INTEGRAL DEPENDENCE AND NORMAL VARIETIES

EYAL Z. GOREN NOVEMBER, 1999

1. Basic definitions

Definition 1.1. *Let $A \subset B$ be rings (always commutative with 1). An element $b \in B$ is called* integral *over A if b satisfies a monic polynomial $f(x) \in A[x]$. That is, exist some $a_0, \dots, a_{n-1}$ in A such that*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Example 1.2. *Let $A = \mathbb{Z}$ and $B = \mathbb{Q}$. Then $b \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $b \in \mathbb{Z}$. Indeed, if $b \in \mathbb{Z}$ then b solves $x - b \in \mathbb{Z}[x]$. Conversely, write $b = c/d$ for relatively prime integers c and d, $d > 0$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients that b satisfies. Substituting b for x and multiplying by d^n we obtain*

$$c^n = -(da_{n-1}c^{n-1} + \cdots + d^n a_0).$$

Since d divides the right hand side, we get that $d|c^n$. But $(d, c) = 1$. Therefore, $d = 1$.

Proposition 1.3. *Let $A \subset B$ be rings and $b \in B$. The following are equivalent:*

(1) b is integral over A.

(2) $A[b]$ is a finitely generated module over A (i.e., exist $b_1, \dots, b_n$ in $A[b]$ such that $A[b] = Ab_1 + \cdots + Ab_n$).

(3) $A[b] \subset M \subset B$, where M is finitely generated A-module.

(4) Exists a faithful $A[b]$-module K, finitely generated over A. ("faithful" means that if $a \in A[b]$ and $ak = 0$ for all $k \in K$ then $a = 0$).

Proof. **(1) implies (2) :** For some $a_0, \dots, a_{n-1}$ we have $b^n = -(a_{n-1}b^{n-1} + \cdots + a_0)$. I claim that

$$A[b] = A + Ab + \cdots + Ab^{n-1}.$$

Let J denote the right hand side. It is enough to prove that $b^r \in J$ for every $r \geq n$. For $r = n$ this is the identity $b^n = -(a_{n-1}b^{n-1} + \cdots + a_0)$. Assume that $b^r \in J$ then $b^r = \alpha_0 + \alpha_1 b + \cdots + \alpha_{n-1}b^{n-1}$ for suitable $\alpha_i \in A$. Therefore $b^{r+1} = \alpha_0 b + \alpha_1 b^2 + \cdots + \alpha_{n-2}b^{n-1} + \alpha_{n-1}b^n$. Since $\alpha_{n-1}b^n$ belongs to J and $\alpha_0 b + \alpha_1 b^2 + \cdots + \alpha_{n-2}b^{n-1}$ belongs to J we get $b^{r+1} \in J$.

(2) implies (3): Take $M = A[b]$.

(3) implies (4): Take $K = M$. Since $1 \in K$, if $r \in A[b]$ annihilates K then, in particular, $r \cdot 1 = 0$. Thus $r = 0$ and K is a faithful $A[b]$-module.

(4) implies (1): Say that

$$K = Ac_1 + \cdots + Ac_n$$

for some $c_i \in K$. Consider the A-linear map

$$\phi_b : K \longrightarrow K, \quad \phi_b(d) = bd.$$

Write

$$\phi_b(c_j) = \sum_{i=1}^{n} a_{ij}c_i, \quad a_{ij} \in A.$$

Let us define a map T by the following $n \times n$ matrix:

$$T = b\dot{I}_n - (a_{ij}).$$

By that we mean the following: If $k \in K$ and $k = \alpha_1 c_1 + \cdots + \alpha_n c_n$ then $T(k) = \beta_1 c_1 + \cdots + \beta_n c_n$, where ${}^t(\beta_1, \ldots, \beta_n) = T\,{}^t(\alpha_1, \ldots, \alpha_n)$. Now, in fact, T is identically zero, because $Tc_j = bc_j - (\sum_{i=1}^n a_{ij} c_i)$. Thus, for *any* expression $k = \alpha_1 c_1 + \cdots + \alpha_n c_n$ we get $T(k) = 0$ (which shows, somewhat perversely, that T is well defined!).

Let $Adj(T)$ be the adjoint matrix to T. Then the transformation $Adj(T) \cdot T = \det(T) \cdot I_n$ is also identically zero. But this is the transformation $k \mapsto \det(T) \cdot k$. Since K is a faithful $A[b]$ module we get $\det(T) = 0$. However, expanding $\det(T)$ we see that for suitable $r_i \in A$ we have

$$b^n + r_{n-1} b^{n-1} + \cdots + r_0 = 0.$$

□

Corollary 1.4. *(1) The integral closure of A in B, defined as*

$$\{b \in B : b \text{ is integral over A}\}$$

and denoted $N_B(A)$, is a sub-ring of B containing A.

(2) $N_B(N_B(A)) = N_B(A)$.

Proof. We first remark that if $A \subset B \subset C$ are three rings such that B is a finitely generated A-module and C is a finitely generated B-module then C is a finitely generated A module. Indeed, let $B = Ab_1 + \cdots + Ab_m$ for some $b_i \in B$ and $C = Bc_1 + \cdots + Bc_n$ for some $c_i \in C$. Then $C = \sum_{i=1,j=1}^{m,n} b_i c_j$. Furthermore, by induction, we get that if $A = B_0 \subset B_1 \subset \cdots \subset B_n$ are rings and B_i is finitely generated B_{i-1}-module for every $i \geq 1$, then B_n is a finitely generated A-module.

We use this as follows. Let $b_1, \ldots, b_n$ be elements of B integral over A. Then $A[b_1, \ldots, b_n]$ is a finitely generated A module. Indeed, let $B_i = A[b_1, \ldots, b_i]$. Note that b_i is integral over B_{i-1}, therefore, by the proposition, B_i is a finitely generated B_{i-1}-module.

We now prove (1). We notice that given $b_1, b_2 \in N_B(A)$ we have $A[-b_1], A[b_1 + b_2], A[b_1 b_2]$ each contained in the finitely generated A-module $A[b_1, b_2]$. Hence, by the proposition, $-b_1, b_1 + b_2, b_1 b_2$ are integral over A. Finally, clearly $a \in A$ solves $x - a$. That is $A \subset N_B(A)$.

Let $b \in N_B(N_B(A))$. Then $b^n + a_{n-1} b^{n-1} + \ldots a_0 = 0$ for some $a_i \in N_B(A)$. Then we see that b is integral over $A[a_0, \ldots, a_{n-1}]$. Therefore $A[a_0, \ldots, a_{n-1}, b]$ is finite over $A[a_0, \ldots, a_{n-1}]$, which, in turn, is finite over A. Therefore $A[a_0, \ldots, a_{n-1}, b]$ is finite over A and contains $A[b]$. The proposition gives that b is integral over A. I.e., that $b \in N_B(A)$. □

The following easy exercises give some further examples and properties of integrality.

Exercise 1. *Show that $\alpha \in \mathbb{Q}(i)$ is integral over $\mathbb{Z}[i]$ if and only if $\alpha \in \mathbb{Z}[i]$.*

Exercise 2. *Prove that $N_{\mathbb{Q}(\sqrt{5})}(\mathbb{Z}) = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.*

(For the exercises above use the following: If $\alpha \in K$, K a finite extension of $\mathbb{Q}$ of degree n, then the minimal polynomial of α over $\mathbb{Q}$ is of degree $\leq n$ and has integer coefficients. Those that know some Galois theory should attempt to prove this (rather easy) fact).

