# Introduction to Arithmetic Geometry

David Rufino

December 2015

## 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 Overview of Algebraic Geometry

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

## 2.1 Algebraic Sets

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 1.** *Correspondence between Algebraic Sets 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* or algebraic sets. We note some simple results

**Lemma 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

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

   For the last equivalence in general we have $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$, so one direction is clear. Conversely suppose $\mathfrak{ab} \subseteq \mathfrak{m}_x$ and $y \in \mathfrak{a} \cap \mathfrak{b}$. Then $y^2 \in \mathfrak{ab} \subseteq \mathfrak{m}_x$, 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 closed sets and radical ideals

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

**Example 2.** *Zariski Topology on $k^1$*
*An important 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 $Y = V(\prod_{p \in Y}(X - p))$.*

In the proof we introduced the ideal $\mathfrak{m}_x = I(\{x\})$ of functions vanishing at a point. We show in more detail

**Lemma 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 $k$ is a field). It's clear that $(X_1 - x_1, \ldots, X_n - x_n) \subseteq \mathfrak{m}_x$. In general you can write

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

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.** *Not all maximal ideals arise in this way, for example $(X^2 - 2)$ is maximal in $\mathbb{Q}[X]$. More generally $f(X)$ irreducible implies $(f)$ is maximal in $k[X]$. When $k$ is algebraically closed every irreducible polynomial in one variable is of degree 1, so all the maximal ideals of $k[X]$ are of the form above. We will show later that in addition all maximal ideals in $k[X_1, \ldots, X_n]$ are of this form when $k$ is algebraically closed.*

**Definition 4.** *Coordinate Ring of an algebraic set*

*Let $\mathfrak{a} \lhd k[X_1, \ldots, X_n]$ be a radical ideal, and $V = V(\mathfrak{a})$ be the corresponding algebraic set. Define the coordinate ring as follows*

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

*There is a canonical injection*

$$k[V] \hookrightarrow \mathrm{Fun}(V, k)$$

*in otherwords $k[V]$ may be regarded as functions.*

Let $\mathfrak{a} \lhd k[V]$ be an ideal, and consider an algebraic set $V = V(\mathfrak{a})$. Define the coordinate ring $k[V] := k[X_1, \ldots, X_n]/\mathfrak{a}$. We obtain a similar Galois connection

**Definition 5.** *Closed subsets of an algebraic set*

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

which satisfies all of the same properties. Moreover the induced topology on $V$ is the same as the subspace topology.

**Lemma 3.** *Topology of an algebraic set*
*Let $\pi : k[X_1, \ldots, X_n] \longrightarrow k[V]$ denote the canonical projection. Then*

- $V(\overline{\mathfrak{b}}) = V(\pi^{-1}(\overline{\mathfrak{b}}))$

- $I(Y) = \pi(I(Y))$

There is some connection with the topological properties of $V$ and the ring-theoretic properties of $k[V]$.

**Lemma 4.** *Irreducible Sets*
*Let $V = V(\mathfrak{a})$ be an algebraic set. Then TFAE*

- *$V$ is irreducible as a topological space*
- *$\mathfrak{a}$ is a prime ideal*
- *$k[V]$ is an integral domain*

Recall the following facts about irreducible topological spaces

**Lemma 5.** *Properties of Irreducible Topological Spaces*

- *Every non-empty open set $V$ is dense*
- *Any two non-empty open sets intersect non-trivially*
- *An irreducible space is necessarily connected*
- *A noetherian topological space decomposes into finitely many (maximal) irreducible components.*

We note in general that the ideal $\mathfrak{a}$ is not uniquely determined by the set $V$, but in an algebraically closed field ($k = \bar{k}$) then this relation becomes somewhat simpler

**Theorem 6.** *Nullstellensatz*
*In the case $k = \bar{k}$ and $V = V(\mathfrak{a})$ is an algebraic set, then*

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

*and so the Galois connection induces a bijection between closed sets and radical ideals. Moreover under this bijection singletons correspond to maximal ideals*

$$V(\mathfrak{a}) \ni x \quad \{x\} \longleftrightarrow \mathfrak{m}_x = (\overline{X}_1 - x_1, \ldots, \overline{X}_n - x_n)$$

*and every maximal ideal of $k[V]$ arises in this way.*

So in the case of an algebraically closed field in some sense everything important is captured by the algebraic invariant $k[V]$.

