$. Then $IA_{g_i} = (f_i)A_{g_i}$ and no prime of $A$ can contain all of the $g_i$, so that $\text{Spec } A = \bigcup_{i=1}^n \text{Spec } A_{g_i}$ is the desired open cover. \hfill \Box

Definition 13.19. Let $I$ be a locally principal ideal in a ring $A$. $I$ is said to be invertible if $\text{Spec } A$ can be covered by affine charts of the form $A_g$, $g \in A$, such that for each $g$, $IA_g = (x_g)A_g$, where $x_g \in A_g$ is not a zero divisor. Of course, if $A$ is a domain, then invertible and locally principal are the same thing (in that case, both properties are equivalent to saying that $II^{-1} = A$ by Exercise 10.21, hence the name “invertible”). Note also that if $I$ is invertible, then we can strengthen Corollary 13.18 to say, in addition, that for each $i$, $1 \leq i \leq n$, $f_i$ is not a zero divisor in $A_{g_i}$. This fact is obtained by the same argument as Corollary 13.18, if we replace (13.2) by the stronger equality $\sum_{\lambda \in \Lambda} (\text{Ann } (f_\lambda))(f_\lambda) : I = A$.

The point is that an element $x \in A$ is not a zero divisor if and only if $\text{Ann } x = (0) \iff \text{Ann } \text{Ann } x = A$.

Definition 13.20. An ideal sheaf $\mathcal{I}$ on a scheme $X$ is locally principal if there exists an affine open cover $X = \bigcup_i U_i$, $U_i = \text{Spec } A_i$, such that $\mathcal{I}_{U_i}$ is a principal
ideal of $A_i$ for all $i$. $\mathcal{I}$ is said to be **invertible** if each of the $\mathcal{I}_U$, is principal and generated by an element which is not a zero divisor.

Again, if $X$ is integral, then invertible and locally principal are the same thing.

**Example 13.21.** Let $A$ be a ring and $I = (f_1, \ldots, f_n)$ a finitely generated ideal of $A$. Let $\tilde{X} = \text{Gr}_I A$ be the blowing up of Spec $A$ along $I$. By definition, $\tilde{X} = \bigcup_{i=1}^{n} U_i$, where $U_i = \{ P \in \text{Proj} \ Gr_I A \ | \ f_i \notin P \}$. Then $U_i = \text{Spec} ((\text{Gr}_I A)_{f_i})_0$, where $f_i$ is viewed as an element of degree 1 in $\text{Gr}_I A$. Localization by $f_i$ annihilates $\text{Ann}(f_i)$, so that $f_i$ is not a zero divisor in $(\text{Gr}_I A)_{f_i}$. Then we may identify $(\text{Gr}_I A)_{f_i} \equiv A_{\text{Ann}(f_i)}[f_1 f_i, \ldots, f_i^{-1} f_i, f_i+1 f_i, \ldots, f_n f_i]$, where $f_i$ in the denominator makes sense since $f_i$ is not a zero divisor in this chart. Thus

$$U_i = \text{Spec} \ A_{\text{Ann}(f_i)}[f_1 f_i, \ldots, f_i^{-1} f_i, f_i+1 f_i, \ldots, f_n f_i].$$

We have

$$I \frac{A}{\text{Ann}(f_i)}[f_1 f_i, \ldots, f_i^{-1} f_i, f_i+1 f_i, \ldots, f_n f_i] = \frac{A}{\text{Ann}(f_i)}[f_1 f_i, \ldots, f_i^{-1} f_i, f_i+1 f_i, \ldots, f_n f_i]$$

$$= (f_1, \ldots, f_n) \frac{A}{\text{Ann}(f_i)}[f_1 f_i, \ldots, f_i^{-1} f_i, f_i+1 f_i, \ldots, f_n f_i],$$

so that $\pi^* I$ is invertible on $\tilde{X}$. Since we are dealing with a local property, this statement remains valid even if $X$ is not affine. In other words, if $\pi : \tilde{X} \to X$ is the blowing up of a coherent ideal sheaf $\mathcal{I}$, then $\pi^* \mathcal{I}$ is invertible.

We now point out that this property is also sufficient to characterize blowing up. Namely, the blowing up $\pi$ of $\mathcal{I}$ is the smallest (in the sense explained in Theorem 13.22 below) projective morphism such that $\pi^* \mathcal{I}$ is invertible. More precisely, we have the following theorem.

**Theorem 13.22 (the universal mapping property of blowing up [2, Proposition II.7.14, p. 164]).** Let $X$ be a scheme, $\mathcal{I}$ a coherent ideal sheaf on $X$ and $\pi : \tilde{X} \to X$ the blowing up of $\mathcal{I}$. Let $\rho : Z \to X$ be another morphism such that $\rho^* \mathcal{I}$ is invertible. Then $\rho$ factors through $\tilde{X}$ in a unique way.

The Noetherian hypothesis appearing in the statement of this result in [2] is superfluous.

**Proof of Theorem 13.22.** Because of the asserted uniqueness of the factorization, the problem is local on $X$: once we solve the problem over each affine chart of $X$, uniqueness will guarantee that the resulting morphisms will patch together nicely.
Thus we may assume that $X = \text{Spec } A$ is affine and $I = (f_1, \ldots, f_n) \subset A$ is a finitely generated ideal. Similarly, according to Corollary 13.18, we may assume that $Z = \text{Spec } B$ is affine, $IB = (f_i)B$ for some $i$, $1 \leq i \leq n$, and that $f_i$ is not a zero divisor in $B$. Write

$$\tilde{X} = \bigcup_{j=1}^{n} \text{Spec } \frac{A}{\text{Ann}(f_j)} \left[ \frac{f_1}{f_j}, \ldots, \frac{f_{j-1}}{f_j}, \frac{f_{j+1}}{f_j}, \ldots, \frac{f_n}{f_j} \right].$$

By assumption, we are given a homomorphism $\rho^* : A \to B$. It is sufficient to check that $\rho^*$ factors in a unique way through $\frac{A}{\text{Ann}(f_j)} \left[ \frac{f_1}{f_j}, \ldots, \frac{f_{i-1}}{f_j}, \frac{f_{i+1}}{f_j}, \ldots, \frac{f_n}{f_j} \right]$, where $i$ is as above. Since $IB = (f_i)B$ for some $i$, for each $j \neq i$ there exists $b_j \in B$ such that $f_j = b_j f_i$. Since $f_i$ is not a zero divisor in $B$, $b_j$ is unique. Hence the unique homomorphism $\psi : \frac{A}{\text{Ann}(f_j)} \left[ \frac{f_1}{f_i}, \ldots, \frac{f_{i-1}}{f_i}, \frac{f_{i+1}}{f_i}, \ldots, \frac{f_n}{f_i} \right] \to B$, factoring $\rho^*$ is given by

$$\psi \left( \frac{f_j}{f_i} \right) = b_j.$$

The fact that (13.3) gives a well defined homomorphism $\psi$ follows easily from the fact that $f_i$ is not a zero divisor. $\Box$

Let $X$ be an integral scheme. We saw that every blowing up of $\tilde{X} \to X$ is a birational and projective morphism. Next, we show that, conversely, every birational, projective morphism $\tilde{X} \to X$ is locally the blowing up of some coherent ideal sheaf, so that blowings up and birational projective morphisms are essentially the same thing.

**Theorem 13.23.** Let $X$ be an integral scheme and $\pi : \tilde{X} \to X$ a birational projective morphism. Then there exists an open affine cover $X = \bigcup_i \text{Spec } A_i$ and finitely generated ideals $I_i \subset A_i$ such that for each $i$, $\pi|_{\pi^{-1}(A_i)}$ is the blowing up of $I_i$.

