Chapter 1

Varieties

In this starting chapter we adopt the viewpoint explained in the introduction and work with equations defined over $R = k$ being a field, often under the assumption that $k = \bar{k}$. The case that R is a commutative ring will be studied in the next chapter. Nevertheless, results in algebra will be presented for more general cases if no extra difficulties will arise (so that they are also be applicable in later chapters).

1. Affine and projective varieties

1.1. Affine algebraic sets. Let $A = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables over the field k. For any subset $T \subset A$ the common zero loci $Z(T) = Z(\langle T \rangle) \subset k^n = \mathbb{A}_k^n$ is called an (affine) algebraic set, where $\langle T \rangle$ is the ideal generated by T. Since

$$\bigcap Z(T_i) = Z(\bigcup T_i), \qquad Z(T_1) \cup Z(T_2) = Z(T_1 T_2),$$

and $Z(A) = Z(\{1\}) = \emptyset$, $Z(\emptyset) = k^n$, algebraic sets in k^n satisfy the axiom of closed sets for a topology. This is called the Zariski topology of k^n.

Conversely, for any subset $S \subset k^n$, the polynomials which vanish on it $I(S) := \{f \in A \mid f(a) = 0, \forall a \in S\}$ is an ideal in A. Moreover, it is readily seen to be a radical ideal $\sqrt{I} = I$. By definition we have

$$I(Z(I)) \supset \sqrt{I}, \qquad Z(I(S)) \supset \overline{S},$$

where $\overline{S}$ is the closure of S in the Zariski topology. However in general this does not gives a one to one correspondence between radical ideals and closed sets. For example if $k = \mathbb{Q}$ then $(x^2 + y^2 + 1)$ is a prime hence a radical ideal in $\mathbb{Q}[x, y]$ but $Z(x^2 + y^2 + 1) = \emptyset$ and $I(\emptyset) = A$.

There are (at least) two different ways to resolve the problem to achieve a one to one correspondence. The first method is due to Hilbert by working on algebraic closed fields ($k = \bar{k}$).

Theorem 1.1 (Hilbert Nullstellensatz)**.** *If $k = \bar{k}$, then $I(Z(I)) = \sqrt{I}$.*

From this we see easily that $Z(I(S)) = \overline{S}$ as well. Hence $Z(I) \subset Z(J) \Leftrightarrow \sqrt{I} \supset \sqrt{J}$. The theorem follows from (in fact is equivalent to)

Proposition 1.2 (Weak Nullstellensatz)**.** *If $k = \bar{k}$, then any maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a = (a_i) \in k^n$.*

Such an $\mathfrak{m}$ is clearly maximal (for any field k) since $A/\mathfrak{m} \cong k$.

Proposition 1.2 $\Longrightarrow$ Theorem 1.1. Let $g \in A$ such that $g|_{Z(I)} = 0$. We introduce one more variable x_{n+1} and consider the ideal

$$J := (I, 1 - gx_{n+1}) \subset k[x_1, \ldots, x_{n+1}].$$

Since $Z(J) = \emptyset$ in k^{n+1}, we claim that in fact $J = (1)$. If not then J is contained in some maximal ideal which by the weak Nullstellensatz must provide a common zero $(a_1, \ldots, a_{n+1}) \in Z(J)$, a contradiction.

Now we have a finite expression

$$1 = \sum h_i f_i + h_{n+1}(1 - gx_{n+1})$$

for some $f_i \in I$. Substitute $x_{n+1} = 1/g$ into it and multiply by a high power g^n to clear the denominator then leads to $g^n \in I$, that is $g \in \sqrt{I}$. □

There are many different proofs of Hilbert's theorems, either the weak or strong form. We will soon prove Proposition 1.2 using "Noether's Normalization" since the NN procedure is a very basic operation in polynomial rings which will also be useful later.

Definition 1.3. An affine variety $X \subset \mathbb{A}^n_k$ is an algebraic set which is irreducible. Namely $X \neq X_1 \cup X_2$ for two proper closed subset $X_i \subsetneq X$.

Open subset of affine varieties $U = V(I) \setminus V(J)$ are called quasi-affine varieties. They are quipped with the Zariski topology induced from k^n.

Corollary 1.4. *Affine varieties are precisely those algebraic sets defined by prime ideals. Furthermore, any algebraic set has a unique irreducible decomposition.*

Indeed, if $Z(I)$ is irreducible and $fg \in I$ then $Z(f) \cup Z(g) \supset Z(I)$ and we must have say $Z(f) \supset Z(I)$. That is, $f^n \in \sqrt{I} = I$ and then $f \in I$.

Conversely if I is prime then $Z(I) \subset Z(J) \cup Z(J') = Z(JJ')$ implies that $I \supset JJ'$. Hence we must have say $I \supset J$ and then $Z(I) \subset Z(J)$.

The decomposition into irreducible components is a formal consequence of Noetherian rings: $\sqrt{I} = \bigcap_{i=1}^r \mathfrak{p}_i$ where $\mathfrak{p}_i$ are the minimal primes in I.

Definition 1.5. For an affine algebraic set X, the reduced ring $A(X) := A/I(X)$ is called its coordinate ring. $A(X)$ is a domain $\iff X$ is a variety. Also, a finitely generated k-algebra is usually called an affine k-algebra since it can be presented as A/I for some ideal $I \subset A = k[x_1, \ldots, x_n]$.

1.2. Prime spectrum. The second method leading to the one to one correspondence is technically easier but conceptually more abstract. It works for any commutative ring A.

Let Spec A be the set of all prime ideals $\mathfrak{p} \subset A$. In the previous case $A = k[x_1, \ldots, x_n]$ with $k = \bar{k}$, points correspond precisely to the maximal ideals by the weak Nullstellensatz (Proposition 1.2) and irreducible subvarieties correspond precisely to the prime ideals (Corollary 1.4), hence Spec A can be regarded as a "space" with "fat points" corresponding to subvarieties.

To equip Spec A a topology, we define closed subset to be

$$V(T) = V(\langle T \rangle) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supset T\}$$

for any subset $T \subset A$, where $\langle T \rangle$ is the ideal generated by T. Since

$$\bigcap V(T_i) = V(\bigcup T_i), \qquad V(T_1) \cup V(T_2) = V(T_1 T_2),$$

and $V(A) = Z((1)) = \emptyset$, $V((0)) = \operatorname{Spec} A$, $V(T)$'s satisfy the axiom of closed sets for a topology. This is called the Zariski topology of Spec A.

By Krull's formula for the radical of an ideal I:

$$\sqrt{I} = \bigcap\nolimits_{\mathfrak{p} \supset I} \mathfrak{p},$$

we see easily that $V(I) \subset V(J) \iff \sqrt{I} \supset \sqrt{J}$.

Remark 1.6. This is the correspondence we seek for. The role of Nullstellensatz for varieties over $k = \bar{k}$ is eplaced by Krull's formula in this setting.

For $f \in A$, it is a bit trickier to evaluate f at a point $\mathfrak{p} \in \operatorname{Spec} A$. We will do this in the next chapter when we discuss scheme structure on Spec A. At this moment we simply notice that $f(\mathfrak{p}) = 0$ should mean $\mathfrak{p} \in V(f)$, equivalently $f \in \mathfrak{p}$. Hence $f(\mathfrak{p}) \neq 0$ is equivalent to $f \notin \mathfrak{p}$. This defines a fundamental open set

$$D(f) := V(f)^c = \operatorname{Spec} A \setminus V(f)$$

and all of them form a basis of the topology since $V(I)^c = \bigcup_{f \in I} D(f)$.

The functorial property is particularly simple in this setting. For a ring homomorphism $\phi : A \to B$ we get $\tilde{\phi} : \operatorname{Spec} B \to \operatorname{Spec} A$ via

$$\mathfrak{p} \mapsto \tilde{\phi}(\mathfrak{p}) \equiv \mathfrak{p}^c := \phi^{-1}\mathfrak{p}.$$

This is a continuous map since $\mathfrak{p} \supset I \iff \phi^{-1}\mathfrak{p} \supset \phi^{-1}I$.

Example 1.7. To see the behavior of $\tilde{\phi}$, it is enough to consider surjective and injective homomorphisms.

(1) If $\phi : A \twoheadrightarrow B$ then $B \cong A/I$ with $I = \ker \phi$ and $\operatorname{Spec} B \cong V(I) \hookrightarrow \operatorname{Spec} A$ as a closed subset.

(2) If $\phi : A \hookrightarrow B$, in general we can only conclude that $\tilde{\phi}$ is dominant, i.e. $\operatorname{im} \tilde{\phi}$ is dense. For otherwise $\operatorname{im} \tilde{\phi} \subset V(J)$ for some ideal $J \neq (0)$ in A and then ϕ factor through $A \to A/J \to B$ which can not be injective.

(3) Fundamental open subsets correspond to special localizations: $A \to A_f$ gives $\operatorname{Spec} A_f \cong D(f) \subset \operatorname{Spec} A$. Lozalizations might not be injective if A is not a domain. Even if A is a domain so that $\tilde{\phi} : A \hookrightarrow A_f$, we see that $\tilde{\phi}$ is not surjective (though dominant).

(4) What happens to $\phi : A \to A_{\mathfrak{p}}$? For A being a domain, the zero ideal (0) has the strange property that $\overline{(0)} = \operatorname{Spec} A$ (called a generic point), hence the dominance of $\operatorname{Spec} A_p \to \operatorname{Spec} A$ simply follows from $\tilde{\phi}((0)) = ((0))$ which is dense! By definition a point is closed if and only if it is a maximal ideal. Hence there is only one closed point in the local ring $A_{\mathfrak{p}}$. The detailed structure will be studied in the next chapter.

Now it is a good point to recall a nice property in integral extensions:

Proposition 1.8 (Going-up and Going-down of Cohen–Sidenberg)**.**

(i) *If $S \hookrightarrow R$ is integral, then $\operatorname{Spec} R \twoheadrightarrow \operatorname{Spec} S$. The surjectivity extends in the upward direction: if $\mathfrak{p} = \mathfrak{q}^c$ and $\mathfrak{p} \subset \mathfrak{p}'$ then there is a $\mathfrak{q} \subset \mathfrak{q}'$ such that $\mathfrak{q}'^c = \mathfrak{p}'$. Moreover, if $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ in R then $\mathfrak{q}_1^c \subsetneq \mathfrak{q}_2^c$ in S.*

(ii) *If moreover R is a domain and S is normal (i.e. integrally closed in $Q(S)$), then the surjectivity extends in the downward direction as well.*

Even in considering problems for varieties, it could happen that the setting of prime spectrum can help in various ways. Below we give such an example on the number of equations needed to describe an algebraic set.

Let k be a field and $I \subset k[x_1, \ldots, x_n]$ be an ideal. Hilbert basis theorem asserts that $I = (f_1, \ldots, f_r)$ for some finite elements $f_i \in I$. However, it gives no information on the smallest possible r. Famous examples due to Macaulay in 1916 say that r could be unbounded among all I even for $n = 3$. Thus the following result is of some conceptual interest.

Definition 1.9. The Krull dimension of a commutative ring R, denoted by $\dim R$, is the largest number $d \in \{0, 1, 2, \dots, \infty\}$ among all prime ideal chains $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_d$ in R.

Theorem 1.10 (Eisenbud-Evans 1973)**.** *Let R be a Noetherian ring of dimension $d < \infty$ and $I \subset R[x]$ be an ideal. Then there are $f_i \in I$, $i \in [1, d+1]$ such that $\sqrt{I} = \sqrt{(f_1, \dots, f_{d+1})}$.*

Proof. We may assume that R is reduced, i.e. $\sqrt{0} = 0$. Let $S \subset R$ be the multiplicative closed subset consisting of non-zero divisors. It is known that $S = R \setminus \bigcup_{i=1}^n \mathfrak{p}_i$ where $\mathfrak{p}_i$ are the minimal primes. Hence the total quotient ring decomposes into a product of fields

$$Q := R_S \cong K_1 \times \dots K_n,$$

where $K_i = Q(R/\mathfrak{p}_i)$. In particular $Q[x] \cong \prod_{i=1}^r K_i[x]$ is a principal ideal ring and we have

$$I_S = (f_1) \subset Q[x], \qquad f_1 \in I.$$

If $I = (g_1, \dots, g_r)$ then $g_i = h_i f_1 / s_i = H_i f_1 / s$ for some $s_i \in S$, $h_i \in R$, and $s := \prod s_i \in S$, $H_i \in R$. Then

$$sI \subset f_1 R[x] \subset I. \tag{1.1}$$

If s is a unit, which is always the case if $d = 0$, then we are done. If not, then $\bar{R} := R/(s)$ has $\dim \bar{R} \leq d - 1$. Hence by induction on d the ideal $\bar{I} \subset \bar{R}[x]$ satisfies $\sqrt{\bar{I}} = \sqrt{(\bar{f}_2, \dots, \bar{f}_{d+1})}$, where $f_i \in I$. This means that

$$\sqrt{R[x]s + I} = \sqrt{(s, f_2, \dots, f_{d+1})}. \tag{1.2}$$

From (1.1) we find $V(s) \cup V(I) \supset V(f_1) \supset V(I)$, and from (1.2) we get $V(s) \cap V(I) = V(s, f_2, \dots, f_{d+1})$. So

$$\begin{aligned} V(f_1, \dots, f_{d+1}) &= V(f_1) \cap V(f_2, \dots, f_{d+1}) \\ &\subset (V(s) \cup V(I)) \cap V(f_2, \dots, f_{d+1}) \\ &\subset V(s, f_2, \dots, f_{d+1}) \cup V(I) = V(I). \end{aligned}$$

Since $f_i \in I$ for all i, we conclude that $V(I) = V(f_1, \dots, f_{d+1})$. □

Corollary 1.11. *Let k be a field, then any algebraic set in k^n can be defined by no more than n equations.*

Notice that the same proof works in the variety setup. But then we get the corollary only for the case $k = \bar{k}$.

1.3. Noether normalization and Krull dimension.

Theorem 1.12. *Let R be a finitely generated integral domain over a field k with $n = \mathrm{tr.deg}_k R$. Then there are $x_1, \dots, x_n \in R$ which are algebraically independent over k such that R is integral over $k[x_1, \dots, x_n]$.*

PROOF. (After Nagata) Write $R = k[Y_1, \dots, Y_m]/\mathfrak{p}$ where $\mathfrak{p}$ is prime. If $m = n$ then $Y_i \mapsto y_i \in R$ must be algebraically independent. Hence $\mathfrak{p} = 0$ and we are done. Otherwise $m > n$ and the theorem will be proved by induction on m.