Exercise 3. *Let U be a multiplicative set in A. Then $A \subset B$ is an integral extension implies $A[U^{-1}] \subset B[U^{-1}]$ is an integral extension.*

Exercise 4. *$A \subset B$ is an integral extension, $\mathfrak{m} \lhd B$, $\mathfrak{n} = \mathfrak{m} \cap A$. Then $A/\mathfrak{n} \subset B/\mathfrak{m}$ is an integral extension.*

One of the things we just showed is the following: Given a map of rings $\phi : A \longrightarrow B$, there is a canonical ring $N_B(A)$ containing the image of A. Note that $N_B(A)$ is really $N_B(\phi(A))$ We don't assume ϕ is injective.

2. Some geometrical remarks

Let us go back to algebraic geometry. Almost every result we'll prove below has a geometric content. One has to be careful about sneering at the geometric content in some cases. The reason is that though some geometric content is pretty obvious over an algebraically closed field, the algebraic theorems we prove will work for schemes as well, where the geometric content is more subtle!

First, let us take a closer look at affine varieties over an algebraically closed field k. Let

$$f : X \longrightarrow Y$$

be a morphism of affine varieties. Say $B = \mathcal{O}(X)$ and $A = \mathcal{O}(Y)$. Let

$$\phi : A \longrightarrow B$$

be the corresponding homomorphism of k-algebras.

1. Let Z be a closed subset of X. Say $Z = Z(\mathfrak{q})$ for a $\mathfrak{q}$ an ideal of B. Then, I claim, $\overline{f(Z)}$ $= Z(\phi^{-1}(\mathfrak{q}))$. That is, $I(f(Z)) = \phi^{-1}(\mathfrak{q})$. Let $g \in I(f(Z))$ then $g(f(t)) = 0$ for every $t \in Z$. That is $\phi(g) = f^*(g) \in I(Z) = \mathfrak{q}$. Otherwise said, $g \in \phi^{-1}(\mathfrak{q})$. Conversely, let $g \in \phi^{-1}(\mathfrak{q})$. Then $\phi(g) = f^*(g) \in \mathfrak{q}$. Thus $f^*(g)(t) = 0$ for every $t \in Z$. Or, $g(f(t)) = 0$ for every $t \in Z$. Thus $g \in I(f(Z))$.

2. Let Z be a closed set in Y. Say $Z = Z(\mathfrak{a})$ then $f^{-1}(Z)$ is the closed set $Z(\phi(\mathfrak{a})B)$. Let $y \in Z$, $g \in \mathfrak{a}$. Then $\phi(g)(f^{-1}(y)) = g(y) = 0$. Thus $f^{-1}(Z) \subset Z(\phi(\mathfrak{a})B)$. Conversely, if $t \in Z(\phi(\mathfrak{a})B)$ then for any $g \in \mathfrak{a}$ we have $g(f(t)) = \phi(g)(t) = 0$. Thus, $Z(\phi(\mathfrak{a})B) \subset f^{-1}(Z)$.

3. Going up and down

Proposition 3.1. *Let $A \subset B$ be an integral extension. Assume that A and B are domains. Then A is a field iff B is a field.*

Proof. Assume A is a field. Let $b \in B$ and $b \neq 0$. Then for some $a_i \in A$ we have $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. We assume that n is the minimal possible. Thus $a_0 \neq 0$ else $b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = 0$ and that implies that $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 = 0$ and n is thus not minimal. We therefore get $b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)(-a_0)^{-1} = 1$ and we see b is invertible.

Conversely, assume that B is a field. Let $a \in A$, $a \neq 0$. Then $a^{-1} \in B$ is integral over A. Thus for some $a_i \in A$ we get $(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. This gives $a^{-1} = -(aa_{n-1} + \cdots + a^{n-1}a_0)$. Thus $a^{-1} \in A$. □

Exercise 5. *What is the geometric content of this statement?*

Corollary 3.2. *Let $A \subset B$ be an integral extension. Let $\mathfrak{q} \lhd B$ be a prime ideal. Let $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal iff $\mathfrak{p}$ is maximal.*

Proof. $\mathfrak{p}$ is maximal if and only if $A/\mathfrak{p}$ is a field. That holds iff $B/\mathfrak{q}$ is a field because $A/\mathfrak{p} \subset B/\mathfrak{q}$ is an integral extension. But $B/\mathfrak{q}$ is a field iff $\mathfrak{q}$ is maximal. □

Exercise 6. *Give an example of $A \subset B$ where: (i) $\mathfrak{q}$ is maximal and $\mathfrak{p}$ is not; (ii) $\mathfrak{p}$ is maximal and $\mathfrak{q}$ is not.*

Geometric Content: Let $f : X \longrightarrow Y$ be a dominant *integral morphism* of affine varieties, i.e., the extension of rings $\mathcal{O}(Y) \hookrightarrow \mathcal{O}(X)$ is integral. A sub-variety in X is a point iff its image is a point! (I.e., the fibres are zero-dimensional).

Proposition 3.3. *Let $A \subset B$ be an integral extension. Let $\mathfrak{q}_1 \subset \mathfrak{q}_2$ be prime ideals of B. Then $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$ implies that $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Proof. Let $\mathfrak{p} := \mathfrak{q}_1 \cap A$. Note that $U = A \setminus \mathfrak{p}$ is a multiplicative set. Consider the extension $A[U^{-1}] \subset B[U^{-1}]$. It is an integral extension. The ideals $\mathfrak{q}_i B[U^{-1}]$ are prime ideals whose intersection with $A[U^{-1}]$ is $\mathfrak{p}A[U^{-1}]$. This follows from the following exercise (applied to $M = B, M_1 = \mathfrak{q}_1, M_2 = A$):

Exercise 7. *Let A be a ring. U a multiplicative set and M_1, M_2 two submodule of an A module M. Then $M_1[U^{-1}] \cap M_2[U^{-1}] = (M_1 \cap M_2)[U^{-1}]$.*

Now, since $A[U^{-1}] \subset B[U^{-1}]$ is an integral extension and $\mathfrak{p}A[U^{-1}]$ is a maximal ideal of $A[U^{-1}]$ we get that both $\mathfrak{q}_i B[U^{-1}]$ are maximal ideals of $B[U^{-1}]$. But $\mathfrak{q}_1 B[U^{-1}] \subset \mathfrak{q}_2 B[U^{-1}]$. Hence $\mathfrak{q}_1 B[U^{-1}] = \mathfrak{q}_2 B[U^{-1}]$. This implies that $\mathfrak{q}_1 = \mathfrak{q}_2$. □

Geometric Content: A chain of distinct irreducible sets $Z_1 \subset \cdots \subset Z_n$ in X has distinct images in Y (even after taking closure). In particular, $\dim(X) \leq \dim(Y)$.

Theorem 3.4. *(Cohen-Seidenberg) Let $A \subset B$ be an integral extension.*

(1) (Going-up) Let $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be prime ideals of A. Let $\mathfrak{q}_1$ be a prime ideal of B such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there exist prime ideals of B, $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

(2) (Going-down) Assume that A and B are also domains and that A is integrally closed (i.e., $N_{Quot(A)}(A) = A$). Let $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be prime ideals of A. Let $\mathfrak{q}_n$ be a prime ideal of B such that $\mathfrak{q}_n \cap A = \mathfrak{p}_n$. Then there exist prime ideals of B, $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

Proof. (Of part (1) of the theorem). We first give a

Lemma 3.5. *Let $A \subset B$ be an integral extension and $\mathfrak{p}$ a prime ideal of A. Then, there exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. Let $U = A \setminus \mathfrak{p}$. Let $\mathfrak{m} = \mathfrak{p}A[U^{-1}]$ be the maximal ideal of $A[U^{-1}]$. Let $\mathfrak{n}$ be a maximal ideal of $B[U^{-1}]$ such that $\mathfrak{n} \supset \mathfrak{m}$. Then $\mathfrak{n} \cap A[U^{-1}] \supset \mathfrak{m}$ and does not contain 1. Hence $\mathfrak{n} \cap A[U^{-1}] = \mathfrak{m}$.

