Introduction to Arithmetic Geometry

David Rufino

Apr 2020

Contents

1 Introduction

The purpose of this note is to provide an overview of the modern formulation of algebraic geometry (specifically scheme theory), and how it relates to classical algebraic geometry over fields. I try to simultaneously demonstrate the following

- Classical algebraic geometry over an algebraically closed field (Such as in Chapter I of Hartshorne, ...)
- Abstract varieties over a non-algebraically closed field (Ultraschemes in EGA I)
- Schemes (e.g. Chapter II Hartshorne)

with the view that introducing these concepts simultaneously will sufficiently motivate the abstract theory. My main motivation is to understand the statement and proof of the Weil conjectures. For the statement it is enough to work with abstract varieties, though the proof typically requires more advanced techniques, which were more or less invented to address the Weil conjectures.

Recall the Weil conjectures concern the Zeta function of a complete projective variety over a finite field given by

$$Z(V,T) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} T^r\right)$$

and N_r is the number of solutions of V over the finite field F_{q^r}. The Weil conjectures concern many surprising features of $Z(V,T)$, of which the most striking is the connection to the geometry of the variety when viewed as a Riemann surface. In the simplest case one has for a smooth curve C

$$Z(C,T) = \frac{P(T)}{(1-T)(1-qT)}$$

and the degree of $P(T)$ is $2g$ where g is the genus ("number of holes") of the curve (as viewed over $\mathbb{C}$, though it has an intrinsic definition over $\mathbb{F}_q$ too). Furthermore it also satisfies an analogue of the Riemann Hypothesis, so providing a connection between Geometry and Number Theory.

2 Algebraic Aspects of Differential Geometry

Many of the constructions in Algebraic Geometry are inspired from the theory of Differentiable Geometry. Although many concepts do not necessarily transfer verbatim, we may rephrase them in a more "algebraic" and "intrinsic" form, which is more amenable to applications in Algebraic Geometry. Therefore we provide a very brief introduction to the theory of manifolds, stating the concepts in a way which provides motivation for the constructions in Algebraic Geometry. The primary references for this section are [War13] and [Lan72].

2.1 Charts and differentiable functions

We consider two types of manifold in parallel

- A $\mathcal{C}^\infty$ manifold modelled on $\mathbf{E} = \mathbb{R}^n$
- A complex-analytic surface modelled on $\mathbf{E} = \mathbb{C}$

Definition 2.1 (Locally Euclidean Space [War13, Defn 1.3])
A Locally Euclidean Space X *of dimension d is a Hausdorff topological space X for which each point has a neighbourhood homeomorphic to an open subset of $\mathbb{R}^d$. Such a homeomorphism is a pair $(U, \phi : U \to \mathbb{R}^d)$, which we call a coordinate system. The functions $x_i = \pi_i \circ \phi$ are the "local coordinates" relative to this coordinate system.*

Definition 2.2 (Real Smooth Manifold [War13, Defn 1.3])
A differentiable manifold is a pair $(X, \mathcal{F})$ where X is a d-dimensional locally Euclidean space and $\mathcal{F}$ is a differentiable structure, namely a collection of coordinate systems

$$\{(U_\alpha, \phi_\alpha) : \alpha \in A\}$$

with

- $\bigcup_{\alpha \in A} U_\alpha = X$
- *The transition maps $\phi_\alpha \circ \phi_\beta^{-1}$ are $\mathcal{C}^\infty$ for all α, β*
- *$\mathcal{F}$ is maximal with respect to these properties, namely if there is a (U, ϕ) which is compatible in the sense of the above, then it is already in $\mathcal{F}$.*

Definition 2.3 (Riemann Surface [For81, Defn 1.1])
A Riemann surface is a 2-dimensional real manifold $(X, \mathcal{F})$ under which the transition maps are holomorphic under the obvious identification $\mathbb{R}^2 = \mathbb{C}$.

For this section we let $k = \mathbb{R}$ when considering Smooth Manifolds, and $k = \mathbb{C}$ when considering Riemann Surfaces

Definition 2.4 (Smooth (resp. holomorphic) functions [War13, Defn 1.6], [For81, Defn 1.6])
Let X be a Smooth Manifold (resp. Riemann Surface) and $U \subset X$ an open set then a function

$$f : U \to k$$

is smooth (resp. holomorphic) if

$$f \circ \phi^{-1}$$

is smooth (resp. holomorphic) for all coordinate maps ϕ.

Let $\mathcal{O}_X(U)$ denote the smooth (resp. holomorphic) functions on an open set U. This is naturally a k-algebra, where k maps to constant functions.

The fact that smoothness is a local property, can be formalized by saying that the mapping $U \to \mathcal{O}_X(U)$ constitutes a "sheaf"

Definition 2.5 (Sheaf [War13, Defn 5.7] [For81, Defn 6.3])
A sheaf of k-algebras (resp. sets, k-modules, groups) $\mathcal{F}$ on a topological space X is a mapping

$$U \longrightarrow \mathcal{F}(U)$$

of k-algebras (resp. sets, k-modules, groups) together with a collection of restriction k-algebra (resp. set, k-module, group) homomorphisms ρ_{UV}, for any pair of open sets $V \subset U$ satisfying the following properties

1. $\rho_{VW} \circ \rho_{UV} = \rho_{UW}$
2. *Suppose* $U = \bigcup_{i \in I} U_i$ *and* $\sigma, \tau \in \mathcal{O}_X(U)$ *satisfy*

$$\sigma|_{U_i} = \tau|_{U_i} \quad \forall i \in I$$

then $\sigma = \tau$.

3. *Suppose* $U = \bigcup_{i \in I} U_i$ *and there exists elements* $\sigma_i \in \mathcal{O}_X(U_i)$ *satisfying*

$$\sigma_i|_{U_i \cap U_j} = \sigma_j|_{U_i \cap U_j} \quad \forall i, j \in I$$

then there exists an element $\sigma \in \mathcal{O}_X(U)$ *such that* $\sigma|_{U_i} = \sigma_i$. *Moreover in this case the extension* σ *is unique.*

Elements of $\mathcal{F}(U)$ *are called sections.*
If it only satisfies the first property, then it is called a "presheaf". If it also satisfies the second then it is called a "separated presheaf".

The following will be useful later

Definition 2.6 ($\mathcal{B}$-sheaf)
Let $\mathcal{B}$ *be a basis of open sets which are closed under finite intersection, then we say a* $\mathcal{B}$*-sheaf is a mapping*

$$\mathcal{B} \ni U \to \mathcal{F}(U)$$

which satisfies the above sheaf axioms wrt $\mathcal{B}$.
As before if it only satisfies the first property it is called a $\mathcal{B}$*-presheaf.*

Clasically structure sheaves take the following form

Definition 2.7 (Space of k-functions)
We say $(X, \mathcal{O}_X)$ *is a space of* k*-functions if* $\mathcal{O}_X$ *is a presheaf such that*

$$\mathcal{O}_X(U) \subset \mathrm{Fun}(U, k)$$

with restriction maps corresponding to restriction of functions and

- *It contains all constant functions*
- $\mathcal{O}_X(U)$ *is a* k*-algebra*
- $\mathcal{O}_X$ *is a sheaf, equivalently for any open cover* $U = \bigcup_i U_i$ *we have*

$$f \in \mathcal{O}_X(U) \iff f|_{U_i} \in \mathcal{O}_X(U_i) \quad \forall i$$

- *If* $f \in \mathcal{O}_X(U)$ *is non-zero on* U *then*

$$D(f) = \{x \in U \mid f(x) \neq 0\}$$

is open and $1/f \in \mathcal{O}_X(D(f))$

Note for $D(f)$ *to be open it's enough for* f *to be continuous in the cofinite (or natural) topology on* k

It's then fairly clear to see the following

Proposition 2.1 (Space of smooth functions)
For a manifold X*, the* k*-algebra* $O_X(U)$ *of smooth functions on an open set* U *constitutes a space of* k*-functions.*

In what follows we usually denote by $\mathcal{F}$ an arbitrary sheaf, and $(X.\mathcal{O}_X)$ an arbitrary space of k-functions.

Definition 2.8 (Morphism of spaces of k-functions)
Let $(X, \mathcal{O}_X)$ *and* $(Y, \mathcal{O}_Y)$ *be two spaces of* k*-functions. A morphism consists of a continuous map*

$$f : X \to Y$$

such that

$$\sigma \in \mathcal{O}_Y(U) \implies \sigma \circ f \in \mathcal{O}_X(f^{-1}(U))$$

It's an easy result to show that in the case of a manifold such morphisms correspond to smooth maps of manifolds.

2.2 Stalks and Germs

For a sheaf $\mathcal{F}$ and a point $x \in X$ we may consider the stalk $\mathcal{F}_x$, which consists of equivalence classes of sections in an arbitrarily small neighbourhood. When $\mathcal{F}$ is a sheaf of k-functions, then this corresponds to the notion of "germ" of functions. The motivation is that the set of germs may be identified with the ring of convergent power series.

Definition 2.9 (Stalk of a sheaf)
Let $\mathcal{F}$ be a sheaf of sets (resp. k-algebras, groups, R-modules), then define the stalk $\mathcal{F}_x$ for $x \in X$ to be the directed limit

$$\mathcal{F}_x := \varinjlim_{x \in U} \mathcal{F}_U$$

under the directed system of restriction maps. Explicitly this may be constructed as

$$\mathcal{F}_x = \{(U, f) \mid f \in \mathcal{F}(U)\}/\sim$$

where $(U, f) \sim (V, g)$ if there is an open set $x \in W \subset U \cap V$ such that $f|_W = g|_W$.

In the case of a sheaf of k-functions $\mathcal{O}_X$ we may identify the stalks with germs of functions

Every germ $f_x \in \mathcal{O}_{X,x}$ has a well-defined value so we may define

Definition 2.10
Let $(X, \mathcal{O}_X)$ be a space of k-functions, and define the ideal of germs which vanish

$$\mathfrak{m}_x = \{f \in \mathcal{O}_{X,x} \mid f(x) = 0\}$$

We will show that the pair $(\mathcal{O}_{X,x}, \mathfrak{m}_x)$ is an example of a *local ring*

Definition 2.11 (Local Ring)
A pair $(A, \mathfrak{m})$ is a local ring if $\mathfrak{m}$ is the unique maximal ideal of the ring A. In this case we may write

$$\kappa(\mathfrak{m}) := A/\mathfrak{m}$$

which we call the "residue field".

It's easy to show that for a space of k-functions, $(\mathcal{O}_{X,x}, \mathfrak{m}_x)$ is a local ring by the following result

Lemma 2.2 (Stalks are local rings)
Suppose $(X, \mathcal{O}_X)$ is a space of k-functions on X, then $(\mathcal{O}_{X,x}, \mathfrak{m}_x)$ is a local ring such that the residue field is

$$\kappa(\mathfrak{m}_x) = k$$

Proof. By Lemma A.4 it is enough to show

$$\sigma_x \in \mathcal{O}_{X,x} \setminus \mathfrak{m}_x \implies \sigma_x \in (\mathcal{O}_{X,x})^\star \ .$$

Let σ_x be such a stalk then it corresponds to a section $\sigma \in \mathcal{O}_X(U)$. Define

$$U' = U \cap D(f)$$

This is an open neighbourhood of x (because $\sigma_x(x) \neq 0$), on which σ is clearly non-zero, and therefore invertible. Clearly $(1/\sigma)_x$ is the inverse of σ_x, and we are done by the previous result.
Finally it's clear that $\mathfrak{m}_x$ is the kernel of the evaluation morphism so $\kappa(\mathfrak{m}_x) = k$. □

It's easy to see that in general $\mathfrak{m}/\mathfrak{m}^2$ is a $\kappa(\mathfrak{m})$-vector space. In the case of a space of k-functions we call it the cotangent space.

Definition 2.12 (Cotangent space)
For a space of k-functions $(X, \mathcal{O}_X)$ define the cotangent space at x to be the k-vector space

$$T^\star_x X := \mathfrak{m}_x/\mathfrak{m}_x^2$$

If the ring $\mathcal{O}_{X,x}$ is Noetherian then clearly the co-tangent space is finite-dimensional. However in the smooth manifold case, the local rings are no longer Noetherian, but the cotangent space is still finite-dimensional as we demonstrate in the next section.

In order to illustrate that it's non-Noetherian consider the the ideals $\mathfrak{m}_x^k$, of linear combinations of k-fold products of $\mathfrak{m}_x$. The significance of these is that they are the functions which vanish to k-th order. One feature of differentiable manifolds is that there exist smooth functions (e.g. e^{-1/x^2}) which vanish to arbitrary order, which means that

$$\bigcap_{i=1}^{\infty} \mathfrak{m}_x^i \neq \emptyset$$

This is actually false when the ring $\mathcal{O}_{X,x}$ is Noetherian (Krull's Intersection theorem, see for example [Mil14, Thm 3.16]). Usually rings in Algebraic Geometry will be Noetherian, highlighting one difference to the analytic case.

2.3 Tangent Space

Recall for $\mathbb{R}^n$, there is the concept of directional derivative. Namely for a point $p \in \mathbb{R}^n$ and a vector $v \in \mathbb{R}^n$ one may define the derivative of a function

$$D_{v,p}f := \left.\frac{df(p+tv)}{dt}\right|_{t=0} = \left.\sum_{i=1}^{n} v_i \partial_{x_i} f\right|_p .$$

As definition of derivative is purely local this actually acts on germs of functions at p

$$D_{v,p} : \mathcal{O}_{X,x} \to \mathbb{R}$$

and satisfies certain standard properties, e.g. the Liebniz Product Rule. The concept of tangent space generalizes this to a general manifold

Definition 2.13 (Tangent Space)
Let $\mathcal{O}_X$ be a sheaf of k-functions and define the k-vector space of derivations

$$T_pX := \{D : \mathcal{O}_{X,x} \to k \mid D \text{ satisfies eqns (1)-(3) }\}$$

$$\begin{aligned} D(\lambda f) &= \lambda D_{v,p}(f) && (1)\\ D(f+g) &= D(f) + D(g) && (2)\\ D(fg) &= g(p)D(f) + f(p)D(g) && (3) \end{aligned}$$

Given a coordinate chart (U, ϕ) and a point $p \in U$ and a vector $v \in \mathbb{R}^d$ we can define the directional derivative

$$D_{v,p}f := D_{v,\phi(p)}(f \circ \phi^{-1}) = \left.\frac{d(f \circ \phi^{-1})(\phi(p)+tv)}{dt}\right|_{t=0} = \sum_{i=1}^{d} v_i \partial_{x_i}(f \circ \phi^{-1})$$

We show in the next section this induces an isomorphism between $\mathbb{R}^d$ and T_pX, depending on the coordinate chart. It is convenient to first identify explicitly the dual of T_pX.