It is enough to find a subring $S \subset R$ generated by $m - 1$ elements such that R is integral over S. Since then we have two integral extensions $k[x_1, \dots, x_n] \subset S \subset R$ and the composition gives the result.

Since $m > n$, there is a $0 \neq f(Y_1, \dots, Y_m) \in \mathfrak{p}$ such that $f(y_1, \dots, y_n) = 0$. By substituting $y_j = z_j + y_1^{r_j}$, $r_j \in \mathbb{N}$ for all $j \in [2, m]$, we rewrite it as

$$f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = 0.$$

By picking r_j large we get $(y_1, z_2, \dots, z_m)$ is a root of

$$f(Y_1, Z_2 + Y_1^{r_2}, \dots, Z_m + Y_1^{r_m}) = bY_1^N + \text{lower degree terms in } Y_1,$$

where $b \neq 0$. That is, y_1 is integral over $k[z_2, \dots, z_m]$. Then $y_j = z_j + y_1^{r_j}$ is also integral over $k[z_2, \dots, z_m]$ for $j \in [2, m]$ and we are done. □

Remark 1.13. The procedure is called a Noether normalization (NN for short). If k is an infinite field then we may also use a linear change of variables $y_j = z_j + a_j y_1$, $a_j \in k$, $j \in [2, m]$ in the above proof. In this case NN is a projection to certain n-dimensional affine space $k^n \subset k^m$.

Example 1.14. Let $R = k[x, y, z]/(xy + yz + zx)$. It is not integral over $k[y, z]$. After the substitution $y = u + x$, we get

$$R \cong k[x, u, z]/(x^2 + (u + 2z)x + uz)$$

which is then integral over $k[u, z]$.

For $R = \mathbb{F}_2[x, y]/(x^2y + xy^2 + 1)$, such a linear change of variable does not work since $y = u + x$ leads to $(x + y)xy + 1 = ux(u + x) + 1$. Nevertheless using Nagata's change of variable $y = u + x^2$ we get

$$x^2y + xy^2 + 1 = x^5 + x^4 + ux^2 + u^2x + 1.$$

Hence R is integral over $\mathbb{F}_2[x, u]$

Here is our first application of Noether normalization:

Proof to the weak Nullstellensatz (Proposition 1.2). Let $\mathfrak{m}$ be a maximal ideal of $k[x_1, \dots, x_n]$. Then $R = k[x_1, \dots, x_n]/\mathfrak{m}$ is a finitely generated field over k. NN implies that R is integral over $S = k[y_1, \dots, y_r] \subset R$ with y_j's being algebraically independent. Now Cohen–Sidenberg's going-up (Proposition 1.8) implies that S is also a field. Hence $r = 0$ and $S = k = \bar{k}$, and then $R = k$ since it is integral over S. Let $a_i := \bar{x}_i \in R = k$. Then $\mathfrak{m} \supset (x_1 - a_1, \dots, x_n - a_n)$, which is maximal, hence they are equal. □

The NN procedure can be stated in a generalized form:

Theorem 1.15 (Noether Normalization)**.** *Let A be a finitely generated algebra over k and $I \subsetneq A$ be a proper ideal. Then there are two numbers $\delta \leq d$ and a polynomial subalgebra $B = k[y_1, \dots, y_d] \subset A$ such that*

(i) *A is a finitely generated B-module,*
(ii) *$I \cap B = (y_{\delta+1}, \dots, y_d)$.*

If k is an infinite field and $A = k[x_1, \dots, x_n]$ is the polynomial ring then we may choose $y_i = \sum_{k=1}^{n} a_{ik} x_k$ with $a_{ij} \in k$.

From the finite B-module structure $i : B \hookrightarrow A$ we get also that

$$j : B/I \cap B \cong k[x_1, \dots, x_\delta] \hookrightarrow A/I$$

is a finite $k[x_1, \dots, x_\delta]$-module. Thus if A is a domain then i is an integral extension and $d = \text{tr.deg}\, A$ and if I is furthermore a prime then j is also an integral extension and $\delta = \text{tr.deg}\, A/I$. The theorem will be applied mainly in these cases. But identically the same proofs works for the cases as stated.

Remark 1.16. The theorem has the following geometric interpretation. In constructing the "finite projection" $\operatorname{Spec} A \to \operatorname{Spec} B = \mathbb{A}^d$ we have the freedom to project a chosen closed subset $\operatorname{Spec} A/I$ to $\mathbb{A}^\delta \subset \mathbb{A}^n$.

In fact it is then clear at least intuitively that the theorem holds for a chain of ideals $I_1 \subset \cdots \subset I_m$ with $\dim A/I_i = d_i > d_{i+1}$, with the conclusion being $I_i \cap B = (y_{d_i+1}, \dots, y_d)$. Namely, $\operatorname{Spec} A/I_i$ is projected onto $\mathbb{A}^{d_i}$ in a descending manner when $i = 1, 2, \dots, m$ (c.f. Eisenbud 1995).

Exercise 1.1. Prove Theorem 1.15 in 3 steps: (i) $A = k[x_1, \dots, x_n]$, $I = (f)$ is principal. (ii) $A = k[x_1, \dots, x_n]$ and I is general. Notice that for cases (i) and (ii) the theorem is almost identical with the previous form (Theorem 1.12) except that we keep the ideal I unchanged. It is clear that $d = n$. (iii) The general case that $A = k[x_1, \dots, x_n]/J$. (Hint: apply (ii) twice. First apply it to $I = J$ and then to $I' = I \cap k[y_1, \dots, y_d]$.)

Now we apply the NN procedure to study the Krull dimension.

Proposition 1.17. *Let A be an affine k-algebra.*

(i) *If $k[y_1, \ldots, y_d] \hookrightarrow A$ is a Noether normalization then $\dim A = d$.*
(ii) *If A is a domain, any maximal prime chain has length d.*

PROOF. For (i), Proposition 1.8 implies that $\dim A = \dim k[y_1, \ldots, y_d] \geq d$ (e.g. the prime chain $(0) \subset (y_1) \subset (y_1, y_2) \subset \ldots \subset (y_1, \ldots, y_d)$).

Now for any prime chain $P_0 \subsetneq \ldots \subsetneq P_m$ in A, we prove by induction on $d \geq 0$ that $m \leq d$. The case $d = 0$ is trivial. Let $d > 0$.

Consider the induced prime chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_m$ in $k[y_1, \ldots, y_d]$. Let $k[z_1, \ldots, z_d] \subset k[y_1, \ldots, y_d]$ be a Noether normalization for $\mathfrak{p}_1$ such that $\mathfrak{p}_1 \cap k[z_1, \ldots, z_d] = (z_{\delta+1}, \ldots, z_d)$. Since $\mathfrak{p}_1 \neq (0)$, we get $\delta \leq d - 1$. Modulo $\mathfrak{p}_1$ we get $k[z_1, \ldots, z_\delta] \subset k[y_1, \ldots, y_d]/\mathfrak{p}_1 =: A'$ which is also a Noether normalization. By induction the prime chain in A':

$$(0) = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1 \tag{1.3}$$

has length $\leq \delta$. Hence $m - 1 \leq \delta \leq d - 1$. That is, $m \leq d$.

For (ii), let A be a domain and $P_\bullet$ be a maximal prime chain. Hence $P_0 = (0)$ and P_m is a maximal ideal. We claim that $\mathfrak{p}_\bullet := P_\bullet \cap k[y_1, \ldots, y_d]$ is also a maximal prime chain. If not, then there exists $\mathfrak{p}_i \subsetneq \mathfrak{q} \subsetneq p_{i+1}$ for some i and prime $\mathfrak{q}$. Apply Noether normalization to $I = \mathfrak{p}_i$ as above we get

$$(0) \subsetneq \bar{\mathfrak{q}} \subsetneq \overline{\mathfrak{p}_{i+1}} = \mathfrak{p}_{i+1}/\mathfrak{p}_i.$$

But $k[z_1, \ldots, z_\delta] \subset A/\mathfrak{p}_i$ is also a Noether normalization and $k[z_1, \ldots, z_\delta]$ is a normal domain. The violates the Going-down theorem, a contradiction.

Now we conclude that $m = d$ by induction on d. The case $d = 0$ is trivial. Let $d > 0$. By Noether normalization as in (i), $\mathfrak{p}_1 \cap k[z_1, \ldots, z_d] = (z_{\delta+1}, \ldots, z_d)$ has hight $= \operatorname{ht} \mathfrak{p}_1 = 1$ as we had just shown. Hence $\delta = d - 1$. By induction this implies that the maximal chain (1.3) in $k[z_1, \ldots, z_{d-1}]$ has $m - 1 = d - 1$. That is $m = d$. □

Remark 1.18. Of course (ii) fails for product rings $A_1 \times A_2$ with $\dim A_1 \neq \dim A_2$. Strikingly it also fails for certain Noetherian domains as shown by famous examples due to Zariski–Samuel (c.f. their book, II, 1958).

Corollary 1.19. *Let A be an affine k-algebra and $\mathfrak{p} \subset \mathfrak{q}$ are primes in A. Then any maximal prime chain from $\mathfrak{p}$ to $\mathfrak{q}$ has length $\dim A/\mathfrak{p} - \dim A/\mathfrak{q}$.*

Indeed, Proposition 1.17-(ii) implies that one may start at any prime and construct the maximal prime chain on both sides.

Corollary 1.20. *Let $\{\mathfrak{p}_i\}_{i=1^s}$ be the minimal primes in an affine k-algebra A. Then*

(i) $\dim A = \max_i \dim A/\mathfrak{p}_i$ *and*

$$\dim A/\mathfrak{p}_i = \operatorname{tr.deg}_k Q(A/\mathfrak{p}_i).$$

(ii) *If* $\dim A/\mathfrak{p}_i$ *is independent of i then*

$$\dim A = \operatorname{ht}\mathfrak{p} + \dim A/\mathfrak{p}$$

for any prime $\mathfrak{p}$ in A.

We may assume A is a domain. Then (i) follows from Proposition 1.17-(i). For (ii), simply consider $(0) \subset \mathfrak{p}$ in the above corollary (ii).

Corollary 1.21. *Let A be an affine k-algebra which is an UFD, $(0) \neq I \subsetneq A$ be a radical ideal. Then I is a principal ideal if and only if* $\dim A/I = \dim A - 1$.

Proof. If $I = \mathfrak{p}$ is a prime ideal, then it is easy to see from the UFD condition that $\operatorname{ht}\mathfrak{p} = 1$ if and only $\mathfrak{p} = (p)$ for a prime element $p \in A$.

For general radical I, simply consider all its minimal prime divisor $\mathfrak{p}_i$ and use $I = \sqrt{I} = \bigcap_{i=1}^{s} \mathfrak{p}_i$. □

1.4. Projective varieties.

Definition 1.22. Let k be a field. The projective n-space over k is

$$\mathbb{P}^n_k := (k^{n+1} \setminus \{0\})/\sim$$

where $(a_i)_{i=0}^n \sim (b_i)_{i=0}^n$ if $b_i = \lambda a_i$ for some $\lambda \in k^\times$. It is the set of all lines through $0 \in k^{n+1}$. Usually we denote a point on it as $[a] = (a_0 : \ldots : a_n)$.

Let $S = k[x_0, \ldots, x_n] = \bigoplus_{d \geq 0} S_d$ be a graded ring with the natural grading. An ideal $I \subset S$ is homogeneous if it is generated by homogeneous elements. Equivalently $I = \bigoplus_{d \geq 0}(I \cap S_d)$. By decomposing elements into homogeneous components and argue inductively, it is easy to see that I is prime if and only if "for homogeneous elements $f, g \in S$",

$$fg \in I \Longrightarrow f \in I \text{ or } g \in I.$$

For $f \in S_d$, the value of f at a point $[a] \in \mathbb{P}^n_k$ is not well-derfined since since $f(\lambda a) = \lambda^d f(a)$. Nevertheless its vanishing set $Z(f)$ is well-defined.

As in the affine case, for any subset $T \subset S$ of homogeneous elements we declare $Z(T) = Z(\langle T \rangle)$ to be a closed set in $\mathbb{P}^n_k$. The collection of closed sets are also called algebraic sets which define the Zariski topology on $\mathbb{P}^n_k$.

Conversely for a closed set $X \subset \mathbb{P}^n_k$ we have the vanishing ideal $I(X)$ generated by all homogeneous f with $f|_X = 0$. The homogeneous coordinate ring

Remark 1.23. Notice that the unique maximal homogeneous ideal $S_+ := \bigoplus_{d \geq 1} S_d = (x_0, \ldots, x_n)$ gives $Z(S_+) = \{0\} \in k^{n+1}$, which is excluded in our definition. Hence we define $Z(S_+) = \emptyset$ in the projective setting.

With S_+ being excluded, under the further assumption that $k = \bar{k}$, then $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ and $Z(I(Y)) = \overline{Y}$ for any homogeneous ideal $\mathfrak{a} \neq S_+$ and any subset $Y \subset \mathbb{P}^n_k$. Hence the correspondences between algebraic sets and homogeneous radical ideals holds as in the affine case.

In fact all the proofs are all reduced to the "homogeneous Nullstellensatz", which follows from the affine case, hence are left as exercises.

Definition 1.24. A projective variety X is an irreducible algebraic set in $\mathbb{P}^n_k$. A quais-projective variety is an open subset of a projective variety. In general, a k-variety is always referred as a quasi-projective variety in some $\mathbb{P}^n_k$.