**Remark 6.** *As remarked earlier when $k$ is not algebraically closed, not all maximal ideals arise in this way. In the case $k[X]$ there is a one-to-one correspondence between monic irreducible polynomials $f(X)$ and maximal ideals $\mathfrak{m} \lhd k[X]$. Nevertheless $f$ will split into linear factors in some finite field extension of $k$, inside some fixed algebraic closure. For example $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ in $\mathbb{Q}(\sqrt{2})[X]$. Moreover the roots of $f$ will be Galois conjugate. Therefore we may identify $\mathfrak{m}$ with conjugacy classes of elements in some extension field of $k$. This may be generalized to the $n$-dimensional case, which is described in the next section*

## 2.2 $K$-rational points

**Definition 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 7.** *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 Galois action 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 $\phi$ 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 $\sigma \in \mathrm{Gal}(\bar{k}/k)$, then $\sigma(f(x)) = f(\sigma(x))$, whence $\sigma \circ \phi_x = \phi_{\sigma x}$.

The map $\phi_x$ 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 8.** *There is a bijection of rational points*

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

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

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.

## 2.3 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

$$\begin{aligned} I(Y) &:= \bigcap_{x \in Y} \mathfrak{m}_x && (1)\\ V(\mathfrak{b}) &:= \{x \mid \mathfrak{b} \subseteq \mathfrak{m}_x\} && (2)\\ \implies IV(\mathfrak{b}) &= \bigcap_{\mathfrak{b} \subseteq \mathfrak{m}_x} \mathfrak{m}_x\,. && (3) \end{aligned}$$

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 8.** *Maximal Spectrum*
*Let $A$ be a reduced finitely-generated $k$-algebra, then define as follows*

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

**Remark 9.** *This corresponds to Definition 1, for when $k = \bar{k}$ and $V = V(\alpha)$ we have a commutative diagram*

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

*The vertical isomorphism arises from Theorem 6 and the commutativity from Equations* (1), (2).
*When $k$ is not algebraically closed we nevertheless have a correspondence between Galois orbits and "points"*

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

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

The Nullstellensatz in this setting is

**Proposition 9.** *Generalized Nullstellensatz ([Mil14, Prop 13.10])*
*Let $k$ be an arbitrary field, and $A$ a reduced f.g. $k$-algebra then*

$$IV(\mathfrak{a}) = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m} \lhd A} \mathfrak{m} = \sqrt{a} \tag{4}$$

We may generalize this to arbitrary rings $A$, provided we insist that the Nullstellensatz hold. Therefore we make the somewhat arbitrary and non-standard definition

**Definition 10.** *Affine Ring*
*A pair $(A, X)$ is an affine ring if $A$ is a ring and $X$ is a set of prime ideals satisfying the Nullstellensatz*

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

*for all ideals $\mathfrak{a} \lhd A$. As before we define*

$$\begin{aligned} I(Y) &:= \bigcap_{[\mathfrak{m}] \in Y} \mathfrak{m}\,, \\ V(\mathfrak{b}) &:= \{[\mathfrak{m}] \mid \mathfrak{b} \subseteq \mathfrak{m}\} \end{aligned}$$

*which induces a natural topology on $A$. Note that the condition necessarily implies*

$$\operatorname{Specm}(A) \subseteq X \subseteq \operatorname{Spec}(A)$$

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

**Example 11.** *Affine Variety over a field*
*$(A, \operatorname{Specm}(A))$ where $A$ is a f.g. reduced $k$-algebra, the Nullstellensatz stated above. More generally a Jacobson ring ([Eme10], [Sta15, 00FZ]) will also work.*

**Example 12.** *Affine Scheme*
*$(A, \operatorname{Spec}(A))$ where $A$ is an arbitrary ring (the Nullstellensatz here is an elementary result [Sta15, 00E0] Lemma 10.16.2 (7)).*

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

**Lemma 10.** *Let $(A, X)$ be an affine ring*

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 $A$.*

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

**Example 13.** *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. We formalise this phenomenon as follows

**Lemma 11.** *Specialization*
*Let $X$ be a topological space and $x, y \in X$, then TFAE*

- $x \in \overline{\{y\}}$
- *Every neighbourhood of $x$ also contains $y$*

*In this case we say $x$ is a specialization of $y$. In the case $(A, X)$ an affine ring then*

$$[\mathfrak{p}] \text{ specialization of } [\mathfrak{q}] \iff \mathfrak{q} \subseteq \mathfrak{p}$$

*When $[(0)] \in X$ then every prime ideal $[\mathfrak{p}]$ is a specialization of $[(0)]$.*

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 14.** *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*

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

$\Diamond$ *We say a topological space $X$ is Jacobson if the inclusion*

$$X^0 \hookrightarrow X$$

*is a quasi-homeomorphism. The topological space $\mathrm{Spec}(A)$ is Jacobson $\iff$ $A$ is a Jacobson ring.*

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. In any case one may show

## 2.4 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 12.** *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.