**Proof.** Since the problem is local on $X$, we may assume that $X = \text{Spec } A$ is affine and that $\tilde{X}$ is a closed subscheme of $\mathbb{P}^{n-1}_A$ for some $n$. Let $x_1, \ldots, x_n$ be the homogeneous coordinates on $\mathbb{P}^{n-1}$. For $1 \leq i \leq n$, let

$$U_i = \text{Spec } A \left[ \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right].$$

Since $V_i = \tilde{X} \cap U_i$ is a closed subscheme of $U_i$ and an open subscheme of $\tilde{X}$, Spec $\mathcal{O}_{V_i}$ is an affine open subscheme of $\tilde{X}$ and $\mathcal{O}_{V_i}$ is a homomorphic image of $A \left[ \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right]$. For $1 \leq i, j \leq n$, $j \neq i$, let $f_{ij}$ denote the image of $\frac{x_j}{x_i}$ in $\mathcal{O}_{V_i}$. Let $K$ denote the field of fractions of $A$. Since $\pi$ is birational, all the $f_{ij}$ are elements of $K$. By definition, we have the following relations among the $f_{ij}$, for all the allowed values of $i$, $j$, and $l$:

$$f_{ij} f_{ji} = 1$$

$$f_{ij} f_{jl} f_{li} = 1.$$
To complete the proof of the Theorem, it is sufficient to find \( f_1, \ldots, f_n \in A \) such that \( f_{ij} = \frac{f_i}{f_j} \) for all \( i, j \) (for then \( \pi \) is the blowing up of \( I = (f_1, \ldots, f_n) \)). To construct \( f_1, \ldots, f_n \), let \( g \) be a common denominator of the \( f_{ij} \), that is, an element of \( A \) such that \( gf_{ij} \in A \) for all \( i, j \). Put \( f_1 = g, f_i = gf_{ii} \) for \( 2 \leq i \leq n \). Then for all the allowed \( i, j \), we have \( \frac{f_i}{f_j} = \frac{gf_{ii}}{f_{jj}} = f_{ij} \) by (13.4), as desired. \( \square \)

Let \( X \) be a scheme, \( \mathcal{I} \) a coherent ideal sheaf on \( X \), \( \pi : \tilde{X} \to X \) the blowing up along \( \mathcal{I} \). The closed subscheme \( Y = V(\mathcal{I}) \) is called the **center** of the blowing up \( \pi \). We will sometimes refer to \( \pi \) as “the blowing up along \( Y \)”. The coherent ideal sheaf \( \pi^* \mathcal{I} \) defines the closed subscheme \( \pi^{-1}(Y) \subset \tilde{X} \). Since \( \pi^* \mathcal{I} \) is invertible, \( \pi^{-1}(Y) \) has codimension 1 in \( \tilde{X} \) in the case when \( \tilde{X} \) is Noetherian (Corollary 8.11). Codimension 1 subschemes are called **divisors**. The subscheme \( \pi^{-1}(Y) \) is called the **exceptional divisor** of the birational map \( \pi \). By definition, \( \pi \) induces an isomorphism \( \tilde{X} \setminus \pi^{-1}(Y) \cong X \setminus Y \).

**Strict Transforms.** Let \( Z \) be a scheme, \( \mathcal{I} \) a coherent ideal sheaf on \( Z \). Let \( \iota : X \hookrightarrow Z \) be a closed subscheme of \( Z \) with its natural inclusion \( \iota \). Let \( \pi : \tilde{Z} \to Z \) be the blowing up of \( \mathcal{I} \). Let \( \tilde{X} := \pi^{-1}(X \setminus V(\mathcal{I})) \subset \tilde{Z} \), where “"" denotes the closure in the Zariski topology.

**Definition 13.24.** \( \tilde{X} \) is called the **strict transform** of \( X \) under \( \pi \).

Of course, \( \tilde{X} \subset \pi^{-1}(X) \subset \tilde{X} \cup \pi^{-1}(V(\mathcal{I})) \). To distinguish it from the strict transform, \( \pi^{-1}(X) \) is sometimes called the **total transform** of \( X \) under \( \pi \).

**Theorem 13.25.** \( \tilde{X} \) together with the induced morphism \( \rho : \tilde{X} \to X \) is nothing but the blowing up of the coherent ideal sheaf \( \iota^* \mathcal{I} \) on \( X \).

**Proof.** Again, the problem is local on \( Z \), so that we may assume that \( Z = \text{Spec } B \) is affine and \( I \subset B \) is a finitely generated ideal. It is sufficient to prove that \( \tilde{X} \) has the universal mapping property of blowing up (that is, \( \tilde{X} \) satisfies the conclusion of Theorem 13.22). Here we are using a general fact about universal mapping properties: any object satisfying the conclusion of Theorem 13.22 is necessarily unique up to a canonical isomorphism, since given any two such objects Theorem 13.22 guarantees the existence of a canonical morphism in both directions.

Let \( J \) denote the defining ideal of \( X \) in \( B \), \( A = \frac{B}{J}, \ I = IA \). By definition, \( \iota^* \mathcal{I} \) is the coherent ideal sheaf \( \mathcal{I} \) on \( \text{Spec } A \) given by the ideal \( I \). Let \( \iota \) be the inclusion map \( \iota : \tilde{X} \to \tilde{Z} \).

First, we show that \( \rho^* \mathcal{I} \) is invertible. Let \( I = (f_1, \ldots, f_n) \). Let \( \tilde{f}_i \) denote the natural image of \( f_i \) in \( A \). Then \( \tilde{I} = (\tilde{f}_1, \ldots, \tilde{f}_n) \). Cover \( \tilde{Z} \) by open affine charts: \( \tilde{Z} = \bigcup_{i=1}^n \text{Spec } B_i \), where \( B_i = \frac{B}{\mathcal{A}_{mn} f_i} \left[ \frac{f_1}{f_i}, \ldots, \frac{f_n}{f_i} \right] \). For \( 1 \leq i \leq n \), let \( V_i = \tilde{X} \cap \text{Spec } B_i \). Then \( V_i \) is a closed subscheme of \( \text{Spec } B_i \); let \( J_i \) denote the defining ideal of \( V_i \) in \( B_i \). Let \( A_i = \text{Spec } B_i/J_i \), so that \( V_i = \text{Spec } A_i \). For each \( i \) we have a commutative
diagram
\[
\begin{array}{ccc}
B_i & \longrightarrow & A_i \\
\uparrow & & \uparrow \\
\downarrow & & \downarrow \\
B & \longrightarrow & A
\end{array}
\]

Now, since \( IB_i = (f_i)B_i \) for each \( i \), \( IA_i = IA = (f_i)A_i \) is principal. To show that \( f_i \) is not a zero divisor in \( A_i \), suppose \( f_i \bar{x} = 0 \) for some \( \bar{x} \in A_i \). Let \( x \) be any representative of \( \bar{x} \) in \( B_i \). Then \( f_i x \in J_i \), so that \( x \in J_i(B_i)_{f_i} \). Now, \( \text{Spec}(B_i)_{f_i} = U_i \setminus V(\pi^*I) \) and \( J_i B_{f_i} \) is the defining ideal of \( V_i \setminus V(\pi^*I) \) in \( B_{f_i} \).