It is clear that projective varieties X correspond to homogeneous prime ideals $\mathfrak{p} = I(X)$ in S. The affine variety $C(X) \subset k^{n+1}$ defined by the same ideal $\mathfrak{p}$ is called the cone over X. Many properties of projective varieties can be studied by way of consideration on the affine cones. Another common consideration related to affine varieties is to view the latter as local charts:

We may write $\mathbb{P}^n_k = U_0 \cup \ldots \cup U_n$ where $U_i = \mathbb{P}^n_k \setminus H_i$, $H_i := Z(x_i) \cong \mathbb{P}^{n-1}_k$ is called the i-th hyperplane of $\mathbb{P}^n_k$. Then we have homeomorphisms

$$\phi_i : U_i \longrightarrow \mathbb{A}^n_k, , \qquad [a] \mapsto \Big(\frac{a_0}{a_i}, \ldots, \frac{\widehat{a_i}}{a_i}, \ldots, \frac{a_n}{a_i}\Big).$$

Corollary 1.25. *Projective varieties can be written as union of open affine varieties via $X = \bigcup_{i=0}^n (X \cap U_i)$. Conversely, any affine variety $Y \subset \mathbb{A}^n_k$ has a unique closure $\overline{Y}$ as a projective variety via $\mathbb{A}^n_k \cong U_0 \subset \mathbb{P}^n_k$*

To perform computations it is convenient to introduce

Definition 1.26. Let $A = k[y_1, \ldots, y_n]$. The de-homogenization map is

$$\alpha : S \to A, \qquad f \mapsto \alpha(f) := f(1, y_1, \ldots, y_n),$$

and the homogenization map is

$$\beta : A \to S, \qquad g \mapsto \beta(g) := x_0^d g(x1/x_0, \dots, x_n/x_0) \quad \text{if } g \in S_d.$$

Proposition 1.27. *Let $I = I(Y)$ then $\overline{Y} = Z(\beta(I))$.*
If $\{f_i\}$ is a Grobner basis of I in a graded order then $(\beta(I)) = (\beta(f_i))$.

The first statement is an exercise. For an arbitrary generating set $I = (f_1, \dots, f_r)$ it might happen that $(\beta(f_i)) \subsetneqq (\beta(I))$ and $Z((\beta(f_i)))$ is strictly larger than $\overline{Z(I)}$ as shown in the following examples (2) and (3):

Example 1.28 (On projective closure).

(1) A hypersurface $Z(f) \subset \mathbb{A}^n_k$ has projective closure $Z(\beta(f)) \subset \mathbb{P}^n_k$. For example, if $f = y^2 - 4x^3 - ax - b$ then $\beta(f) = ZY^2 - 4X^3 - aZ^2X - bZ^3$. This is the standard Weierstrass equation for an elliptic curve.

(2) The twisted cubic curve $C \subset \mathbb{A}^3_k$ is the image of $\mathbb{A}^1_k$ under $t \mapsto (t, t^2, t^3)$. It has $I(C) = (y - x^2, z - x^3)$. $(k[x, y, z]/((y - x^2, z - x^3)) \cong k[x]$ is a domain so the ideal is already a prime.) Let

$$J := (\beta(y - x^2), \beta(z - x^3)) = (WY - X^2, W^2Z - X^3).$$

Then $Z(J)$ contains two components. If $W = 0$ then $X = 0$ as well, which gives a line $L = Z((X, W))$ contained in the infinity hyperplane $H_W = Z(W)$. If $W \neq 0$ then we go back to the original affine chart $\mathbb{A}^3 = \mathbb{P}^3 \setminus H_W$ and recover the curve C. Hence $Z(J) = L \cup \overline{C}$.

Notice that $xy - z \in I(C)$ and $\beta(xy - z) = XY - ZW$. Adding this element does not resolve the problem since $L \subset Z(XY - ZW)$. On the other hand $xz - y^2 \in I(C)$ too and $\beta(xz - y^2) = XZ - Y^2$ does not contain L in its zero loci. Hence $\overline{C} = Z(\beta(y - x^2), \beta(z - x^3), \beta(xz - y^2))$.

We have $xz - y^2 = x(z - x^3) - (y + x^2)(y - x^2)$. However such a formula does not preserve under homogenization.

(3) Even if $\dim Z(I) = 0$, $I = (f_1, \dots, f_r)$, $Z(\beta(f_1), \dots, \beta(f_r))$ may contain positive dimensional components at infinity! For example, consider the 6 equations $\sum_{i=1}^3 x_i^k - \sum_{i=1}^3 y_i^k = 1$, $x_k y_k = 1$, $k = 1, 2, 3$ in $\mathbb{C}^3$. Then the homogenized equations contains lines at infinity.

Now we prove of the Grobner basis part of Proposition 1.27. Given a monomial order $>$, a Grobner bases of an ideal $I \subset A = k[x_1, \dots, x_n]$ is a generating set of I: $I = (f_1, \dots, f_r)$ such that

$$(\operatorname{LT} I) = (\operatorname{LT} f_1, \dots, \operatorname{LT} f_r),$$

where LT is an abbreviation for "leading term". Such a bases can be effectively constructed by the Buchburger algorithm which is not needed here.

A monomial order $>$ is graded if we compare the total degree first. With it, we claim that $\beta(f_1), \ldots, \beta(f_r)$ generate $(\beta(I))$, in fact as a Grobner bases, in the extended monomial order $>_\beta$ in $S = k[x_0, x_1, \ldots, x_n]$:

$$x_0^p x^\alpha >_\beta x_0^q x^\beta \iff x^\alpha > x^\beta \quad \text{or} \quad x^\alpha = x^\beta, \quad p > q.$$

In this order, it is clear that $\operatorname{LT}_{>_\beta} \beta(f) = \operatorname{LT} f$ for any $f \in A$.

To show $(\beta(f_i)) = (\beta(I))$, let $g \in (\beta(I))$. By definition,

$$g = \sum_i a_i(x_0, \ldots, x_n)\, \beta(h_i), \qquad h_i \in I.$$

Then $f := \alpha(g) = \sum_i a_i(1, x_1, \ldots, x_n)\, h_i \in I$. Hence $g = x_0^d \beta(f)$ for some $d \geq 0$, and $\operatorname{LT}_{>_\beta} g = x_0^d \operatorname{LT}_{>_\beta} \beta(f) = x_0^d \operatorname{LT} f$. Now $\operatorname{LT} f$ is divisible by some $\operatorname{LT} f_i = \operatorname{LT}_{>_\beta} \beta(f_i)$, hence the same is true for $\operatorname{LT}_{>_\beta} g$. The result follows.

We have seen three kind of spaces with Zariski topology, the affine varieties, $\operatorname{Spec} A$ and projective varieties. In the same spirit we may define homogeneous prime spectrum $\operatorname{Proj} S$ with Zariski topology for a commutative graded ring $S = \bigoplus_{d \geq 0} S_d$ and declare the closed sets are of the form

$$V(I) = \{\mathfrak{p} \in \operatorname{Proj} S \mid \mathfrak{p} \supset I\}$$

where $I \subset S$ is a a homogeneous ideal not containing $S_+ = \bigoplus_{d \geq 1} S_d$. It has an open cover by affine spectrum as well. We will discuss this in details in chapter 2 when we introduce scheme theory.

We formalize the Zariski topology on them by the notion of Noetherian topological spaces.

Definition 1.29. A topological space X is Noetherian if any descending chain of irreducible closed subset stops. The Krull dimension $\dim X$ is then defined to be the largest d in irreducible closed chain $Z_0 \supsetneq Z_1 \supsetneq \ldots \supsetneq Z_d$, and $\dim X = \infty$ if this is unbounded. This does happen for varieties.

$\mathbb{A}_k^n$, $\mathbb{P}_k^n$ and their closed subset are clearly Noetherian topological spaces by the correspondence with radical/prime ideals. For $\operatorname{Spec} A$ and $\operatorname{Proj} S$, they are Noetherian topological spaces if A or S are Noetherian rings. But this requirement might not be necessary.

2. Morphisms and rational maps

2.1. Regular functions and morphisms. Let $Y \subset \mathbb{A}_k^n$ be a quasi-affine variety. A function $f : Y \to k = \mathbb{A}_k^1$ is regular at $p \in Y$ if

$$f = g/h, \qquad g, h \in k[x_1, \ldots, x_n]$$

on an open neighborhood $p \in U \subset Y$ with $h \neq 0$ on U.

Since $f(x) = c \iff g(x) - ch(x) = 0$, which is a closed set, f is necessarily continuous. (But not conversely.) Similarly, $\{x \in Y \mid h(x) \neq 0\}$ is open in Y. So it enough to require $h(p) \neq 0$ in the above definition.

If $Y \subset \mathbb{P}_k^n$ is quasi-projective, then $p \in Y \cap U_i$ for some i, which is quasi-affine. Then the definition is equivalent to that $f = g/h$ where $g, h \in S = k[x_0, \ldots, x_n]$ are homogeneous of the same degree. For an open set $V \subset Y$, we denote by $\mathscr{O}_Y(V)$ the space of functions regular at every $p \in U$.

A continuous map $\phi : X \to Y$ between varieties is a morphism, denoted by $\phi \in \mathrm{Hom}(X, Y)$, if ϕ pulls back regular functions. That is,

$$f \in \mathscr{O}_Y(V) \Longrightarrow f \circ \phi \in \mathscr{O}_X(\phi^{-1}(V)).$$

This defines the category of k-varieties Var_k. In particular X, Y are isomorphic if there is a morphism $\psi : Y \longrightarrow X$ with $\psi \circ \phi = \mathrm{id}_X$ and $\phi \circ \phi = \mathrm{id}_Y$.

Denote by $\mathscr{O} \equiv \mathscr{O}(Y) = \Gamma(Y, \mathscr{O}_Y) \equiv \mathscr{O}_Y(Y)$ the global regular functions. To the other extreme, for $p \in Y$ we define

$$\mathscr{O}_p \equiv \mathscr{O}_{Y,p} := \lim_{p \in V} \mathscr{O}_Y(V)$$

to be the space of germs of functions regular at p.

Elements in $\mathscr{O}_p$ are equivalence classes of pairs (V, f) with $f \in \mathscr{O}_Y(V)$, where $(V, f) \sim (W, g)$ if $f = g$ on some open subset $p \in U \subset V \cap W$. In the current case we then have $f = g$ on $V \cap W$ since the set where $f = g$ is both open and closed in $V \cap W$.

The ring $\mathscr{O}_p$ is a local ring, with maximal ideal $m_p := \{f \in \mathscr{O}_p \mid f(p) = 0\}$. Indeed if $f \in \mathscr{O}(V)$ and $f(p) \neq 0$ then $1/f \in \mathscr{O}(V \setminus Z(f))$.

For a variety Y, the function field $K(Y)$ is the equivalence classes of local regular functions (V, f)'s. $K(Y)$ is a field since $1/f$ is regular on $V \setminus Z(f)$. It depends only on the isomorphism class of Y. Thus for any $p \in Y$ we have

$$\mathscr{O}(Y) \subset \mathscr{O}_p \subset K(Y).$$

Remark 1.30. In contrast to $K(Y)$, the homogeneous coordinate ring $S(Y)$ for a projective variety does depend on chosen presentation $Y \subset \mathbb{P}_k^n$.

Here is the fundamental theorem for regular functions:

Theorem 1.31. *Let Y be an affine k-variety with $k = \bar{k}$. Then the natural map*

$$\alpha : A(Y) \xrightarrow{\sim} \mathscr{O}(Y)$$

is an isomorphism with $A(Y)_{m_p} \cong \mathscr{O}_p$ for $p \in Y$.

In particular, $\dim \mathscr{O}_p = \dim Y$ *and* $K(Y) = Q(A_p) = Q(A(Y))$.

Proof. By definition we have

$$A(Y) = k[\mathbf{x}]/I \overset{\alpha}{\hookrightarrow} \mathscr{O}(Y)$$

which leads to $A(Y)_{m_p} \hookrightarrow \mathscr{O}_p$. An element in $\mathscr{O}_p$ has the form (V, f) where V is quasi-affine, hence this map is also surjective by the definition or regular function on quasi-affine varieties. Thus $A(Y)_{m_p} \cong \mathscr{O}_p$.

Now

$$A(Y) \subset \mathscr{O}(Y) \subset \bigcap_{p \in Y} \mathscr{O}_p = \bigcap_{m} A(Y)_m$$

since there is a one to one correspondence between points and maximal ideals (this is the only place we use $k = \bar{k}$). Then we use the simple fact that $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} = R$ for any integral domain R. □

Remark 1.32. It is well known that for $Y = \mathbb{A}^n_k$, $k = \mathbb{F}_q$ a finite field, the natural map α has kernel $(x_1^q - x_1, \ldots, x_n^q - x_n)$.

As the first corollary, in contrast to the affine case, the only global regular functions on projective varieties over $k = \bar{k}$ are constant functions!

Theorem 1.33. *Let Y be a projective k-variety with $k = \bar{k}$, with homogeneous coordinate ring $S(Y)$. Then $\mathscr{O}_p \cong S(Y)_{(m_p)}$, $K(Y) \cong S(Y)_{(0)}$ and*

$$\mathscr{O}(Y) \equiv \Gamma(Y, \mathscr{O}_Y) \cong k.$$

Proof. Under the standard affine cover $\mathbb{P}^n_k = U_0 \cup \ldots \cup U_n$, the maps $\phi_i : U_i \cong \mathbb{A}^n_k$ are isomorphism of varieties. Let $Y = \bigcup Y_i$, $Y_i := Y \cap U_i$. Then

$$\phi_i^* : A(Y_i) \cong S(Y)_{(x_i)}.$$

For $p \in Y$, say $p \in Y_i$, by Theorem 1.31 and further localizations, we get

$$\mathscr{O}_p \cong A(Y_i)_{m'_p} \cong S(Y)_{(m_p)}$$

where m'_p denote the maximal ideal of $p \in Y_i$. Now $K(Y) \cong K(Y_i)$. Via ϕ_i^* this is just $S(Y)_{(0)}$ with all non-zero elements being inverted.

For a global regular function $f \in \mathscr{O}(Y) = \bigcap_i \mathscr{O}(Y_i) = \bigcap_i S(Y)_{(x_i)}$, for each i this means $x_i^{d_i} f \in S(Y)_{d_i}$ for some $d_i \in \mathbb{N}$. Let $d = \sum d_i$, every monomial $x^\alpha \in S(Y)_d$ contains some factor $x_i^{d_i}$ for some i. This implies that

$$fS(Y)_d \subset S(Y)_d.$$

Since $S(Y)_d$ is a finite dimensional k vector space, this implies that f is integral over k by the standard criterion of integral elements. Indeed, if $\{v_j\}$ is basis of $S(Y)_d$ and $fv_j = \sum_l a_{jl} v_l$ for $a_{jl} \in k$, then

$$\det((f\delta_{jl} - a_{jl})) = 0$$

gives the monic polynomial equation over k.

Now we use the assumption $k = \bar{k}$ to conclude that $f \in k$. □

The second corollary is a categorical correpondence:

Theorem 1.34. *Let Y be an affine k-variety over $k = \bar{k}$.*

There is a contravariant isomorphism

$$\lambda : \mathrm{Hom}(X, Y) \xrightarrow{\sim} \mathrm{Hom}(A(Y), \mathscr{O}(X)),$$

where for $\phi : X \to Y$, $\lambda(\phi)$ is defined by composition: $f \in A(Y) \mapsto f \circ \phi$.