□

## 2.5 Morphisms of Algebraic Sets and Affine Varieties

We wish to define what are the morphisms between algebraic sets. Recall that the we have a canonical inclusion $k[V] \hookrightarrow \mathrm{Fun}(V, k)$ and such functions are called regular. We say $f : X \to Y$ is regular if it is given by polynomials.

**Definition 15.** *Morphisms of Algebraic Sets*
*Let $X = V(\mathfrak{a}) \subseteq k^n$ and $Y = V(\mathfrak{b}) \subseteq k^m$ be algebraic sets. We say that a function $f : X \to Y$ is regular if it is coordinate-wise given by polynomial functions*

$$f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$$

*for $f_i \in k[X_1, \ldots, X_n]$.*

*Equivalently $f$ is regular iff it induces a $k$-algebra homomorphism given by composition*

$$\begin{aligned} f_\sharp : k[Y] &\longrightarrow k[X] \\ \phi &\longrightarrow \phi \circ f \end{aligned}$$

*One may show this induces a bijection*

$$\mathrm{Mor}(X, Y) \longrightarrow \mathrm{Hom}_k(k[Y], k[X])$$

We note an important result needed later

**Lemma 13.** *Let $V = V(\mathfrak{a})$ an algebraic set. Any regular maps $f, g \in k[V]$ which agree on a Zariski dense subset of $V$ are in fact equal.*

A fancy way of saying is that the functor $X \to k[X]$ is full and faithful. In general however, for projective varieties, this is too crude a way of characterising morphisms of varieties, not least because projective varieties generally have no non-trivial regular sections (the equivalent statement for Riemann surfaces is that any holomorphic function of a compact Riemann surface is necessarily constant). As a result we consider the regular functions over an arbitrary open set.

In the abstract case

**Definition 16.** *Suppose $(A, X)$ and $(B, Y)$ are affine rings. A morphism consists of a ring homomorphism*

$$\phi : A \to B$$

*such that $[\mathfrak{p}] \in Y \implies [\phi^{-1}(\mathfrak{p})] \in X$*

Note that in the case $(A, \mathrm{Spec}(A))$ then this consists of all ring homomorphisms. In the case $(A, \mathrm{Specm}(A))$,$(B, \mathrm{Specm}(B))$ where $A, B$, are f.g. $k$-algebras then a similar statement holds because

**Lemma 14.** *Let $\phi : A \to B$ be a morphism of finitely-generated $k$-algebras, then the inverse image of a maximal ideal is maximal.*

*Proof.* We know $\phi^{-1}(\mathfrak{m})$ is at least prime and this induces an injection $A/\phi^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$. Zariski's Lemma [Mil14, Theorem 13.1] implies that $B/\mathfrak{m}$ is a finite $k$-module. Therefore $\bar{A} = A/\phi^{-1}(\mathfrak{m})$ is a subring of the field $B/\mathfrak{m}$, and by [Sta15, 0BID] must also be a field. This shows that $\mathfrak{m}$ is a maximal ideal as required. □

**Remark 17.** *This works for Jacobson rings if we assume in addition that $\phi$ is of finite type (or integral)*

## 2.6 Structure Sheaf of an Algebraic Set (alg. closed case)

In this section we assume that $k$ is algebraically closed. Let $X = V(\mathfrak{a})$ be an algebraic set. We define the ring of regular functions over $U$ as follows

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

where regular at $P$ means that it is locally of the form $g(Q)/h(Q)$ for $g, h \in k[X]$ and $Q \in V$ for some neighbourhood $V$ of $P$. The fact this is determined locally means it constitutes a sheaf

**Definition 18.** *Sheaf*
*Let $X$ be a topological space. We say $\mathcal{O}_X$ is a pre-sheaf of rings (or $k$-algebras, abelian groups etc) if*