Let $\phi : B \longrightarrow B[U^{-1}]$ be the natural map. Let $\mathfrak{q} = \phi^{-1}(\mathfrak{n})$. Then $\mathfrak{q}$ is prime (in fact, maximal). We claim that $\mathfrak{q} \cap A = \mathfrak{p}$. Since $\mathfrak{q} \cap A$ is disjoint from U, it is enough to show that $(\mathfrak{q} \cap A)[U^{-1}] = \mathfrak{m}$. But $(\mathfrak{q} \cap A)[U^{-1}] = \mathfrak{q}[U^{-1}] \cap A[U^{-1}] = \mathfrak{n} \cap A[U^{-1}] = \mathfrak{m}$. □

Geometric Content: A dominant integral morphism is surjective. (Take $\mathfrak{p}$ to be a maximal ideal).

Exercise 8. *Give a geometric proof of the lemma in the case when A and B are the rings of regular functions of algebraic varieties and the corresponding map between the varieties is surjective.*

Now, to prove (1), we may assume that $n = 2$. The general case follows by induction. We have then the following situation: $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Consider the integral extension $A/\mathfrak{p}_1 \subset B/\mathfrak{q}_1$. The ideal $\mathfrak{p}_2/\mathfrak{p}_1$ is a prime ideal of $A/\mathfrak{p}_1$. The lemma gives a prime ideal $\mathfrak{q}$ of $B/\mathfrak{q}_1$ such that $\mathfrak{q} \cap A/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. Let $\mathfrak{q}_2$ be the preimage in B of $\mathfrak{q}$. Then $\mathfrak{q}_2$ is a prime ideal containing $\mathfrak{q}_1$ and $(\mathfrak{q}_2 \cap A)/\mathfrak{p}_1 = \mathfrak{q}_2/\mathfrak{q}_1 \cap A/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$ (we have used: if $f : G \longrightarrow H$ is a group homomorphism, $I \supset \mathrm{Ker}(f)$. Then $f(I \cap J) = f(I) \cap f(J)$). □

Geometric Content: Let $f : X \longrightarrow Y$ be a dominant integral morphism. Given a chain of closed irreducible sets $Z_1 \supset \cdots \supset Z_n$ in Y, there exists a closed irreducible set $\widetilde{Z_1}$ of X such that $\overline{f(\widetilde{Z_1})} = Z_1$. (This is the lemma). Moreover (this is part (1) of the theorem), for any such $\widetilde{Z_1}$ there exists a chain $\widetilde{Z_1} \supset \cdots \supset \widetilde{Z_n}$ of closed irreducible sets in X such that for every i we have $\overline{f(\widetilde{Z_i})} = Z_i$. In particular, $\dim(Y) \leq \dim(X)$. Hence, $\dim(X) = \dim(Y)$.

Part (2) of the theorem has a similar interpretation, only that one starts form $\widetilde{Z_n}$ such that $\overline{f(\widetilde{Z_n})} = Z_n$.

A further corollary is that *a dominant integral morphism $\phi : X \longrightarrow Y$ is a closed map.*

Let Z be closed in X. We may assume w.l.o.g. that Z is irreducible and thus corresponds to a prime ideal $\mathfrak{q}_1 \lhd \mathcal{O}(X)$. Then $\overline{\phi(Z)}$ corresponds to the prime ideal $\mathfrak{q}_1 \cap \mathcal{O}(Y) =: \mathfrak{p}_1$. Let $y \in \overline{\phi(Z)}$. It corresponds to a maximal ideal $\mathfrak{p}_2$ such that $\mathfrak{p}_1 \subset \mathfrak{p}_2$. There exists a prime ideal $\mathfrak{q}_2$ of $\mathcal{O}(X)$ such that $\mathfrak{q}_2 \cap \mathcal{O}(Y) = \mathfrak{p}_2$. It is necessarily a maximal ideal. Let t be the point in X corresponding to $\mathfrak{q}_2$. Then $\phi(t) = \overline{\phi(t)}$ is defined by $\mathfrak{p}_2$. That is $\phi(t) = y$.

4. Some local properties of rings

Proposition 4.1. *Let R be a domain. Then R is integrally closed (i.e., if $K = Quot(R)$ then $R = N_K(R)$) if and only if $R_\mathfrak{p}$ is integrally closed for every maximal (or prime) ideal $\mathfrak{p}$.*

Proof. Say R is integrally closed. Let $\alpha \in K$ be integral over $R_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ Then, for suitable $a_i \in R$ and $b_i \in R \setminus \mathfrak{p}$ we have

$$\alpha^n + \frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \cdots + \frac{a_0}{b_0} = 0.$$

Taking common denominator we find that for suitable $c_i \in R$ and $b \in R \setminus \mathfrak{p}$ we have

$$\alpha^n + \frac{c_{n-1}}{b}\alpha^{n-1} + \cdots + \frac{c_0}{b} = 0.$$

This gives

$$(b\alpha)^n + c_{n-1}(b\alpha)^{n-1} + \cdots + c_0 b^n = 0.$$

Therefore $b\alpha$ is integral over R, hence in R. Thus, $\alpha \in R_\mathfrak{p}$.

Conversely, suppose that for every maximal ideal $\mathfrak{p}$ we have that $R_\mathfrak{p}$ is integrally closed. Let $\alpha \in K$ integral over R. Then the same polynomial α satisfies shows that α is integral over $R_\mathfrak{p}$ for all $\mathfrak{p}$. Therefore

$$\alpha \in \bigcap_{\mathfrak{p} \text{ maximal}} R_\mathfrak{p} = R.$$

(We have proved the last equality in the past). □

Recall that a ring is noetherian if every ascending chain of ideals becomes stationary.

Exercise 9. *Prove that R is noetherian implies that $R_\mathfrak{p}$ is noetherian for every prime ideal $\mathfrak{p}$.*

Exercise 10. *Let R be a domain. Then R has dimension 1 if and only if $R_\mathfrak{p}$ has dimension 1 for every prime ideal $\mathfrak{p}$.*

Definition 4.2. *R is called a Dedekind domain if :*
(i) R is integrally closed.
(ii) R is noetherian.
(iii) R is of dimension 1.

The following proposition follows easily from the exercises and the previous proposition.

Proposition 4.3. *Let R be a noetherian ring. Then R is a Dedekind domain if and only if $R_\mathfrak{p}$ is a Dedekind domain for every (maximal) prime ideal $\mathfrak{p}$.*

We cite the following

Theorem 4.4. *(Emmy Noether) Let R be a finitely generated domain over a field or over the integers and let L be a finite extension of K, the quotient field of R. Then $N_L(R)$ is a finitely generated R-module.*

Corollary 4.5. *If R is a Dedekind domain so is $N_L(R)$.*

Proof. Since $N_L(R)$ is finitely generated over the Noetherian ring R it is also Noetherian. It is integrally closed: $N_L(N_L(R)) = N_L(R)$. Finally, being an integral extension we have $\dim(N_L(R)) = \dim(R) = 1$. □

Definition 4.6. *A variety X/k is called normal if the local ring of every point is integrally closed. Equivalently, for every affine $U \subset X$ the ring $\mathcal{O}(U)$ is integrally closed.*

Corollary 4.7. *Let X/k be an affine variety. Let R be the coordinate ring of X. We define the normalization of X, denoted $\widetilde{X}$, to be the affine variety with coordinate ring $N_{Quot(R)}(R)$. By Noether's theorem this is a finitely generated ring. Hence, there indeed exists a variety $\widetilde{X}$ as stated. It is a normal variety.*

Note that there is a natural dominant morphism

$$\pi : \widetilde{X} \longrightarrow X.$$

Moreover, if Y is any normal affine variety and $f : Y \longrightarrow X$ is a dominant morphism, then there exists a unique morphism $g : Y \longrightarrow \widetilde{X}$ such that $\pi \circ g = f$.