Proposition 2.3
Suppose $\mathcal{O}_X$ is a sheaf of k-functions. Then there is an isomorphism of k-vector spaces

$$\psi_L : T_pX \to \hom_k(\mathfrak{m}_p/\mathfrak{m}_p^2, k)$$

given by

$$d \longrightarrow (f_p \to f_p - f_p(p))$$

When $\dim_k \mathfrak{m}_p/\mathfrak{m}_p^2 < \infty$ this induces a perfect pairing

$$T_pX \times \mathfrak{m}_p/\mathfrak{m}_p^2 \to k$$

Proof. Suppose that $f - g \in \mathfrak{m}^2$ then $f - g = \sum_i \lambda_i a_i b_i$ for $a_i, b_i \in \mathfrak{m}$. Then it's clear that by the derivation property $d(f-g) = 0$, and so $d(f) = d(g)$. This shows that the mapping is well-defined.

Firstly suppose $\theta \in (\mathfrak{m}/\mathfrak{m}^2)^\star$. Define $d_\theta(f) := \theta(f - f(p))$. Then

$$d_\theta(fg) = \theta(fg - f(p)g(p)) = \theta((f-f(p))(g-g(p)) + g(p)(f-f(p)) + f(p)(g-g(p)))$$

The first term vanishes because it lies in $\mathfrak{m}^2$, showing that d_θ satisfies the Liebniz Rule. The other properties are immediate. It's clear that $\psi_L(d_\theta) = \theta$ showing that ψ_L is surjective.

We claim $d(\lambda) = 0$ for all scalars λ. Observe that for any derivation d, we have $d(1) = d(1.1) = 1.d(1) + 1.d(1)$ which shows that $d(1) = 0$, and therefore $d(\lambda) = 0$.

To show that it's injective, suppose $d(f) = 0$ for all $f \in \mathfrak{m}_x$, then it must be identically zero, because $d(f) = d(f - f(p)) + d(f(p)) = 0$. This shows that ψ_L is injective, and therefore bijective.
In the finite-dimensional case Lemma A.1 shows that the given pairing is perfect. □

2.4 Taylor's Theorem and Cotangent Space

The purpose of this section is to use specifically the geometry of $\mathbb{R}^d$ to show that

- $\dim_k \mathfrak{m}_p/\mathfrak{m}_p^2 = d$
- T_pX is dual to $\mathfrak{m}_p/\mathfrak{m}_p^2$ as a k-vector space

An important result in differentiable geometry is Taylor's theorem, which says that a differentiable function may locally be approximated as a linear function plus a suitable remainder term (and higher order generalizations). We state this in concrete terms and algebraic terms. First we establish some notation

Definition 2.14 (Gradient)
Suppose $f : U \to \mathbb{R}^m$ is a differentiable function on some open set $U \subset \mathbb{R}^n$. Define the gradient as follows

$$\nabla(f)(x) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1}(x) & \dots & \dots & \frac{\partial f_1}{\partial x_n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_1}(x) & \dots & \dots & \frac{\partial f_m}{\partial x_n}(x) \end{bmatrix}$$

Definition 2.15 (Hessian)
Suppose $f : U \to \mathbb{R}$ is a twice differentiable function on some open set $U \subset \mathbb{R}^n$. Define the hessian as follows

$$\nabla^2(f)(x) = \begin{bmatrix} \frac{\partial^2 f}{\partial x_1^2} & \dots & \frac{\partial^2 f}{\partial x_n \partial x_1} \\ \vdots & \frac{\partial^2 f}{\partial x_i \partial x_j} & \vdots \\ \frac{\partial^2 f}{\partial x_1 \partial x_n} & \dots & \frac{\partial^2 f}{\partial x_n^2} \end{bmatrix}$$

Theorem 2.4 (Taylor's Theorem for $\mathbb{R}^n$)
Suppose $f \in \mathcal{C}^2(U)$, where $U \subset \mathbb{R}^n$ is open. Let x, h be two points such that $x + th \in U$ for all $t \in [0, 1]$. Then

$$f(x+h) = f(x) + (\nabla f)(x)h + R(x,h)$$

where

$$R(x,h) = \frac{1}{2}h^T \cdot \int_0^1 (1-t)(\nabla^2 f)(x+th)dt \cdot h$$

and in particular $|R(x,h)| \leq C(x)|h|^2$.

Proposition 2.5 (Taylor's Theorem for Manifolds)
Let $f \in \mathcal{O}_X(U)$ be a regular function of a manifold X, and fix a point $p \in U$. Then in some neighbourhood V of p there exists a representation

$$f(q) = f(p) + f^{(1)}(q) + f^{(2)}(q) \quad \forall q \in V$$

such that $(f^{(k)})_p \in \mathfrak{m}_p^k$. This implies the relation of germs

$$f_p = f(p) + f_p^{(1)} + f_p^{(2)}$$

and every germ may be represented in this way. Explicitly given a (small enough) chart (V, ϕ) with local coordinates $x_1, \dots, x_n$, we have

$$\begin{aligned} f^{(1)}(q) &= \sum_{i=1}^n \frac{\partial(f \circ \phi^{-1})}{\partial x_i}\bigg|_{f(\phi(p))} (\phi_i(q) - \phi_i(p)) \\ f^{(2)}(q) &= \frac{1}{2}\sum_{i,j=1}^n \left(\int_0^1 (1-t)\, \frac{\partial^2(f \circ \phi^{-1})}{\partial x_i \partial x_j}\bigg|_{\phi(p)+t(\phi(q)-\phi(p))} dt \right) (\phi_i(q) - \phi_i(p))(\phi_j(q) - \phi_j(p)) \end{aligned}$$

Proof. Let (U, ϕ) be a chart containing p. Since $\phi(U)$ is an open set containng $x := \phi(p)$, there is radius $r > 0$ such that $B(x; r) \subset \phi(U)$. Define $V = \phi^{-1}(B(x; r))$. Consider the function

$$g = f \circ \left(\phi^{-1}|_{\phi(V)}\right)$$

Then for any $q \in V$, define $y = \phi(q)$ and $h = y - x$. These points, together with g satisfy the conditions of Taylor's Theorem. So we have

$$g(y) = g(x) + (\nabla g)(x)(y-x) + \frac{1}{2}(y-x)^T \int_0^1 (1-t)(\nabla^2 f)(x+th)dt \cdot h$$

Substituting $x = \phi(p)$ and $y = \phi(q)$, we obtain

$$f(q) = f(p) + f^{(1)}(q) + f^{(2)}(q)$$

with terms defined in the proposition. It's clear that $f_p^{(1)} \in \mathfrak{m}_x$ because each individual $(\phi_i(q) - \phi_i(p))_p$ is. Similarly it's clear that $f_p^{(2)} \in \mathfrak{m}_p^2$.

□

We may use Taylor's theorem to show that the cotangent space is finite-dimensional

Corollary 2.6 (Cotangent space is finite-dimensional)
A k-basis for $\mathfrak{m}_p/\mathfrak{m}_p^2$ is given by

$$\{(x_i)_p - x_i(p)\}_{i=1\ldots d}$$

where (U, ϕ) is a chart and $x_1, \ldots, x_d$ are local coordinates. We denote these by $(dx_1)_p, \ldots, (dx_d)_p$. In particular

$$\dim_k \mathfrak{m}_p/\mathfrak{m}_p^2 = d$$

Proof. By Proposition 2.5 the given germs are spanning. Suppose they are linearly dependent, then

$$\sum_{i=1}^{n} \lambda_i((\phi_i)_p - x_i(p)) = 0$$

Then there is some neighbourhood U of p such that

$$g(q) := \sum_{i=1}^{n} \lambda_i(\phi_i(q) - \phi_i(p)) = 0 \quad \forall q \in U$$

Translating this into $\mathbb{R}^n$ shows that

$$G(x) := \sum_{i=1}^{n} \lambda_i(x_i - \phi_i(p)) = 0$$

for all x in a neighbourhood of $\phi_i(p)$. Then $\frac{\partial G}{\partial x_i} = \lambda_i = 0$ as required. □

Note this isn't entirely trivial as it will not hold for the case of C^k manifolds. Recall that there is a canonical perfect pairing between $\mathcal{D}_p X$ and $T_p^\star X$.

Definition 2.16 (Tangent Basis)
Consider the standard basis $\{(dx_i)_p\}_{i=1\ldots n}$ of $T_p^\star X$ relative to some chart (U, ϕ) defined in Corollary 2.6. Denote the corresponding dual basis of $T_p X$ (with respect to the pairing just defined) by

$$\left\{ \left(\frac{\partial}{\partial x_i} \right) \Big|_p \right\}_{i=1\ldots n}$$

Finally we clarify the meaning of the standard basis

Proposition 2.7
Let (U, ϕ) be a coordinate chart and $v \in \mathbb{R}^d$. Then the directional derivative at v is given by

$$D_{v,p} = \sum_{i=1}^{n} v_i \left(\frac{\partial}{\partial x_i} \right) |_p$$

and this induces an isomorphism

$$\mathbb{R}^d \longrightarrow T_p X$$

Proof. We show that $D_{e_i,p}((dx_j)_p) = \delta_{ij}$, which means that $D_{e_i,p} = \left(\frac{\partial}{\partial x_i} \right)_p$ by definition of the dual basis. This follows almost immediately because

$$D_{e_i,p}((dx_j)_p) = \frac{\partial((x_i - x_i(p)) \circ \phi^{-1})}{\partial x_j}|_{\phi(p)} = \delta_{ij}$$

As $D_{v,p}$ is linear in v we find that

$$D_{v,p} = \sum_{i=1}^{n} v_i \left(\frac{\partial}{\partial x_i} \right)_p$$

Given any $d \in T_p(X)$, let $v_i := d((x_i)_p)$. We claim that $d = D_{v,p}$. By Corollary 2.6, any $f \in \mathcal{O}_{X,x}$ may be represented as $f = f(p) + \sum_{i=1}^n \lambda_i (dx_i)_p \bmod \mathfrak{m}_p^2$. In this case $d(f) = \sum_{i=1}^n \lambda_i v_i = D_{v,p}(f)$ using the formula above. This shows that the mapping is surjective.
Suppose $D_{v,p} = D_{w,p}$, then apply $(dx_i)_p$ in turn to show $v = w$, which shows the mapping is injective. □

Finally the chain rule becomes a matter of linear algebra, via Proposition A.2.

Proposition 2.8 (Change of variable/coordinates formulae)
Let $x_1^\alpha, \ldots, x_n^\alpha$ and $x_1^\beta, \ldots, x_n^\beta$ be local coordintes corresponding to two charts (U_α, ϕ_α) and (U_β, ϕ_β). Then we have the change of variable formulae (with respect to a fixed point p, which we elide from below)

$$dx_i^\alpha = \sum_{j=1}^n \left.\frac{\partial(x_i^\alpha \circ \phi_\beta^{-1})}{\partial x_j^\beta}\right|_{\phi_\beta(q)} dx_j^\beta$$

$$\frac{\partial}{\partial x_i^\alpha} = \sum_{j=1}^n \frac{\partial(x_j^\beta \circ \phi_\alpha^{-1})}{\partial x_i^\alpha}\frac{\partial}{\partial x_j^\beta}$$

or in (co) vector form

$$dx^\alpha = \nabla(\phi_\alpha \circ \phi_\beta^{-1})dx^\beta$$

$$\frac{\partial}{\partial x^\alpha} = \nabla(\phi_\beta \circ \phi_\alpha^{-1})^T\frac{\partial}{\partial x^\beta}$$

NB the change of basis matrix for tangents and cotangents is inverse

Proof. We have two pairs of dual bases, therefore we may apply the second part of Proposition A.2 with $e_i = \frac{\partial}{\partial x_i^\alpha}$, $e_i^\star = dx_i^\alpha$, $f_i = \frac{\partial}{\partial y_i^\beta}$ and $f_i^\star = dy_i^\beta$, to obtain

$$dx_i^\alpha = \sum_{j=1}^n \left(\left.\frac{\partial}{\partial x_j^\beta}\right|_p dx_i^\alpha\right) dx_j^\beta$$

By definition

$$\left.\frac{\partial}{\partial y_j}\right|_p dx_i = \left.\frac{\partial((x_i - x_i(p)) \circ \psi^{-1})}{\partial y_i}\right|_{\psi(p)} = \left.\frac{\partial(x_i \circ \psi^{-1})}{\partial y_i}\right|_{\psi(p)}$$

which yields the first result. The second is similar. The vector form is immediate from the first two relations.
Check:

$$\frac{\partial}{\partial x}dx^T = J^{-T}\frac{\partial}{\partial y}dy^T J^T = I$$

□

2.5 Differential Forms

A differential form is a family of cotangent elements, smoothly varying in the point $p \in X$. Explicitly a 1-form ω over U is a mapping $U \to T^\star X := \bigcup_{p\in X} T_p^\star X$ such that $\omega(p) \in T_p^\star X$ and satisfying a certain smoothness condition. For every chart (U_α, ϕ_α) with local coordinates $x_1^\alpha, \ldots, x_n^\alpha$ there is a representation

$$\omega(q) = \sum_i a_i^\alpha(q)(dx_i^\alpha)_q \quad \forall q \in U_\alpha$$

and $a_i^\alpha(q)$ is some function on X. We require that $a_i^\alpha \in \mathcal{O}_X(U_\alpha)$. Note that

$$\omega(q) = \sum_i a_i^\alpha(q)(dx_i^\alpha)_q = \sum_{i,j} a_i^\alpha(q)\nabla(\phi_\alpha \circ \phi_\beta^{-1})(\phi_b(q))_{ij}(dx_j^\beta)_q$$

so we have the change of variable formula

$$a^\beta(q) \quad = \quad \nabla(\phi_\alpha \circ \phi_\beta^{-1})(\phi^\beta(q))^T a^\alpha(q) \tag{4}$$

Given a differential form it's possible to define a path integral. Let $\gamma : [a, b] \to X$ be a continuously differentiable function such that $\gamma([a, b]) \subseteq U_\alpha$. Then define

$$\int_\gamma \omega = \int_a^b (\phi_\alpha \circ \gamma)'(t)^T(a^\alpha(\gamma(t)))dt$$

Suppose $\gamma([a, b]) \subset U_\alpha \cap U_\beta$, then we may apply the change of variable formulae

$$\begin{aligned}\int_\gamma \omega &= \int_a^b \left(\phi_\alpha \circ \phi_\beta^{-1} \circ \phi_\beta \circ \gamma\right)'(t)^T (a^\alpha \circ \gamma)(t) dt \\ &= \int_a^b (\phi_\beta \circ \gamma)'(t)^T \nabla(\phi_\alpha \circ \phi_\beta^{-1})(\phi_\beta(\gamma(t)))^T a^\alpha(\gamma(t)) dt \\ &= \int_a^b (\phi_\beta \circ \gamma)'(t)^T a^\beta(\gamma(t)) dt\end{aligned}$$

which shows that the path integral is independent of the choice of chart.