Since \( \pi \) induces an isomorphism \( \tilde{Z} \setminus V(\pi^*I) \to Z \setminus V(I) \), \( \tilde{X} \setminus V(\pi^*I) \cong X \setminus V(I) \). Hence \( V_i = \tilde{X} \cap U_i \) is the Zariski closure of \( V_i \setminus V(\pi^*I) \). Now, since \( x \) vanishes on \( V_i \setminus V(\pi^*I) \) in \( U_i \), it belongs to the ideal of its Zariski closure in \( U_i \). This proves that \( x \in J_i \), hence \( \bar{x} = 0 \), as desired. We have shown that \( \rho^* \tilde{I} \) is invertible.

Now, let \( \alpha : Y \to X \) be another morphism such that \( \alpha^* \tilde{I} \) is invertible. It remains to show that \( \alpha \) has a unique factorization \( \beta : Y \to \tilde{X} \); then we can conclude that \( \tilde{X} \) is the blowing up of \( X \) along \( \tilde{I} \) by Theorem 13.22. Since \( \alpha^* \tilde{I} = \alpha^* \iota^* \tilde{I} = (\iota \circ \alpha)^* \tilde{I} \), \( \iota \circ \alpha \) has a unique factorization \( \gamma : Y \to \tilde{Z} \) by Theorem 13.22. In view of the asserted uniqueness of \( \beta \), we may assume that \( Y = \text{Spec} C \) is affine and that \( \alpha(Y) \) is entirely contained in one of the coordinate charts of \( \tilde{Z} \), say in the first one, \( \text{Spec} B_1 \). Thus we have ring homomorphisms
\[
\begin{array}{ccc}
B_1 & \longrightarrow & C \\
\uparrow & & \uparrow \\
\downarrow & & \downarrow \\
B & \longrightarrow & A
\end{array}
\]

It remains to show that \( \gamma^* \) factors through \( A_1 \), that is, \( \gamma^*(J_1) = (0) \). By (13.5), \( \gamma^*(JB_1) = (0) \). We have natural maps \( B \to B_1 \to B_{f_1} \), so that
\[
(\gamma^* \otimes B_{f_1}) (JB_{f_1}) = 0.
\]
Since \( f_1 \) is not a zero divisor in \( B_1 \) and \( J_1 B_{f_1} = JB_{f_1} \), we have \( f_1^l J_1 \subset JB_1 \) for some \( l \in \mathbb{N} \), so that \( \gamma^*(J_1) = (0) \) by (13.6). This completes the proof of Theorem 13.25. \( \square \)

**Example 13.26.** Let \( k \) be a field, \( u, v \) independent variables. Let \( Z = \text{Spec} k[u, v], I = (u, v), X = \text{Spec} k[u, v, \frac{u}{v}] \subset Z \).

The blowing up \( \tilde{Z} \) of \( Z \) along \( I \) is covered by two affine charts: \( \tilde{Z} = \text{Spec} k[\frac{u}{v}, v] \cup \text{Spec} k[u, \frac{u}{v}] \). Let us denote the coordinates in the first chart \( U_1 \) by \( u_1, v_1 \), so that \( v = v_1, u = u_1 v_1 \). Let \( u_2, v_2 \) be the coordinates in the second chart \( U_2 \), so that \( u = u_2, v = u_2 v_2 \).

To calculate the strict transform \( \tilde{X} \) of \( U_2 \), we first find its full inverse image. This inverse image is defined by the equation \( u^2 - v^3 \), but written in the new coordinates:
\[
u^2 - v^3 = u_2^2 - u_2^3 v_2^3 = u_2^2 (1 - u_2 v_2^3).
\]
Here \( u_2 = 0 \) is the equation of the exceptional divisors. To obtain the strict transform \( \tilde{X} \), we must factor out the maximal power of \( u_2 \) out of the equation. In this case, \( \tilde{X} \cap U_2 \) is defined by \( 1 - u_2v_3^3 \). In \( U_1 \), we have
\[
u^2 - v^3 = u_1^2v_1^2 - v_1^3 = v_1^2(u_1^2 - v_1).
\]

Here \( v_1 = 0 \) is the equation of exceptional divisor, so that \( \tilde{X} \cap U_1 = V(u_1^2 - v_3) \). In particular, note that although \( X \) had a singularity at the origin, \( \tilde{X} \) is non-singular. Thus, in this example we started with a singular variety \( X \) with one singular point, blew up the singularity and found that the strict transform of \( X \) became non-singular. This procedure is called **resolution of singularities** of \( X \).

**The problem of Resolution of Singularities.**

**Definition 13.27.** A scheme \( X \) is said to be **Noetherian** if there exists a finite affine open cover \( X = \bigcup_{i=1}^{n} \text{Spec} \ A_i \), such that each \( A_i \) is a Noetherian ring.

**Definition 13.28.** A scheme \( X \) is said to be **regular** if for every \( \xi \in X \), the local ring \( \mathcal{O}_{X,\xi} \) is regular. This is equivalent to saying that \( X \) can be covered by affine charts \( \text{Spec} \ A_i \), such that each \( A_i \) is a regular ring.

**Exercise 13.29.** Let \( X = \text{Spec} k[x,y,z] \) denote the non-singular quadratic cone, embedded in \( \mathbb{A}^3_k \). Construct a resolution of singularities of \( X \) by blowing up a suitable ideal of \( k[x,y,z] \) and showing that the strict transform of \( X \) under this blowing up is regular.

**Question.** Let \( X \) be a reduced Noetherian scheme. Does there exist a sequence of blowings up \( X_n \to X_{n-1} \to \cdots \to X \) such that \( X_n \) is regular?

It is known, though we will not prove it here, that some mild technical conditions must be imposed on the ring \( A \) in order for the answer to above question to be affirmative. We have not yet developed enough tools to state all of these conditions, but we will state one of them. This condition has to do with the closedness of singular locus, and we will discuss it right now.

Let \( A \) be a Noetherian ring. The **regular locus** of \( A \) is, by definition, \( \text{Reg}(A) = \{ P \in \text{Spec} \ A \mid A_P \text{ is regular} \} \). The **singular locus** is \( \text{Sing} A = \text{Spec} A \setminus \text{Reg}(A) \).

Using Theorem 10.13, it is possible to show that if \( A \) is an algebra of finite type over a field, then \( \text{Sing} A \) is closed in \( A \). For example, if \( A = \frac{k[x_1,\ldots,x_n]}{(f_1,\ldots,f_l)} \) is a domain and \( r = \text{ht}(f_1,\ldots,f_l) \), then \( \text{Sing}(A) \) is defined in \( \text{Spec} A \) by the ideal generated by all the \( r \times r \) minors of the Jacobian matrix \( \left( \frac{\partial f_i}{\partial x_j} \right) \). Similar Jacobian criteria exist in the case of formal power series rings and complex-analytic local rings. However, there are some pathological Noetherian rings whose singular locus is not closed. This is only one of the pathologies which needs to be ruled out in order to have resolution of singularities.
Definition 13.30 [3, Chapter 13, (32.B)]. A Noetherian ring $A$ is said to be

1. $J$-0 if $\text{Reg } A$ contains a non-empty Zariski open set
2. $J - 1$ if $\text{Reg } A$ is open in $\text{Spec } A$
3. $J - 2$ if any reduced finite type $A$-algebra is $J - 1$.

Note that if $A$ is reduced, then $\text{Reg } A$ is always non-empty since it contains all the minimal primes of $A$. Thus $J$-1 implies $J$-0 for reduced rings, but not in general.

As we already mentioned, finite type algebras over a field and their localizations, formal and convergent power series rings are all known to be $J$-2. The $J$-2 condition is known to be necessary for the existence of resolution of singularities. There is one other property of Noetherian rings, called the $G$ property (for Grothendieck), which is known to be necessary, but we will state it later, in the continuation of this course.