Here are the main examples of Dedekind domains:

(1) Let $R = \mathbb{Z}$. It is a Dedekind domain. Let L be a finite extension of $\mathbb{Q}$. Then $N_L(R)$ – the ring of algebraic integers in L – is a Dedekind domain.

(2) If X is a non-singular affine variety of dimension 1 (i.e., a curve) then $R = \mathcal{O}(X)$ is a noetherian ring (because S noetherian implies $S[x]$ noetherian and S/I noetherian), of dimension 1 (because $\dim(X) = \dim(R_\mathfrak{p})$ for every prime ideal p) and is integrally closed because all the local rings are integrally closed due to the following theorem we cite without proof:

Theorem 4.8. *Let R be a regular local ring then R is integrally closed.*

5. Discrete valuation rings

Let K be a field. A discrete valuation on K is a function

$$v : K^\times \longrightarrow \mathbb{R},$$

such that $v(K^\times)$ is an abelian group of rank 1 and

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

We have:

(i) $v(1) = 0$, because $v(1) = v(1 \cdot 1) = v(1) + v(1)$.

(ii) $v(-1) = 0$, because $v(1) = v(-1) + v(-1)$.

(iii) $v(x^{-1}) = -v(x)$, because $v(1) = v(x) + v(1/x)$.

(iv) $v(-x) = v(x)$, because $v(x) = v(-x) + v(-1)$.

(v) If $v(x) > v(y)$ then $v(x+y) = v(y)$, because $v(x+y) \geq v(y)$ but also $v(y) = v(x+y-x) \geq \min(v(x+y), v(-x)) = \min(v(x+y), v(x)) = v(x+y)$.

Exercise 11. *Fix a rational prime p. For an integer a define $v(a)$ to be the largest power of p dividing a. For a rational number $m = a/b$ let $v(m) = v(a) - v(b)$. Show that v is a valuation on $\mathbb{Q}$.*

Given v define

$$R = R_v = \{r \in K : v(r) \geq 0\}, \quad \mathfrak{m} = \mathfrak{m}_v = \{r \in K : v(r) > 0\}.$$

Theorem 5.1. *The ring $(R, \mathfrak{m})$ is a local ring of dimension 1. The ideal $\mathfrak{m}$ is principal, $\mathfrak{m} = (\pi)$, and every other non-trivial ideal of R is of the form (π^n) for some $n \geq 1$.*

Proof. Let I be any ideal of R. Let r be any element of I such that $v(r)$ is minimal amongst the elements of I. We claim that $I = (r)$. One inclusion is clear. Let s be in I. Then $v(s/r) = v(s) - v(r) \geq 0$. Therefore $s/r \in R$ and hence $s = r \cdot s/r \in (r)$.

Note that because every element a of $R \setminus \mathfrak{m}$ has valuation zero the same holds for a^{-1}. Thus the units of R are precisely $R \setminus \mathfrak{m}$ and therefore $(R, \mathfrak{m})$ is a local ring. Moreover, arguing as above, we see that if $I = (r)$ is an ideal and $v(r') \geq v(r)$ then $r' \in I$. That is, if $v(K^\times) = \alpha\mathbb{Z}$ for $\alpha > 0$, then the ideals of R are precisely the ideals

$$\{r \in R : v(r) \geq n\alpha\}.$$

Taking $I = \mathfrak{m}$, we see that an element π such that $(\pi) = \mathfrak{m}$ exists. It is clear that $v(\pi) = \alpha$. Therefore, for any ideal I a minimal element in I can be chosen as π^n. It follows also that R has a unique prime ideal. □

Definition 5.2. *Let R be a domain with quotient field K. We say R is a discrete valuation ring (DVR) if there exists a discrete valuation v on K such that $R = R_v$.*

Theorem 5.3. *Let R be a local noetherian domain of dimension 1. Then R is integrally closed if and only if R is a DVR.*

Proof. One direction is easy. If R is DVR then R is integrally closed:

Let α be an element of the quotient field K that is integral over R. Write $\alpha = m/n$ where m and n are elements of R. Then, for suitable $a_i \in R$ we have

$$(m/n)^s + a_{s-1}(m/n)^{s-1} + \cdots + a_0 = 0.$$

W.l.o.g. $a_0 \neq 0$. Now, in K we have the strong triangle inequality: $v(x + y) \geq \min(v(x), v(y))$ with equality if $v(x) \neq v(y)$. If $v(m) < v(n)$ then one sees that $v((m/n)^s + a_{s-1}(m/n)^{s-1} + \cdots + a_1) = s \cdot v(m/n) < 0$ while $v(-a_0) \geq 0$. Thus, $v(m) \geq v(n)$ and hence $\alpha = m/n$ is an element of R.

Conversely, assume that R is integrally closed local noetherian domain of dimension 1. Let $\mathfrak{m}$ be the unique prime ideal.

Step 1. $\mathfrak{m}$ is a principal ideal.
Let $a \in \mathfrak{m}$. For every $b \in R \setminus Ra$ we consider the ideal

$$(a : b) = \{r \in R : rb/a \in R\} = \{r \in R : rb \in Ra\}.$$

Choose b such that $(a : b)$ is maximal with respect to inclusion. We claim that $(a : b)$ is a prime ideal. Indeed, if $xy \in (a : b)$ and $x \notin (a : b)$ and $y \notin (a : b)$ (so $yb \notin Ra$). Then, since $x \in (a : yb)$ and $(a : yb) \supset (a : b)$ we get that $(a : b)$ is not maximal. Contradiction. Therefore $(a : b)$ is prime. Now, since R is of dimension 1, $(a : b)$ is a maximal ideal, and since R is local $(a : b) = \mathfrak{m}$.

We next show that $\mathfrak{m} = R(a/b)$. First, $(b/a)\mathfrak{m} \subset R$. If equality doesn't hold then $(b/a)\mathfrak{m} \subset \mathfrak{m}$. Now, $\mathfrak{m}$, being an ideal of a noetherian ring, is a finitely generated R module and is mapped to itself under multiplying by (b/a). This implies that (b/a) is integral over, and hence belong to, R. But that means that $b \in Ra$, contradiction. Therefore, $(b/a)\mathfrak{m} = R$, or, $\mathfrak{m} = R(a/b)$.

Step 2. Every ideal is a principal ideal.
Suppose not. Then we may take an ideal I which is maximal with respect to the property of not being principal (this uses noetherianity). We have $I \subset \mathfrak{m} = R\pi$. We get

$$I \subset \pi^{-1}I \subset R.$$

If $I = \pi^{-1}I$ then since I is a finitely generated R-module π^{-1} is integral over R, hence in R, hence $\mathfrak{m} = R$. Contradiction. It follows that $\pi^{-1}I$ strictly contains I, therefore principal. But $\pi^{-1}I = (d)$ implies $I = (\pi d)$. Contradiction. Thus every ideal is principal.

Step 3. A principal local domain $(R, \mathfrak{m})$ is a DVR.