For an open set $U \subset X$ we write $\Omega(U)$ for the set of smooth (resp. holomorphic) 1-forms on X.

2.6 Meromorphic forms

Now specialize to the case of X a Riemann surface, in which case $n = 1$. We generalize the notion of holomorphic 1-form to allow finitely many poles.

Definition 2.17 (Pole of a holomorphic form)
Let $Y \subset X$ be an open subset and $\omega \in \Omega_X(Y)$. We say that ω has a pole at $a \in X \setminus Y$ if a is an isolated point, and there is a chart (U, z) such that $a \in U$ and $U \setminus \{a\} \subset Y$ and furthermore

$$\omega|_Y = f dz$$

where $f(z)$ is meromorphic and has a removable singularity or pole at a.

Definition 2.18 (Meromorphic forms)
c.f. Forster
For an open set $Y \subset X$, we say ω is a meromorphic 1-form if there exists an open set $Y' \subset Y$ such that

- *ω is a holomorphic 1-form on Y'*
- *$Y \setminus Y'$ consists of only isolated points*
- *ω has a removable singularity or pole at every $a \in Y \setminus Y'$*

Let $a \in Y \setminus Y'$ and (U, z) a local chart such that $z(a) = 0$ and $\omega = f dz$, then by general theory there is a Laurent series' expansion

$$f(z) = \sum_{n>>-\infty}^{\infty} c_n z^n$$

We define

$$\mathrm{Res}_p(\omega) = c_{-1}$$

Then we have the following important result

Theorem 2.9 (Residue Theorem)
Suppose X is a compact Riemann surface and ω is a meromorphic 1-form with poles at $a_1, \ldots, a_n$, then one has

$$\sum_{i=1}^{n} \mathrm{Res}_{a_i}(\omega) = 0$$

3 Basics of Algebraic Geometry

Primary references for this section are [Sha94] and [Mil17].

In this section we suppose that k is perfect, but not necessarily algebraically closed. In particular any algebraic extension of k is separable, and any normal algebraic extension is Galois.

3.1 Affine algebraic sets over a field

Consider the polynomial ring $k[X] := k[X_1, \ldots, X_n]$. Note that $k[X]$ is an *integral* f.g. k-algebra. Define an order reversing Galois connection as follows

Definition 3.1
Correspondence between Zero Loci and Coordinate Ring Ideals

$$\begin{array}{rcl} \{V \subseteq k^n\} & \underset{I}{\overset{V}{\leftrightarrows}} & \{S \subseteq k[X_1, \ldots, X_n]\} \\ V(S) & := & \{x \in k^n \mid f(x) = 0 \quad \forall f \in S\} \\ I(Y) & := & \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0 \quad \forall x \in Y\} \end{array}$$

in other words $V(S)$ is the zero-locus of S, we say sets of this form are *closed*. We note some simple results

Lemma 3.1
Trivialities

1. *V and I are order reversing*
2. *$V(S) = V(\langle S \rangle) = V(\sqrt{\langle S \rangle})$ and $I(Y)$ is a radical ideal*
3. *$V(1) = \emptyset$ and $k^n = V(0)$*
4. *$\cap_{i \in I} V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$*
5. *$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$*
6. *$I(\emptyset) = k[X]$ (by convention at least)*
7. *$I(k^n) = (0)$ when k is an infinite field (NB $X^q - X$ in $\mathbb{F}_q[X]$)*
8. *$I(\cup_i W_i) = \cap_i I(W_i)$*
9. *$IV(\mathfrak{a}) \supseteq \sqrt{\mathfrak{a}}$*
10. *$VI(Y) = \overline{Y}$*

Proof. We list proofs in order

1. Suppose $S \subseteq T$ then $V(T) \subseteq V(S)$ a-fortiori. Similarly $Z \subseteq Y \implies I(Y) \subseteq I(Z)$.
2. In light of the previous result we only need to show $V(S) \subseteq V(\langle S \rangle) \subseteq V(\sqrt{\langle S \rangle})$. If $x \in V(S)$ then $f(x) = 0 \implies (gf)(x) = 0$. Suppose $x \in V(\mathfrak{a})$ and $f \in \sqrt{\mathfrak{a}}$. Then $f^n \in \mathfrak{a} \implies f^n(x) = 0$ for some n. As k is a field we have $f(x) = 0$, so that $x \in V(\sqrt{\mathfrak{a}})$.

   Similarly $f^n \in I(Y) \implies (f^n)(x) = 0 \implies f(x) = 0 \implies f \in I(Y)$, which shows that $I(Y)$ is radical.
3. This is obvious
4. We have $x \in \cap_{i \in I} V(\mathfrak{a}_i) \iff f(x) = 0 \quad \forall f \in \bigcup_{i \in I} \mathfrak{a}_i \iff x \in V(\bigcup_{i \in I} \mathfrak{a}_i) \overset{2}{=} V(\sum_{i \in I} \mathfrak{a}_i)$.
5. Observe that $\mathfrak{m}_x := I(\{x\})$ is prime (actually maximal) and $x \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{m}_x$. Therefore

$$\begin{array}{rcl} x \in V(\mathfrak{a}) \cup V(\mathfrak{b}) & \iff & \mathfrak{a} \subseteq \mathfrak{m}_x \vee \mathfrak{b} \subseteq \mathfrak{m}_x \\ & \overset{\mathfrak{m}_x \text{ prime}}{\iff} & \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{m}_x \iff x \in V(\mathfrak{a}\mathfrak{b}) \\ & \iff & \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{m}_x \iff x \in V(\mathfrak{a} \cap \mathfrak{b}) \end{array}$$

   For the last equivalence in general we have $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, so one direction is clear. Conversely suppose $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{m}_x$ and $y \in \mathfrak{a} \cap \mathfrak{b}$. Then $y^2 \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{m}_x$, and by primality $y \in \mathfrak{m}_x$ as required.
6. This is by convention so that later results hold
7. Suppose $0 \neq f \in I(k^n)$. Consider $f(X_1, x_2, \ldots, x_n) \in k[X_1]$ for some $x_2, \ldots, x_n \in k$. By general theory f may have at most $\deg(f)$ roots, which is a contradiction.
8. $f \in I(\bigcup_{i \in I} W_i) \iff f(W_i) = 0 \quad \forall i \iff f \in I(W_i) \quad \forall i \iff f \in \bigcap_{i \in I} I(W_i)$
9. By definition $\mathfrak{a} \subseteq IV(\mathfrak{a})$, as the right hand side is radical we have $\sqrt{\mathfrak{a}} \subseteq IV(\mathfrak{a})$, as $\sqrt{\mathfrak{a}}$ is the smallest radical ideal containing $\mathfrak{a}$.
10. Clearly $Y \subseteq VI(Y)$, as the right-hand side is closed we have $\overline{Y} \subseteq VI(Y)$.

□

Therefore the algebraic sets determine a topology on $\mathbb{A}^n_k := k^n$, which we call the **Zariski topology**. Moreover the Galois connection above restricts to a relation between closed sets and radical ideals

$$\{W \subseteq \mathbb{A}^n_k \mid W \text{ closed } \} \underset{I}{\overset{V}{\leftrightarrows}} \{\mathfrak{a} \lhd k[X_1, \ldots, X_n] \quad \mathfrak{a} \text{ radical } \}.$$

Example 3.2 (Zariski Topology on k^1)
A simple example is the Zariski topology on the affine line k^1. We claim that it has the co-finite topology, namely the topology in which finite sets are precisely the closed sets. Recall $k[X]$ is a PID, so every ideal is of the form (f). By general theory f has at most $\deg(f)$ roots, so $Z(f)$ is finite. Conversely given a finite set Y then it's clear that $Y = V(\prod_{p \in Y}(X - p))$.

We study in more detail the singletons $\{x\}$ and the associated ideals $\mathfrak{m}_x := I(\{x\})$

Lemma 3.2 (Functions vanishing at a point)
For $x \in k^n$ define

$$\mathfrak{m}_x := \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0\} = I(\{x\})$$

then

- *$\mathfrak{m}_x$ is the kernel of the evaluation homomorphism*

$$\begin{aligned} \phi_x : k[X_1, \ldots, X_n] &\longrightarrow k \\ f &\longrightarrow f(x) \end{aligned}$$

- *$\mathfrak{m}_x = (X_1 - x_1, \ldots, X_n - x_n)$ and is maximal*

Proof. The first result is clear, which shows that $\mathfrak{m}_x$ is maximal (as ϕ_x is surjective, k is a field). It's clear that $(X_1 - x_1, \ldots, X_n - x_n) \subseteq \mathfrak{m}_x$. In general it is possible to show that

$$f(X_1, \ldots, X_n) = f(x) + \sum_{i=1}^{n} (X_i - x_i) h_i(X_1, \ldots, X_n)$$

for some polynomials $h_1, \ldots, h_n$ so that one has in general f lies in the coset

$$f \in f(x) + (X_1 - x_1, \ldots, X_n - x_n)$$

so that $f \in \mathfrak{m}_x \iff f(x) = 0 \iff f \in (X_1 - x_1, \ldots, X_n - x_n)$ as required. □

Remark 3.3
In general not all maximal ideals arise in this way, for example $(X^2 - 2)$ is maximal in $\mathbb{Q}[X]$.

For $n = 1$ the situation is easy to understand: $k[X_1]$ is a PID and therefore any maximal ideal $\mathfrak{m}$ is of the form (f) for f irreducible. When $k = \bar{k}$ is algebraically closed then clearly f must also be linear, which is to say (f) is of the form $\mathfrak{m}_x$.

Later we will show that every maximal ideal is of this form even when $n > 1$ (and $k = \bar{k}$) (the weak Nullstellensatz).

For the moment we show how to generate maximal ideals not of this form when $k \neq \bar{k}$ and $n \geq 1$. Later we will also show that this accounts for all remaining maximal ideals of $k[X_1, \ldots, X_n]$.

Proposition 3.3
Suppose $k \subset K$ is an algebraic extension and $0 \neq x \in K^n$. Then define as before

$$\mathfrak{m}_x := \ker(\phi_x)$$

where ϕ_x is the evaluation homomorphism at x. Then $\mathfrak{m}_x$ is a maximal ideal of $k[X_1, \ldots, X_n]$.

Proof. Clearly $\mathrm{Im}(\phi_x)$ is a subring of K containing k, and is therefore an integral domain which is integral over k. It is therefore a field by Proposition A.20, which shows that $\mathfrak{m}_x$ is maximal. □

Definition 3.4 (Coordinate Ring of an algebraic set)
Let $\mathfrak{a} \lhd k[X_1, \ldots, X_n]$ be a radical ideal, and $X = V(\mathfrak{a})$ be the corresponding zero locus. Define the coordinate ring on X as follows

$$k[X] := k[X_1, \ldots, X_n]/\mathfrak{a}$$

Proposition 3.4
With notation as in 3.4, then

- *$k[X]$ is a reduced f.g. k-algebra*
- *X is a closed subset of k^n in the Zariski topology*
- *There is a canonical injection*

$$i : k[X] \hookrightarrow \mathrm{Fun}(X, k)$$

given by evaluation $\bar{f} \to (x \to f(x))$.

Proof. The first two statements are obvious. Given $x \in V(\mathfrak{a})$ define $i(\bar{f})(x) = f(x)$. This is well-defined because $\bar{f} = \bar{g} \implies (f-g) \in \mathfrak{a} \implies (f-g)(x) = 0$. Similarly suppose $f(x) = g(x)$ for all $x \in V$, then $(f-g) \in \mathfrak{a} \implies \bar{f} = \bar{g}$, so i is injective. □

Using interpretation of $k[X]$ as a space of functions we obtain a similar Galois connection

Definition 3.5
Closed subsets of an algebraic set

$$\begin{array}{rcl} \{W \subseteq V\} & \underset{I}{\overset{V}{\leftrightarrows}} & \{S \subseteq k[V]\} \\ V(S) & := & \{x \in V \mid f(x) = 0 \quad \forall f \in S\} \\ I(Y) & := & \{f \in k[V] \mid f(x) = 0 \quad \forall x \in Y\} \end{array}$$

which satisfies all of the same properties as before (CHECK). Moreover the induced topology on V is the same as the subspace topology (CHECK)

When k is algebraically closed then we may show that the connection $I \leftrightarrow V$ induces a bijection between closed subsets and radical ideals, which is the content of the following theorem

Theorem 3.5 (Strong Nullstellensatz)
In the case $k = \bar{k}$ and $X = V(\mathfrak{a})$ is an algebraic set, then

$$IV(\mathfrak{b}) = \sqrt{\mathfrak{b}} \quad \mathfrak{b} \lhd k[X]$$

Corollary 3.6 (Points and ideal correspondence)
In the case $k = \bar{k}$ and $X = V(\mathfrak{a})$ is an algebraic set then the Galois correspondence (I, V) inducesa a bijection between closed sets and radical ideals.

$$\{\textit{closed subsets of } X\} \longleftrightarrow \{\mathfrak{a} \lhd k[V] \mid \mathfrak{a} \textit{ radical }\}$$

and further between maximal ideals and points

$$\{\textit{points of } X\} \longleftrightarrow \{\mathfrak{m} \lhd k[V] \mid \mathfrak{m} \textit{ maximal }\}$$

So in the case of an algebraically closed field in some sense everything important is captured by the algebraic invariant $k[V]$. We remark that this implies the apparently weaker result

Proposition 3.7 (Weak Nullstellensatz)
Let $k = \bar{k}$ be an algebraically closed field and $X = V(\mathfrak{a})$ a zero-locus, then every proper ideal $\mathfrak{b} \lhd k[V]$ has a non-trivial zero

$$\emptyset \neq V(\mathfrak{b})$$

and if it is maximal consiststs of a single point.

Typically one shows that the weak result implies the strong result, however we briefly show the opposite direction.