Proof. Clearly $\lambda(\phi)$ is a k-algebra homomorphism $\mathscr{O}(Y) \to \mathscr{O}(X)$. Now use Theorem 1.31 to get $\mathscr{O}(Y) \cong A(Y)$.

Given a ring homomorphism

$$\psi : A(Y) = k[x_1, \ldots, x_n]/I(Y) \to \mathscr{O}(X),$$

let $y_i := \psi(\bar{x}_i)$. We define a morphism $\phi : X \to Y$ by

$$p \in X \mapsto \phi(p) := (y_i(p)) \in \mathbb{A}_k^n.$$

The image lies in Y since for any $f \in I(Y)$ we have

$$f(y_1(p), \ldots, y_n(p)) = \psi(\overline{f(x)}) = 0.$$

To see that $\lambda(\phi) = \psi$, notice that $\lambda(\phi)(\bar{x}_j) = \bar{x}_j \circ \phi$, which maps p to $\bar{x}_j(\phi(p)) = \bar{x}_j((y_i(p))_{i=1}^n) = \bar{x}_j((\psi(\bar{x}_i)(p))_{i=1}^n) = \psi(\bar{x}_j)(p)$. This holds for all $p \in X$, hence $\lambda(\phi) = \psi$ as expected. □

Corollary 1.35. *For $k = \bar{k}$, $Y \mapsto A(Y)$ induces an anti-equivalence of categories between affine k-varieties and finitely generated domains over k.*

2.2. Rational maps and birational equivalence. Throughout this subsection we assume all varieties are over $k = \bar{k}$.

We start with a simple fact: given two morphisms of varieties $\phi, \psi : X \to Y$, if $\phi = \psi$ on some open (hence dense) subset $U \subset X$ then $\phi = \psi$ on X. We have seen the case $Y = \mathbb{A}^1_k$, and the general case reduces to this case by taking affine charts on Y.

Definition 1.36. (i) A rational map $\phi : X \dashrightarrow Y$ is an equivalence class of (U, ϕ_U) where $\phi_U : U \to Y$ is a morphism and $U \subset X$ is open. It is dominant if $\operatorname{im} \phi_U$ is dense for some (hence all) U.

(ii) $\phi : X \dashrightarrow Y$ is birational if there is a rational map $\psi : Y \dashrightarrow X$ such that $\phi\psi = \mathrm{id}_Y$ and $\psi\phi = \mathrm{id}_X$. (This makes sense by the above fact.)

For $Y = \mathbb{A}^1_k$ in (i) we go back to the definition of $K(X)$. If X and Y are birational, then it follows that $K(X) \cong K(Y)$.

The converse is also true. In fact we have a more general result:

Theorem 1.37. *There is an anti-equivalence of categories between varieties with dominant rational maps and finitely generated extension fields over k.*

The proof is based on two basic facts:

Lemma 1.38. *Let X be affine with $A = A(X)$, then $X_f := X \setminus Z(f)$ is also affine with coordinate ring $A_f = A[1/f] \cong A[T]/(fT - 1)$.*

PROOF. For $X = \mathbb{A}^n$, consider

$$\phi : Q = Z(fT - 1) \subset \mathbb{A}^{n+1} \longrightarrow \mathbb{A}^n \setminus Z(f)$$

defined by the projection $(a_1, \ldots, a_{n+1}) \mapsto (a_1, \ldots, a_n)$. Then ϕ is an isomorphism with $\phi^{-1}(a_1, \ldots, a_n) = (a_1, \ldots, a_n, 1/f(a_1, \ldots, a_n))$.

For a general affine variety $X \subset \mathbb{A}^n$, $X \setminus Z(f) \subset \mathbb{A}^n \setminus Z(f)$ is also closed. Since the latter ($\cong Q$) is affine, we conclude that $X \setminus Z(f)$ is also affine with coordinate ring $A[T]/(fT - 1)$. □

Lemma 1.39. *Any variety has an open affine base for its Zariski topology.*

PROOF. Let $p \in U \subset X$. Since $U = \bigcup U_i$ with U_i being quasi-affine, may we assume that U is quasi-affine. Then $Z := \overline{U} \setminus U$ is closed. That is, $Z = Z(I) \subset \mathbb{A}^n$. Pick $f \in I$ but $f(p) \neq 0$. Then $\overline{U} \setminus Z(f) \subset \overline{U} \setminus Z = U$. Now $\overline{U} \setminus Z(f)$ is affine by Lemma 1.38. □

PROOF OF THEOREM 1.37. Given a dominant $\phi : X \dashrightarrow Y$, we get a field extension $\phi^* : K(Y) \to K(X)$ by $\phi^*(f) = f \circ \phi$.

Conversely, any finitely generated field over k is the function field $K(Y)$ for some affine variety Y. And given a field extension $\theta : K(Y) \to K(X)$, since $K(Y) \supset A(Y) = k[y_1, \ldots, y_n]/I(Y)$, we get $\theta(\bar{y}_i) \in K(X)$ for $i \in [1, n]$.

Let $U \subset X$ such that all $\theta(\bar{y}_i)$ are regular on U. By Lemma 1.39 we may assume that U is affine. Hence we get an inclusion $A(Y) \subset A(U)$. By Theorem 1.34 this corresponds to a morphism $\phi : U \to Y$. If ϕ is not dominant, then $\phi(U)$ is contained in a closed subset $Z \subset Y$. Let $Z = Z(J)$ for some $J \supsetneqq I(Y)$. Pick $f \in J \setminus I(Y)$ leads to $\phi^* f = f \circ \phi = 0$, which contradicts to the injectivity of $A(Y) \subset A(U)$. □

Corollary 1.40. *Two varieties X and Y are birational if and only if there are open subsets $U \subset X$ and $V \subset Y$ such that $U \cong V$, which is also equivalent to that $K(X) \cong K(Y)$.*

Corollary 1.41. *Any k-variety X of dimension r is birationally equivalent to a hypersurface in $\mathbb{P}^{r+1}_k$.*

PROOF. We have $k(x_1, \ldots, x_r) \subset K(X)$ for a transcendental base x_i's. This finite algebraic extension is automatically a separable extension if k is a perfect field. (In fact the separability holds for any k with $\operatorname{char} k = 0$. For $\operatorname{char} k = p > 0$ we have $k = k^p$ if $k = \bar{k}$ hence k is perfect.)

By the theorem of primitive element, we have $K(X) = k(x_1, \ldots, x_r, y)$. Since y is algebraic over $k(x_1, \ldots, x_r)$, we have an equation

$$\sum_{i=0}^{d} \frac{f_i(x_1, \ldots, x_r)}{g_i(x_1, \ldots, x_r)}\, y^i = 0.$$

This leads to an irreducible polynomial equation $f(x_1, \ldots, x_r, y) = 0$ in $k[x_1, \ldots, x_r, y]$. Hence $H = Z(f) \subset \mathbb{A}^{r+1}_k$ has $K(H) = K(X)$. Corollary 1.40 then implies that X is birational to $\overline{H} \subset \mathbb{P}^r_k$. □

Below we will prove the existence of separating transcendental base $x_1, \ldots, x_r$ used in the above proof, following Zariski–Samuel.

Theorem 1.42 (MacLane). *If a finitely generated field K/k is separably generated, i.e. K contains a separating transcendental base over k, then any generating set $x_1, \ldots, x_n$ contains such a base.*

PROOF. Only need to consider k with $\operatorname{char} k = p > 0$. Let $r = \text{tr.deg}_k K$.

If $r = 1$, the assumption that $K/k(z)$ is separable for some transcendental $z \in K$ implies that $z \notin k(z^p)$. So $X^p - z^p$ is irreducible over $k(z^p)$, i.e. z is inseparable over $k(z^p)$. This implies that in the given generating set x_i's there exists one, say x_1, which is inseparable over $k(z^p)$. We will show that x_1 is also a separable transcendental base for K/k.

Let $f(X, Z)$ be an irreducible polynomial with $f(x_1, z) = 0$. Then f is also irreducible in $k(Z)[X] \cong k(z)[X]$. That is, $f(X, z)$ is the minimal polynomial $m_{x_1}(X)$ up to a factor in $k[z]$. So $D_1 f(x, z) \neq 0$.

Notice that $f(X, Z)$ is not independent of Z, for otherwise x_1 is separable over k and hence separable over $k(z^p)$, which contradicts to the choice of x_1. So z is algebraic over $k(x_1)$. If z is not separable over $k(x_1)$ then $f(X, Z) = \phi(X, Z^p)$ for some polynomial ϕ. Then $D_1\phi(x, z^p) = D_1 f(x, z) \neq 0$, i.e. x_1 is separable over $k(z^p)$, a contradiction. So z is separable over $k(x_1)$. Since $K/k(z)$ is separable, $K/k(x_1)$ is also separable as expected.

Now let $r > 1$ and assume the theorem holds up to dimension $r - 1$. Let $z_1, \ldots, z_r$ be a sep. trans. base of K/k and $k_1 := k(z_1)$. Then $K = k_1(x_1, \ldots, x_n)$ has a sep. trans. base $z_2, \ldots, z_n$ over k_1. By induction we may assume that $x_1, \ldots, x_{r-1}$ is a sep. trans. base of K/k_1. Let $k' = k(x_1, \ldots, x_{r-1})$. Then $K = k'(x_r, \ldots, x_n)$ has $\text{tr.deg}_{k'} K = 1$. By the $r = 1$ case we get x_r (after reordering) is sep. trans. over k'. This proves the theorem. □

Corollary 1.43. *If $K = k(x_1, \ldots, x_n)/k$ is not separably generated, then after reordering $k(x_1, \ldots, x_{r+1})/k$ is also not separably generated, where $r = \text{tr.deg}_k K$.*

PROOF. If $n = r + 1$ then we are done. Assume $n > r + 1$ and the statement holds for $n - 1$. After reordering $k_1 := k(x_2, \ldots, x_n)$ has $\text{tr.deg}_k k_1 = r$. If k_1/k is not separably generated then we are done by the $n - 1$ case. Otherwise MacLane's theorem implies that we may assume $x_2, \ldots, x_{r+1}$ is a sep. trans. base of k_1/k. Then $k(x_1, \ldots, x_{r+1})$ is the field required. □

Theorem 1.44 (Schmidt)**.** *If k is perfect, i.e. $k = k^p$, then any finitely generated field $K = k(x_1, \ldots, x_n)$ is separably generated.*

PROOF. If not, by the above corollary we may assume $n = r + 1$ where $r = \text{tr.deg}_k K$. Let $f(x_1, \ldots, x_{r+1}) = 0$ be an irreducible relation. Since x_{r+1} is not separable over $k(x_1, \ldots, x_r)$, we have $f \in k[X_1, \ldots, X_r, X_{r+1}^p]$. Working over all x_i and using $k = k^p$ we get $f = g^p$, a contradiction! □

2.3. Blowing up. The most important and basic kind of birational maps are birational morphisms called blowing-ups. Usually they are designed for resolving singularities, a notion to be studied in the next section. Here we talk singularities naively to motivate the definition of blowing-ups.

Example 1.45. Consider a plane curve $C \subset \mathbb{A}^2_k$ defined by

$$y^2 = x^2(x+1).$$

C has a nodal singularity at $(0,0)$ with two branches of different slops $y = x$ and $y = -x$. The idea to take apart the two branches near $(0,0)$ is to consider their slops (tangent directions) as well. Explicitly, consider the quadratic transformation

$$y = ux$$

($u = y/x$ is the slope), then $x^2u^2 = x^2(x+1)$. Together with $y = ux$ we get an one-dimensional algebraic set $\phi^{-1}(C)$ where $\phi : \mathbb{A}^3_k \to \mathbb{A}^2_k$, $(x, y, u)) \mapsto (x, y)$:

If $x \neq 0$ then $u^2 = x + 1$. On the (x, u)-plane it is a non-singular parabola $\tilde{C}$.

If $x = 0$ then $y = 0$ but $u \in k = \mathbb{A}^1_k$ is arbitrary—it is the u-axis which intersects $\tilde{C}$ at two points $u = \pm 1$ corresponding to the slops of the two branches.

In fact all curve singularities can be resolved by repeating the process in finite steps, though the proof is not immediate. We will discuss it in different ways later.

Definition 1.46. (i) The blowing-up of $\mathbb{A}^n$ at 0 is the subvariety X in $\mathbb{A}^n \times \mathbb{P}^{n-1}$ defined by $\{ x_iy_j = x_jy_i \mid 1 \leq i, j \leq n \}$, where $(x_i) \in \mathbb{A}^n$, $[y_j] \in \mathbb{P}^{n-1}$:

$$\begin{tikzcd}
X \arrow[r, hook, "\iota"] \arrow[dr, "\phi"'] & \mathbb{A}^n \times \mathbb{P}^{n-1} \arrow[d, "p_1"] . \\
& \mathbb{A}^n
\end{tikzcd}$$

Clearly $\phi^{-1}(0) = \{0\} \times \mathbb{P}^{n-1} =: E$, called the exceptional divisor. But $\phi^{-1}(p)$ is unique if $p = (x_i) \neq 0$: since then $[y_j] = [x_j]$ is the direction of $\overrightarrow{op}$. Thus ϕ is a birational morphism which induces $X \setminus E \cong \mathbb{A}^n \setminus \{0\}$.

(ii) For a general algebraic set $0 \in Y \subset \mathbb{A}^n$, we define

$$\mathrm{Bl}_0 Y = \tilde{Y} := \overline{\phi^{-1}(Y \setminus \{0\})} \subset X,$$

which is also called the strict (or proper) transform of Y in X. The induced morphism $\phi : \tilde{Y} \to Y$ is then a birational morphism.

The definition of $\mathrm{Bl}_0 Y$ actually does not depend on the chosen coordinates $Y \subset \mathbb{A}^n$ and the center "0" can be more general closed subsets. We will develop this further later using scheme theory.

3. Nonsingular varieties and curves

3.1. Non-singular points on a variety.

Definition 1.47. Let $(A, \mathfrak{m})$ be a Noetherian local ring, $k = A/\mathfrak{m}$ its residue field. Then A is regular if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$. This is equivalent to that $\mathfrak{m}$ can be generated by $\dim A$ elements.