Exercise 12. *Prove Step* 3. *Here are some hints: First, put* $\mathfrak{m} = (\pi)$. *Define for* $x \in R$, $v(x) = \max\{m : x \in (\pi^m)\}$. *Use that in a principal ideal domain the concepts of prime* ($x|ab$ *implies* $x|a$ *or* $x|b$) *and irreducible* ($x = ab$ *implies* $a \in R^\times$ *or* $b \in R^\times$) *are the same, and that a PID is a UFD, to prove that* v *is a valuation on* R.

□

Corollary 5.4. *Let* R *be a Dedekind ring. Then* $R_\mathfrak{p}$ *is a DVR for every prime ideal* $\mathfrak{p} \lhd R$.

6. Curves

Let k be an algebraically closed field.

Definition 6.1. *A curve over* k *is a variety of dimension* 1 *over* k.

If X is a curve, then for every regular point $p \in X$ the local ring $\mathcal{O}_{X,p}$ is a DVR. Note that since a DVR is a regular ring, if a point $p \in X$ has the property that $\mathcal{O}_{X,p}$ is a DVR (or integrally closed) then it is a regular point.

Now, if p is a regular point and, say, $X \subset \mathbb{A}^n$ (if needed, pass to an affine neighbourhood), and $p = (p_1, \dots, p_n)$, take a coordinate function $x_i - p_i$ on $\mathbb{A}^n$ that is not in $I(X)$. Then $x_i - p_i$ generates $\mathfrak{m}_p/\mathfrak{m}_p^2$. This shows that the discrete valuation of the local ring $\mathcal{O}_{X,p}$ is that of the order of vanishing of a function at the point p.

On the other hand, if p is a singular point then one cannot talk in general about the order of vanishing of a function at p in such terms. Indeed, if this is possible, we get that the local ring at p is a DVR and hence p is a regular point.

Example 6.2. *Consider that curve* $\mathcal{C} : y^2 = x^3$ *in* $\mathbb{A}^2$. *The map*

$$\mathbb{A}^1 \longrightarrow \mathcal{C}, \quad t \mapsto (t^2, t^3),$$

is a dominant morphism. Via this map we may view $\mathcal{O}(\mathcal{C})$ *as the sub ring of the field* $k(t)$ *generated by* t^2 *and* t^3. *Its integral closure is non else then* $k[t]$. *Indeed,* t *is integral over* $k[t^2, t^3]$ *since it solves* $X^2 - t^2 = 0$. *On the other hand* $k[t]$ *is integrally closed in* $k(t)$ *since it is the coordinate ring of the non-singular variety* $\mathbb{A}^1$.

Therefore,

$$\mathbb{A}^1 \longrightarrow \mathcal{C}, \quad t \mapsto (t^2, t^3),$$

is the normalization of $\mathcal{C}$. *Now, at the singular point of* $\mathcal{C}$, *namely at* $(0,0)$, *one cannot define the order of vanishing of a function naively. Certainly* y *vanishes there and* $y \in \mathfrak{m}_0 \setminus \mathfrak{m}_0^2$. *The same holds for* x. *If we put* $v(y) = v(x) = 1$, *as is "natural" to do, we get an immediate contradiction because* $v(y^2) = 2$, $v(x^3) = 3$ *and* $y^2 = x^3$! *(Note that* $v(y) = 3, v(x) = 2$ *works, though).*

Exercise 13. *Discuss the case of the curve* $\mathcal{C} : y^2 = x^2(x+1)$. *That is, find its normalization* $\widetilde{\mathcal{C}} \longrightarrow \mathcal{C}$. *Discuss the local ring at zero. Show it is not integral and why we can't make it into a DVR.*

The main result in this section is the following

Theorem 6.3. *(MAIN THEOREM) The following categories are equivalent:*

(i) Non-singular projective curves and dominant morphisms.
(ii) Quasi-projective curves and dominant rational maps.
(iii) Function fields of tr. deg. 1 *over* k *and* k*-morphisms.*

The equivalence of (ii) and (iii) is already known to us. It is a special case of the equivalence between function fields and varieties up to birational equivalence. Also the transition from (i) to (ii) is quite clear. Every object of the first category is also an object of the second. Also every dominant morphism is a dominant rational map. Moreover, this functor of going from (i) to (ii) is faithful. That is, if two morphisms give the same birational map then they are equal to begin with. Indeed, the set where two morphisms are equal is closed, and if they agree as a rational map then it also contains a non-empty open set, thus equal to the whole curve.

Therefore, the new part in the theorem above is going from (ii) to (i). Namely, to associate to any quasi-projective curve $\mathcal{C}$ a non-singular projective curve $\widetilde{\mathcal{C}}$ in a canonical fashion, that depends only on the birational class of the initial curve, and to associate to every dominant rational map $f : \mathcal{C} \longrightarrow \mathcal{D}$ a morphism $\widetilde{f} : \widetilde{\mathcal{C}} \longrightarrow \widetilde{\mathcal{D}}$, in a functorial way.

It is not hard to guess how $\widetilde{\mathcal{C}}$ should look like. If we take a projective closure $\mathcal{C}'$ of $\mathcal{C}$ in some projective space and let K be the function field of (the closure of) $\mathcal{C}$, then for every open affine set $U \subset \mathcal{C}'$ the preimage of U in $\widetilde{\mathcal{C}}$ should simply be the normalization of U. All those normalizations are done in the same field K and are compatible with intersections. Thus one hopes that there is a way to "glue" all of them together to a projective curve $\widetilde{\mathcal{C}}$. The main point of what we are about to do is to show this is indeed possible. We remark that the gluing procedure itself, that is difficult from the point of view we are taking so far, becomes trivial in the category of schemes!

Let K/k be a *function field*. That is, K is a finitely generated field extension of k of transcendence degree one. Let C_K be the **set** of all discrete valuation rings of K/k. By that we mean a DVR, say R, contained in K, such that the valuation gives value zero to every non zero element of k, and $Quot(R) = K$.

We shall attempt to view the set C_K itself as a curve! For that we need first to define a topology on C_K. We define a **topology** by taking the closed sets to be $\emptyset, C_K$, and every finite subset.

Before proceeding to define regular functions on open sets of C_K we immerse in some algebra.

Lemma 6.4. *(MAIN LEMMA) For every $x \in K$ the set $\{R \in C_K : x \notin R\}$ is a finite set.*

Proof. Since $Quot(R) = K$ for every $R \in C_K$, if $x \notin R$ then $x^{-1} \in \mathfrak{m}_R$. Thus, it is enough to prove that for every $y \neq 0$ the set

$$(y)_0 := \{R \in C_K : y \in \mathfrak{m}_R\}$$

is finite.

If $y \in k$ then $(y)_0$ is empty. Hence, we assume that $y \notin k$. In this case, the ring $k[y]$ is a free polynomial ring and K is a finite extension of the field $k(y)$.

Let B be the integral closure of $k[y]$ in K. It is a finitely generated k-algebra (by Noether's theorem), integrally closed and of dimension 1. That is, B is a Dedekind domain. Note that if $s \in K$ then s is algebraic over $k(y)$. Therefore, for some $g \in k[y]$ the element gs is integral over $k[y]$ (clear denominator in the minimal polynomial of s over $k(y)$). This shows that the quotient field of B is K. Therefore B defines a normal, hence non-singular, affine curve X with ring of regular functions B and function field K.

Now, suppose that $y \in R$ for some $R \in C_K$ then $k[y] \subset R$ and hence $B \subset R$. Let $\mathfrak{m} = \mathfrak{m}_R$ be the maximal ideal of R and consider $\mathfrak{n} = \mathfrak{m} \cap B$. It is a prime, hence maximal, ideal of B. We have an inclusion of DVRs

$$B_\mathfrak{n} \subset B_\mathfrak{m}$$

with quotient field K. They must therefore be equal. We leave that as an exercise.