Strong $\implies$ Weak Nullstellensatz. For suppose $\emptyset = V(\mathfrak{b})$ then $IV(\mathfrak{b}) = k[X] = \mathfrak{b}$ a contradiction. Suppose $x \in V(\mathfrak{b})$ then clearly $\mathfrak{b} \subseteq \mathfrak{m}_x$. If it is maximal then these must be equal, so that $V(\mathfrak{b}) = V(\mathfrak{m}_x) = \{x\}$. □

We may generalize the Weak Nullstellensatz to non-algebraically closed fields as follows

Lemma 3.8 (Zariski's Lemma)
Let $k \subset K$ be a field extension such that K is finitely generated as a k-algebra. Then K is algebraic over k, and even finite as a k-module.

Corollary 3.9
Let A be a finitely generated k-algebra and $\mathfrak{m}$ a maximal ideal, then

$$k \to A/\mathfrak{m}$$

is a finite extension of fields.

The reason it's a generalization is it naturally leads to a proof of the Weak Nullstellensatz when $k = \bar{k}$

Proof of 3.7 Zariski's Lemma $\implies$ Weak Nullstellensatz. A maximal ideal $\mathfrak{m}$ of $k[X]$ corresponds to a maximal ideal $\mathfrak{m}'$ of $k[X_1, \ldots, X_n]$ containing $\mathfrak{a}$ (by ...). A zero of $\mathfrak{m}'$ in k^n is necessarily a zero of $\mathfrak{m}$ in X. Therefore we may reduce to the case of $X = k^n$ and $k[X] = k[X_1, \ldots, X_n]$. There are canonical morphisms

$$k \to k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/\mathfrak{m} =: K$$

which induces a field extension $k \to K$ which is finitely generated. By Zariski's Lemma this is algebraic and therefore an isomorphism. Therefore we can find $x_i \in k$ such that $(X_i - x_i) \in \mathfrak{m}$. Then by construction $\mathfrak{m} \subseteq \mathfrak{m}_x$, and by maximality these are equal. □

Finally we illustrate how to prove the Strong Nullstellensatz using the "Rabinowitsch Trick"

Proof of 3.5 Weak $\implies$ Strong Nullstellensatz. First work in $k[X_1, \ldots, X_n]$. We have shown in (...) that $\sqrt{a} \subset IV(\mathfrak{a})$ therefore we only need to show that $f \in IV(\mathfrak{a}) \implies f^r \in \mathfrak{a}$ for some $r > 0$.

Suppose $\mathfrak{a} = (f_1, \ldots, f_m)$ and $f \in IV(\mathfrak{a})$, so that $V(\mathfrak{a}) \subset V(f)$. Then we may introduce a new indeterminate and consider the zero set in k^{n+1} of $V(f_1, \ldots, f_m, 1 - Yf)$. It's clear that this is empty, so that $(f_1, \ldots, f_m, 1 - Yf) = k[X_1, \ldots, X_n, Y]$ by the Weak Nullstellensatz. Therefore there are polynomials $h_i \in k[X_1, \ldots, X_n, Y]$ such that

$$\begin{aligned} 1 &= \sum_{i=1}^{n} h_i f_i + h_0(1 - Yf) \\ &= \sum_{j=0}^{N} Y^j \left(\sum_{i=1}^{n} h_{ij} f_i \right) + (\sum_{j=0}^{N} h_{0j} Y^j)(1 - Yf) \end{aligned}$$

for $h_{ij} \in k[X_1, \ldots, X_n]$ and some sufficiently large N.
Method 1: Note that the substitution map $A[X] \to A$ at an element $a \in A$ is a ring homomorphism. Work in $k(X_1, \ldots, X_n)[Y]$, substitute $Y = f^{-1}$ and multiply by f^N, to find

$$f^N = \sum_{i=1}^{n} f^{N-j} \sum_{i=1}^{n} h_{ij} f_i \in \mathfrak{a}$$

Method 2:
Work in $(k[X_1, \ldots, X_n]/\mathfrak{a})[Y]$ to find

$$\begin{aligned} 1 &= \bar{h}_{00} + \sum_{j=1}^{N} Y^j \left(\bar{h}_{0j} - f\bar{h}_{0(j-1)} \right) \\ \bar{h}_{0j} &= f\bar{h}_{0(j-1)} \\ \bar{f}^N &= \bar{f}^N \bar{h}_{00} = \bar{f}^{N-1} \bar{h}_{01} = \ldots = \bar{h}_{0N} = 0 \end{aligned}$$

so that $f^N \in \mathfrak{a}$ as required.

□

Remark 3.6
Define the open subset of $V(\mathfrak{a})$, $D(\bar{f}) = \{x \in V(\mathfrak{a}) \mid f(x) \neq 0\}$ then the proof has identified a bijection between this open subset and a closed subset of k^{n+1}

$$D(\bar{f}) \longrightarrow V(f_1, \ldots, f_m, 1 - Yf)$$

$$(x) \longrightarrow (x, f(x)^{-1})$$

For example the parabola $V(xy - 1) \subset k^2$ may be identified with the punctured line $k \setminus \{0\}$ by projection.

3.2 K-rational points

Definition 3.7
Let $V = V(\mathfrak{a})$ be an algebraic subset of k^n and $k \subset K \subset \bar{k}$ an algebraic extension. Define the K-rational points to be

$$V(K) := \{x \in K^n \mid f(x) = 0 \quad \forall x \in \mathfrak{a}\}$$

The totality of rational points is $V(\bar{k})$. For an element $x \in K^n$ let the field of definition be

$$k(x) := k(x_1, \ldots, x_n)$$

and define the degree of a rational point $x \in V(\bar{k})$ to be

$$\deg(x) := \dim_k k(x)\,.$$

Let $G_k = \mathrm{Gal}(\bar{k}/k)$ be the absolute galois group, then there is a natural action

$$G_k \times V(\bar{k}) \to V(\bar{k})$$

given pointwise on the elements.

Note that this definition depends not only on the original zero-locus $V \subset k^n$ but on the equations $\mathfrak{a}$ used to define them. There is another way of characterizing rational points purely in terms of the algebraic invariant

Proposition 3.10 (Functor of points)
For any algebraic extension $k \subseteq K \subseteq \bar{k}$ there is a bijection

$$\begin{array}{rcl} V(K) & \longleftrightarrow & \mathrm{Hom}_k(k[V], K) \\ x & \to & \phi_x : (f \to f(x)) \end{array}$$

which respects the action of $Gal(K/k)$ in the sense that

$$\sigma \circ \phi_x = \phi_{\sigma x}$$

and the notion of degree in the sense that $\deg(x) = \dim_k \ker(\phi_x)$.

Proof. We suppose that $k[V] = k[X_1, \ldots, X_n]/\mathfrak{a}$ for some radical ideal $\mathfrak{a}$. By assumption $f(x) = 0$ for all $f \in \mathfrak{a}$, so $\phi_x(f) = f(x_1, \ldots, x_n)$ is a well-defined homomorphism. Conversely given a homomorphism ϕ define $x_\phi = (\phi(\bar{X}_1), \ldots, \phi(\bar{X}_n))$. It's clear that $\phi_{x_\phi}(\bar{X}_i) = \phi(\bar{X}_i)$ so being k-algebra homomorphisms they must agree. Similarly $\phi_x(\bar{X}_i) = x_i$ so the associations are mutually inverse.

Suppose $\sigma \in \mathrm{Gal}(K/k)$, then $\sigma(f(x)) = f(\sigma(x))$, whence $\sigma \circ \phi_x = \phi_{\sigma x}$.

The map ϕ_x induces an isomorphism between $k[V]/\ker(\phi_x)$ and $k(x)$. □

In light of this it's useful to identify the two sets (indeed this is the point of view taken in the coordinate-free approach). In the case k is not algebraically closed this yields an interpretation of the maximal ideals.

Proposition 3.11
There is a bijection between Galois orbits of rational points maximal ideals of the coordinate ring

$$\begin{array}{rcl} V(\bar{k})/G_k & \longleftrightarrow & \{\mathfrak{m} \lhd k[V]\} \\ [x] & \to & \mathfrak{m}_x := \ker\left(f \to f(x)\right) \end{array}$$

under which $\deg(x) = \dim_k k[V]/\mathfrak{m}_x =: \deg(\mathfrak{m}_x)$.

Proof. The map given in the proposition is well-defined, for suppose $x' = \sigma(x)$, then

$$f(x') = \sigma(f(x))$$

so that $f(x') = 0 \iff f(x) = 0$. Given a maximal ideal $\mathfrak{m}$, by Zariski's Lemma, $k[V]/\mathfrak{m}$ is algebraic over k, and so has an embedding into $\bar{k}$. Let $(x_1, \ldots, x_n)$ by the image of the indeterminates, then $\mathfrak{m}_x \subseteq \mathfrak{m}$ and so are equal by maximality. This means the map is surjective. Suppose that x,y are not Galois conjugate, then at least one of x_i, y_i are not Galois conjugate. Let $f(t) \in k[t]$ be the minimum polynomial of x_i, then $f(X_i) \in k[V]$ lies in $\mathfrak{m}_x$ but not $\mathfrak{m}_y$, because roots of the minimum polynomial are necessarily Galois conjugate (...).

□

Then we see that the "points" of $V(\mathfrak{a})$ correspond to either $\bar{k}$-rational points of degree 1 or maximal ideals of degree 1. As an application of this we explain the construction of the Zeta function of an affine variety.

3.3 Abstract Affine Varieties (Specm(A) and Spec(A))

We wish to generalize these constructions to a non-algebraically closed field k (such as $\mathbb{Q}$ or $\mathbb{F}_q$). One problem in this case is that the algebraic sets may in general be uninteresting (e.g. a smooth surface in $\mathbb{C}$ may have no $\mathbb{Q}$ points). One manifestation of this is that the Nullstellensatz fails, in particular there exists ideals in $k[V]$ which have no k-rational zeros. In order to apply geometric techniques in this case we need a construction which identifies the $\mathbb{Q}$ (or arithmetic) points but nevertheless "remembers" the geometric points. In particular it's clear this is important for the Weil conjectures.

As motivation we provide an "intrinsic" definition of $V(\mathfrak{a})$ purely in terms of the algebraic invariant $k[V]$ when $\bar{k} = k$. Recall given a point $x \in V(\mathfrak{a})$ there is a maximal ideal

$$\mathfrak{m}_x := \left(\bar{X}_1 - x_1, \ldots, \bar{X}_n - x_n\right) = I(\{x\}).$$

and $x \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{m}_x$. Therefore we can restate the definitions of the Galois connection (I, V) as follows

$$\begin{aligned} I(Y) &:= \bigcap_{x \in Y} \mathfrak{m}_x && (5) \\ V(\mathfrak{b}) &:= \{x \mid \mathfrak{b} \subseteq \mathfrak{m}_x\} && (6) \\ \implies IV(\mathfrak{b}) &= \bigcap_{\mathfrak{b} \subseteq \mathfrak{m}_x} \mathfrak{m}_x \,. && (7) \end{aligned}$$

As mentioned before we would like a version of the Nullstellensatz, namely $IV(\mathfrak{b}) = \sqrt{\mathfrak{b}}$, and in particular for a maximal ideal $IV(\mathfrak{m}) = \mathfrak{m}$. As noted previously this will not hold in general because not all maximal ideals are of the form $\mathfrak{m}_x$, so we would have $IV(\mathfrak{m}) = A$ by convention. To this end we enlarge the set of "points" to contain all maximal ideals

Definition 3.8 (Maximal Spectrum)
Let A be a reduced finitely-generated k-algebra, then define as follows

$$\begin{aligned} \operatorname{Specm}(A) &:= \{[\mathfrak{m}] \mid \mathfrak{m} \lhd A\}\,, \\ I(Y) &:= \bigcap_{[\mathfrak{m}] \in Y} \mathfrak{m}\,, \\ V(\mathfrak{b}) &:= \{[\mathfrak{m}] \mid \mathfrak{b} \subseteq \mathfrak{m}\} \\ \operatorname{Specm}(A) &\underset{I}{\overset{V}{\leftrightarrows}} \{\mathfrak{b} \lhd A \quad \textit{radical}\,\} \end{aligned}$$

The closed sets $V(\mathfrak{b})$ induce a topology (see.)

Remark 3.9
This corresponds to Definition 3.1, for when $k = \bar{k}$ and $V = V(\alpha)$ we have a commutative diagram

$$\begin{array}{ccc} \operatorname{Specm}(k[V]) & \underset{I}{\overset{V}{\leftrightarrows}} & k[V] \\ \uparrow\downarrow \simeq & & \downarrow = \\ V(\mathfrak{a}) & \underset{I}{\overset{V}{\leftrightarrows}} & k[V] \end{array}$$

The vertical isomorphism arises from the correspondence between maximal ideals and points (Corollary 3.6) and the commutativity foolows from Equations (5), (6).
When k is not algebraically closed we nevertheless have a correspondence between Galois orbits and "points"

$$\begin{array}{ccc} \operatorname{Specm}(k[V]) & \underset{I}{\overset{V}{\leftrightarrows}} & k[V] \\ \uparrow\downarrow \simeq & & \downarrow = \\ V(\bar{k})/G_k & \underset{I}{\overset{V(\cdot)(\bar{k})}{\leftrightarrows}} & k[V] \end{array}$$

where the bottom row involves taking $\bar{k}$-rational points of sub-algebraic sets.

The Nullstellensatz in this setting is

Proposition 3.12 (Nullstellensatz for a reduced f.g. k-algebra)
Let k be an arbitrary field, and A a reduced f.g. k-algebra then

$$IV(\mathfrak{a}) = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m} \lhd A} \mathfrak{m} = \sqrt{a} \tag{8}$$

In particular the correspondence identified in Definition 3.8 induces a bijection between closed sets and radical ideals
See also [Mil14, Prop 13.10]

This will not hold for a general A, so we may generalize this as follows

Definition 3.10 (Prime spectrum)
For a ring A define as follows

$$\begin{aligned} \operatorname{Spec}(A) &:= \{[\mathfrak{p}] \lhd A \mid \mathfrak{p} \textit{ prime}\,\} \\ I(Y) &:= \bigcap_{[\mathfrak{p}] \in Y} \mathfrak{p}, \\ V(\mathfrak{b}) &:= \{\mathfrak{p} \mid \mathfrak{b} \subseteq \mathfrak{p}\} \\ \operatorname{Spec}(A) &\underset{I}{\overset{V}{\leftrightarrows}} \{\mathfrak{b} \lhd A \textit{ radical}\,\} \end{aligned}$$

Definition 3.11 (Admissable Spetrum)
We say a pair (A, X) where $X \subseteq \mathrm{Spec}(A)$ is admissable if it satisfies the "Nullstellensatz"

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in X : \mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}\,.$$

Note this implies it contains at least the maximal ideals, by considering the case $\mathfrak{a} = \mathfrak{m}$.