- *For every open set $U \subseteq X$ there is a corresponding ring $\mathcal{O}_X(U)$*
- *For every pair $V \subseteq U$ there is a restriction morphism $\rho_{UV} : \mathcal{O}_X(U) \longrightarrow \mathcal{O}_X(V)$*
- *The restriction morphisms are transitive in the sense that $\rho_{VW}\rho_{UV} = \rho_{UW}$ and $\rho_{UU} = \mathbf{1}$*

*We say elements of $\mathcal{O}_X(U)$ are sections. For a section $\sigma \in \mathcal{O}_X(U)$, use the notation $\sigma|_V = \rho_{UV}(\sigma)$.*
*In addition we say that $\mathcal{O}_X(U)$ is a sheaf if it satisfies the following glueing conditions*

- *Given $\sigma, \tau \in \mathcal{O}_X(U)$ and an open covering $U = \bigcup_{i\in I} U_i$, then*

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

- *Given an open covering $U = \bigcup_{i\in I} U_i$ and sections $\sigma_i \in \mathcal{O}_X(U_i)$, then these lift to a unique section $\sigma$ provided the glueing condition is satisfied*

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

  *That is there exists $\sigma \in \mathcal{O}_X(U)$ such that $\sigma|_{U_i} = \sigma_i$.*

*Furthermore*

It's reasonably clear that this a sheaf by definition and moreover for any $f \in k[X]$ there is a natural map

$$\begin{aligned} k[X]_f = k[X][1/f] &\longrightarrow \mathcal{O}_X(D(f)) \\ \frac{a}{f^r} &\longrightarrow \left(P \to \frac{a(P)}{f(P)^r}\right) \\ D(f) &:= \{P \mid f(P) \neq 0\} \end{aligned}$$

It can be shown that these are in general isomorphisms

**Proposition 15.** *The natural map*

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

*is an isomorphism and in particular*

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

*Proof.* This is adapted from `http://www.math.leidenuniv.nl/~edix/teaching/2010-2011/AG-mastermath/ag.pdf` Theorem 6.1.6
Let $\phi$ 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.

□

When $X$ is irreducible the situation is easier to understand. Recall in this case every non-empty open set is dense and $k[X]$ is an integral domain. Define $k(X)$ to be the ring of fractions. We claim there is a well-defined injection

$$\mathcal{O}_X(U) \hookrightarrow k(X)$$

This is well-defined and injective essentially because regular functions which agree on a dense open set are equal (and every open set is dense). Therefore any representative will do and

$$\mathcal{O}_X(U) = \bigcap_{x \in U} k[X]_{\mathfrak{m}_x} \subseteq k(X)\,.$$

It then follows from the ring-theoretic result

$$A_f = \bigcap_{f \notin \mathfrak{m}} A_{\mathfrak{m}}$$

and the correspondence between points and maximal ideals.

## 2.7 Structure Sheaf of an (Affine) Ring

When $X = \mathrm{Spec}(A)$ then no condition is required as the inverse image of a prime ideal is always prime. Finally we may generalize the structure sheaf construction using Proposition (...) as motivation

**Proposition 16.** *Let $(A, X)$ be an affine ring with the Zariski Topology. Define as follows*

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

*Then*

1. *The natural localization maps make $\mathcal{O}_X$ into a pre-sheaf*
2. *There is a canonical isomorphism $A_f \to \mathcal{O}_X(D(f))$ which also respects the localization maps*
3. *$\mathcal{O}_X$ is a sheaf*

**Remark 19.** *This construction is somewhat non-standard (see [Sta15, 01HR], [Sta15, 009H]), in that one normally defines the sheaf according to $\mathcal{O}_X(D(f)) = A_f$ and show that it is a presheaf, and extends uniquely to a sheaf with the same sections. We prefer this construction because*

- *It is immediate that $\mathcal{O}_X$ is a pre-sheaf*
- *The connection to the corresponding construction in the domain case is clear*
- *It obviates the need for a sheafification construction*
- *The stalk isomorphism $\mathcal{O}_{X,x} = A_{\mathfrak{p}}$ is clear*

In the next section we complete the (mostly formal) proof of these facts.