Exercise 14. *Let $A \subset B$ be two DVRs with the same quotient field. Then $A = B$.*

We may more pleasantly rephrase what we proved as follows. Let $R \in C_K$ such that $y \in R$ then R is isomorphic to the local ring of some point x_R on X. (Thus every $R \in C_K$ is isomorphic to the local ring of some point on a non-singular affine curve with quotient field K !) If furthermore $y \in \mathfrak{m}_R$ then y, viewed as a function on X vanishes at x_R. That, for $y \neq 0$, can happen for only finitely many points. Hence, $\{R \in C_K : y \in \mathfrak{m}_R\}$ is a finite set. □

Corollary 6.5. *1. Every $R \in C_K$ is isomorphic to the local ring of some point on a non-singular affine curve with quotient field K.*

2. The set C_K is infinite, hence an irreducible topological space.

3. For every $R \in C_K$ we have a canonical isomorphism $R/\mathfrak{m}_R = k$.

Proof. The first claim was noted before. As for the second, the proof showed that all the local rings of X are element of C_K. There are infinitely many such (if two points $x, y \in X$ define the same local ring, then the maximal ideals are equal. But the maximal ideals determine the point.) The last assertion follows immediately from the first. □

We may now define **functions** on C_K. Let $U \in C_K$ be a non-empty open set. We define

$$\mathcal{O}(U) = \bigcap_{R \in U} R.$$

We may make this more "function like" as follows. Every $f \in \mathcal{O}(U)$ defines a function

$$f : U \longrightarrow k, \quad f(R) = f \pmod{\mathfrak{m}_R}.$$

If f and g are two elements of $\mathcal{O}(U)$ giving rise to the same function then $f - g \in \mathfrak{m}_R$ for any $R \in U$. Since C_K is infinite and U is not empty, U is infinite and therefore $f - g \in \mathfrak{m}_R$ for infinitely many $R \in C_K$. The main lemma implies that $f = g$.

Definition 6.6. *An abstract non-singular curve is an open non-empty subset U of C_K with its induced topology and sheaf of regular functions.*

Let us now consider the category whose objects consist of all quasi-projective curves over k and all abstract non-singular curves. We define a morphism,

$$f : X \longrightarrow Y,$$

between two objects of this category to be a continuous map of topological spaces, such that for every open subset $V \subset Y$, and every regular function $g : V \longrightarrow k$, the composition

$$g \circ f : f^{-1}(V) \longrightarrow k$$

is a regular function on $f^{-1}(V)$. There are no surprises in checking that this is a category. We may therefore speak on an isomorphism in this category.

More generally, given any object $\mathcal{C}$ in the above category, we define a morphism,

$$f : \mathcal{C} \longrightarrow Y,$$

from $\mathcal{C}$ to a variety Y to be a continuous map, such that for every open set V in Y, and any regular function $g : V \longrightarrow k$, the composition $g \circ f$ is a regular function of $f^{-1}(V)$.

Theorem 6.7. *Every non-singular quasi-projective curve Y is isomorphic to an abstract non-singular curve.*

Proof. It is pretty clear how to proceed. Let K/k be the function field of Y. Every local ring of a point $y \in Y$ is a DVR of K/k. Let $U \subset C_K$ be the set of the local rings of points of Y. Let $\phi : Y \longrightarrow U$ be given by $\phi(y) = \mathcal{O}_{Y,y}$.

We first show that U is open. That is, that $C_K \setminus U$ is a finite set. If $Y' \subset Y$ is an open affine set, then it is enough to show that $C_K \setminus \phi(Y')$ contains finitely many points. We may therefore assume, to prove U is open, that Y is affine.

Let B be the affine coordinate ring of Y. It is a Dedekind ring with quotient field K and it is finitely generated over k. The proof of the main lemma shows that U consists precisely of all the DVRs of K/k that contain B. But if $x_1, \dots, x_n$ are generators for B over k then $A \subset R$ for some $R \in C_k$ if and only if $x_1, \dots x_n$ belong to R. That is to say, if R is not in U then R does not contain at least one x_i and therefore

$$R \in \bigcup_{i=1,\dots,n} \{R \in C_K : x_i \notin R\}.$$

The r.h.s. is a finite set by the main lemma.

By construction ϕ is a bijection. Moreover, a non-empty set in Y is open iff it is co-finite and the same holds in U, Thus (trivially!) ϕ is bi-continuous. Moreover, if $V \subset Y$ is an open set then $\mathcal{O}(V) = \bigcap_{y \in V} \mathcal{O}_{Y,y} = \mathcal{O}(\phi(V))$. Thus, ϕ is an isomorphism. □

Lemma 6.8. *Let X be an abstract non-singular curve, let $P \in X$, and let Y be a projective variety. Let*

$$\phi : X \setminus \{P\} \longrightarrow Y$$

be a morphism. Then there exists a unique morphism,

$$\widetilde{\phi} : X \longrightarrow Y,$$

extending ϕ.

Proof. The uniqueness of $\widetilde{\phi}$, if it exists, is clear: The set where two morphisms agree is closed.

To prove ϕ exists we may reduce to the case $Y = \mathbb{P}^n$. Indeed, since $Y \subset \mathbb{P}^n$ for some n, we may view ϕ as a morphism

$$\phi : X \setminus \{P\} \longrightarrow \mathbb{P}^n.$$

If it extends to

$$\widetilde{\phi} : X \longrightarrow \mathbb{P}^n,$$

then the preimage of Y under $\widetilde{\phi}$ is a closed set containing $X \setminus \{P\}$, thus equal to X. That is, $\widetilde{\phi}$ factors through Y.

Let therefore $\phi : X \setminus \{P\} \longrightarrow \mathbb{P}^n_{x_0,\dots,x_n}$ be a morphism. Let

$$U = \{(x_0 : \cdots : x_n) : x_i \neq 0 \ \forall i\}.$$

If $\phi(X \setminus \{P\}) \cap U = \emptyset$, then $\phi(X \setminus \{P\})$ being irreducible is contained in one of the hyperplanes $\{x_i = 0\}$ forming the complement of U. However, each such hyperplane is isomorphic to $\mathbb{P}^{n-1}$ and we are done by induction on the dimension. We may therefore assume that $\phi(X \setminus \{P\}) \cap U \neq \emptyset$. Therefore, for every i, j the function $f_{ij} = \phi^*(x_i/x_j)$ is a regular function on $X \setminus \{P\}$. In particular, $f_{ij} \in K(X)$.

Let v_P be the valuation associated to the local ring P. Let

$$r_0 = v_P(f_{00}), r_1 = v_P(f_{10}), \dots, r_n = v_P(f_{n0}).$$

Let i be an index such that r_i is minimal. Then, for every j we have

$$v_P(f_{ji}) = v_P(f_{j0}/f_{i0}) = r_j - r_i \geq 0.$$

Thus, $f_{ji} \in P$ for every j. We define

$$\widetilde{\phi}(P) = (f_{0i}(P), \dots, f_{ni}(P)).$$

Note that this is well defined! First $f_{ii} = 1$ and for every j we have $f_{ji}(P) \in k$.