The only reason to do this is to cover both the classical case of affine varieties and affine schemes simultaneously.

Example 3.12 (Affine Variety over a field)
$(A, \mathrm{Specm}(A))$ where A is a f.g. reduced k-algebra is admissable More generally a Jacobson ring ([Eme10], [Sta15, 00FZ]) will also work.

Example 3.13
Affine Scheme $(A, \mathrm{Spec}(A))$ where A is an arbitrary ring is admissable (the Nullstellensatz here is an elementary result [Sta15, 00E0] Lemma 10.16.2 (7)).

We have an abstract version of Lemma (...)

Lemma 3.13
Let $(A, \mathcal{P})$ be an admissable spectrum

1. *V and I are order reversing and $V(I(Y)) \supseteq Y$ and $I(V(\mathfrak{a})) \supseteq \mathfrak{a}$*
2. *$V(0) = X$ and $V(A) = \emptyset$*
3. *$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ and $V(\sqrt{\mathfrak{a}}) = V(\mathfrak{a})$*
4. *$V(I(Y)) = \overline{Y}$*
5. *$I(X) = \sqrt{(0)}$ and $I(\emptyset) = A$*
6. *$V(\sum_i I_i) = \bigcap_i V(I_i)$*
7. *$V(IJ) = V(I \cap J) = V(I) \cup V(J)$*

In particular V,I induces an order-reversing bijection between the closed subsets of X and the radical ideals in A.

Corollary 3.14 (Generalized Zariski Topology)
For $(A, \mathcal{P})$ an admissable spectrum the sets $V(I)$ form a topology on $\mathcal{P}$.

We examine the difference between $\mathrm{Spec}(A)$ and $\mathrm{Specm}(A)$ in some simple cases

Example 3.14 (Rings of Integers)
Consider a finite extension K/Q and the corresponding ring of integers $\mathcal{O}_K$. Then it's well known that every non-zero prime ideal is maximal (or it has Krull dimension 1). Therefore

$$\mathrm{Spec}(\mathcal{O}_K) = \mathrm{Specm}(\mathcal{O}_K) \cup \{(0)\}$$

or more explicitly

$$\begin{aligned} \mathrm{Specm}(\mathbb{Z}) &= \{(2), (3), (5), \ldots\} \\ \mathrm{Spec}(\mathbb{Z}) &= \mathrm{Specm}(\mathbb{Z}) \cup \{(0)\} = \{(2), (3), (5), \ldots\} \cup \{(0)\} \end{aligned}$$

In otherwords $\mathrm{Spec}(\mathcal{O}_K)$ has an extra point (0) which in terms of the topology behaves oddly, in the sense that it is "close" to every other point.
Often we are only interested in the "real" points corresponding to maximal ideals. These are characterized by purely topological condition which will be useful later

Definition 3.15 (Closed Point)
Let X be a topological space, then we say $x \in X$ is a closed point if $\{x\}$ is closed (or equivalently it has no other specializations). Define X^0 to be the subset of closed points in X.

The closed points of $(A, \mathrm{Spec}(A))$ are precisely the maximal ideals $\mathrm{Specm}(A)$, that is

$$\mathrm{Spec}^0(A) = \mathrm{Specm}(A)$$

Note strictly speaking these are not varieties or schemes until we embed them in a more general category, but the terminology will suffice for now.

3.4 Zeta function of an Affine Variety

As an application of the notion of abstract algebraic set and rational points, we define the Zeta function of a variety. This is a central object of the Weil conjectures, which relates analytic properties of the function to combinatorial properties of the K-rational points (or solutions) of the variety over a finite field. As motivation for this definition recall that the Euler product form of the Riemann zeta function is

$$\zeta(s) := \prod_p \left(1 - p^{-s}\right)^{-1} = \prod_p \left(1 - (\#\mathbb{Z}/p\mathbb{Z})^{-s}\right)^{-1}$$

The key observation being that the Zeta function of an affine variety over a finite field may be defined in an entirely analogous way by considering only the coordinate ring $k[V]$.

Proposition 3.15 (Zeta function of an affine variety)
Let $k = \mathbb{F}_q$ be a finite field and $V = V(\mathfrak{a})$ be an algebraic set with coordinate ring $k[V]$. Define the integers

$$N_n := \#V(\mathbb{F}_{q^n})$$

for every $n \geq 1$. Then we claim

$$N_n = \sum_{d|n} d b_d$$

where

$$b_d = \#\{\mathfrak{m} \lhd k[V] \mid \deg(\mathfrak{m}) = d\}$$

is the number of maximal ideals of degree d. Furthermore we have the following formal relation in $\mathbb{Q}[[T]]$

$$Z(V,T) := \prod_{\mathfrak{m} \lhd k[V]} \left(1 - T^{\deg(\mathfrak{m})}\right)^{-1} = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\right)$$

and the usual zeta function is given by

$$\zeta(V,s) := Z(V, q^{-s}) = \prod \left(1 - (\#k[V]/\mathfrak{m})^{-s}\right)^{-1}$$

Proof. Consider the sets

$$\begin{aligned} V_d &:= \{x \in V(\overline{\mathbb{F}_q}) \mid \deg(x) = d\} \\ B_d &:= \{\mathfrak{m} \lhd k[V] \mid \deg(\mathfrak{m}) = d\} \end{aligned}$$

then we have a disjoint union

$$V(\mathbb{F}_{q^n}) = \bigcup_{d|n} V_d \,.$$

Furthermore we claim the group action restricts to a faithful action of $G_{\mathbb{F}_{q^n}} = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ on V_n (to prove...) so that we have a bijection

$$V_d / G_{\mathbb{F}_{q^d}} \longleftrightarrow B_d$$

and since it's faithful, summing over the Galois orbits yields

$$\#V_d = d \times \#B_d =: d b_d,$$

whence it follows from the earlier decomposition.

□

3.5 Regular functions on an affine algebraic set (alg. closed case)

Just as we defined the space of smooth functions over a manifold we can define the space of regular functions

Definition 3.16 (Regular functions on an affine algebraic set)
Suppose k is algebraically closed and let $X = V(\mathfrak{a})$ be an algebraic set. Define the sheaf of regular functions as follows

$$\mathcal{O}_X(U) := \{f : U \longrightarrow k \mid f \text{ regular at } P \text{ for all } P \in U\}$$

Where f regular at P means that there is an neighbourhood V of P and functions $g, h \in k[X]$ such that

$$f(Q) = \frac{g(Q)}{h(Q)} \quad \forall Q \in V$$

It's easy to show that $(X, \mathcal{O}_X)$ is a space of k-functions (first show that regular $\implies$ continuous). In the affine case the definition is more restrictive that it would first appear

Proposition 3.16
There is a canonical isomorphism

$$k[X]_f \longrightarrow \mathcal{O}_X(D(f))$$

and in particular

$$k[X] = \mathcal{O}_X(X)\,.$$

Furthermore there is a canonical isomorphism

$$k[X]_{\mathfrak{m}_x} \longrightarrow \mathcal{O}_{X,x}$$

Proof. Let ϕ denote the canonical morphism given above. Given $\sigma \in \mathcal{O}_X(D(f))$ consider

$$J_f := \left\{ g \in k[V]_f \mid \phi(g)\sigma \in \mathrm{Im}(\phi) \right\}$$

If $J_f = k[V]_f$ then we are done because it contains 1. Suppose not then it is contained in a proper maximal ideal $J_f \subseteq \mathfrak{m}_f \lhd k[V]_f$. This corresponds to a maximal ideal $\mathfrak{m}_x \lhd k[V]$ not containing f, i.e. $x \in D(f)$. By definition there exists $h_1, h_2 \in k[V]$ such that $\sigma(y) = \frac{h_1(y)}{h_2(y)}$ for all $y \in V$ for some nbhd V of x. There exists some h_3 such that $x \in D(h_3) \subseteq V$, so $D(f) \subseteq V \cup V(h_3)$. Therefore

$$h_3(y)h_2(y)\sigma(y) = h_1(y)h_3(y) \quad \forall y \in D(f)$$

meaning that $(h_3h_2)/1 \in J_f \subseteq \mathfrak{m}_f \implies h_3h_2 \in \mathfrak{m}_x$. However $(h_3h_2)(x) \neq 0$, a contradiction. □

3.6 Regular "functions" on an affine ring

We attempt to generalize the construction in Proposition 3.16 to more general rings. This will still constitute a sheaf, but no longer a space of k-functions.

Proposition 3.17
Let $X = \mathrm{Spec}(A)$ (or $\mathrm{Specm}(A)$ satisfying the Nullstellensatz) with the Zariski toplogy. Consider the basis of open sets $\mathcal{B}$ of the form

$$D(f) := \{[\mathfrak{p}] \in X \mid f \notin \mathfrak{p}\}\,.$$

and define the $\mathcal{B}$-presheaf

$$\begin{aligned} \mathcal{O}'_X(U) &:= \Delta(U)^{-1}A \quad U \in \mathcal{B} \\ \Delta(U) &:= A \setminus \bigcup_{\mathfrak{p} \in U} \mathfrak{p} \end{aligned}$$

where $S^{-1}A$ is defined in Section A.3. Define the restriction maps

$$\rho_{UV} := i_{\Delta(U)\Delta(V)}$$

as in Proposition A.7. Then

1. $\mathcal{O}'_X(X) = A_1 = A$
2. *There is a canonical isomorphism $A_f \to \mathcal{O}'_X(D(f))$ which commutes with $A \to A_f$ and $A_1 = \mathcal{O}'_X(X) \to \mathcal{O}'_X(D(f))$*
3. *$\mathcal{O}'_X$ satisfies the sheaf conditions 2.5 over $\mathcal{B}$ (this is well-defined because $\mathcal{B}$ is closed under finite intersections).*
4. *There is a canonical isomorphism $A_{\mathfrak{p}} \to \mathcal{O}'_{X,x}$ which commutes with $A \to A_{\mathfrak{p}}$ and $A = \mathcal{O}'_X(X) \to \mathcal{O}'_{X,x}$.*

where we have identified a point $x \in X$ with a prime ideal $\mathfrak{p} \lhd A$. Further there is a sheaf $\mathcal{O}_X$ over the whole topology such that

$$\mathcal{O}_X|_{\mathcal{B}} \equiv \mathcal{O}'_X$$

with isomorphic stalks.

Remark 3.17
Though it is no longer a space of k-functions, there are some similarities

- *The stalks $\mathcal{O}_{X,x}$ are local rings (since $A_{\mathfrak{p}}$ has unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$), which mirrors Lemma 2.2.*

- *We may interpret sections $\sigma \in \mathcal{O}_X(U)$ as generalized functions by considering the composite map to the residue field*

$$\mathcal{O}_X(U) \to \mathcal{O}_{X,x} \to \mathcal{O}_{X,x}/\mathfrak{m}_x =: k(x)$$

and write $\sigma(x)$ for the value in the residue field $k(x)$.

Proof. The construction and proof of various properties relies heavily on the construction of localization defined in Section A.3, and the arguments are similar to those presented in [Sha94, Chap V. Sec 2.3 Thm 1].

The restriction maps ρ_{UV} are well-defined because $U \supseteq V \implies \Delta(U) \subseteq \Delta(V)$. They commute by Proposition A.7.
Recall that $A_f := S_f^{-1}A$ where S_f is the m.c. set

$$S_f := \{1, f, \ldots, f^n, \ldots\}$$

By Proposition A.14 $\Delta(D(f))$ equals the saturation $\overline{S}_f$. Therefore by Proposition A.8 there is an isomorphism

$$A_f \longrightarrow \mathcal{O}_X(D(f))$$

which commutes with the maps stated. In particular $\Delta(X) = S_1 = \overline{S_1}$ so that $\mathcal{O}_X(X) = A_1$ which may trivially be identified with A, and the restriction maps $i_{S_1 S}$ may be identified with the canonical maps i_S.

Suppose that we have an open cover of $U = D(f) = \bigcup_i D(f_i)$. By Lemma 3.21 we have a canonical isomorphism between $\mathcal{O}'_X|_{D(f)}$ and $\mathcal{O}'_{\mathrm{Spec}}(A_f)$. By reducing to this case we may assume $U = X$.

Suppose $\sigma, \tau \in \mathcal{O}'_X(X) = A$ and suppose $\sigma|_{U_i} = \tau|_{U_i}$. Then by definition we have $f_i^N \sigma = f_i^N \tau$ for some N. By Lemma 3.18 we have $1 = \sum_{i=1}^m f_i^N h_i$. Multiplying by σ and τ shows that they're equal.

Similarly suppose $\sigma_i \in \mathcal{O}'_X(D(f_i))$. Then $\sigma_i = v_i/f_i^N$ for $v_i \in A$ and sufficiently large N. By definition $\sigma_i|_{D(f_i f_j)} = v_i f_j^N/(f_i f_j)^N$. Then compatibility shows that $(f_i f_j)^M (v_i f_j^N - v_j f_i^N) = 0$ for some M.
Suppose that we had σ such that $\sigma|_{D(f_i)} = \sigma_i$, then we would have

$$f_i^r \left(f_i^N \sigma - v_i\right) = 0 \tag{9}$$

for some $r > 0$. By Lemma 3.18 there is a decomposition (for every r)

$$1 = \sum_{j=1}^m g_j^{(r)} f_j^{N+r}\,.$$

Multiplying equation (9) by $g_i^{(r)}$ and summing shows that σ must be of the form (for some r)

$$\sigma^{(r)} := \sum_{j=1}^m g_j^{(r)} f_j^r v_j\,.$$

In order for $\sigma^{(r)}|_{D(f_i)} = \sigma_i$ it's enough for the following to be zero

$$f_i^r (f_i^N \sigma^{(r)} - v_i) = \sum_{j=1}^m g_j^{(r)} f_i^{N+r} f_j^r v_j - f_i^r v_i$$

Set $r = M$ and apply the compatibility condition to find

$$f_i^M (f_i^N \sigma^{(M)} - v_i) = f_i^M v_i \sum_{j=1}^m g_j^{(M)} f_j^{N+m} - f_i^M v_i = 0$$

which shows $\sigma := \sigma^{(M)}$ is the required section.