In practice, resolution of singularities is usually achieved by locally embedding the given singular scheme $X$ in a regular scheme $Z$, constructing a sequence of blowings up of regular subschemes of the ambient regular scheme and studying the effect of these transformations on the strict transform of $X$. The following fact comes in very useful in the above setup.

Problem 13.31. Let $Z$ be a regular scheme, $Y \subset Z$ a regular subscheme. Let $\tilde{Z} \to Z$ be the blowing up along $Y$. Then $\tilde{Z}$ is regular.

The significance of resolution of Singularities:

1. There are many constructions which can only be defined for non-singular schemes, or at least which are much easier to define and study for non-singular schemes or varieties. These include Hodge theory, singular and étale cohomology, the canonical divisor, etc.

2. Inasmuch as one is interested in the problem of classification of algebraic varieties, it is natural to separate all the reduced and irreducible varieties (or integral schemes) into birational equivalence classes, that is, to group together all the schemes having the same field of rational functions. From that point of view, resolution of singularities answers a very natural question: does every birational equivalence class contain a non-singular scheme? Once this question has been answered affirmatively (as it will be in the continuation of this course), one may, on the one hand, look for birational invariants, that is, numbers associated to the given birational equivalence class and defined in terms of some non-singular model, and, on the other hand, address the finer questions about the relation between different non-singular models in the given birational equivalence class and also what can be said about the relation between resolution of singularities and the original singular variety or scheme which it dominates. This is a very active area of research, known as the Mori program; it has been the stage of some spectacular recent developments, particularly in the case of 3-dimensional varieties, or 3-folds.

3. Embedded desingularization is a somewhat stronger form of resolution of singularities, which is particularly useful for applications. Suppose that $X$ is embedded in a regular scheme $Z$. Embedded desingularization asserts that there
exists a sequence $\pi: \tilde{Z} \to Z$ of blowings up along non-singular centers, under which the total transform $\pi^{-1}(X)$ of $X$ becomes a divisor with normal crossings, which means that locally at each point of $\tilde{Z}$, $\pi^{-1}(X)$ is defined by a monomial with respect to some regular system of parameters. Geometrically, it means that at every point of $\tilde{Z}$ there exists a local coordinate system such that $\pi^{-1}(X)$ looks locally like a union of coordinate hyperplanes, counted with certain multiplicities. Thus divisors with normal crossings locally have a very simple structure. There are many situations in which it is useful to know that any closed subscheme can be turned into a divisor with normal crossings by blowing up. For example, this is used for compactifying algebraic varieties. Let $X$ be a regular algebraic variety over a field $k$, embedded in some projective space $\mathbb{P}^n_k$. If $X$ is not projective over $\text{Spec } k$, that is, if $X$ is not closed in $\mathbb{P}^n_k$, we can always consider its Zariski closure $\bar{X}$, which is, by definition, projective over $\text{Spec } k$. The problem is that even though we started with a regular $X$, $\bar{X}$ may well turn out to be singular. Resolution of singularities, together with its embedded version, assures us that, after blowing up closed subschemes, disjoint from $X$, we may embed $X$ in a regular projective variety $X'$ such that $X' \setminus X$ is a normal crossings divisor.

(4) Finally, resolution of singularities is useful for studying the singularities themselves. Namely, let $\xi \in X$ be a singularity and let $\pi: \tilde{X} \to X$ be a desingularization. We may adopt the following philosophy for studying the singularity $\xi$. All the regular points are locally the same; every singular point is singular in its own way. We may regard resolution of singularities as a way of getting rid of the local complexity of the singularity $\xi$ and turning it into global complexity of the regular scheme $\tilde{X}$. Thus some global invariant of $\tilde{X}$ may also be regarded as invariants of the singularity $\xi$. For example, if $X$ is a surface and $\xi$ is isolated, then $\pi^{-1}(\xi)$ is a collection of curves on the regular surface $\tilde{X}$. By embedded resolution, we may further assume that $\pi^{-1}(\xi)$ is a normal crossings divisor. If $\{E_i\}$, $1 \leq i \leq n$, are the irreducible components of $\pi^{-1}(\xi)$, then the intersection matrix $(E_i . E_j)$ (or, equivalently, the dual graph of the configuration $\bigcup_{i=1}^n E_i$) is an important numerical invariant associated to the singularity $\xi$. A good illustration of the usefulness of replacing local difficulties by global is Mumford’s theorem which asserts that a normal surface singularity which is topologically trivial is regular. More precisely, given a normal surface singularity $\xi \in X$ over $\mathbb{C}$, one may consider its link, which is the intersection of $X$ with a small Euclidean sphere centered at $\xi$. The link is a real 3-dimensional manifold. Mumford’s theorem asserts that if the link is simply connected, then $\xi$ is regular. At first, it seems unlikely that anything intelligent at all can be said about the link, until one realizes that the link is nothing but the boundary of a tubular neighbourhood of the collection $\bigcup_{i=1}^n E_i$ of non-singular curves on a non-singular surface. After that the link becomes relatively easy to analyze.

We now turn to the theory of valuations, which is a very important tool in the subject of resolution of singularities and in all of birational geometry.

We will start with the algebraic definition of valuations and will then move on to their beautiful geometric interpretation in birational geometry.

**Definition 14.1.** An ordered group is an abelian group Γ together with a subset $P \subset \Gamma$ (here $P$ stands for “positive elements”) which is closed under addition and such that $\Gamma = P \bigcup \{0\} \bigcup (-P)$.

**Remark 14.2.** $P$ induces a total ordering on $\Gamma$: $a < b \iff b - a \in P$. Thus an equivalent way to define an ordered group would be “a group with a total ordering, which respects addition, that is, $a > 0, b > 0 \implies a + b > 0$.”

Note that an ordered group is necessarily torsion-free.

**Examples 14.3.** $\mathbb{Z}, \mathbb{R}$ with the usual ordering are ordered groups. Any subgroup $\Gamma \subset \mathbb{R}$ is an ordered group with the induced ordering (more generally, any subgroup of an ordered group is an ordered group). $\mathbb{Z}^n$ with the lexicographical ordering (cf. Definition 14.4) are ordered groups.

**Definition 14.4.** Let $\Gamma_1, \ldots, \Gamma_r$ be ordered groups. The lexicographical ordering on their direct sum $\bigoplus_{i=1}^r \Gamma_i$ is defined by

$$(a_1, \ldots, a_n) < (b_1, \ldots, b_n) \iff \exists \ i, 1 \leq i \leq n \text{ such that } a_1 = b_1, a_2 = b_2, \ldots, a_{i-1} = b_{i-1}, a_i < b_i.$$

All the ordered groups which will appear in this course will be of the form $\bigoplus_{i=1}^r \Gamma_i$, where $\Gamma_i \subset \mathbb{R}$ for all $i$ and the total order is lexicographic.

We are now ready to define valuations. Let $K$ be a field, $\Gamma$ an ordered group. Let $K^*$ denote the multiplicative group of $K$.