The inequality $\dim_k \mathfrak{m}/\mathfrak{m}^2 \geq \dim A$ always holds, which is a consequence of dimenison theory of Noetherian local rings. The proof needs the technique of Hilbert polynomials, which will be given later.

Definition 1.48. Let $Y \subset \mathbb{A}^n$ be an affine variety with $I(Y) = (f_1, \ldots, f_t)$. Denote by $DF = (\partial f_i / \partial x_j)$ be the Jacobian matrix. Then Y is non-singular at $p \in Y$ if the rank $DF(p) = n - r$, where $r = \dim Y$.

Theorem 1.49. *For any $p \in Y$, we have*

$$\dim_k m_p/m_p^2 + \operatorname{rank} DF(p) = n.$$

Thus, Y is non-singular at $p \in Y \iff \mathscr{O}_p$ is a regular local ring.

Proof. Let $p = (a_i)_{i=1}^n$, $I_p = (x_1 - a_1, \ldots, x_n - a_n)$ be the corresponding maximal ideal in $A := k[x_1, \ldots, x_n]$. Then the map

$$\theta : A \longrightarrow k^n, \qquad f \mapsto Df(p)$$

gives an isomorphism

$$\theta' : I_p/I_p^2 \xrightarrow{\sim} k^n.$$

Also for $I(Y) = (f_1, \ldots, f_t)$, via θ and θ' we have

$$\operatorname{rank} DF(p) = \dim\, \theta(I(Y)) = \dim(I(Y) + I_p^2)/I_p^2.$$

Together with $m_p/m_p^2 \cong I_p/(I(Y) + I_p^2)$, we get

$$\dim_k m_p/m_p^2 + \operatorname{rank} DF(p) = n.$$

This clearly implies the last statement of the theorem. □

Corollary 1.50. *The notion of a non-singular point $p \in Y$ is independent of the affine charts containing it. Hence the notion is defined for all varieties.*

Theorem 1.51. *The set of singular points* $\operatorname{Sing} Y \subset Y$ *is a proper closed subset.*

PROOF. We may assume that $Y \subset \mathbb{A}^n$ is affine. Then, by Theorem 1.49, $\operatorname{Sing} Y$ is defined by $I(Y)$ and all the $(n-r) \times (n-r)$ minors (determinant of sub-matrix) of DF, where $r = \dim Y$. Hence it is closed.

To show that $Y \setminus \operatorname{Sing} Y \neq \emptyset$, take $H \subset \mathbb{A}^{r+1}$ be a hypersurface which is birational to Y (by Corollary 1.41). If the theorem is proved for H, then there are non-singular points $p \in U \subset H$ where U is isomorphic to an open set in Y. Then Y will also contain non-singular points.

So we are reduced to the case that $Y \subset \mathbb{A}^{r+1}$ which is defined by one irreducible polynomial $f(x_1, \ldots, x_{r+1}) = 0$.

If $Y \setminus \operatorname{Sing} Y = \emptyset$, then $\partial f / \partial x_i \in I(Y) = (f)$ for all i. This leads to a contradiction for the obvious degree reason unless $\operatorname{char} k = p > 0$. In the latter case we have then $f \in k[x_1^p, \ldots, x_{r+1}^p]$. But we assume $k = \bar{k}$, in particular $k = k^p$, hence $f = g^p$ is not irreducible, a contradiction. □

In order to have further information on the structure of regular local rings, we need to study the formal (analytic) structure at a point $p \in Y$.

For $(A, \mathfrak{m})$ being a local ring, the inverse limit

$$\hat{A} := \varprojlim A/\mathfrak{m}^n$$

is complete in the $\mathfrak{m}$-adic topology. Here are some basic facts:

(i) $\hat{A}$ has maximal ideal $\hat{\mathfrak{m}} = \mathfrak{m}\hat{A}$.

(ii) $\bigcap \mathfrak{m}^n = 0$ (this is known as Krull's intersection theorem, cf. Corollary 1.72), hence $A \hookrightarrow \hat{A}$ and the topology is Hausdorff.

(iii) If M is a finitely generated A-module then

$$\widehat{M} := \varprojlim M/\mathfrak{m}^n M \cong M \otimes_A \hat{A}.$$

(iv) $\operatorname{Gr} A \cong \operatorname{Gr} \hat{A}$, Hence $\dim A = \dim \hat{A}$ and A is regular if and only if $\hat{A}$ is regular.

Here is the fundamental result we quote without giving a proof:

Theorem 1.52 (Cohen). *If $(A, \mathfrak{m})$ is a complete regular local ring containing a field, then $A \cong k[[x_1, \ldots, x_n]]$ where $n = \dim A$ and $k = A/\mathfrak{m}$.*

For $p \in Y$, we get its complete local ring $\widehat{\mathscr{O}_p}$.

Definition 1.53. We call $p \in X$ and $q \in Y$ in Var_k are analytically (or formally) isomorphic if $\widehat{\mathscr{O}_p} \cong \widehat{\mathscr{O}_q}$ as k-algebras.

Thus non-singular points with the same dimension are all analytically isomorphic. They all have $\widehat{\mathscr{O}_p} \cong k[[x_1, \ldots, x_n]]$. For singular points, the complete local ring is also a useful tool in analyzing their structure.

Example 1.54. The main technical tools in complete local rings are formal inverse or implicit function theorem, which is known as Hensel's lemma.

As a simple example, let $A = k[x,y]/(xy)$ and $B = k[x,y]/(xy + x^3 + y^4)$. Then $\hat{A} = k[\![x,y]\!]/(xy)$ and $\hat{B} = k[\![x,y]\!]/(xy + x^3 + y^4)$. We may solve two power series $u = x + f_2(x,y) + f_3(x,y) + \ldots$ and $v = y + g_2(x,y) + g_3(x,y) + \ldots$ inductively on degree such that $uv = xy + x^3 + y^4$. Hence $\hat{A} \cong \hat{B}$.

3.2. Normal points and integrally closed domains.

Definition 1.55. A domain A is normal if it is integrally closed in its quotient field $K = Q(A)$. Often this is termed "A is integrally closed".

Let $C \subset K$ be the integral closure of A in K and $S \subset A$ be a multiplicative closed subset. The it is easy to see that $S^{-1}A$ has integral closure $S^{-1}C$ in K. Since normality of A is equivalent to the surjectivity of the inclusion $A \to C$. It follows from the local-global principle that A is normal $\Longleftrightarrow A_p$ is normal for all prime $p \Longleftrightarrow A_{\mathfrak{m}}$ is normal for all maximal ideal $\mathfrak{m}$.

Definition 1.56. A variety X is normal if all its local rings $\mathscr{O}_p$ are normal (integrally closed). This is equivalent to that $X = \bigcup X_i$, X_i is affine with normal (integrally closed) coordinate ring $A(X_i)$.

The fundamental theorem to be established is the finite A-module structure of C when A is an affine k-algebra. We first prove a general result:

Theorem 1.57. *Let A be normal and F be a finite separable extension of $K = Q(A)$. Let A' be the integral closure of A in F. Then there is a K-basis $x_1, \ldots, x_n$ of F such that $A' \subset \sum_{i=1}^n Ax_i$.*

PROOF. We may write $F = \bigoplus_{i=1}^n Ku_i$ for $u_i \in A'$. F/K is separable implies that the pairing $F \times F \to K$:

$$(x,y) \longmapsto \operatorname{Tr} xy$$

is non-degenerate, where $\operatorname{Tr} a := \sum_\sigma \sigma(a)$ is a sum over all embeddings $\sigma : F \to \overline{K}$. Let $\{v_i\}_{i=1}^n$ be the dual basis of $\{u_i\}_{i=1}^n$ with respect to the pairing, i.e. $\operatorname{Tr} u_i v_j = \delta_{ij}$. Then $F = \bigoplus_{j=1}^n Kv_j$.

If $x = \sum x_j v_j \in A'$ with $x_j \in K$ then $xu_i \in A'$ and then $x_i = \operatorname{Tr} xu_i$ which lies in A. The last statement follows from the fact that A is integrally closed implies that all coefficients of the minimal polynomials of elements in A' must lie in A. In particular, this applies to trace. □

Remark 1.58. The proof implies if A is also Noetherian then A' is Noetherian, and if A is a pid then there is a base x_i's such that $A' = \bigoplus_{i=1}^n A\, x_i$.

Theorem 1.59 (Finiteness of integral closure)**.** *Let A be an affine k-algebra which is also a domain, and F be a finite extension of $K = Q(A)$.*

Then A', the integral closure of A in F, is also an affine k-algebra. Moreover A' is a finite A-module.

Proof for the case $k = \bar{k}$. Write $F = \bigoplus_{i=1}^q K\, y_i$ with $y_i \in A'$. Let $A^\circ := k[y_1, \ldots, y_q]$. Then A° is integral over A and $Q(A^\circ) = F$. Replacing A by A° then it suffices to prove the theorem when $F = K = Q(A)$.

Under the assumption $k = \bar{k}$, we have $|k| = \infty$ and $F = k(x_1, \ldots, x_n)$ is separably generated over k (by Theorem 1.44).

Noether normalization implies that there are $z_i = \sum_{i=1}^n a_{ij}\, x_j$, $i \in [1, d]$, $d = \text{tr.deg}_k F$ such that A is integral and separable over the polynomial algebra $B := k[z_1, \ldots, z_d]$, which is integrally closed and Noetherian. Hence A' is also the integral closure of B in F.

By Theorem 1.57 and the remark following it, we see that A' is a finite B-module. In particular it is also a finite A-module. □

The general case can be reduced to the case $k = \bar{k}$. See Zariski–Samuel for the details.

Exercise 1.2. Let Y be an affine k-variety with $k = \bar{k}$. Then the normal points form an open subset. Moreover there is a normal affine k-variety Y' and a birational morphism $\pi : Y' \to Y$ with the universal property that any dominant morphism $\phi : Z \to Y$ with Z a normal k-variety factors through Y' uniquely. What happens if Y is a quasi-projective variety?

Corollary 1.60. *Let A be a Dedekind domain. i.e. a Noetherian integrally closed domain of dimension one. Let F be a finite extension of $K = Q(A)$. Then the integral closure of A in F is also Dedekind.*

The is fundamental in algebraic number theory. In our treatment here, to preserve the Noetherian condition requires that F/K being separable. Again we refer to Zariski–Samuel for the reduction to the separable case.

3.3. Valuation rings. In general, normal points are far from being nonsingular, since integrally closed domains are far from being regular local rings. However in dimension one they coincide. This makes the study of curves more manageable. A notion connecting them is "valuation rings".

Let K be a field and $(\Gamma, +, >)$ a totally ordered abelian group. A valuation $v : (K^\times, \bullet) \to (\Gamma, +)$ is a group homomorphism such that

$$v(x+y) \geq \min(v(x), v(y)).$$

The ring $R = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$ is called the valuation ring of v. The set $m = \{x \in K^\times \mid v(x) > 0\} \cup \{0\} \subset R$ is easily seen to be the unique maximal ideal of R and thus (R, m) is a local ring.

In general, an integral domain R is called a valuation ring if it comes from a valuation v on it quotient field $K = Q(R)$. Also if v restricts to zero on some subfield $k \subset K$ then we called v a valuation on K/k. For study on k-varieties we mainly consider valuations of this type.

Notice that we have the basic property that for $x \in K$,

$$x \notin R \Longrightarrow x^{-1} \in R.$$

We will see shortly that this characterizes valuation rings!

When $\Gamma = \mathbb{Z}$, we call v a discrete valuation and R a discrete valuation ring, denoted by DVR for short.

Theorem 1.61. *Let $(A, \mathfrak{m})$ be a Noetherian local domain with $\dim A = 1$, and let $k = A/\mathfrak{m}$ be its residue field. Then the following are equivalent.*

(1) *A is a DVR.*
(2) *A is normal (i.e. integrally closed in $K = Q(A)$).*
(3) *A is regular (i.e. $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$).*
(4) *$\mathfrak{m}$ is principal.*

PROOF. (3) $\Longleftrightarrow$ (4) by Nakayama's lemma.

(1) $\Longrightarrow$ (2): let $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, $x \in K$, $a_i \in A$. We claim that $x \in A$. If not then $x^{-1} \in A$, hence

$$x = -(a_{n-1} + a_{n-1}x^{-1} + \ldots + a_0 x^{-(n-1)}) \in A,$$

which is a contradiction.

(2) $\Longrightarrow$ (3) $\equiv$ (4): let $a \in \mathfrak{m} \setminus \{0\}$. Since $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n = 0$ for Noetherian local rings (cf. Corollary 1.72), there is an $n \in \mathbb{N}$ such that $(a) \supset \mathfrak{m}^n$ but $(a) \not\supset \mathfrak{m}^{n-1}$. Let $b \in \mathfrak{m}^{n-1} \setminus (a)$, then $x := a/b \in K$ but $x^{-1} = b/a \notin A$. So x^{-1} is not integral over A (since A is integrally closed). This implies that

$$x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$$

since m is finitely generated. By construction $x^{-1}\mathfrak{m} \subset \mathfrak{m}^n/a \subset A$. Hence in fact $x^{-1}\mathfrak{m} = A$. That is, $\mathfrak{m} = xA = (x)$.

(3) $\equiv$ (4) $\Longrightarrow$ (1): $\mathfrak{m} = (x)$ implies that $\mathfrak{m}^n = (x^n)$. Also $\mathfrak{m}^{n+1} = \mathfrak{m}(\mathfrak{m}^n) \subsetneq \mathfrak{m}^n$ for otherwise $\mathfrak{m}^n = 0$ (Nakayama lemma) and then $\dim A = 0$, a contradiction. In particular for any $0 \neq a \in A$ we have $(a) = \mathfrak{m}^{n(a)}$ for a unique $n(a) \geq 0$. That is, an unique factorization

$$a = ux^{n(a)} \qquad \text{for some unit } u \in A.$$

The valuation $v : K^\times \to \mathbb{Z}$ is then defined by $v(a/b) := n(a) - n(b)$. □

Notice that the proof of (1) $\Rightarrow$ (2) is valid for general valuation rings. Namely, valuation ring are all integrally closed.

General valuation rings are considerably more abstract and complicate. But we do have a simple characterization:

Lemma 1.62. *Let R be a domain with $K = Q(R)$. Then R is a valuation ring of $K \Longleftrightarrow$ for every $x \in K^\times$ either $x \in R$ or $x^{-1} \in R$ (or both).*

PROOF. We have seen the direction $\Rightarrow$ which is easy. For $\Leftarrow$, we need to construct the valuation map $v : K^\times \to \Gamma$.