In order to extend to the whole topology we appeal to Proposition 3.20. □

Lemma 3.18 (Partition of unity)
Suppose $X = \mathrm{Spec}(A)$ (or $\mathrm{Specm}(A)$ satisfying the Nullstellensatz)and $X = \bigcup_i D(f_i)$, then for any $N > 0$ there exists a partition of unity

$$1 = \sum_{r=1}^m g_r f_{i_r}^N$$

for $g_r \in A$ and some indices i_r.

Proof. It's clear that $D(f_i) = D(f_i^N)$. So wlog we may assume $N = 1$. By definition

$$V(\sum_i f_i) = \cap_i V(f_i) = X \setminus \cup_i D(f_i) = \emptyset$$

Taking $I(.)$ of both sides and applying Nullstellensatz shows that

$$A = \sqrt{\sum_i f_i}\,.$$

By definition of radical this means $1^r = 1 \in \sum_i f_i$ which gives the result. □

Lemma 3.19 (Sheaves are separated)
Let $\mathcal{F}$ be a ($\mathcal{B}-$)sheaf (or just separated presheaf) then for any sections

$$\sigma, \tau \in \mathcal{F}(U)$$

if $\sigma_x = \tau_x$ for all $x \in U$ then $\sigma = \tau$

Proof. For each $x \in U$ there is a neighbourhood V_x such that $\sigma|_{V_x} = \tau|_{V_x}$. By the sheaf conditions we then have $\sigma = \tau$. □

The following proposition allows to sensibly extend to the whole topology by gluing sections together. This uses the "espace etale" construction which is quite convenient. A more direct approach is to use directed limits [Sha94, Chap. V Sec. 2].

Proposition 3.20 (Extending to non-principal open sets)
Let $\mathcal{F}'$ be a $\mathcal{B}$-sheaf where $\mathcal{B}$ is a basis closed under finite intersections, then define

$$\mathcal{F}(U) := \{f : U \to \coprod_{x \in U} \mathcal{F}'_x\}$$

where we restrict to functions which are locally of the form σ_x for $\sigma \in \mathcal{F}'(V)$ for $V \in \mathcal{B}$.
Then $\mathcal{F}$ is naturally a sheaf for which there is a canonical isomorphism

$$\mathcal{F}' \to \mathcal{F}|_{\mathcal{B}}$$

See also [Sta15, Lemma 009M]

Proof. Clearly $\mathcal{F}$ is a sheaf, as the condition is local. The natural map is given by

$$\sigma \to (x \to \sigma_x)$$

and yields a sheaf morphism. By Lemma 3.19 it is injective. Conversely suppose $f \in \mathcal{F}(U)$ is given by sections $\sigma_i \in \mathcal{F}'(V_i)$. For $x \in V_i \cap V_j$ we have $(\sigma_i)_x = f(x) = (\sigma_j)_x$. So by Lemma 3.19 again we have $\sigma_i|_{V_i \cap V_j} = \sigma_j|_{V_i \cap V_j}$, and so by the second sheaf condition there exists a $\sigma \in \mathcal{F}(U)$ such that $\sigma|_{V_i} = \sigma_i$, whence $\sigma_x = (\sigma_i)_x = f(x)$. This shows the map is also surjective, and therefore bijective. □

Lemma 3.21 (Principal open subsets are affine)
Let $X = \mathrm{Spec}(A)$ then the localization homormophism

$$i_S : A \to S^{-1}A$$

induces a bijection

$$\{\mathfrak{p} \mid \mathfrak{p} \cap S = \emptyset\} \leftrightarrow \mathrm{Spec}(S^{-1}A)$$

given by

$$\mathfrak{p} \longrightarrow (S^{-1}A) i_S(\mathfrak{p})$$
$$i_S^{-1}(\mathfrak{p}) \longleftarrow \mathfrak{p}$$

In particular there is a homeomorphism

$$D(f) \longleftrightarrow \mathrm{Spec}(\Delta(D(f))^{-1}A)$$

and a canonical isomorphism

$$\mathcal{O}_X|_{D(f)} \to \mathcal{O}_{\mathrm{Spec}(\Delta(D(f))^{-1}A)}$$

A similar statement holds when $X = \mathrm{Specm}(A)$ satisfies the Nullstellensatz.

4 Counting Points over Finite Fields

Let p be an odd prime and $q = p^r$. Denote by $\mathbb{F}_q$ the unique finite field of order q. Recall it's a standard result that $\mathbb{F}_q^\star$ is cyclic group of order $\phi(q)$.

4.1 A Simple Example

We consider the problem of counting points over $\mathbb{F}_q$ of the curve

$$C_1 : x^2 + y^2 = a$$

for some $a \in \mathbb{F}_q^\star$. First we consider the case

$$N_q(X^2 = a) := \#\{x \in \mathbb{F}_q^\star \mid x^2 = a\}$$

There is a homomorphism

$$\begin{array}{rcl} \psi_2 & : & \mathbb{F}_q^\star \longrightarrow \mathbb{F}_q^\star \\ & & x \longrightarrow x^2 \end{array}$$

with kernel exactly $\{\pm 1\}$ and image the quadratic residues. Therefore ψ_2 is 2-to-1 and

$$N_q(X^2 = a) \quad = \quad \begin{cases} 1 & a = 0 \\ 2 & a \in \mathrm{Im}(\psi_2) \\ 0 & a \notin \mathrm{Im}(\psi_2) \end{cases}$$

One has therefore that

$$N_q(X^2 = a) = 1 + \left(\frac{a}{q}\right)$$

where $\left(\frac{a}{q}\right)$ is the quadratic residue symbol (but applied to $q = p^r$). Note this is the unique character of order 2 on $\mathbb{F}_q^\star$ which motivates the later discussion. Recall that there are the same number of quadratic residues and non-residues, so we have the fundamental relation

$$\sum_a \left(\frac{a}{p}\right) = 0$$

Now using this we my consider the number of points on C_1

$$\begin{array}{rcl} N_q(x^2 + y^2 = 1) & = & \displaystyle\sum_{a+b=1} \left(1 + \left(\frac{a}{q}\right)\right)\left(1 + \left(\frac{b}{q}\right)\right) \\ & = & \displaystyle\sum_a \left(1 + \left(\frac{a}{q}\right)\right)\left(1 + \left(\frac{1-a}{q}\right)\right) \\ & = & \displaystyle p + \sum_a \left(\frac{a(1-a)}{q}\right) \end{array}$$

Consider the map $x \to x^{-1}$ which is an automorphism of $\mathbb{F}_q^\star$. So this equals

$$\begin{array}{rcl} & = & \displaystyle q + \sum_{a \neq 0} \left(\frac{(a-1)/a^2}{q}\right) \\ & = & \displaystyle q + \sum_{a \neq 0} \left(\frac{a-1}{q}\right) \\ & = & \displaystyle q - \left(\frac{-1}{q}\right) + \sum_a \left(\frac{a-1}{q}\right) \\ & = & \displaystyle q - \left(\frac{-1}{q}\right) \end{array}$$

Remark 4.1
It is possible to simplify this expression by extending C_1 to a projective variety. Consider the projective curve

$$\tilde{C}_1 : X^2 + Y^2 = Z^2$$

where it considered as a subset of $\mathbb{P}^2(\mathbb{F}_q)$. Clearly C_1 is identified with the points with $Z \neq 0$. The points with $Z = 0$ are termed the points at infinity. When $\left(\frac{-1}{q}\right) = 1$ these consist of $(1 : \pm\sqrt{-1} : 0)$ and otherwise there are none. Therefore we find the total number of points is $q + 1$. This is essentially because the projective curve $V(X^2 + Y^2 - Z^2)$ is parameterized by $\mathbb{P}^1(\mathbb{F}_q)$ using the standard pythagorean method

$$\begin{array}{rcl} \mathbb{P}^1(\mathbb{F}_q) & \longrightarrow & \tilde{C}_1 \\ (S:T) & \longrightarrow & (S^2 - T^2 : 2ST : S^2 + T^2) \\ (X + Z : Y) = (Y : Z - X) & \longleftarrow & (X : Y : Z) \end{array}$$

4.2 Abelian Character Theory

Note that in the previous section $\left(\frac{a}{p}\right)$ is the unique character of order 2, and it allowed us to solve polynomial equations of order 2. To generalize this we consider characters of arbitrary order on abelian groups. As $\mathbb{F}_q^\star$ is cyclic we often only consider the cyclic case, as this is simpler. However most of the results generalize to the abelian case because any finite abelian group is a direct product of cyclic groups.

Definition 4.2
Character Group
Let G be a finite abelian group, define group of characters on G by

$$\hat{G} := \{\chi : G \to \mathbb{C} \mid \chi(xy) = \chi(x)\chi(y)\}$$

which is a group under pointwise multiplication. We denote by ϵ the trivial character. When $G = \mathbb{F}_q^\star$ by convention we extend the definition to 0 by

$$\chi(0) = \begin{cases} 1 & \chi = \epsilon \\ 0 & \chi \neq \epsilon \end{cases}$$

WARNING: This means in general that $\chi_1(a)\chi_2(0) \neq (\chi_1\chi_2)(0)$, so care must be taken in algebraic manipulations

Furthermore define for a non-zero integer n

$$\begin{array}{rcl} G^n & = & \{g^n \mid g \in G\} \\ G[n] & = & \{g \in G \mid g^n = e\} \end{array}$$

Example 4.3
In the case before we have $G = \mathbb{F}_q^\star$, $N = q - 1$ and $n = 2$. In this case $G[n] = \{\pm 1\}$ and G^n are the quadratic residues, and $\left(\frac{a}{p}\right)$ is the only non-trivial quadratic character.

The two main results of this section are as follows

Proposition 4.1
Counting solutions
Let G be a finite cyclic group of order N , n a non-zero integer and $a \in G$. Then

$$\begin{array}{rcll} \#\{g \mid g^n = a\} = & & \sum_{\chi \in \widehat{G[n]}} \chi(a) = \sum_{\chi : \chi^n = \epsilon} \chi(a) & \\ & = & \begin{cases} \gcd(n, N) & \text{a solution exists} \\ 0 & \text{otherwise} \end{cases} & \end{array}$$

Proof. See below. □

Example 4.4
We saw already that

$$N_q(X^2 = a) = 1 + \left(\frac{a}{p}\right)$$

We also make use of of the orthogonality of characters

Proposition 4.2
Orthogonality of characters
Let G be an arbitrary abelian group and $\chi \in \widehat{G}$. Then

$$\sum_{a\in G}\chi(a)=\begin{cases}|G| & \chi=\epsilon\\ 0 & \chi\neq\epsilon\end{cases}$$

Similarly

$$\sum_{\chi\in\widehat{G}}\chi(a)=\begin{cases}|G| & a=e\\ 0 & a\neq e\end{cases}$$

Proof. See below. □

As a preliminary result

Lemma 4.3
Let G be a finite abelian group of order N. For a non-zero integer n define

$$\hat{n}=\gcd(n,|G|)$$

- *$\phi_n : G/G[n]\longrightarrow G^n$ given by $\bar{x}\to x^n$ is an isomorphism*
- *$G[\hat{n}]=G[n]$*
- *$G^{\hat{n}}=G^n$*

In otherwords we may wlog assume that $n\mid|G|$. To count solutions we have

$$N(X^n=a)\quad:=\#\{g\mid g^n=a\}=\begin{cases}|G[n]| & a\in G^n\\ 0 & a\notin G^n\end{cases}\tag{10}$$

Finally when G is cyclic we have in addition

$$|G[n]|=\hat{n}$$

Proof. We prove each in turn

- This is obvious because $G[n]$ is the kernel of the map $x\to x^n$.
- By euclid's extended algorithm there are integers a,b such that $an+b|G|=\hat{n}$. Therefore $g^{\hat{n}}=(g^n)^a$ and $g^n=\left(g^{\hat{n}}\right)^{n/\hat{n}}$. Therefore $g^n=e\iff g^{\hat{n}}=e$ as required.
- Define the two maps $G^n\leftrightarrow G^{\hat{n}}$ given by $x\to x^a$ and $y\to y^{n/\hat{n}}$. We claim these are mutually inverse. They are well-defined by the previous relations noted. Note that the composition of the two maps is $z\to z^{1-\frac{b|G|}{\hat{n}}}$. When z is a n-th or $\hat{n}$-th power then this is the identity as required.

Note if $a\in G^n$ then $\{g\mid g^n=a\}=\phi^{-1}(a)$ then it follows from general group theory the fibres have $|G[n]|=|\ker(\phi_n)|$ elements.
For the last part suppose for simplicity of notation that $G=\mathbb{Z}/N\mathbb{Z}$. Then as $G[n]=G[\hat{n}]$ then $[r]\in G[n]\iff[\hat{n}][r]\equiv 0 \mod N$. This has exactly $\hat{n}$ solutions, namely $N/\hat{n},2N/\hat{n},\ldots,\hat{n}N/\hat{n}$.

□

Now we show that the character group of a cyclic group is also cyclic of the same order, and therefore (non-canonically) isomorphic.

Proposition 4.4
Cyclic character group
Let G a finite cyclic group of order N. Then for any generator $g\in G$ there is an isomorphism

$$\begin{array}{ccc}\widehat{G} & \longrightarrow & \mu_N\\ \chi & \longrightarrow & \chi(g)\end{array}$$

where μ_N consists of the Nth roots of unity in $\mathbb{C}$. The character corresponding to $\zeta_N=\exp\left(\frac{2\pi i}{N}\right)$ is denoted by λ_g. It is given by

$$\lambda_g(g^r)=\exp\left(\frac{2\pi ir}{N}\right)$$

and it generates $\widehat{G}$ as a cyclic group of order N.

Proof. Clearly $\chi(g)^n = \chi(g^n) = 1$ so the map is well-defined. Moreover it's injective as each character is uniquely determined by the image of g. The character λ_g is well-defined because $g^r = g^s \implies r \equiv s \mod N$. Furthermore this shows the map is surjective because the image of λ_g^j is $\exp\left(\frac{2\pi ij}{N}\right)$. Finally as ζ_N generates μ_N as a cyclic group of order N, the same statement applies to λ_g and $\widehat{G}$. □

In order to succinctly prove the "dual results", we need a simple lemma

Lemma 4.5
Let G be a finite abelian group of order N and n be an integer. Then there exists a canonical isomorphism

$$\begin{aligned} \widehat{G/G^n} &\longrightarrow \widehat{G}[n] \\ \bar{\chi} &\longrightarrow \bar{\chi} \circ \pi \end{aligned}$$

where $\pi : G \to G/G^n$ is the projection map. In particular when G is cyclic

$$|\widehat{G}[n]| = |G[n]|$$

Proof. It's clear that the so given $\bar{\chi} \circ \pi$ has order dividing n. Conversely given χ we define $\bar{\chi}(gG^n) = \chi(g)$. This is well-defined because $gG^n = hG^n \implies gh^{-1} \in G^n \implies \chi(gh^{-1}) = \chi(x^n) = \chi^n(x) = 1 \implies \chi(g) = \chi(h)$. These are clearly mutually inverse and the result is proven. The final part follows from G/G^n being cyclic and

$$|\widehat{G}[n]| = |\widehat{G/G^n}| = |G/G^n| = |G[n]|$$

□

Lemma 4.6
Let G be a finite cyclic group of order N. Then

$$a \in G^n \iff \chi(a) = 1 \quad \forall \chi \in \widehat{G}[n]$$

In particular when $n = N$

$$a = e \iff \chi(a) = 1 \quad \forall \chi \in \widehat{G}$$

Proof. We prove the second statement first. This follows by simply considering a generator λ_g of $\widehat{G}$ is given above. Then $a \neq e \implies \lambda_g(e) \neq 1$ as required.