To show that $\widetilde{\phi}$ is a morphism, it is enough to show that regular functions in a neighbourhood of $\widetilde{\phi}(P)$ pull back to regular functions in a neighbourhood of P. Note that in fact

$$\widetilde{\phi}(P) \in U_i = \{x : x_i \neq 0\} \cong \mathbb{A}^n_{\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}}.$$

It is enough to prove the assertion for open sets contained in U_i. Thus, it would be enough to show that $\widetilde{\phi}^* x_j/x_i$ is a regular function (the assertion then follows for any open set in U_i). But, at every point in the preimage of U_i that is not P this is already known and at P we have $\widetilde{\phi}^* x_j/x_i = f_{ji} \in P$. ☐

Theorem 6.9. *Let K/k be a function field. Then C_K is isomorphic to a non-singular projective curve.*

Proof. We saw that given $R \in C_K$ there exists some non-singular affine curve X_R and a point $x_R \in X_R$ such that $R \cong \mathcal{O}_{X,x_R}$. The curve X_R is isomorphic to the abstract curve $U \subset C_K$, where $U = \{\mathcal{O}_{X,x} : x \in X\}$. Therefore, we may write

$$C_K = \cup_R U_R,$$

where each U_R is isomorphic to an affine non-singular curve. However, since open sets are cofinite, C_K is quasi compact. Thus,

$$C_K = U_1 \cup \dots \cup U_t,$$

where each U_i is an open affine subset, that is, isomorphic to a non-singular affine curve X_i. Say $\phi_i : U_i \longrightarrow X_i$. Let Y_i be the closure of X_i in some projective space $\mathbb{P}^{n(i)}$. Applying the previous lemma successively, we see that there exists a morphism

$$\phi_i : C_K \longrightarrow Y_i,$$

extending the one on U_i. Let

$$\phi : C_K \longrightarrow Y_1 \times \dots \times Y_t \subset \mathbb{P}^{n(1)} \times \dots \times \mathbb{P}^{n(t)} \subset \mathbb{P}^N,$$

be the diagonal morphism. That is

$$\phi(R) = (\phi_1(R), \dots, \phi_t(R)).$$

Let Y be the closure of the image of ϕ. It is a projective curve. We shall show that $\phi : C_K \longrightarrow Y$ is an isomorphism.

Let $P \in C_K$. Then $P \in U_i$ for some i. Let $\pi : Y \longrightarrow Y_i$ be the projection induced from $Y \subset \prod Y_i$. Then $\pi \circ \phi = \phi_i$ on the set U_i. We get inclusions of local rings

$$\mathcal{O}_{Y_i,\phi_i(P)} \xrightarrow{\pi^*} \mathcal{O}_{Y,\phi(P)} \xrightarrow{\phi^*} \mathcal{O}_{C_K,P}.$$

Moreover, since ϕ_i is an isomorphism on U_i, we get that all three rings are isomorphic ($\phi^* \circ \pi^*$ is an isomorphism) . In particular, for every $P \in C_K$ the rings $\mathcal{O}_{Y,\phi(P)}$ and $\mathcal{O}_{C_K,P}$ are isomorphic under ϕ^*.

We next show ϕ is surjective. Let $Q \in Y$ and take some discrete valuation ring R containing $\mathcal{O}_{Y,Q}$ (localize the integral closure of $\mathcal{O}_{Y,Q}$ at a suitable prime ideal). Then R is the local ring of some point $P \in C_K$ and the argument above shows that $\mathcal{O}_{Y,\phi(P)}$ is isomorphic to R. If Q and Q' are points on a curve such that $\mathcal{O}_Q \subset \mathcal{O}_{Q'}$ then $Q = Q'$ (Exercise 14). Thus $\phi(P) = Q$ and therefore ϕ is surjective. This rational also shows that ϕ is injective, because $\mathcal{O}_{Y,\phi(P)} \cong \mathcal{O}_{C_K,P}$.

We got so far that ϕ is a bijective morphism such that ϕ^* induces an isomorphism of local ring. This implies that ϕ^{-1} is a morphism (use that the set where a function f on a variety Z is regular is precisely $\bigcup_{f \in \mathcal{O}_{Z,z}} z$). ☐

Theorem 6.10. *(MAIN THEOREM) The following categories are equivalent:*
(i) Non-singular projective curves and dominant morphisms.
(ii) Quasi-projective curves and dominant rational maps.
(iii) Function fields of tr. deg. 1 *over* k *and* k*-morphisms.*

Proof. The functors $(i) \Rightarrow (ii)$ and $(ii) \Rightarrow (iii)$ are known to us. We also know that $(ii) \Rightarrow (iii)$ is an equivalence of categories. It would therefore be enough to construct a functor $(iii) \Rightarrow (i)$ and show that $(i) \Rightarrow (iii)$ and $(iii) \Rightarrow (i)$ give an equivalence of categories.

Given a function field K/k associate to it the curve C_K. This curve is isomorphic to a non-singular projective curve. Given another function field K'/k and a homomorphism of k-algebras $K'/k \longrightarrow K/k$ we have a rational map $C_K \longrightarrow C_{K'}$, and therefore a morphism $U \longrightarrow C_{K'}$ for some open non empty set U in C_K. Thus, the morphism extends uniquely to a morphism $C_K \longrightarrow C_{K'}$. It is immediate to verify that this process takes compositions to compositions, hence gives a functor $(iii) \Rightarrow (i)$.

Obviously, the objects associated to C_K and $C_{K'}$ under $(i) \Rightarrow (iii)$ are just K and K', and the induced map $K' \longrightarrow K$ is just the one we have started with. Thus, the functors $(i) \Rightarrow (iii)$ and $(iii) \Rightarrow (i)$ are equivalences of categories. □

7. SUMMARY

To every affine variety X be have associated a canonical affine variety $\pi : \widetilde{X} \longrightarrow X$ by the property that $\mathcal{O}(\widetilde{X})$ is the integral closure of $\mathcal{O}(X)$ in its function field. This is a functor on the category of affine varieties: to every morphism $f : X \longrightarrow Y$ there exists a canonical morphism $\widetilde{f} : \widetilde{X} \longrightarrow \widetilde{Y}$ such that the following diagram commutes

$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{\widetilde{f}} & \widetilde{Y} \\ \downarrow & & \downarrow \\ X & \xrightarrow{f} & Y \end{array}.$$

The morphism $\pi : \widetilde{X} \longrightarrow X$ is an example of an integral dominant morphism. It enjoys the many fine properties of a general dominant integral morphism $f : X \longrightarrow Y$:

(i) f is a surjective closed morphism.

(ii) $\dim(X) = \dim(Y)$ (and the fibres are zero dimensional, but this is in fact automatic as a general theorem says).

(iii) The hierarchy of closed sets in X and Y is very similar, as the the Cohen-Seidenberg theorem tells us: Given a chain of closed irreducible sets $Z_1 \supset \cdots \supset Z_n$ in Y, there exists a closed irreducible set $\widetilde{Z_1}$ of X such that $\overline{f(\widetilde{Z_1})} = Z_1$. Moreover, for any such $\widetilde{Z_1}$ there exists a chain $\widetilde{Z_1} \supset \cdots \supset \widetilde{Z_n}$ of closed irreducible sets in X such that for every i we have $\overline{f(\widetilde{Z_i})} = Z_i$.

Furthermore, every non-singular variety is a normal variety and normal varieties have important properties not shared by general varieties. For example:

(i) The singular set is of codimension ≥ 2. (In particular a normal curve is non singular).

(ii) The local ring of every sub-variety of codimension one is a discrete valuation ring (see next section).

The connection between normality and discrete valuation rings was crucial in the study of curves. Given a curve $\mathcal{C}$ over k with function field K, we associated to it a canonical non singular projective curve "consisting of all the discrete valuation rings of K/k". This description, in fact, was a technical gadget to glue together all the normalizations of affine open sets in $\mathcal{C}$. Note that for a curve the sub-varieties of codimension 1 are just points. We used heavily the general fact that if the curve is normal the local rings are discrete valuation rings. This discrete valuation was an algebraic mean to talk precisely about the order of vanishing (or pole) of a function at a point.