Consider the multiplicative group $\Gamma := K^\times/U(R)$. For $\bar{x}, \bar{y} \in \Gamma$, we define $\bar{x} \geq \bar{y}$ if $x/y \in R$. By assumption we have either $x/y \in R$ or $y/x \in R$, hence $(\Gamma, \bullet, >)$ is a totally ordered abelian group and we get the natural map $v : K^\times \to \Gamma$ by $x \mapsto v(x) := \bar{x}$.

This is a valuation of K with valuation ring R as expected. □

Remark 1.63. (1) In some literature (e.g. Atiyah–MacDonald) a valuation ring is defined by the above equivalent property.

(2) Similar reasoning shows that for any two ideals I, J in R, either $I \subset J$ or $J \subset I$. Indeed if there are $a \in I \setminus J$ and $b \in J \setminus I$, then we may assume that $a/b \in R$ and then $a \in bR \subset J$, a contradiction.

To construct valuation rings out from local rings, we need the notion of domination of local rings.

Definition 1.64. Let (A, m_A) and (B, m_B) be two local rings in a field K. We say that B dominants A ($B > A$) if $A \subset B$ such that $m_B^c := m_B \cap A = m_A$.

Theorem 1.65. *A local ring R is a valuation ring in $K \Longleftrightarrow R$ is a maximal element under domination. In particular, any local ring $R \subset K$ with $Q(R) = K$ is dominated by a valuation ring.*

PROOF. $\Rightarrow$: let $S > R$ but $S \neq R$. For any $a \in S \setminus R$ we have $a^{-1} \in R$. Then in fact $a^{-1} \in m_R$ (otherwise it is a unit and then $a = (a^{-1})^{-1} \in R$).

Since $m_S \cap R = m_R$, we have $a^{-1} \in m_S$. Then $1 = aa^{-1} \in m_S$, which is a contradiction. Hence such a local ring S does not exist.

$\Leftarrow$: suppose that $(R, \mathfrak{m})$ is maximal under domination.

Let $x \in K^\times$. We claim that

$$\text{either} \quad \mathfrak{m}[x] \neq R[x] \quad \text{or} \quad \mathfrak{m}[x^{-1}] \neq R[x^{-1}].$$

For otherwise we have two shortest relations

$$\textstyle\sum_{i=0}^m u_i x^i = 1, \qquad \sum_{j=0}^n v_j x^{-j}, \qquad u_i, v_j \in m.$$

Say $m \geq n$. Multiplying the second equation by x^m we get $(1 - v_0)x^m = \sum_{j=1}^n v_j x^{m-j}$. Since $1 - v_0 \in U(R)$ and $m > m - j \geq 0$ in the expression, this allows us to substitute x^m by lower degree terms into the first equation and get a shorter relation, which leads to a contradiction.

Consider the case that $\mathfrak{m}[x] \subsetneq R[x]$. There is a maximal ideal $M \subset R[x]$ such that $\mathfrak{m}[x] \subset M$. Hence $M \cap R \supset \mathfrak{m}$. But then $M \cap R = \mathfrak{m}$ since $\mathfrak{m}$ is a maximal ideal. That is, $(R[x], M)$ dominates $(R, \mathfrak{m})$. The maximality of R then implies that $R[x] = R$, i.e. $x \in R$.

The other case that $\mathfrak{m}[x^{-1}] \subsetneq R[x^{-1}]$ is done similarly, with the consequence being $x^{-1} \in R$. Hence R is a valuation ring by Lemma 1.62.

The last existence statement now follows easily by Zorn's lemma. □

Similar idea can be used to prove the following extension result:

Exercise 1.3. Let $\psi : R \to F$ be a ring homomorphism from a domain to an algebraically closed field. Let $0 \neq a \in K = Q(R)$. Then ψ can be extended to a ring homomorphism from either $R[a]$ or $R[a^{-1}]$ to F.

There could be many valuation rings containing a given domain. The collection of them together determines the integral closure:

Theorem 1.66. *Let A be a subring of a field K, then the integral closure A' of A in K is the intersection of all valuation rings in K which contain A.*

PROOF. We have shown that valuation rings are integrally closed in the proof of Theorem 1.61 (1) $\Rightarrow$ (2). Hence A' is contained in the intersection of all such valuation rings. To see they are equal, let $x \in K$ which is not integral over A. Then it is clear that x^{-1} is not a unit in $A[x^{-1}]$. Let $M \subset A[x^{-1}]$ be a maximal ideal containing x^{-1} and consider the map

$$\phi : A[x^{-1}] \to A[x^{-1}]/M =: F.$$

Hence $x^{-1} \in \ker \phi$. Consider the ring homomorphism $\psi : A[x^{-1}] \to \overline{F}$ to the algebraic closure of F. By Zorn's lemma there is a maximal extension $\tilde{\psi}$ of ψ inside K: namely $A[x^{-1}] \subset B \subset K$, $\psi' : B \to \overline{F}$ with $\psi'|_{A[x^{-1}]} = \psi$. By the above exercise, B is a valuation ring. We claim that $x \notin B$, for otherwise $1 = \psi'(1) = \psi'(xx^{-1}) = \psi'(x)\psi'(x^{-1}) = 0$. This completes the proof. □

Theorem 1.65 and 1.66 will play fundamental role in the study of properties of schemes. For applications to curves in the following subsection, we need only DVR and Theorem 1.61.

3.4. Non-singular curves. A curve C over k is by definition a one dimensional k-variety. We assume that $k = \bar{k}$.

Theorem 1.67. *The normalization of a curve is a non-singular curve.*

Proof. By taking closure, it suffices to consider a projective curve $C \subset \mathbb{P}^n$, and we may assume that $C \cap H_0$ consists of non-singular points of C (here $H_0 = Z(x_0) \cong \mathbb{P}^{n-1}$). Thus the theorem is reduced to the affine case $C_0 \subset \mathbb{A}^n$. Let $A = A(C_0) = k[x_1, \ldots, x_n]/I$. By Theorem 1.59, the integral closure A' of A in $K(C_0)$ can be presented as

$$\big(k[x_1, \ldots, x_n]/I\big)[y_1, \ldots, y_m]/J \cong k[\mathbf{x}, \mathbf{y}]/(I + J).$$

That is, the normalization is $C_0' \subset \mathbb{A}^{n+m}$ defined by $I + J$. This is a non-singular curve by Theorem 1.61. Consequently the normalization of C is $\overline{C_0'} \subset \mathbb{P}^{n+m}$ which is non-singular. □

Theorem 1.68. *Every curve is birational equivalent to a unique non-singular projective curve. Moreover, the following three categories are equivalent:*

1. *Non-singular projective curves with dominant morphisms.*
2. *Quasi-projective curves with dominant rational maps.*
3. *Function fields K/k of dimension one with k-homomorphisms.*

Proof. The equivalence of (2) and (3) is a special case of Theorem 1.37. Also a dominant $f : C \to C'$ of non-singular projective curves in (1) clearly induces $K(C') \hookrightarrow K(C)$ in (3) via pull back. So we are left to show that k-homomorphism of function fields $K(C') \to K(C)$ leads to morphisms $C \to C'$. [This is the algebraic version of the "Riemann extension theorem" in the context of Riemann surfaces.] With this proved, then it also follows that $K(C) \cong K(C') \Longrightarrow C \cong C'$, which is the first statement of the Theorem.

Now we have a rational map $C \dashrightarrow C' \subset \mathbb{P}^n$, which gives a morphism

$$\phi : C \setminus \{p_1, \ldots, p_m\} \longrightarrow \mathbb{P}^n.$$

It suffices to show there is an extension $\tilde{\phi} : C \to \mathbb{P}^n$ since then the image lies in $\overline{\phi(C)} = C'$ automatically, and the uniqueness is a basic property of morphisms on varieties.

We will do this for each p_i separately, so we are in the situation that $p \in X$ with $X \subset C$ being open, and

$$\phi : X \setminus p \to \mathbb{P}^n, \qquad \phi(X \setminus p) \cap U \neq \emptyset,$$

where $U = \bigcap_{i=0}^n D(x_i)$. (Otherwise replace $\mathbb{P}^n$ by a hyperplane $\mathbb{P}^{n-1}$.)

In this setup, by Theorem 1.61, $(\mathscr{O}_p, m_p)$ is a DVR. [More precisely, $m_p = (x)$ for x being a "local parameter defining p" and the discrete valuation $v(f)$ is the order of f at p: $f = ux^{v(f)}$ in $\mathscr{O}_p$, where u is a unit.]

Let $f_{ij} := (x_i/x_j) \circ \phi$. It is regular on some open set in X, hence $f_{ij} \in K = K(X) = K(C)$. Let $r_i = v(f_{i0})$, then $v(f_{ij}) = r_i - r_j$. Suppose that r_k is minimal among r_i's, then $f_{ik} \in \mathscr{O}_p$ for all i. We use them to define a map

$$\tilde{\phi}(q) = (f_{0k}(q), \ldots, \widehat{f_{kk}(q)}, \ldots, f_{nk}(q)) \in U_k \cong D(x_k) \subset \mathbb{P}^n.$$

This is a morphism in a neighborhood of $V \ni p$ which coincides with ϕ outside p by our construction. This completes the proof. □

Remark 1.69. There are at least two other methods to obtain the non-singular projective curve to represent a function field K of a given curve:

(1) Instead of using finiteness of integral closure, one may also use blow-ups inductively to resolve the singularities of a curve C. It requires to define numerical invariants of a singular point and to show that they decreases under blowing-up. A version of it will be developed later.

(2) There is also a more abstract approach. For a f.g. field K/k with $\text{tr.deg}_k K = 1$, one may define an "abstract non-singular curve" C_K to be the set of all DVR of K/k. A point $p \in C_K$ corresponds to a DVR called R_p. When $k = \bar{k}$, $|C_K| = \infty$ and a topology can be defined such that closed subsets consist of finite subset of C_K. For each open set U we define $\mathscr{O}(U) = \bigcap_{p \in U} R_p$. Then it C_K is in fact isomorphic to a non-singular projective curve (cf. Hartshorne Ch.1 Theorem 6.9, compare the proof given there with the approach used in this subsection).

4. Hilbert polynomials

So far the only invariants we have defined for a variety X are $\dim X$ and $K(X)$. To find other interesting invariants the most powerful tool used today is the homological method, which will be studied later. Nevertheless, the Hilbert polynomial provides a equally powerful tool when the problem considered is over a local ring or a graded ring.

4.1. Artin–Ress and Nakayama.

Definition 1.70. For $I \subset R$ be an ideal, the Ress algebra is

$$T = T_I := \bigoplus_{i=0}^{\infty} I^i\, x^i \subset R[x].$$

For noetherian R, T is also noetherian. For $M \in \mathrm{mod}_R$,

$$T_M := \bigoplus_{i=0}^{\infty} I^i M\, x^i \subset M[x] := M \otimes_R R[x].$$

If M is finitely generated then T_M is a finitely generated T-module. If R is also Noetherian, then T_M is a Noetherian T-module.

Lemma 1.71 (Artin–Ress). *If R is noetherian and M is a f.g. R-module, then for any two submodule $M_1, M_2 \subset M$ there exists $k \in \mathbb{N}$ such that for all $n \geq k$,*

$$I^n M_1 \cap M_2 = I^{n-k}(I^k M_1 \cap M_2).$$

PROOF. "$\supset$" is clear. For "$\subset$", consider the "generating function"

$$N := \bigoplus_{i=0}^{\infty} I^i (M_1 \cap M_2) x^i \subset T_M,$$

which is a T-submodule. Hence it is generated by some $u_i = \sum_{j=0}^{k} n_{ij}\, x^j$, $i \in [1, m]$ with $n_{ij} \in I^j M_1 \cap M_2$. Let $n \geq k$.

$$u \in I^n M_1 \cap M_2 \Longrightarrow u x^n = \sum f_i u_i = \sum f_{il}\, x^l\, n_{ij}\, x^j.$$

In the expression $f_{il} \in I^l$, comparing degree we see that $f_{il} \in I^{n-j}$. That is, $u \in I^{n-j}(I^j M_1 \cap M_2) = I^{n-k} I^{k-j} (J^j M_1 \cap M_2) \subset I^{n-k}(I^k M_1 \cap M_2)$. □

Corollary 1.72 (Krull's intersection theorem). *Let R be noetherian and M be a f.g. R-module. Denote $I^\infty M := \bigcap_{i=1}^{\infty} I^i M$, then $I(I^\infty M) = I^\infty M$.*

In particular, if $J = J_R$ is the Jacobson radical then $\bigcap_{n=1}^{\infty} J^n M = 0$.

PROOF. Put $M_1 = M$ and $M_2 = I^\infty M$ in Atrin-Ress lemma and get the number k, then $I^\infty M = I^{k+1} M \cap I^\infty M = I(I^k M \cap I^\infty M) = I(I^\infty M)$.

The second statement then follows from the Nakayama Lemma. □

For convenience we recall that $J_R = \bigcap_{I:\text{maximal}} I$ and

Lemma 1.73 (Nakayama). *Let M be a f,g, R-module, $J_R\, M = M \Rightarrow M = 0$.*

Indeed if $M \neq 0$, let $x_1, \dots, x_m$ be a shortest generating set, then $x_m = r_1 x_1 + \dots + r_m x_m$ for $r_j \in J_R$. Then $(1 - r_m) = r_1 x_1 + \dots r_{m-1} x_{m-1}$ and $1 - r_m$ is invertible. So x_m is redundant and we get a contradiction!

Corollary 1.74. *Let M be a f,g, R-module. Then $x_1, \dots, x_n$ generate $M \iff \bar{x}_1, \dots, \bar{x}_n$ generate $\overline{M} := M/JM$.*

For "$\Leftarrow$", let $N = \sum R x_i$. Then $M = N + JM$ and so $M/N = J(M/N)$.

Corollary 1.75. *A finitely generated projective module over a local ring is free.*

For a local ring $(R, \mathfrak{m})$ we have $J_R = \mathfrak{m}$. If $P \oplus Q = R^n$, we get $P/\mathfrak{m}P \oplus Q/\mathfrak{m}Q = R^n/\mathfrak{m}R^n$ as $k = R/\mathfrak{m}$ vector spaces. Now a vector space basis $\bar{x}_1, \dots \bar{x}_p$ for $P/\mathfrak{m}P \cong k^p$ and $\bar{y}_1, \dots, \bar{y}_q$ for $Q/\mathfrak{m}Q \cong k^q$, $p + q = n$, leads to n elements $\{x_i, y_j\}$ which generate R^n, hence they must be a free basis. In particular both P and Q are free R-modules.