For the first statement, denote $\bar{a}$ by the image of a in G/G^n. Then $a \in G^n \iff \bar{a} = e \iff \bar{\chi}(\bar{a}) = 1 \quad \forall \bar{\chi} \in \widehat{G/G^n} \iff \chi(a) = 1 \quad \forall \chi \in \widehat{G}[n]$ where we have used the second statement applied to G/G^n and the correspondence in Proposition 4.5.

□

Proposition 4.7
Orthogonality of characters
Let G be a finite cyclic group of order N and n a non-zero integer then

$$\sum_{\chi \in \widehat{G}[n]} \chi(a) = \begin{cases} |\widehat{G}[n]| = |G[n]| & a \in G^n \\ 0 & a \notin G^n \end{cases}$$

in particular when $n = N$ we have

$$\sum_{\chi \in \widehat{G}} \chi(a) = \begin{cases} |G| & a = e \\ 0 & a \neq e \end{cases}$$

Proof. When $a \in G^n$ then by Lemma 4.6, we have $\chi(a)$ for each term in the sum and Proposition 4.5 gives the order. When $a \notin G^n$ then by Lemma 4.6 again there exists $\chi' \in \widehat{G}[n]$ such that $\chi'(a) \neq 1$. Then

$$\sum_{\chi \in \widehat{G}[n]} \chi(a) = \sum_{\chi \in \widehat{G}[n]} (\chi'\chi)(a) = \chi'(a) \sum_{\chi \in \widehat{G}[n]} \chi(a)$$

and the result follows by cancellation. Finally observe that $G^N = \{e\}$ and $G[N] = G$ to obtain the final statement. □

Proof. We can now prove Proposition 4.1. This follows from combining Proposition 4.7 and the fact $N(X^n = a) = |G[n]|$ from Proposition 4.3 □

4.3 Gauss and Jacobi Sums

Let ψ be a non-trivial additive character on $\mathbb{F}_q$ and χ a multiplicative character. Define the Gauss sum as follows

$$G(\chi,\psi) := \sum_{a\in\mathbb{F}_q} \chi(a)\psi(a)$$

where we have used the extension of χ to zero. Furthermore define the Jacobi Sum as follows

$$J(\chi_1,\chi_2) = \sum_{t\in\mathbb{F}_q} \chi_1(t)\chi_2(1-t)$$

Note by definition that

$$\chi(0) = \mathbf{1}\{\chi = \epsilon\}$$

so that orthogonality of multiplicative characters takes the form

$$\sum_{a\neq 0} \chi(a) = (q-1)\cdot\chi(0)$$

Proposition 4.8 *1.* $G(\epsilon,\psi) = 0$

2. For $\chi_1\chi_2 \neq \epsilon$ *we have*

$$G(\chi_1,\psi)G(\chi_2,\psi) = G(\chi_1\chi_2,\psi)J(\chi_1,\chi_2)$$

3. For $\chi_1\chi_2 = \epsilon$ *we have*

$$G(\chi_1,\psi)G(\chi_2,\psi) = \mathbf{1}\{\chi_1=\epsilon\}\mathbf{1}\{\chi_2=\epsilon\} + \chi_1(-1)(q-1) - J(\chi_1,\chi_2)$$

4. $J(\epsilon,\epsilon) = q$

5. $\chi\neq\epsilon \implies J(\epsilon,\chi) = 0$

6. $\chi\neq\epsilon \implies J(\chi,\chi^{-1}) = -\chi(-1)$

7. $\overline{G(\chi,\psi)} = \chi(-1)G(\chi^{-1},\psi)$

8. $\chi\neq\epsilon \implies G(\chi,\psi)G(\chi^{-1},\psi) = \chi(-1)q$

9. $\chi\neq\epsilon \implies |G(\chi,\psi)| = q^{1/2}$

10. $\chi_1,\chi_2,\chi_1\chi_2\neq\epsilon \implies |J(\chi_1,\chi_2)| = q^{1/2}$

Proof. We prove in turn

1. $G(\epsilon,\phi) = \sum_{a\in\mathbb{F}_q}\chi(a)$ which follows by orthogonality of characters (to state!)
2. We prove a slightly more general formula from which both relations follow

$$\begin{aligned}
G(\chi_1,\psi)G(\chi_2,\psi) &= \sum_{a,b}\chi_1(a)\chi_2(b)\psi(a+b)\\
&= \sum_{a,c}\chi_1(a)\chi_2(c-a)\psi(c)\\
&= \sum_{a,c\neq 0}\chi_1(a)\chi_2(c-a)\psi(c) + \sum_a \chi_1(a)\chi_2(-a)\\
&= \sum_{t,c\neq 0}\chi_1(ct)\chi_2(c(1-t))\psi(c) + \sum_{a\neq 0}\chi_1(a)\chi_2(-a) + \chi_1(0)\chi_2(0)\\
&= \sum_{c\neq 0}\chi_1(c)\chi_2(c)\psi(c)\sum_t \chi_1(t)\chi_2(1-t) + \chi_1(0)\chi_2(0) + \chi_1(-1)\sum_{a\neq 0}(\chi_1\chi_2)(a)\\
&= \left(G(\chi_1\chi_2,\psi) - (\chi_1\chi_2)(0)\right)J(\chi_1,\chi_2) + \chi_1(0)\chi_2(0) + \chi_1(-1)\,(q-1)\,\mathbf{1}\{\chi_1\chi_2=\epsilon\}\\
&= G(\chi_1\chi_2,\psi)J(\chi_1,\chi_2) + \mathbf{1}\{\chi_1=\epsilon\}\mathbf{1}\{\chi_2=\epsilon\} + \left(\chi_1(-1)(q-1) - J(\chi_1,\chi_2)\right)\mathbf{1}\{\chi_1\chi_2=\epsilon\}
\end{aligned}$$

When $\chi_1\chi_2\neq\epsilon$ then $\chi_1\neq\epsilon$ or $\chi_2\neq\epsilon$. Therefore

$$G(\chi_1,\psi)G(\chi_2,\psi) = G(\chi_1\chi_2,\psi)J(\chi_1,\chi_2)$$

as required.

3. Similarly when $\chi_1\chi_2 = \epsilon$ the relation follows from the previous result.
4. This is immediate from the definition
5. $J(\epsilon, \chi) = \sum_t \chi(t) = \chi(0) = 0$ by orthogonality of characters
6. $J(\chi, \chi^{-1}) = \sum_t \chi(t)\chi^{-1}(1-t) = \sum_{t\neq 0,1} \chi\left(\frac{t}{1-t}\right) = \sum_{a\neq 0,-1} \chi(a) = -\chi(-1)$ again by orthogonality of characters
7. Suppose $\chi \neq \epsilon$, then

$$\begin{aligned}\overline{G(\chi,\psi)} &= \sum_a \overline{\chi}(a)\overline{\psi(a)} = \sum_{a\neq 0} \chi(a^{-1})\psi(-a) \\ &= \chi(-1)\sum_{a\neq 0} \chi(a^{-1})\psi(a) \\ &= \chi(-1)G(\chi^{-1},\psi)\end{aligned}$$

   one may show directly that it holds when $\chi = \epsilon$.
8. By 3 and 6 we have

$$G(\chi,\psi)G(\chi^{-1},\psi) = -J(\chi,\chi^{-1}) + \chi(0)\chi^{-1}(0) + \chi(-1)(q-1) = \chi(-1)q$$

9. By 8 and 7 we have

$$|G(\chi,\psi)|^2 = G(\chi,\psi)\overline{G(\chi,\psi)} = \chi(-1)G(\chi,\psi)G(\chi^{-1},\psi) = \chi^2(-1)q$$

   as required.
10. This follows immediately from 2 and 9.

□

NB Lemmermeyer uses a slightly different convention, omitting the term at a, but they are easy to relate.

A Algebra

A.1 Bilinear Pairings

Definition A.1 (Bilinear Pairing)
Let V, W be k-vector spaces, we say a map

$$\psi : V \times W \to k$$

is bilinear if it is k-linear in each variable separately. ψ induces two linear maps

$$\psi_L : V \to W^\star$$
$$\psi_R : W \to V^\star$$

by $\psi_L(v)(w) = \psi_R(w)(v) = \psi(v, w)$. We say that the pairing is

- **Non-degenerate** *if ψ_L and ψ_R are injective*
- **Perfect** *if ψ_L and ψ_R are bijective*

We state a simple criterion for being perfect

Lemma A.1
Let ψ be a bilinear pairing on $V \times W$, such that W is finite-dimensional and ψ_L is bijective then ψ is perfect.

Proof. ψ_L bijective shows $\dim_k V = \dim_k W^\star = \dim_k W$ since it's finite dimensional.

Consider a basis $v_1, \ldots, v_n$ of V, which maps under ψ_L to a basis $w_1^\star, \ldots, w_n^\star$ of $W^\star$. Let $w_1, \ldots, w_n$ be the corresponding dual basis of W, and similarly $v_1^\star, \ldots, v_n^\star$ the dual basis of $V^\star$. Then we claim that $\psi_R(w_i) = v_i^\star$ which shows that ψ_R is an isomorphism. But $\psi_R(w_i)(v_j) = \psi(v_j, w_i) = \psi_L(v_j)(w_i) = w_j^\star(w_i) = \delta_{ij} \quad \forall j$, so $\psi_R(w_i) = v_i^\star$ as required. □

Definition A.2 (Dual basis with respect to a perfect pairing)
Suppose $\psi : V \times W \to \mathbb{R}$ is a perfect pairing.

We say two bases, $\{e_1, \ldots, e_n\}$ of V and $\{e_1^\star, \ldots, e_n^\star\}$ of W are dual if they satisfy the following orthogonality relationship

$$\psi(e_i, e_j^\star) = \delta_{ij}$$

Remark A.3
Given any basis, there exists a unique dual basis due to the fact ψ_L (or ψ_R) is an isomorphism.

Proposition A.2 (Change of variables)
Suppose $\psi : V \times W \to \mathbb{R}$ is a perfect pairing.
Consider two sets of dual bases, $\{e_i\}_{i=1\ldots n}$, $\{e_i^\star\}_{i=1\ldots n}$ and $\{f_i\}_{i=1\ldots n}$, $\{f_i^\star\}_{i=1\ldots n}$.
Then we have the following change of variables formulae

$$e_i = \sum_{j=1}^{n} \psi(e_i, f_j^\star) f_j$$
$$e_i^\star = \sum_{j=1}^{n} \psi(f_j, e_i^\star) f_j^\star$$

Proof. Let $x := e_i - \sum_{j=1}^n \psi(e_i, f_j^\star) f_j$. Then

$$\psi(x, f_k^\star) = \psi(e_i, f_k^\star) - \psi(e_i, f_k^\star) = 0$$

for all k. Therefore $x \in \ker(\psi_L)$ which shows $x = 0$ by non-degeneracy. The other case follows similarly. □

A.2 Local Rings

Definition A.4 (Local Ring)
A pair $(A, \mathfrak{m})$ is a local ring if $\mathfrak{m}$ is the unique maximal ideal of the ring A. In this case we may write

$$\kappa(\mathfrak{m}) := A/\mathfrak{m}$$

which we call the "residue field".
We say it is a local k-algebra if A is also a k-algebra.

Generally we expect the residue field to be at most a finite extension of the base field k, as in the following

Proposition A.3 (Finite residue field)
If $(A, \mathfrak{m})$ is a local k-algebra then there is a natural field extension

$$k \to A \to A/\mathfrak{m} = \kappa(\mathfrak{m})$$

If in addition A is a finitely generated k-algebra then $\kappa(\mathfrak{m})$ is a f.g. field extension of k, which is therefore finite algebraic. Finally if k is algebraically closed then $k = \kappa(\mathfrak{m})$.

Proof. See [AM69, Cor 7.10] for the second statement. □

Lemma A.4 (Local ring criterion)
Let $\mathfrak{m} \lhd A$ be an ideal such that

$$x \notin \mathfrak{m} \implies x \in A^\star$$

then $(A, \mathfrak{m})$ is a local ring.

Proof. See [AM69, Prop 1.6] □

A.3 Localization

Reference for this section is [**?** , Chap 1], [AM69, Sec. 3] and [AM69, Ex 7-9].

Algebraically, localization can be seen as enlargening a ring to include inverses. In terms of the ideal structure this means removing (proper) ideals which contain the newly inverted elements. Geometrically ideals correspond to points/subsets, so localization may be viewed as reducing the set of interest.

Definition A.5 (Multiplicatively Closed)
For a ring A a multiplicatively closed (m.c.) subset is a subset S of A which satisfies

- $1 \in S$
- $s, t \in S \implies st \in S$

It is proper if $0 \notin S$. Further it is saturated *if*

$$st \in S \implies s, t \in S$$

Example A.6
Multiplicative group of units $A^\star$ is a saturated m.c. set

Example A.7
The set $S_f = \{1, f, f^2, \ldots\}$ is m.c. but not necessarily saturated. As an example consider $A = \mathbb{Z}$ and $S_n = \{1, n, n^2, \ldots\}$ for n compositive. Then $pq \in S_n$ but $p \notin S_n$.

Example A.8
The set $A \setminus \mathfrak{p}$ is a saturated multiplicatively closed set. More generally any set of the form

$$A \setminus \bigcup_i \mathfrak{p}_i$$

is a saturated multiplicatively closed subset.