**Definition 14.5.** A valuation of $K$ with value group $\Gamma$ is a surjective group homomorphism $\nu : K^* \to \Gamma$, such that for any $x, y \in K^*$,

$$(14.1) \quad \nu(x + y) \geq \min\{\nu(x), \nu(y)\} \text{ and}$$

**Exercise 14.6.** Let $K$ be a field, $\nu$ a valuation of $K$ and $x, y$ non-zero elements of $K$ such that $\nu(x) \neq \nu(y)$. Show that in this case equality must hold in (14.1), that is,

$$(13.2) \quad \nu(x + y) = \min\{\nu(x), \nu(y)\}.$$

**Example 14.7.** Let $X$ be an integral scheme, $K = K(X)$, $\xi \in X$ such that $\mathcal{O}_{X,\xi}$ is a regular local ring. As usual, let $m_{X,\xi}$ be the maximal ideal of $\mathcal{O}_{X,\xi}$. 
Define $\nu : k(x) \to \mathbb{Z}$ by

$$\nu(f) = \max\{n \mid f \in m_{X,\xi}^n, \ f \in \mathcal{O}_{X,\xi}\}.$$

$\nu$ extends from $\mathcal{O}_{X,\xi}$ to all of $K$ in the obvious way by additivity: $\nu(\frac{f}{g}) = \nu(f) - \nu(g)$. $\nu$ induces a group homomorphism because $\bigoplus m_{X,\xi}^n + 1$ is an integral domain.

In the above example, note that $\xi$ is any scheme-theoretic point; for example, it could stand for the generic point of an integral codimension 1 subscheme. In that case, the condition that $\mathcal{O}_{X,\xi}$ is non-singular holds automatically whenever $X$ is normal (Theorem 10.19).

**Remark 14.8.** Let $A$ be a domain, $K$ its field of fractions, $I \subset A$ an ideal. We can generalize the above example as follows. Define

$$\nu_I(f) = \max\{n \mid f \in I^n\}, \text{ for } f \in A.$$

In general, $\nu_I$ is a pseudo-valuation, which means that the condition of additivity in the definition of valuation is replaced by the inequality $\nu_I(xy) \geq \nu_I(x) + \nu_I(y)$. $\nu_I$ is a valuation if and only if $\bigoplus I^n$ is an integral domain (a condition which always holds if $I$ is maximal and $A/I$ is regular).

Valuations of the form $\nu_{\mathfrak{I}}$, $\mathfrak{I} \in \text{Spec } A$ are called divisorial. The reason for this name is that even if $\dim A_I > 1$, we can always blow up Spec $A$ along $I$. Let $\pi : \tilde{X} \to \text{Spec } A$ be the blowing up along $I$. Then $K(X) = K(\tilde{X})$.

The property that $\bigoplus I^n$ is a domain means that $\tilde{D} := V(\pi^* I) = \text{Proj } \bigoplus I^n$ is irreducible. Then $\mathcal{O}_{\tilde{X},\tilde{D}}$ is a regular local ring of dim 1 and $\nu_I = \nu_{\tilde{D}}$. This example illustrates an important philosophical point about valuations: a valuation is an object associated to the field $K$, that is, to an entire birational equivalence class, not to a particular model in that birational equivalence class. Thus to study a given valuation, one is free to perform blowings up until one arrives at a model which is particularly convenient for understanding the given valuation.

The next several examples will be located on the plane. Let $k$ be a field, $K = k(u, v)$ a pure transcendental extension of $k$ of degree 2. Surprisingly, valuations of $K$ are already highly non-trivial and interesting to study. They display almost all of the same properties as valuations of arbitrary fields, at least those arising in algebraic geometry.

**Example 14.9.** Let $\Gamma = (1, \pi) = \{a + b\pi \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$. Let

$$\nu(v) = 1,$$

$$\nu(u) = \pi.$$

A very important fact for us is the observation that (14.3) determines $\nu$ completely.

Indeed, by additivity, specifying $\nu(u)$ and $\nu(v)$ determines the value of every monomial: for any $\alpha, \beta \in \mathbb{N}_0$, we have $\nu(u^\alpha v^\beta) = \alpha \pi + \beta$. Now, let $f = \sum c_{\alpha\beta} u^\alpha v^\beta$. 

By (14.2), \( \nu(f) = \min\{\pi \alpha + \beta \mid c_{\alpha \beta} \neq 0 \} \). Now it is clear that \( \nu \) extends uniquely to all of \( K \) by additivity.

**Example 14.10.** Let \( K \) be as in the previous example. Let \( \Gamma = \mathbb{Z}^2 \) with lexicographical ordering. Let \( \nu(v) = (0, 1), \nu(u) = (1, 0) \).

As above, this data determines \( \nu \) completely, that is, \( \nu(u^\alpha v^\beta) = (\alpha, \beta) \) and \( \nu(\sum c_{\alpha \beta} u^\alpha v^\beta) = \min\{(\alpha, \beta) \mid c_{\alpha \beta} \neq 0 \} \).

**Exercise 14.11.** Generalize Examples 14.7 and 14.10 as follows. Let \( X \) be an integral scheme. Consider a collection \( X_1 \subseteq X \), \( X_2 \subseteq X \), \( \cdots \subseteq X_n \subseteq X \) of closed integral subschemes such that the local ring \( \mathcal{O}_{X_i, X_{i-1}} \) is regular for each \( i \). Define a valuation \( \nu : K(X)^* \to \mathbb{Z}^n \) with lexicographical ordering in a way which yields Example 14.7 if \( n = 1 \) and Example 14.10 in the case \( n = 2 \), \( X = \text{Spec} \ k[u, v], X_1 = \{(u, v)\} \) and \( X_2 = V(u) \).

Since an abelian group is automatically a \( \mathbb{Z} \)-module, it makes sense to talk about elements of \( \Gamma \) being linearly independent over \( \mathbb{Z} \). In view of the above examples, it is very easy to show that any valuation of \( k(u, v) \) such that \( \nu(u) \) and \( \nu(v) \) are linearly independent is completely determined by \( \nu(v) \) and \( \nu(u) \). We now give an example of a valuation with \( \nu(u) \) and \( \nu(v) \) linearly dependent over \( \mathbb{Z} \), such that \( \nu \) is not determined by \( \nu(u) \) and \( \nu(v) \).

**Example 14.12.** Take \( K = k(u, v) \), as before. We define a valuation \( \nu : K^* \to \mathbb{Q} \) as follows.

Let \( Q_{-1} = v, Q_0 = u \). Let \( \nu(Q_{-1}) = 1, \nu(Q_0) = \frac{3}{2} \).

Let \( p_n \) be the \( n \)-th prime number, assume that \( Q_n \) is defined and that \( \nu(Q_n) = \beta_n = \frac{2}{p_n} \) for some \( q_n \in \mathbb{N} \).

Put \( Q_{n+1} = Q_n^{p_n} - v^{q_n} \) and define \( \nu(Q_{n+1}) = q_n + \frac{1}{p_{n+1}} \). We define a valuation \( \nu \) with value group \( \mathbb{Q} \) as follows. Let \( f \in k[u, v] \). For \( \alpha \in \mathbb{Q} \), let \( P_\alpha \) denote the ideal of \( k[u, v] \) generated by all the products of the form \( \prod_{i=1}^{n} Q_i^{\gamma_i} \) with \( \sum_{i=1}^{n} \gamma_i \beta_i \geq \alpha \).

Put \( \nu(f) = \max\{\alpha \mid f \in P_\alpha\} \). It is not too hard to show that this valuation \( \nu \) has the following alternative description. Let \( t \) be a new variable. Let \( k[[t^{\mathbb{Q}^+}]] \) denote the ring of formal power series in \( t \) with exponents in the set of non-negative rational numbers, such that the set of exponents appearing in any given series is well ordered. There is an infinite increasing sequence \( \alpha_1 < \alpha_2 < \alpha_3 < \ldots \) of rational numbers and an infinite sequence of constants \( c_n \in k \), such that the denominator of \( \alpha_n \) is \( p_n \) and such that \( \nu \) is induced from the obvious \( t \)-adic valuation on \( k[[t^{\mathbb{Q}^+}]] \) via the injection

\[
v \to t
\]

\[
u(u) \to \sum_{i=0}^{\infty} c_i t^{\alpha_i}.
\]
Example 14.13. The next example may be regarded as a special case of Example 14.12, in which \( \alpha_i \in \mathbb{Z} \) for all \( i \in \mathbb{N}_0 \). Let \( K = k(u, v) \), as before.