### 2.7.1 Formal Results on Localization

**Definition 20.** *Multiplicatively closed subset*
*Let $A$ be a ring and $S \subseteq A$ a subset. We say $S$ is multiplicatively closed (m.c.) if*

$$x, y \in S \implies xy \in S$$

*Furthermore we say that $S$ is saturated*

$$x, y \in S \iff xy \in S$$

**Example 21.** *The multiplicative group of units $A^\star$ is a saturated m.c. set.*

**Example 22.** *The set $S_f := \{1, f, f^2, \dots, \}$ is m.c., but not necessarily saturated. As an example consider $A = \mathbb{Z}$ and $S_n = \{1, n, n^2, \dots\}$ for $n$ composite. Then $pq \in S_n$ but $p \notin S_n$.*

**Example 23.** *The set $A \setminus \mathfrak{p}$ is a saturated multiplicatively closed set. More generally any set of the form*

$$A \setminus \bigcup_{\mathfrak{p} \in U} \mathfrak{p} =: \Delta(U)$$

*is a saturated multiplicatively closed subset.*

We define the localization at a set $S$ to be the solution to universal problem

**Definition 24.** *Localization*
*Let $A$ be a ring and $S$ a multiplicatively closed subset. We say that the pair $(i_S, S^{-1}A)$ is localization of $A$ at $S$ if*

- *$S^{-1}A$ is a ring*
- *$i_S : A \to S^{-1}A$ is a ring morphism such that $i_S(S) \subseteq \left(S^{-1}A\right)^\star$*
- *For any other $\phi : A \to B$ such that $\phi(A) \subseteq B^\star$ there exists a unique $\tilde{\phi}$ making the following diagram commute*

$$\begin{array}{ccc} A & \xrightarrow{i_S} & S^{-1}A \\ & \searrow^{\phi} & \downarrow{\scriptstyle \tilde{\phi}} \\ & & B \end{array}$$

**Example 25.** *The case $k[V]$ makes the intuition clearer, for given a m.c. set $S \subseteq k[V]$ then $S^{-1}k[V]$ consists of rational polynomial functions which are well-defined (and regular) on the open set $V \setminus V(S)$. The substance of Proposition 15 is that in the case $S = S_f$ this accounts for* all *the regular functions (for $S^{-1}k[V] = k[V]_f$).*

Clearly localization is unique up to a unique isomorphism. There is a canonical construction as ring of fractions

**Proposition 17.** *Let $A$ be a ring and $S$ a multiplicatively closed subset. Then $(i_S, S^{-1}A)$ exists and is given by*

$$\begin{aligned} S^{-1}A &= \left\{ \frac{a}{s} \mid a \in A, s \in S \right\} / \sim \\ \frac{a}{s} \sim \frac{a'}{s'} &\iff s''(as' - a's) = 0 \text{ for some } s'' \in S \end{aligned}$$

*and*

$$i_S(s) = \frac{s}{1}$$

*The ring operations are the obvious ones*

$$\begin{aligned} \frac{a}{s} + \frac{a'}{s'} &= \frac{as' + a's}{ss'} \\ \frac{a}{s}\frac{a'}{s'} &= \frac{aa'}{ss'} \end{aligned}$$

As this is elementary we omit the proof. Now fix a ring $A$ and localizations $S^{-1}A$ for all multiplicatively closed subsets $S \subseteq A$. We consider the relationships between different localizations. First we define the saturation of a multiplicatively closed set to be

$$\overline{S} := i_S^{-1}\left((S^{-1}A)^\star\right)$$

One may show that it's independent of the concrete realization of $S^{-1}A$ because a ring isomorphism will preserve the group of units. Furthermore it's saturated because the group of units are. So we can state the following

**Lemma 18.** *Let $A$ be a ring and consider two m.c. sets $S, T$. Then*

- $\overline{S} = \{t \in A \mid at \in S\, a \in A\}$
- *$\overline{S}$ is the smallest saturated m.c. set containing $S$ and $\overline{\overline{S}} = \overline{S}$.*
- *There exists a morphism $i_{ST} : S^{-1}A \to T^{-1}A$ such that $i_{ST} \circ i_S = i_T$ iff $S \subseteq \overline{T}$ iff $\overline{S} \subseteq \overline{T}$. In this case it is unique.*
- $i_{SS} = \mathbf{1}$
- *Given a third m.c. set $U$, then $i_{TU} \circ i_{ST} = i_{SU}$ whenever this is well-defined*
- *$i_{ST}$ is an isomorphism iff $\overline{S} = \overline{T}$.*
- *$i_{S\overline{S}}$ is an isomorphism*