The localization of A at a m.c. set S is denoted by $S^{-1}A$ and is typically defined as the set of fractions

$$S^{-1}A := \{ \left[\frac{a}{s}\right] \mid a \in A \, s \in S \} / \sim$$

under the equivalence relation

$$\left[\frac{a}{s}\right] \sim \left[\frac{b}{t}\right] \iff u(at - bs) = 0 \quad \text{some } u \in S \, .$$

Proposition A.5
Thus defined $S^{-1}A$ is a ring under the obvious operations. It is non-zero precisely when S is proper. When $S = \{1\}$ then $S^{-1}A$ is canonically isomorphic to A.

Note when A is an integral domain and S is proper then the equivalence relation may be weakened to $at - bs = 0$.
The localization may be characterized more abstractly.

Definition A.9 (S-invertible)
Let A be a ring with a m.c. subset S, then a homomorphism

$$\phi : A \to B$$

is said to be S-invertible if $\phi(S) \subseteq B^\star$.

We show that localization satisfies the following universal property

Proposition A.6 (Universal Property of Localization)
Let A be a ring and S a proper m.c. subset, then the canonical map

$$i_S : A \to S^{-1}A$$

is S-invertible, and for any other S-invertible morphism $\phi : A \to B$ there is a unique factorization

$$\phi = \tilde{\phi} \circ i_S$$

Any morphism factoring in this way is automatically S-invertible.

Example A.10 (Field of fractions)
Let A be an integral domain, then we define the field of fractions

$$\mathrm{Frac}(A) := (A \setminus 0)^{-1} A$$

Consider all the proper m.c. sets S, and fix all the rings $S^{-1}A$ and morphisms i_S. Then we show the conditions under which there are canonical maps $S^{-1}A \to T^{-1}A$ which satisfy all the obvious commutativity relations

Proposition A.7 (Localization maps factor)
Let S, T be two m.c. sets, then the following two conditions are equivalent

- *There exists a morphism i_{ST} such that $i_{ST} \circ i_S = i_T$.*
- $S \subseteq i_T^{-1}\left((T^{-1}A)^\star\right) =: \overline{T}$

In this case the morphism i_{ST} is unique and we say

$$S \prec T$$

Further

$$i_{TU} \circ i_{ST} = i_{SU}$$

whenever $S \prec T$ and $T \prec U$ (which by the first criterion implies $S \prec U$). Furthermore

$$i_{SS} = \mathbf{1}$$

Proof. $\implies$). Then $i_T(S) = i_{ST}(i_S(S)) \subseteq i_{ST}\left((S^{-1}A)^\star\right) \subseteq \left(T^{-1}A\right)^\star$ as required.
Conversely the i_{ST} exists by the universal property just proven, which also shows uniqueness. □

In light of the condition $S \prec T \iff S \subseteq i_T^{-1}((T^{-1}A)^\star)$ we make the following definition

Lemma A.8 (Saturation)
Let S be a m.c. set then the following sets are the same

1. $i_S^{-1}\left((S^{-1}A)^\star\right)$
2. $\{a \mid \exists x \text{ s.t. } xa \in S\} = \{ \text{ divisors of } S\}$
3. $\bigcap_{S \subseteq T : T \text{ saturated}} T$

and we call this the saturatation of S, denoted by $\overline{S}$. It is the smallest saturated m.c. superset of S.

Proof. Denote the sets by S_1, S_2, S_3 respectively We show each in turn
$S_1 \subseteq S_2$) Suppose $s' \in i_S^{-1}((S^{-1}A)^\star)$ then by definition $\frac{s'}{1}\frac{a}{s} = 1 \implies t(as' - s) = 0 \implies (ta)s' \in S$.

$S_2 \subseteq S_1$) Suppose $as' = s$ then $\frac{s'}{1}\frac{a}{s} = 1$ so $s' \in i_S^{-1}((S^{-1}A))$.

It's clear that S_2 is saturated, therefore $S_3 \subseteq S_2$. Conversely suppose $T \supseteq S$ is saturated, and consider $a \in S_2$. Then $xa \in S \subseteq T \implies a \in T$. Therefore $T \subseteq S_2$, whence $S_3 \subseteq S_2$ as required.

Finally the property of being saturated m.c. is closed under intersection therefore $\overline{S}$ is saturated, and is clearly the smallest such set. □

Example A.11
Fix a prime p and define $S_n = \{p^{rn} \mid r \geq 0\}$. Then clearly $\overline{S_n} = S_1$. It's clear then that $(S_n)^{-1}\mathbb{Z}$ is canonically isomorphic to $(S_m)^{-1}\mathbb{Z}$ as they're both equal to $\mathbb{Z}_p$.

When A is an integral domain it's possible to show that $S^{-1}A$ is always a subring of the field of fractions $\mathrm{Frac}(A)$. More generally

Lemma A.9
i_S is injective $\iff$ S has no zero-divisors

Corollary A.10
If A is an integral domain then all (proper) localizations $S^{-1}A$ may be regarded as subrings of the field of fractions $\mathrm{Frac}(A)$

Proof. Let $T = A \setminus 0$. Then every proper S has no zero-divisors so that i_S and i_T are injective. It follows that i_{ST} is also injective. □

When S, T are not too different, then we can show that the map i_{ST} is an isomorphism :

Proposition A.11 (Isomorphism)
Let S, T be two multiplicatively closed subsets then TFAE

1. *$T \prec S$ and $S \prec T$*
2. *i_{ST} is an isomorphism.*
3. *$\bar{S} = \bar{T}$*

In this case $i_{ST}^{-1} = i_{TS}$

Proof. 1 $\implies$ 2). In this case both i_{ST} and i_{TS} are well-defined so that $i_{ST} \circ i_{TS} = i_{SS} = \mathbf{1}$ and $i_{TS} \circ i_{ST} = i_{TT} = \mathbf{1}$.
2 $\implies$ 3). Then $\overline{T} = i_T^{-1}\left((T^{-1}A)^\star\right) = i_S^{-1}(i_{ST}^{-1}((T^{-1}A)^\star)) = i_S^{-1}((S^{-1}A)^\star) = \overline{S}$ as a ring isomorphism preserves the group of units.
3 $\implies$ 1). $T \subseteq \overline{T} = \overline{S}$ and $S \subseteq \overline{S} = \overline{T}$ as required. □

Corollary A.12
Let S be a multiplicatively closed set, then $i_{S\overline{S}}$ is an isomorphism

Proof. By Lemma A.8 $\overline{S}$ is saturated, so $\overline{\overline{S}} = \overline{S}$. Therefore $i_{S\overline{S}}$ is an isomorphism by Proposition A.11. □

This means we may wlog only consider $S^{-1}A$ where S is saturated. In the saturated case $S \prec T \iff S \subseteq T$.
We show another characterization of $\overline{S}$

Lemma A.13
Let A be a ring, S a m.c. closed set and $\mathfrak{b} \lhd A$ such that $\mathfrak{b} \cap S = \emptyset$ then

$$\mathcal{I} = \{\mathfrak{a} \mid \mathfrak{b} \subseteq \mathfrak{a} \quad \mathfrak{a} \cap S = \emptyset\}$$

has a maximal element, which is prime.

Proof. By Zorn's Lemma it has a maximal element, $\mathfrak{p}$. We claim it is prime, for suppose $xy \in \mathfrak{p}$ and $x, y \notin \mathfrak{p}$. Then by maximality $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ intersect S. Therefore S intersects $(\mathfrak{p} + (x))(\mathfrak{p} + (y)) \subseteq \mathfrak{p}$, a contradiction. □

Proposition A.14
Let S be a multiplicatively closed set then

$$\overline{S} = A \setminus \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p}$$

Proof. Denote the right hand side by T. Then clearly $S \subseteq T$ and as noted before T is saturated. Therefore $\overline{S} \subseteq T$.

Conversely suppose $a \notin \overline{S}$. Consider the principal ideal (a) then $(a) \cap S = \emptyset$ (because $ab \in S \implies a \in \overline{S}$ by Lemma A.8). Therefore by the previous Lemma there is a prime ideal $\mathfrak{p}$ containing a which does not intersect S. Therefore $a \notin T$. We have shown that $a \notin \overline{S} \implies a \notin T$, contrapositively $T \subseteq \overline{S}$ as required. □

A.4 Prime Ideal Structure

Definition A.12 (Radical Ideal)
Recall an ideal $\mathfrak{a}$ is radical if

$$x^n \in \mathfrak{a} \implies x \in \mathfrak{a}$$

Recall the implications

$$\text{maximal} \implies \text{prime} \implies \text{radical}$$

It is possible to define the minimal radical ideal containing a given ideal.

Proposition A.15
The set

$$\sqrt{\mathfrak{a}} = \{x \mid x^n \in \mathfrak{a}\}$$

is a radical ideal. Any radical ideal containing $\mathfrak{a}$ also contains $\sqrt{\mathfrak{a}}$. Furthermore it satisfies

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}$$

Proof. Suppose $y^n \in \sqrt{\mathfrak{a}}$, then $y^{mn} \in \mathfrak{a}$, which implies $y \in \sqrt{\mathfrak{a}}$. Therefore $\sqrt{\mathfrak{a}}$ is radical.

Suppose $x \in \sqrt{\mathfrak{a}}$ then $x^n \in \mathfrak{a}$. When $\mathfrak{a} \subseteq \mathfrak{p}$ then it's clear that $x^n \in \mathfrak{p} \implies x \in \mathfrak{p}$. Therefore x lies in the right hand side.

Conversely suppose $x \notin \sqrt{\mathfrak{a}}$ then $S := \{1, x, x^2, \ldots\}$ is a proper multiplicatively closed set such that $S \cap \mathfrak{a} = \emptyset$. By Lemma A.13 there is a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ which does not intersect S. Therefore $x \notin RHS$ as required. □

We say an element x to be nilpotent if $x^n = 0$. These form an ideal.

Definition A.13 (Nilradical)
Define the set of nilpotents ("Nilradical")

$$N(A) := \sqrt{(0)} = \bigcap_{\mathfrak{p}} \mathfrak{p}$$

Remark A.14
When working with rings of functions (with codomain a field), then we wouldn't expect there to be nilpotent elements.

We also make the following definitions

Definition A.15
Let A be a ring.

1. *A is reduced if $N(A) = 0$*
2. *A is irreducible if $N(A)$ is prime*
3. *A is an integral domain if (0) is prime (i.e. $xy = 0 \implies x = 0 \vee y = 0$)*

Lemma A.16 (Integral $\iff$ Reduced and Irreducible)
Let A be a ring. Then A is an integral domain if and only if it is reduced and irreducible

Proof. Suppose A is an integral domain. Since $N(A)$ is the intersection of all prime ideals and (0) is prime it must be equal to (0). Therefore A is reduced and irreducible.
The converse is clear. □

In many contexts it is sufficient to work with minimal primes.

Lemma A.17 (Existence of minimal primes)
Suppose $\mathfrak{a}$ is contained in a prime ideal $\mathfrak{p}$, then there is at least one prime ideal $\mathfrak{q}$ minimal s.t.

$$\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$$

Proof. Define the set of prime ideals

$$\mathcal{I} = \{\mathfrak{q} \mid \mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}\}$$

partially ordered by reverse inclusion. Clearly every chain is closed under intersection, so we may apply Zorn's lemma to find a minimal element $\mathfrak{q}$. □

Corollary A.18 (Nullstellensatz with minimal primes)

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p} : \mathfrak{p} \ minimal} \mathfrak{p}$$

Corollary A.19 (Criteria for Irreducibility)
TFAE

1. *$N(A)$ is prime*
2. *$N(A)$ is the unique minimal prime.*
3. *There is exactly one minimal prime.*

Proof. Note that all prime ideals contain $N(A)$. So if $N(A)$ is prime it is the unique minimal prime ideal. So 1) $\implies$ 2), 3) easily. Similarly 2) $\implies$ 1) tautologically.
Conversely if there's only one minimal prime $\mathfrak{p}$, then it must be equal to $N(A)$ by the previous Corollary. □

Remark A.16
Geometrically the minimal primes correspond to "irreducible components". Consequently if there is only one minimal prime

A.5 Integral Extensions

Definition A.17
Let $\phi : A \to B$ be a ring morphism.

- *We say $b \in B$ is integral over (ϕ, A) if it satisfies $f(b) = 0$ for some non-zero monic polynomial $f \in \phi(A)[X]$.*
- *ϕ is integral if every $b \in B$ is integral over A.*
- *If ϕ is an inclusion, then we say B is integral over A, or that B is an integral extension of A*
- *When A is a field then an element (resp. ring morphism) is integral precisely if it is algebraic*

It is possible to show that integral extensions preserve Krull dimension. As a special case, we show it preserves Krull dimension zero :

Proposition A.20
Let $A \subseteq B$ be integral domains, with B integral over A. Then B is a field if and only if A is a field.

c.f. [AM69][Prop. 5.7]

Proof. Suppose that A is a field and $0 \neq b \in B$. Then by assumption there is a relation

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0 \quad a_i \in A$$

Choose n minimal, then we claim that $0 \neq a_0$. For if not, then we may cancel b to find an integral relation of smaller degree, contradicting the minimality of n. Then it's easy to see that b has an explicit inverse

$$-a_0^{-1}\left(a_1 + \ldots + a_{n-1}b^{n-1}\right)$$

which lies in B. Conversely suppose B is a field and $0 \neq a \in A$. Then $a^{-1} \in B$ is integral over A, so

$$a^{-m} + a_1 a^{-m+1} + a_{m-1}a^{-1} + a_m = 0$$

multiply by a^{m-1} to find

$$a^{-1} = -(a_1 + \ldots + a_m a^{m-1}) \in A$$

□

References

[AM69] M. Atiyah and I.G. McDonald. *Introduction to Commutative Algebra*. Westview Press, 1969.

[Eme10] Matthew Emerton. Jacobson rings. `http://www.math.uchicago.edu/~emerton/pdffiles/jacobson.pdf`, 2010.

[For81] O. Forster. *Lectures on Riemann Surfaces*. 1981.

[Lan72] Serge Lang. *Differential manifolds*, volume 212. Springer, 1972.

[Mil14] J. Milne. Introduction to commutative algebra. `http://www.jmilne.org/math/xnotes/CA.pdf`, 2014.

[Mil17] J. Milne. Algebraic geomtry. `http://www.jmilne.org/math/xnotes/AG.pdf`, 2017.

[Sha94] Igor Shafarevich. *Basic algebraic geometry*, volume 1. Springer-Verlag New York, 1994.

[Sta15] The Stacks Project Authors. *stacks project.* *http://stacks.math.columbia.edu*, *2015.*

[War13] F. Warner. Foundations of Differentiable Manifolds and Lie groups. *Springer-Verlag New York, 2013.*