4.2. Hilbert polynomial for graded modules. Let $R = \bigoplus_{i \geq 0} R_i$ be a graded ring, then R_0 is a subring and R_+ is an ideal.

Proposition 1.76. *(1) R is noetherian $\iff$ R_0 is noetherian and R is a finitely generated R_0-algebra. Under this condition, then*

(2) If $M = \bigoplus_{i \geq 0} M_i$ is finitely generated graded R-module then M_i is a finitely generated R_0-module for all i.

Proof. (1) "$\Leftarrow$" is by Hilbert basis theorem. "$\Rightarrow$": $R_0 = R/R_+$ is Noetherian. Let $R_+ = (x_1, \dots, x_m)$ with x_i homogeneous. By induction on d, every $a \in R_d$ is then polynomial in x_i's with coefficients in R_0.

(2) Let $M = \bigoplus_{i=1}^r R u_i$, with u_i being homogeneous. Then similarly M_n is generated over R_0 by $y_i u_i$ with $y_i = x^\alpha$ such that $\deg y_i + \deg u_i = n$. □

From now on we assume that R is noetherian, M is finitely generated over R, and R_0 is artinian (e.g. a field k). Then M_n is both noetherian and artinian over R_0 and the length $\ell(M_n)$ is defined. The basic question is to get the structure of $\ell(M_n)$ when n varies. It turns out to be almost polynomial!

Definition 1.77 (Poincaré series). *$P(M, t) := \sum_{n \geq 0} \ell(M_n)\, t^n$.*

Theorem 1.78 (Hilbert–Serre)**.** *Let $R_+ = (x_1, \dots, x_m)$ with $x_i \in R_{d_i}$. Then there is a polynomial $f(t) \in \mathbb{Z}[t]$ such that*

$$P(M,t) = \frac{f(t)}{\prod_{i=1}^{m}(1-t^{e_i})}.$$

PROOF. Notice that for any exact sequence $0 \to N_0 \to N_1 \to \dots \to N_s \to 0$ of R_0-modules, we have $\sum_{i=0}^{s}(-1)^i \ell(N_i) = 0$.

We prove the theorem by induction on m. For $m = 0$, $R = R_0$ and M is a finitely generated R_0-module. Then we have

$$f(t) := P(M,t) \in \mathbb{Z}[x].$$

Assume the theorem holds for up to $m-1$ generators. Consider

$$0 \to K_n \to M_n \xrightarrow{x_m \bullet} M_{n+e_m} \to C_{n+e_m} \to 0.$$

Then $\ell(M_n) - \ell(M_{n+e_m}) = \ell(K_n) - \ell(C_{n+e_m})$. Multiplying t^{n+e_m} to it and summing up for $n = 0, \dots, \infty$ we find

$$(t^{e_m} - 1)P(M,t) = P(K,t)\, t^{e_m} - P(C,t) + g(t)$$

for some $g(t) \in \mathbb{Z}[t]$. Now the key observation is that

$$x_m K_\bullet = 0 = x_m C_\bullet.$$

Hence K, C can be regarded as R/Rx_m-module. By induction we get

$$(t^{e_m} - 1)P(M,t) = \frac{f_1(t)}{\prod_{i=1}^{m-1}(1-t^{e_i})} t^{e_m} - \frac{f_2(t)}{\prod_{i=1}^{m-1}(1-t^{e_i})} + g(t).$$

This prove the theorem. □

Corollary 1.79 (Hilbert–Serre)**.** *If R is generated by $R_1 = (x_1, \dots, x_m)$ over R_0, then there is a unique polynomial $p_M(t) \in \mathbb{Q}[t]$ with* $\deg p \le m-1$ *such that $\ell(M_n) = p_M(n)$ for all large n. $p_M(t)$ is known as the Hilbert polynomial of M.*

This follows from a simple manipulation on $f(t)/(1-t)^m$. In fact we have $\ell(M_n) = p_M(n)$ for all $n \ge \deg g(t)$.

Example 1.80. (1) (Global example) Let $I \subset S = k[x_0, \dots, x_n]$ be a homogeneous ideal defining a projective variety $X \subset \mathbb{P}^n_k$, $M := R/I = \bigoplus_{d \ge 0} M_d$. Then the degree and the coefficients of $p_M(t)$ encodes important geometric invariants of X. We will study some of them in the last subsection.

(2) (Local example) Let $I \subset R$ be an ideal in a general commutative ring. Let

$$G_I(R) := \bigoplus_{n \ge 0} I^n / I^{n+1} \cong T/IT$$

be a graded ring generated by I/I^2. Let M be an R-module, let

$$G_I(M) := \bigoplus\nolimits_{n\geq 0} I^n M/I^{n+1}M \cong TM/ITM$$

be the associated $G_I(R)$-graded module. When R is noetherian and M is finitely generated, we see that $G_I(R)$ is also noetherian and $G_I(M)$ is finitely generated.

The theory of Hilbert polynomial can be applied when R/I is artinian. The typical case is a noetherian local ring $(R, \mathfrak{m})$ with $I = Q$ be a $\mathfrak{m}$-primary ideal. This is equivalent to that $\mathfrak{m}^e \subset Q \subset \mathfrak{m}$ for some $e \in \mathbb{N}$.

Let $Q/Q^2 = (y_1, \ldots, y_m)$. Then there is a polynomial $p(t) \in \mathbb{Q}[t]$ with degree $\leq m-1$ such that $p(n) = \ell(Q^n/Q^{n+1})$ for large n.

Corollary 1.81. *Let $(R, \mathfrak{m})$ be a noetherian local ring, Q an $\mathfrak{m}$-primary ideal, $Q/Q^2 = (y_1, \ldots, y_m)$. Then there is a polynomial $\chi_Q(t) \in \mathbb{Q}(t)$ of degree $\leq m$ such that $\chi_Q(n) = \ell(R/Q^n)$.*

Moreover, $\deg \chi_Q$ *is independent of the choices of the m-primary ideal Q.*

Proof. The first statement follows from $\ell(R/Q^{n+1}) - \ell(R/Q^n) = p(n)$. For the second statement, for any two m-primary ideals Q and $\tilde{Q}$ we have $\tilde{Q}^s \subset Q$ for some $s \in \mathbb{N}$. Then

$$\ell(R/Q^n) \leq \ell(R/\tilde{Q}^{sn}),$$

which implies that $\deg \chi_Q \leq \deg \chi_{\tilde{Q}}$. Now switch the roles of Q and $\tilde{Q}$. □

4.3. Dimension theory for local rings.

Theorem 1.82. *Let $(R, \mathfrak{m})$ be a noetherian local ring. The following three integers are the same:*

(i) $d := \deg \chi_Q$ *for a (hence any) $\mathfrak{m}$-primary ideal Q.*
(ii) $m = m(R)$*, the minimal number of generators of some $\mathfrak{m}$-primary ideal.*
(iii) $D = D(R) := \dim R$*, the Krull dimension.*

This is striking since Nagata had found examples showing that $\dim R$ could be infinite for general noetherian rings.

Proof. The proof relies on the Artin–Ress Lemma and the Hilbert polynomial theory in an essential way. We will show that $d \leq m \leq D \leq d$.

Step 1: $d \leq m$ by Corollary 1.81 (Hilbert polynomial theory).

Step 2: $m \leq D$: may assume that $D < \infty$ and do induction on D. $D = 0 \Leftrightarrow \mathfrak{m}$ is the only prime ideal $\Rightarrow \mathfrak{m} = \sqrt{0}$ is nilpotent (since R is noetherian) $\Rightarrow (0)$ is $\mathfrak{m}$-primary $\Rightarrow m = 0$.

Let $D > 0$ and let $\mathfrak{p}_i$, $i \in [1, r]$ be the minimal primes. Then for any prime $\mathfrak{p}$, we have $\mathfrak{m} \supset \mathfrak{p} \supset \mathfrak{p}_i$ for some i. The prime avoidance and $D > 0$ implies that $\mathfrak{m} \not\subset \bigcup \mathfrak{p}_i$. Let $x \in \mathfrak{m} \setminus \bigcup \mathfrak{p}_i$ and consider the local ring $R' = R/(x)$. A prime chain in R'' takes the form

$$\mathfrak{p}_0'/(x) \supsetneq \mathfrak{p}_1'/(x) \supsetneq \dots \supsetneq \mathfrak{p}_s'/(x).$$

Since $x \in \mathfrak{p}_s'$, we have $\mathfrak{p}_s' \supsetneq \mathfrak{p}_i$ for some i. Hence we get a prime chain in R:

$$\mathfrak{p}_0' \supsetneq \mathfrak{p}_1' \supsetneq \dots \mathfrak{p}_s' \supsetneq \mathfrak{p}_i.$$

That is, $D' + 1 \leq D$. [This is a generalization of the simple fact that for a domain R and $0 \neq x \in R$, $\dim R/(x) \leq \dim R - 1$.]

Also, if $\bar{y}_1, \dots, \bar{y}_{m'}$ generate $Q'/(x)$ in R', which is a $\mathfrak{m}' = \mathfrak{m}/(x)$-primary ideal, then $y_1, \dots, y_{m'}, x$ generate Q in R, and Q' is $\mathfrak{m}$-primary. Then by induction we get $m(R) \leq m(R') + 1 \leq D' + 1 \leq D$.

Step 3: $D \leq d$: We prove by induction on d.

If $d = 0$ then $\ell(R/\mathfrak{m}^n)$ is constant for n large. That is, $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \mathfrak{m}(\mathfrak{m}^n)$. Hence $\mathfrak{m}^n = 0$ by Nakayama lemma. Then $\mathfrak{m}$ is the only prime ($\mathfrak{p} \supset (0) = \mathfrak{m}^n \Rightarrow \mathfrak{p} \supset \mathfrak{m}$) and so $D = 0$.

Let $d > 0$. For any maximal prime chain $\mathfrak{m} = \mathfrak{p}_0 \supsetneq \dots \supsetneq \mathfrak{p}_s$ ($s \leq D$, and D is the sup among all s). R is a domain $\Leftrightarrow \mathfrak{p}_s = (0)$. If $\mathfrak{p}_s \neq (0)$ then we consider $\bar{R} = R/\mathfrak{p}_s$ instead. Since

$$\ell(\bar{R}/\bar{\mathfrak{m}}^n) \leq \ell(R/\mathfrak{m}^n) \Longrightarrow d(\bar{R}) \leq d(R),$$

it suffices to consider a domain R to show that $s \leq d$ (so $\mathfrak{p}_s = (0)$).

Let $x \in \mathfrak{p}_{s-1} \setminus \{0\}$ and consider the prime chain in $\bar{R} := R/(x)$:

$$\mathfrak{m}/(x) \supsetneq \mathfrak{p}_1/(x) \supsetneq \dots \supsetneq \mathfrak{p}_{s-1}/(x).$$

We claim that $d(\bar{R}) \leq d(R) - 1$. With this proved then $s - 1 \leq D(\bar{R}) \leq d(\bar{R}) \leq d(R) - 1$ and the then $D(R) = \max s \leq d(R)$ as expected.

To prove the claim, notice that

$$\ell(\bar{R}/\bar{m}^n) = \ell(R/(\mathfrak{m}^m + (x))) = \ell(R/\mathfrak{m}^n) - \ell((\mathfrak{m}^n + (x))/\mathfrak{m}^n),$$

and the last term equals $\ell((x)/\mathfrak{m}^n \cap (x))$. Artin–Ress Lemma (Lemma 1.71) implies that there exists $k \in \mathbb{N}$ such that for all $n \geq k$:

$$\mathfrak{m}^n \cap (x) = \mathfrak{m}^{n-k}(\mathfrak{m}^k \cap (x)) \subset \mathfrak{m}^{n-k}(x),$$

which implies that $\ell((x)/\mathfrak{m}^n \cap (x)) \geq \ell((x)/\mathfrak{m}^{n-k}(x)) = \ell(R/\mathfrak{m}^{n-k})$.

Putting everything together we get $\ell(\bar{R}/\bar{m}^n) \leq \ell(R/\mathfrak{m}^n) - \ell(R/\mathfrak{m}^{n-k})$, which implies the claim. This completes the proof. □

The first application is already used when we define regular local rings.

Corollary 1.83. *For any noetherian local ring $(R, \mathfrak{m})$, $\dim R \le \dim_k \mathfrak{m}/\mathfrak{m}^2$.*

Indeed, by Nakayama lemma $\dim_k \mathfrak{m}/\mathfrak{m}^2$ is the minimal number of generators of $\mathfrak{m}$.

The second application has also been discussed for affine k-algebras.

Corollary 1.84 (Krull's (generalized) principal ideal theorem)**.** *Let R be a noetherian ring, $I \subset R$ be an ideal generated by m elements. Then any minimal "prime ideal $\mathfrak{p}$ containing I" has $\operatorname{ht} \mathfrak{p} \le m$.*

This is readily seen to reduce to the local ring case on $(R_\mathfrak{p}, \mathfrak{p}_\mathfrak{p})$. Since $\mathfrak{p}_\mathfrak{p}$ is the only prime containing $I_\mathfrak{p}$ in $R_\mathfrak{p}$, we see that $I_\mathfrak{p}$ is $\mathfrak{p}_\mathfrak{p}$-primary. If $y_1, \ldots, y_m$ generate I then they also generate $I_\mathfrak{p}$. Then $\operatorname{ht} \mathfrak{p} = \dim R_p \le m$ by the (local) dimension theorem.

Example 1.85. Let $k = \bar{k}$. Then $\dim k[x_1, \ldots, x_m] = m$.

We have proved this in Proposition1.17 (for general k) using Noether normalization. Here we know that all the the maximal ideals are of the form $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_m - a_m)$ and $\dim k[x_1, \ldots, x_m] \ge m$ by an obvious prime chain. By Krrull's theorem, we also have $\dim k[x_1, \ldots, x_m] \le \sup_{a \in k^n} \operatorname{ht} \mathfrak{m}_a \le m$.

4.4. Intersection theory in projective spaces. The classical Bezout theorem says that the total intersection number (counted with multiplicity) of two algebraic curves in $\mathbb{P}^2_k$, $k = \bar{k}$, of degree d_1 and d_2 is $d_1 d_2$.