Let \( \hat{K} = k((u, v)) \) denote the field of fractions of \( k[[u, v]] \). Choose an element \( t \in k[[u, v]] \setminus k(u, v) \) of the form \( t = u - \sum_{i=1}^{\infty} c_i v^i, \ c_i \in k^* \).

Let \( \hat{\nu} : \hat{K} \to \mathbb{Z}^2 \) be given by \( \hat{\nu}(t) = (1, 0) \), \( \hat{\nu}(v) = (0, 1) \), where we take the lexicographical order on \( \mathbb{Z}^2 \). Put \( \nu := \hat{\nu}|_K \). Since \( \hat{\nu}(K^*) \subset (0) \oplus \mathbb{Z} \), we obtain \( \nu : K^* \to \mathbb{Z} \). By definition, \( \nu(v) = 1 \). Since \( \hat{\nu}(u-v(c_1+c_2v+\ldots)) = (1,0) > (0,1) = \hat{\nu}(v(c_1+c_2v+\ldots)) \), we have \( \nu(u) = \nu(v) = 1 \). Since \( \hat{\nu}(u-c_1v-v^2(c_2+c_3v+\ldots)) = (1,0) > (0,2) = \hat{\nu}(v^2(c_2+c_3v+\ldots)) \), we have \( \nu(u-c_1v) = 2 \). Continuing in this way, we obtain

\[
\begin{align*}
\nu(u) &= \nu(v) = 1 \\
\nu(u-c_1v) &= 2 \\
\nu(u-c_1v-c_2v^2) &= 3 \\
&\vdots \\
\nu(u-c_1v-c_2v^2-\cdots-c_nv^n) &= n+1.
\end{align*}
\]

§15. Valuation rings.

Let \( K \) be a field, \( \Gamma \) an ordered group, \( \nu : K^* \to \Gamma \) a valuation of \( K \). Associated to \( \nu \) is a local subring \((R_\nu, m_\nu)\) of \( K \), having \( K \) as its field of fractions:

\[
R_\nu = \{x \in K \mid \nu(x) \geq 0\} \\
m_\nu = \{x \in K \mid \nu(x) > 0\}.
\]

Example 15.1 (Divisorial valuations). Let \( X \) be an integral scheme, \( D \subset X \) a closed integral subscheme, \( \xi \) the generic point of \( D \).

Assume that \( \mathcal{O}_{X,\xi} \) is a regular local ring of dimension 1. Let \( t \) be a generator of \( m_{X,\xi} \). Then \( K = (\mathcal{O}_{X,\xi})_t \). Indeed, any element \( f \in \mathcal{O}_{X,\xi} \) can be written as \( f = t^nu \), where \( n \in \mathbb{N} \) and \( u \) is invertible. For each \( f = t^nu \) as above, we have \( \nu_D(f) = n \). Then \( R_\nu = \mathcal{O}_{X,D} \).

In this example, \( R_\nu \) is Noetherian; in fact, it is a regular local ring of dimension 1. We already know (Theorem 10.19) that if \( (R, m, k) \) is a 1-dimensional local noetherian ring, \( R \) is regular \( \iff R \) is normal. In other words, regular one-dimensional local rings and normal one-dimensional (Noetherian) local rings are the same thing. Below, we show that Example 15.1 is typical in two ways:

1. (1) *Any* valuation ring \( R_\nu \) is normal (whether or not \( \nu \) is divisorial).
2. (2) A local domain \((R, M, k)\) is a valuation ring for a valuation with value group \( \mathbb{Z} \) if and only if it is noetherian, regular and of dimension 1.

(2) says, in other words, that *every* valuation with value group \( \mathbb{Z} \) arises in the way described in Example 15.1; regular 1-dimensional local noetherian rings and
valuation rings $R_\nu$ for $\nu$ with value group $\mathbb{Z}$ are one and the same thing. Later (Proposition 15.8), we will also prove that for any field $K$ and any valuation $\nu$ of $K$, $R_\nu$ is Noetherian if and only if the value group of $\nu$ is $\mathbb{Z}$.

**Theorem 15.2.** Let $K$ be a field and $\nu : K \to \Gamma$ any valuation of $K$. Let $R_\nu$ be the valuation ring of $\nu$. Then $R_\nu$ is normal.

*Proof.* Take any $x \in K$. Suppose $x$ is integral over $R_\nu$, that is,

\[(14.1) \quad x^n + c_1 x^{n-1} + \cdots + c_n = 0\]

for some $c_i \in R_\nu$. Then $\nu(c_i) \geq 0$ for all $i$. By (14.1), $\nu(x^n) = \nu(c_1 x^{n-1} + \cdots + c_n) \geq \min \{\nu(c_i x^{n-i})\}_{1 \leq i \leq n}$. Hence there exists $1 \leq i \leq n$, such that $\nu(x^n) \geq \nu(c_i x^{n-i}) = \nu(c_i) + (n-i)\nu(x)$. Then $\nu(x) \geq \frac{\nu(c_i)}{i} \geq 0$, so that that $x \in R_\nu$. □

**Theorem 15.3.** Let $(R, m, k)$ be a local domain, $K$ the field of fractions of $R$. The following conditions are equivalent:

1. $R$ is Noetherian, regular of dimension 1.
2. $R = R_\nu$ for some valuation $\nu : K^* \to \mathbb{Z}$.
3. There exists $t \in m$ such that every ideal of $R$ is of the form $(t^n)$, $n \geq 0$.
4. Every ideal of $R$ is a power of $m$.

*Proof of Theorem 15.3.*

(1) $\implies$ (2). Take $X = \text{Spec } R$, $D = \{m\}$ in Example 15.1.

(2) $\implies$ (3). Let $t$ be an element of $R$ such that $\nu(t) = 1$. Let $I$ be any ideal of $R$. Let $n = \min \{\nu(x) \mid x \in I\}$ (the minimum exists because all the $\nu(x)$ are non-negative integers; here we are using very strongly that $\Gamma = \mathbb{Z}$ and not, say, $\mathbb{Q}$). For any $x \in I$, $\nu\left(\frac{x}{t^n}\right) \geq 0$, hence

\[(15.1) \quad \frac{x}{t^n} \in R.\]

On the other hand, there exists $y \in I$ such that $\nu(y) = n$. Then $\nu\left(\frac{\nu^n}{y}\right) = 0$, so that $\frac{t^n}{y}$ is a unit of $R$. Thus

\[(15.2) \quad t^n \in (y) \subset I.\]

(15.1) and (15.2) prove that $I = (t^n)$.

(3) $\implies$ (1) is immediate, because by (3), $m = (t)$.

We have proved that (1)–(3) are all equivalent. It remains to show that (4) is equivalent to (1)–(3). We will show that (4) $\iff$ (3).

(3) $\implies$ (4). Clearly, $t \in m$. Then $m = (t)$ and (4) follows.

(4) $\implies$ (3). Take any $t \in m \setminus m^2$. Then $(t) = m^n$ for some $n$. Hence $(t) = m$ and (3) follows. This completes the proof of Theorem 15.3. □.
Rings $R$ satisfying (1)–(4) of Theorem 15.3 are called **discrete valuation rings**. Indeed, Theorem 15.3 says that these are precisely the valuation rings corresponding to valuations with value group $\mathbb{Z}$.