8. Some further properties of normal varieties

Definition 8.1. *Let X be any variety. Let $Z \subset X$ be a sub variety. We define the local ring of Z in X, $\mathcal{O}_{X,Z}$, to be the equivalence classes of pairs (U, f) consisting of an open set U such that $U \cap Z \neq \emptyset$ and f is a regular function on U. We decree that $(U, f) = (U', f')$ if $f = f'$ on $U \cap U'$. (Note that $U \cap U'$ intersects Z at some point. In fact, both $U \cap Z$ and $U' \cap Z$ are dense open in Z in the relative topology on Z).*

It is easy to see that this is indeed a local ring. The ideal $\mathfrak{m}$ defined by all couples $(U, 0)$ is a unique maximal ideal because $\mathcal{O}_{X,Z} \setminus \mathfrak{m}$ consists of invertible elements! The quotient field $\mathcal{O}(X, Z)/\mathfrak{m}$ is canonically $K(Y)$, the function field of Y.

In the case where X is affine and Z is defined by a prime ideal $\mathfrak{p}$ one checks that $\mathcal{O}_{X,Z}$ is non other then the localization of $\mathcal{O}(X)$ at the ideal $\mathfrak{p}$. This remark shows that in general

$$\dim(\mathcal{O}_{X,Z}) = \dim(X) - \dim(Z).$$

In particular, if Z is a point then $\mathcal{O}_{X,Z}$ is just the local ring of the point Z and it has dimension equal to that of X.

In the case where Z is of codimension 1 we see that $\mathcal{O}_{X,Z}$ is a local ring of dimension 1. Furthermore, if X is normal then $\mathcal{O}_{X,Z}$ is integral closed, hence a DVR. Since this is of tantamount importance we formulate it as

Theorem 8.2. *Let X be a normal variety. Then the local ring $\mathcal{O}_{X,Z}$ of any sub variety of codimension 1 is a discrete valuation ring.*

Definition 8.3. *Let X be a normal variety. Let f be a function on X, that is, an element of the function field of X. The divisor of f is*

$$(f) = \sum_Z v_Z(f) \cdot [Z],$$

where the sum extends over all (irreducible) sub varieties $Z \subset X$ of codimension 1, the symbol v_Z stands for the discrete valuation of $\mathcal{O}_{X,Z}$ normalized to have value group $\mathbb{Z}$ and $[Z]$ is a formal symbol.

It is easy to see that (f) is an element of the free abelian group on the symbols $[Z]$ (for $Z \subset X$ sub variety of codimension 1). That is, for only finitely many Z we have $v_Z(f) \neq 0$. This is because $v_Z(f) \neq 0$ implies that f is identically zero on Z or $1/f$ is identically zero on Z and therefore the collection of Z such that $v_Z(f) \neq 0$ is contained in the closed set T defined as follows: Let U be the open set such that f is regular on U. Let $A = f^{-1}(0)$. A closed set in U. Then $T = U \setminus A$: an open dense set (if $f \not\equiv 0$).

Another consequence of the local ring of Z being a discrete valuation ring is the following: Let $U \subset X$ be any open affine subset such that $U \cap Z$ is non empty. Then $\mathcal{O}_{U,Z} = \mathcal{O}_{X,Z} = \mathcal{O}(U)_{\mathfrak{p}}$ where $\mathfrak{p}$ is the prime ideal of $\mathcal{O}(U)$ defining Z in U, and is a discrete valuation ring. Let f be any element that generates the maximal ideal of $\mathcal{O}(U)_{\mathfrak{p}}$. We may shrink U such that f is a regular function on U.

Consider the closed set defined by f. It certainly contains Z. We may therefore choose some open set $W \subset U$ such that $(f) \cap W = Z \cap W$. We may even take W to be affine.

Finally, note that (f) is a radical ideal: If $g^n \in (f)$. Let v be the valuation associated to Z. Then $v(g^n) = n \cdot v(g) = nb$ for some positive b. Consider g/f^b. It has non-negative valuation at every local ring of every closed irreducible set T of codimension 1 in W. Therefore, it is an element of $\mathcal{O}(W)$ and hence $g = f^b \cdot (g/f^b) \in (f)$. [1]

Conclusion: Let X be a normal variety. Let Z be a sub variety of codimension 1, then there exists an open affine set $U \subset X$ such that $U \cap Z \neq \emptyset$ and $U \cap Z = (f)$ for some regular function $f \in \mathcal{O}(U)$.

Theorem 8.5. *Let X be a normal variety. Then $Sing(X)$ is of codimension ≥ 2.*

Proof. Assume not. We know that the singular locus is a closed set. Let Z be a component of the singular locus of codimension 1. Thus, every point on Z is a singular point of X. Replace X by a suitable affine variety, still denoted X, such that Z has the property $I(Z) = (f)$. Let $z \in Z$ such that z in non singular as a point on Z. We shall derive a contradiction by showing that z is a non-singular point of X. Let $n = \dim(X)$.

Let $f_1, \dots, f_{n-1} \in \mathcal{O}(X)$ such that $f_1, \dots, f_{n-1}$ is a basis for $\mathfrak{m}_{Z,z}/\mathfrak{m}_{Z,z}^2$. We claim that $f, f_1, \dots, f_{n-1}$ is a basis for $\mathfrak{m}_{X,z}/\mathfrak{m}_{X,z}^2$. It is enough to show they generate, because always $\dim(\mathfrak{m}_{X,z}/\mathfrak{m}_{X,z}^2) \geq n$. Let $g \in \mathfrak{m}_{X,z}$. We may write $g = \sum a_i f_i \pmod{(f)}$ and we are done.[2] □

The following results will not be proved at this point. We may return to them later on in the course. The following is one of the many formulations of Zariski's Main Theorem

Theorem 8.6. *Let Y be a normal variety over k and $f : X \longrightarrow Y$ a morphism that is birational and has finite fibres. Then f is an isomorphism of X with an open set $U \subset X$.*

Definition 8.7. *Let X be a variety. It is called "non-singular in codimension 1" if the local ring of every sub variety of codimension 1 is regular (equivalently, integrally closed; equivalently, a DVR). Equivalently, the set $Sing(X)$ has codimension ≥ 2.*

Thus, every non-singular variety is normal and every normal variety is non singular in codimension 1. However, the cone $z^2 = xy$ is a normal singular variety, and the affine surface in $\mathbb{A}^4$ whose ring of functions is $k[x, xy, y^2, y^3]$ is not normal but is non-singular at codimension 1.

Theorem 8.8. *Let X be an irreducible affine hypersurface. If X is non-singular in codimension 1, then X is normal.*

Lastly, many properties of a variety X at a point x can be studied via the tangent cone $C_{X,x}$. In particular:

Theorem 8.9. *If $C_{X,x}$ is reduced, normal[3] or regular (as a variety), then so is the local ring $\mathcal{O}_{X,x}$.*

[1] We have tacitly used the following fact: Let R be an integral domain. Then R is equal to the intersection $\cap R_\mathfrak{p}$ over all prime ideals of height 1. In fact one has the following theorem:

Theorem 8.4. *Let R be a noetherian integral domain. Then R is integrally closed iff (i) $R = \cap R_\mathfrak{p}$ – the intersection being taken over all prime ideals of height 1; AND (ii) for all prime ideals $\mathfrak{p}$ of height 1 the ring $R_\mathfrak{p}$ is a DVR.*

[2] Normality was used only to have Z generated by a unique element.

[3] Here normality means that the tangent cone is in particular reduced. That is, the ideal of initial forms defining the tangent cone is a radical ideal.