In this final subsection we use Hilbert polynomial theory to extend it to certain higher dimensional intersections in $\mathbb{P}^n_k$, over $k = \bar{k}$. Firstly we discuss the basic dimension estimates of intersections of varieties:

Theorem 1.86 (Affine dimension theorem)**.** *Let $Y, Z \subset \mathbb{A}^n_k$, $k = \bar{k}$, be affine varieties of dimension r, s respectively. Then every irreducible component $W \subset Y \cap Z$ has dimension $\ge r + s - n$.*

Of course this may fail if $k \ne \bar{k}$. Consider $Y, Z \subset \mathbb{R}^3$ defined by $z = x^2 + y^2$ and $z = 0$ respectively. Then $Y \cap Z = \{(0,0,0)\}$ is a point.

Proof. If $Z = Z(f)$ is a hypersurface and $Y \subset Z$ then done. If $Y \not\subset Z$, W corresponds to a minimal prime divisor of (f) in $A(Y)$. Then Krull's principal ideal theorem (Corollary 1.84) implies that $\operatorname{ht} \mathfrak{p} = 1$. Hence by the dimension formula (Corollary 1.20) we get $\dim A(Y)/\mathfrak{p} = r - 1$.

For general Z, $Y \times Z \subset \mathbb{A}^{2n} \supset \Delta \cong \mathbb{A}^n$, where $\Delta = \{ (a, a) \mid a \in \mathbb{A}^n \}$ is the diagonal. Under the later isomorphism, $Y \cap Z \cong (Y \times Z) \cap \Delta$. Now

Δ is the complete intersection of n hyperplanes defined by $x_i - y_i = 0$. The theorem follows by applying the hypersurface case n-times inductively. □

Corollary 1.87 (Projective dimension theorem)**.** *Let $Y, Z \subset \mathbb{P}^n_k$, $k = \bar{k}$, be projective varieties of dimension r, s respectively. Then*

(i) *Every irreducible component of $Y \cap Z$ has dimension $\geq r + s - n$.*
(ii) *$r + s - n \geq 0 \Longrightarrow Y \cap Z \neq \emptyset$.*

PROOF. (i) follows from the affine case.

For (ii), the affine cones $C(Y), C(Z) \subset \mathbb{A}^{n+1}$ have dimension $r+1$ and $s+1$ respectively. Also $0 \in C(Y) \cap C(Z) \neq \emptyset$. The affine case implies that $\dim C(Y) \cap C(Z) \geq (r+1) + (s+1) - (n+1) = r + s - n + 1 \geq 1$. That is, there exists $Q \neq 0$ and $Q \in C(Y) \cap C(Z)$. Thus $Y \cap Z \neq \emptyset$. □

The above results will be necessary only when we insist to work on varieties (solutions of equations). If we work on the prime spectrum instead (equations) then similar results hold automatically.

Definition 1.88 (Twisting module). Let $S = \bigoplus_{d\geq 0} S_d$ be a graded ring, $M = \bigoplus_{d \in \mathbb{Z}} M_d$ a graded S-module. For any $n \in \mathbb{Z}$, we define the graded S-module $M(n)$ by $M(n)_d := M_{n+d}$.

Notice that $\operatorname{ann} M \subset S$ is a homogeneous ideal.

Proposition 1.89. *If S is noetherian, M is finitely generated, then there is a (non-unique) filtration of graded submodules*

$$0 = M^0 \subsetneq M^1 \subsetneq \ldots \subsetneq M^r = M$$

such that $M^i/M^{i+1} \cong (S/\mathfrak{p}_i)(e_i)$ where $\mathfrak{p}_i$ is a homogeneous prime and $e_i \in \mathbb{Z}$.

Moreover, a homogeneous prime $\mathfrak{p} \supset \operatorname{ann} M$ if and only if $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. Hence each minimal prime $\mathfrak{p} \supset \operatorname{ann} M$ appears in $\mathfrak{p}_i$'s. The number of appearances is precisely $\mu_\mathfrak{p}(M) \equiv \ell_{S_\mathfrak{p}}(M_\mathfrak{p})$, which is independent of the choices of filtrations.

PROOF. To prove the existence of such a filtration, let $X = \{ M' \subset M \mid M' \text{ is graded and such a filtration exists} \} \neq \emptyset$ since $0 \in X$.

S is noetherian implies that there is a maximal element $M' \in X$. Let $M'' = M/M'$. If $M'' \neq 0$, consider the set

$$\mathscr{I} := \{ \operatorname{ann}(m) \mid 0 \neq m \in M'' \text{ being homogeneous} \},$$

and let $\operatorname{ann}(m) \subsetneq S$ be a maximal element in $\mathscr{I}$.

We claim that the homogeneous ideal $\operatorname{ann}(m)$ is prime. Indeed, for homogeneous $a, b \in S$ with $ab \in \operatorname{ann}(m)$ and $b \notin \operatorname{ann}(m)$, $0 \neq bm \in M''$, $\operatorname{ann}(m) \subset \operatorname{ann}(bm)$ hence they are equal. So $a \in \operatorname{ann}(bm) = \operatorname{ann}(m)$.

Denote $\mathfrak{p} = \operatorname{ann}(m)$, $n = \deg m$. Then $M'' \supset N := Sm \cong (S/\mathfrak{p})(-n)$. Take inverse image in M we get $M \supset N' \supset M'$ such that

$$N'/M' \cong (S/\mathfrak{p})(-n).$$

This contradicts the maximality of M'. Hence in fact $M' = M$.

Given such a filtration, it is clear that $\operatorname{ann} M = \bigcap \mathfrak{p}_i$. Hence $\mathfrak{p} \supset \operatorname{ann} M$ implies that $\mathfrak{p} \supset \mathfrak{p}_i$ for some i, and if $\mathfrak{p}$ is minimal over $\operatorname{ann} M$ then $\mathfrak{p} = \mathfrak{p}_i$. More precisely, by the minimality of $\mathfrak{p}$, for any $\mathfrak{p}_j$, by localizing at $\mathfrak{p}$ we get either $M^j_{\mathfrak{p}} \cong M^{j-1}_{\mathfrak{p}}$ or $\mathfrak{p}_i = \mathfrak{p}$. The proposition follows. □

Theorem 1.90. *Let $S = k[x_0, \ldots, x_n]$ and M be a finitely generated S-module. Let $\phi_M(\ell) := \dim_k M_\ell$. Then there is a unique polynomial $p_M(z) \in \mathbb{Q}[z]$ such that $p_M(\ell) = \phi_M(\ell)$ for large $\ell \in \mathbb{N}$. Also $\deg p_m = \dim\ V(\operatorname{ann} M)$.*

PROOF. Except the last statement, this is just a special case of the Hilbert–Serre theorem (cf. Corollary 1.79) for polynomial rings. However in this special case the proof can be done with precise information on $\deg p_M$.

Let $0 \to M' \to M \to M'' \to 0$ be exact, then $\phi_M = \phi_{M'} + \phi_{M''}$ and

$$V(\operatorname{ann} M) = V(\operatorname{ann} M') \cup V(\operatorname{ann} M'').$$

Hence the problem is reduced to $M = (S/\mathfrak{p})(e)$ by Proposition 1.89, hence also to $M = S/\mathfrak{p}$ by a shifting $z \mapsto z + \ell$.

If $\mathfrak{p} = (x_0, \ldots, x_n)$ then $\phi_M(\ell) = 0$ for all $\ell > 0$. So $p_M(z) = 0$. Otherwise let $x_i \notin \mathfrak{p}$ and consider the short exact sequence

$$0 \to M \xrightarrow{x_i \cdot} M \longrightarrow M'' := M/x_iM \to 0.$$

Then $\phi_{M''}(\ell) = \phi_M(\ell) - \phi_M(\ell - 1) = (\Delta\phi_M)(\ell - 1)$ and $V(\operatorname{ann} M'') = V(\mathfrak{p}) \cap V(x_i)$. Hence $\dim V(\operatorname{ann} M'') = \dim V(\operatorname{ann} M) - 1$.

The theorem follows by induction on $\dim V(\operatorname{ann} M)$. □

The theorem works without $k = \bar{k}$ and even for k being an artinian ring. We use $V(\operatorname{ann} M)$ (in prime spectrum) instead of $Z(\operatorname{ann} M)$ (k-variety) in our statement and throughout the proof. It is of fundamental importance when we study the notion of flatness of families of algebraic objects. Below we give a simple application of it, namely the Bezout theorem.

Definition 1.91. Let $\iota : Y \subset \mathbb{P}^n$ be an algebraic set with given imbedding ι. Denote by P_Y the Hilbert polynomial of $S(Y) = k[x_0, \ldots, x_n]/I(Y)$. Let $r = \dim Y = \deg P_Y$. Thne the degree of $Y \subset \mathbb{P}^n$ is defined by the expression

$$P_Y(z) = \frac{\deg Y}{r!} z^r + \ldots \text{lower degree terms in } z.$$

Of course the notion of degree depends on the embedding ι.

Proposition 1.92. (a) *We have* $\deg Y \in \mathbb{N}$ *if* $Y \neq \emptyset$. *Also* $\deg \mathbb{P}^n = 1$.

(b) *Let* $H = Z(f) \subset \mathbb{P}^n$ *then* $\deg H = \deg f$.

(c) *If* $\dim Y_1 = \dim Y_2 = r$ *and* $\dim Y_1 \cap Y_2 < r$ *then*

$$\deg Y_1 \cup Y_2 = \deg Y_1 + \deg Y_2.$$

Proof. (a) Since $P_Y(\ell) \in \mathbb{N}$ for all large ℓ, it is in fact integer valued for all $\ell \in \mathbb{Z}$ and then $P_Y(z) = a_r C^z_r + a_{r-1} C^z_{r-1} + \ldots + a_0$, $a_i \in \mathbb{Z}$, where

$$C^z_r := \frac{1}{r!} z(z-1)\ldots(z-(r-1)).$$

Then $\deg Y = a_r \in \mathbb{N}$. For $Y = \mathbb{P}^n$, $\phi_S(\ell) = H^{n+1}_\ell = C^{n+\ell}_n$. Hence $P_Y(z) = C^{z+n}_n$ has degree 1 by the above expression.

(b) Let $d = \deg f$ and consider the short exact sequence

$$0 \to S(-d) \xrightarrow{\cdot f} S \longrightarrow S/(f) \to 0.$$

Then $\phi_{S/(f)}(\ell) = \phi_S(\ell) - \phi_S(\ell - d) = C^{\ell+n}_n - C^{\ell-d+n}_n$. Hence the top degree term of $P_H(z)$ is computed from

$$\frac{1}{n!}((z+n)\ldots(z+1) - (z-d+n)\ldots(z-d+1)) = \frac{d}{(n-1)!} z^{n-1} + \ldots.$$

(c) Using $0 \to S/I_1 \cap I_2 \to S/I_1 \oplus S/I_2 \to S/(I_1 + I_2) \to 0$. □

Theorem 1.93 (Generalized Bezout Theorem). *Let* $Y \subset \mathbb{P}^n$ *be a projective variety and* $H \subset \mathbb{P}^n$ *be a hypersurface with* $Y \not\subset H$. *If* $Y \cap H = Z_1 \cup \ldots \cup Z_m$ *being the irreducible decomposition then* $\dim Z_j = \dim Y - 1$ *for all* j *and*

$$\sum_{j=1}^m i(Z_j) \deg Z_j = \deg Y \cdot \deg H,$$

where $i(Z_j) := \mu_{I(Z_j)}(S/(I(Y) + I(H)))$ *(cf. Proposition 1.89).*

The number $i(Z_j) = i(Z; Y, H)$ is known as the intersection multiplicity of $Y \cap H$ along Z_j. When $Y = Z(g), H = Z(h) \subset \mathbb{P}^2$ are curves it coincides with the standard definition $\ell_{\mathscr{O}_p}(\mathscr{O}_p/(g_p, h_p))$.

However, when Y, H are both of codimension ≥ 2, the definition should be replaced using homological invariants via "Tor groups" (due to Serre). The homological techniques will be introduced in later chapters.

Proof. Let $H = Z(f)$ with $\deg f = d$. Let $r = \dim Y$, then we have seen that the dimension of each irreducible component Z_j is $r - 1$.

As before, consider the short exact sequence

$$0 \to (S/I(Y))(-d) \xrightarrow{\cdot f} S/I(Y) \longrightarrow S/(I(Y) + I(H)) =: M \to 0.$$

Then $p_M(z) = P_Y(z) - P_Y(z-d)$ which is

$$\frac{\deg Y}{r!}(z^r - (z-d)^r) + \ldots = \frac{\deg Y \cdot d}{(r-1)!} z^{r-1} + \ldots.$$

On the other hand, by Proposition 1.89 we have $p_m(z) = \sum_i p_i(z)$ where p_i is the Hilbert polynomial for $(S/\mathfrak{p}_i)(e_i)$, namely

$$p_i(z) = \frac{\deg Z(\mathfrak{p}_i)}{r_i!}(z + e_i)^{r_i} + \ldots.$$

The theorem follows by picking up those terms with $r_i = r - 1$. □

It is clear that the theorem can be extended to the case that Y is an algebraic set (reducible) and H be a reducible hypersurface. One may also apply it repeatedly by cutting out Y by hypersurfaces H_i's. Namely for $H = Z(f_1, \ldots, f_t)$ being a complete intersection with codimension $s = n - t$.

Exercise 1.4. Let $\dim Y = r$ and $H = \bigcap_{i=1}^t H_i$, $H_i = Z(f_i)$, being a complete intersection of codimenison $n - t$. If $Y \cap H = Z_1 \cup \ldots \cup Z_m$ is the irreducible decomposition, then $\dim Z_j = \dim Y - t$ for all j and

$$\sum_{j=1}^m i(Z_j) \deg Z_j = \deg Y \cdot \deg H = \deg Y \cdot \prod_{i=1}^t \deg f_i,$$

where $i(Z_j) := \prod_{i=1}^t i(Z^{(i)}; Z^{(i-1)}, H_i)$ is defined via

$$Z_j = Z^{(t)} \subsetneq Z^{(t-1)} \subsetneq \ldots \subsetneq Z^{(0)} = Y$$

where $Z^{(i)}$ is a irreducible component of $Z^{(i-1)} \cap H_i$.

In particular, for $t = r$ and H is a codimenison r linear subspace we recover the geometric interpretation of $\deg Y$ as the number of intersections of $Y \cap H$ counted with multiplicities (and degree of $k(p)/k$ if $k \neq \bar{k}$).