Now that we understand the case of discrete valuation rings, we describe the valuation rings in Examples 14.9, 14.10 and 14.12.

**Examples 15.4.**

1. The valuation $\nu: k(u,v)^* \to (1, \pi)$ of Example 14.9. Here

   $$R_\nu = \left(k[u^\alpha v^\beta | \alpha, \beta \in \mathbb{Z}; \alpha \pi + \beta > 0]\right)_m,$$

   where $m$ is the maximal generated by all the monomials $u^\alpha v^\beta$, $\alpha \pi + \beta > 0$.

2. The valuation $\nu: k(u,v)^* \to \mathbb{Z}^2$ (with lexicographical order) of Example 14.10. $R_\nu = \left(k[u^\alpha v^\beta | \alpha > 0 \text{ or } \alpha=0, \beta \geq 0]\right)_m$, where $m$ is the maximal ideal generated by all the monomials $u^\alpha v^\beta$ such that $\nu(u^\alpha v^\beta) \geq 0$.

3. The valuation $\nu: k(u,v)^* \to \mathbb{Q}$ of Example 14.12. Let $Q_{-1} = v$, $Q_0 = u$, $Q_1, \ldots, Q_n, \ldots$ be as in Example 14.12. Let $\beta_{-1} = 1$, $\beta_0 = \frac{3}{2}$, $\beta_n = \nu(Q_n)$ for $n \in \mathbb{N}$. Then $R_\nu = \left(k[Q_i^\gamma]_m\right)$, where $Q_i^\gamma$ ranges over all the products of the form $\prod_{i=1}^n Q_i^\gamma$, with $n \in \mathbb{N}$, $\gamma_i \in \mathbb{Z}$ and $\sum \gamma_i \beta_i \geq 0$, and where $m$ is the maximal ideal generated by all those $\prod_{i=1}^n Q_i^\gamma$ such that $\sum \gamma_i \beta_i > 0$.

Notice that none of the valuation rings in these three examples are Noetherian.

Theorem 15.3 gives several equivalent characterizations of discrete valuation rings. Next, we would like to characterize arbitrary valuation rings. In other words, we pose the questions: given a local domain $(R, m)$ with field of fractions $K$, when does there exist a valuation $\nu$ of $K$ such that $R = R_\nu$?

In the next theorem, we will give three criteria, each of which is equivalent to the existence of such a $\nu$. For geometric applications, the most useful one is the criterion in terms of birational domination, which we will now define.

**Definition 15.5.** Let $(R_1, m_1)$, $(R_2, m_2)$ be two local domains with the same field of fractions $K$. We say that $R_2$ **birationally dominates** $R_1$, denoted $R_1 < R_2$, if $R_1 \subset R_2$ and $m_1 = m_2 \cap R_1$.

Another way of phrasing Definition 15.5 is to say that there is a natural map $\pi: \text{Spec } R_2 \to \text{Spec } R_1$, such that $\pi(m_2) = m_1$. For example, let $X$ be an integral scheme and $\pi: X' \to X$ a blowing up of $X$. Let $\xi \in X$, $\xi' \in X'$ be such that $\xi = \pi(\xi')$. Then $\mathcal{O}_X, \xi < \mathcal{O}_{X', \xi'}$.

**Theorem 15.6.** Let $(R, m)$ be a local domain with field of fractions $K$. The following conditions are equivalent:

1. $R = R_\nu$ for some valuation $\nu: K^* \to \Gamma$
2. for any $x \in K^*$, either $x \in R$ or $\frac{1}{x} \in R$ (or both)
3. the ideals of $R$ are totally ordered by inclusion
4. $(R, m)$ is maximal (among all the local subrings of $K$) with respect to birational domination.
Proof. (1) ⇒ (2). Suppose \( R = R_\nu \) for some \( \nu \). Take any \( x \in K^* \). Then 
\[ \nu(x) + \nu \left( \frac{1}{x} \right) = \nu \left( x \cdot \frac{1}{x} \right) = \nu(1) = 0. \]
Hence either \( \nu(x) \geq 0 \) or \( \nu \left( \frac{1}{x} \right) \geq 0 \). This proves that either \( x \in R_\nu \) or \( \frac{1}{x} \in R_\nu \), as desired.

(2) ⇒ (3). Suppose the ideals of \( R \) are not totally ordered by inclusion. Then there exist ideals \( I_1, I_2 \subset R \) such that \( I_1 \nsubseteq I_2 \) and \( I_2 \nsubseteq I_1 \). Take \( a \in I_1 \setminus I_2 \), \( b \in I_2 \setminus I_1 \). By assumption, either \( \frac{a}{b} \in R \) or \( \frac{b}{a} \in R \). Say, \( \frac{a}{b} \in R \). Then \( b \in I_2 \), \( \frac{a}{b} \in R \Rightarrow a = b \cdot \frac{a}{b} \in I_2 \), which gives the desired contradiction.

(3) ⇒ (1). We are given that the ideals of \( R \) are totally ordered by inclusion and we must construct a valuation \( \nu \) of \( K \), such that \( R = R_\nu \). First, we describe the value group of \( \nu \).

Let \( \Phi \) denote the set of all principal ideals of \( R \) (other than \( R \) itself), with the operation of multiplication.

By assumption \( \Phi \) is totally ordered by the order relation \( I_1 < I_2 \) if and only if \( I_2 \subset I_1 \). Moreover, if \( \alpha, \beta \in \Phi \) and \( \alpha < \beta \), then there exists \( \gamma \in \Phi \) such that \( \gamma + \alpha = \beta \): indeed, write \( \alpha = (a) \), \( \beta = (b) \), with \( a, b \in R \). \( \alpha < \beta \) means \( (b) \subset (a) \), that is, there exists \( x \in R \) such that \( b = ax \). If we set \( \gamma = (x) \), we have \( \gamma + \alpha = \beta \) in \( \Phi \).

Let \( \Gamma = \Phi \bigsqcup \{0\} \bigsqcup (-\Phi) \). It is easy to check that the operation of \( \Phi \) extends to \( \Gamma \) and that \( \Gamma \) becomes an ordered group under this operation. For \( x \in R \), define \( \nu(x) = (x) \in \Phi \). This defines a map \( \nu : R^* \to \Phi \). Extend \( \nu \) to all of \( K \) by additivity. This gives the desired valuation \( \nu : K^* \to \Gamma \). We leave details to the reader.

(2) ⇒ (4). Let \( (R', m') \) be a local domain with field of fractions \( K \) such that \( (R, m) < (R', m') \). Suppose \( R \subsetneq R' \). Take \( x \in R' \setminus R \). Then, by assumption, \( \frac{1}{x} \in R \Rightarrow \frac{1}{x} \in m \Rightarrow \frac{1}{x} \in m' \) (since \( R < R' \) ⇒ \( x \notin R' \)), which is a contradiction.

(4) ⇒ (2). Suppose there is \( x \in K^* \) such that \( x \notin R \) and \( \frac{1}{x} \notin R \).

Consider the birational extension \( R \subset R[x] \). If there exists a maximal ideal \( m' \) in \( R[x] \), containing \( mR[x] \), we would have \( R < R[x]_{m'} \), which contradicts the hypothesis.

Hence we may assume that \( mR[x] \) is not contained in any maximal ideal of \( R[x] \), that is,

\[ mR[x] = R[x]. \]

Applying the same reasoning to \( \frac{1}{x} \) instead of \( x \), we obtain

\[ mR \left[ \frac{1}{x} \right] = R \left[ \frac{1}{x} \right]. \]

(15.3)–(15.4) mean that \( 1 \in mR[x] \) and \( 1 \in mR[\frac{1}{x}] \), that is,

\[ 1 = a_0 + a_1 x + \cdots + a_n x^n \quad \text{for some } a_i \in m \]

\[ 1 = b_0 + b_1 \frac{1}{x} + \cdots + b_l \frac{1}{x}^l \quad \text{for some } b_i \in m. \]
Choose expressions (15.5)–(15.6) so that both $n$ and $l$ are the smallest possible. Say, $l \leq n$. Multiply (15.6) by $x^l$. We obtain:

$$x^l = b_0x^l + b_1x^{l-1} + \cdots + b_l,$$

so that

(15.7) $0 = x^l + \frac{b_1}{b_0 - 1}x^{l-1} + \cdots + \frac{b_l}{b_0 - 1}.$

Multiply (15.7) by $a_n x^{n-l}$ and subtract it from (15.5). We obtain a relation of the form (15.5), but with a smaller $n$. This is a contradiction, and the proof of Theorem 15.6 is complete. □

**Remark 15.7.** It is clear from the proof of (3) $\implies$ (1) that the valuation ring $R_\nu$ completely determines $\nu$.

**Proposition 15.8.** Let $\nu : K^* \to \Gamma$ be a valuation. Then $R_\nu$ is Noetherian $\iff \Gamma \simeq \mathbb{Z}$.

**Proof.** $\Leftarrow$ is contained in the (2) $\implies$ (1) of Theorem 15.3.

$\Rightarrow$ Since the ideals of $R_\nu$ are totally ordered by inclusion, saying that $R_\nu$ is Noetherian is the same as saying that the set of ideals of $R_\nu$ is well ordered. If $R_\nu$ is Noetherian, then the set of ideals of $R_\nu$ is well ordered $\Rightarrow$ the set of principal ideals of $R_\nu$ is well ordered.

By (3) $\implies$ (1) of Theorem 15.6, the set of (proper) principal ideals of $R_\nu$ can be identified with the semi-group $\Phi$ of positive elements of $\Gamma$. Thus to complete the proof of the Proposition, it remains to prove the following lemma.

**Lemma 15.9.** Let $\Gamma$ be an ordered group, $\Phi$ the set of positive elements of $\Gamma$. If $\Phi$ is well ordered, then $\Phi \simeq \mathbb{N}$.

**Proof.** Let $1 := \min\{\alpha : \alpha \in \Phi\}$. For $n \in \mathbb{N}$ let $n := n \cdot 1$. This gives an inclusion $\iota : \mathbb{N} \hookrightarrow \Phi$. We want to show that $\iota$ is an isomorphism.

Suppose not. Take $\alpha \in \Phi \setminus \mathbb{N}$. For any $n \in \mathbb{N}$, we cannot have $n < \alpha < n + 1$: indeed, if $n < \alpha < n + 1$, then $0 < \alpha - n < 1$, which contradicts the definition of 1.

Hence $\alpha > n$ for any $n \in \mathbb{N}$. Let $\beta = \min\{\alpha \in \Phi \mid \alpha > n \text{ for all } n \in \mathbb{N}\}$. Then $\beta - 1 > n \ \forall \ n$. Since $\beta - 1 < \beta$, we have a contradiction. This completes the proof of Lemma 15.9 and with it of Proposition 15.8. □.


In this section we define three important integer invariants associated with valuations and investigate relations between them.

Let $\Gamma$ be an ordered group.

**Definition 16.1.** An isolated subgroup of $\Gamma$ is a subgroup $\Delta \subset \Gamma$, which is a segment in the ordering. This means: for any $a \in \Gamma$, $b \in \Delta$ such that $-b < a < b$, we have $b \in \Delta$. 

Example 16.2. \((0) \oplus \mathbb{Z}\) is an isolated subgroup of \(\mathbb{Z}^2\) with lexicographical ordering.

Remark 16.3. Let \(\nu : K^* \to \mathbb{Z}^2\) be a valuation. Then there is a one-one correspondence between isolated subgroups of \(\Gamma\) and prime ideals of \(R_\nu\), described as follows:

\[
\Delta \subset \Gamma \iff P = \{ x \in R_\nu \mid \nu(x) \notin \Delta \}.
\]

In particular, the set of isolated subgroups of \(\Gamma\) is totally ordered by inclusion (this is also very easy to show directly for any ordered group \(\Gamma\)).

Definition 16.4. For a valuation \(\nu : K^* \to \Gamma\), the rank of \(\nu\), denoted \(rk \nu\), is defined to be the number of distinct isolated subgroups of \(\Gamma\) (not counting \((0)\), but counting \(\Gamma\) itself). In other words, if \((0) \subsetneq \Delta_1 \subsetneq \Delta_2 \subsetneq \cdots \subsetneq \Delta_n = \Gamma\) is the full list of isolated subgroups of \(\Gamma\), then \(rk \nu = n\).

Remark 16.5. \(rk \nu = \dim R_\nu\).

Examples 16.6. If \(\Gamma = \mathbb{Z}^2\) with lexicographical ordering, then \(rk \nu = 2\). More generally, if \(\Gamma = \mathbb{Z}^n\) with lexicographical ordering, then \(rk \nu = n\).

In all the other examples we have encountered so far, we had \(rk \nu = 1\). In fact, \(rk \nu = 1\) if and only if there exists an injection \(\Gamma \subset R\). If \(\Gamma = \bigoplus_{i=1}^r \Gamma_i\) with \(\Gamma_i \subset R\) and the total order on \(\Gamma\) is lexicographical, then \(rk \nu = r\).

Definition 16.7. The rational rank of \(\nu\), denoted \(rat rk \nu\), is defined by \(rat rk \nu = \dim_{\mathbb{Q}} \Gamma \otimes_{\mathbb{Z}} \mathbb{Q}\).

\(rat rk \nu\) is nothing but the maximal number of elements of \(\Gamma\), which are linearly independent over \(\mathbb{Z}\).

Remark 16.8. \(rk \nu \leq rat rk \nu\) for all valuations \(\nu\).

Indeed, let \((0) \subsetneq \Delta_1 \subsetneq \Delta_2 \subsetneq \cdots \subsetneq \Delta_n = \Gamma\) be the isolated subgroups of \(\Gamma\). Pick \(x_i \in \Delta_i \setminus \Delta_{i-1}, i = 1, 2, \ldots, n\). Then \(x_1, x_2, \ldots, x_n\) are linearly independent over \(\mathbb{Z}\) in \(\Gamma\).

Example 16.9. Let \(\Gamma = (1, \pi) \subset R\). Then \(rk \nu = 1 < 2 = rat rk \nu\), since \(1, \pi\) are linearly independent over \(\mathbb{Z}\).

Definition 16.10. Let \((R, m, k)\) be a local domain with field of fractions \(K\) and \(\nu\) a valuation of \(K\). We say that \(\nu\) is centered in \(R\) if \(R < R_\nu\) (this is equivalent to saying that \(\nu(R) \geq 0\) and \(\nu(m) > 0\)).

If \(\nu\) is centered at \(R\), then we have a natural injection \(k \hookrightarrow \frac{R_\nu}{m_\nu}\).

Definition 16.11. The transcendence degree of \(\nu\) over \(k\) is

\[
tr. \deg_{k} \nu := tr. \deg \left( \frac{R_\nu}{m_\nu} / k \right).
\]

Examples:
References