*Proof.* This is shown in the appendix. □

Finally we show the hopefully obvious result

**Lemma 19.** *Let $A$ be a ring and $S_i$ a directed family of m.c. sets ordered by inclusion such that $S = \bigcup_{i \in I} S_i$ is also m.c. Then there is a natural isomorphism*

$$\varinjlim S_i^{-1}A \longrightarrow S^{-1}A$$

### 2.7.2 $\mathcal{O}_{\mathrm{Spec}(A)}$ is a sheaf

The case that $A$ is a domain is somewhat easier because we have all localizations as subrings of $\mathrm{Frac}(A)$, then

$$\Delta(U)^{-1}A = \bigcap_{\mathfrak{p}\in U} A_{\mathfrak{p}}\,.$$

and the restriction maps $\rho_{UV} : \Delta(U)^{-1}A \to \Delta(V)^{-1}A$ are just the inclusion maps, which are then clearly transitive. To prove the general case we introduce some formalism

**Corollary 1.** *$\mathcal{O}_X$ is a presheaf*

We will need a preliminary result

**Lemma 20.** *With the notation as before we have*

$$s \in \Delta(D(f)) \iff f^n = cs \quad c \in A\ n \geq 0 \iff s \in \overline{S_f}$$

*Proof.* This follows from the Nullstellensatz and the earlier characterization of $\overline{S_f}$.

$$\begin{aligned} s \in \Delta(D(f)) &\iff (f \notin \mathfrak{p} \implies s \notin \mathfrak{p}) \iff D(f) \subseteq D(s) \iff V((s)) \subseteq V((f)) \\ &\iff \sqrt{(f)} \subseteq \sqrt{(s)} \iff f \in \sqrt{(s)} \\ &\iff cs = f^n \iff cs \in S_f \iff s \in \overline{S_f} \end{aligned}$$

□

From this it easily follows

**Lemma 21.** *Let $f \in A$ be a non-zero element then there is a commutative diagram*

$$\begin{array}{ccc} A & \xrightarrow{\simeq} & \mathcal{O}_X(X) \\ \downarrow & & \downarrow \\ A_f & \xrightarrow{\simeq} & \mathcal{O}_X(D(f)) \end{array}$$

*where all the maps are of the form $i_{ST}$ and the horizontal arrows are isomorphisms.*

*Proof.* The only non-trivial part is the bottom arrow is an isomorphism, but this follows from the fact just proven $\Delta(D(f)) = \overline{S_f}$ and Lemma 18. □

Finally what's left to show is that it is a sheaf. First we show the following formal result

**Lemma 22.** *Let $(A, X)$ be an affine ring and $U \subseteq X$ an open set. Define the map*

$$\begin{aligned} i : U &\longrightarrow \mathrm{Spec}(\Delta(U)^{-1}A) \\ \mathfrak{p} &\longrightarrow \mathfrak{p}\Delta(U)^{-1}A \end{aligned}$$

*Then $i$ is a continuous bijection onto a set $U'$ which also satisfies (4) with respect to the ring $\Delta(U)^{-1}A$. Moreover we have by formal properties of localization*

$$i_\star\left(\mathcal{O}_X|_U\right) \simeq \mathcal{O}_{U'}$$

*When $X = \mathrm{Spec}(A)$ (resp. $\mathrm{Specm}(A)$) then $i$ is a surjection onto $\mathrm{Spec}(\Delta(U)^{-1}A)$ (resp. $\mathrm{Specm}(\Delta(U)^{-1}A)$).*

This means we can reduce to the case $U = X$. Consider an open cover $X = \bigcup_i U_i$, which we can assume to be principal, $U_i = D(f_i)$.
Consider a section $a \in \mathcal{O}_X(X)$ such that $a|_{U_i} = 0$. Then $f_i^{n_i} a_i = 0$. As $D(f_i) = D(f_i^{n_i})$ we may w.l.o.g. assume $n_i = 1$. Clearly $\emptyset = \cap_i V(f_i) = V(\sum_i (f_i))$, so by the Nullstellensatz

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

whence there is a finite partition of unity

$$1 = \sum_{i=1}^{n} f_i b_i$$

(in particular we can always reduce to a finite open covering $X = \bigcup_{i=1}^{n} D(f_i)$). Multiplying by $a$ yields $a = 0$ as required.
Now suppose that there are compatible sections $\sigma_i = a_i/s_i \in \mathcal{O}_X(D(f_i))$. Then by an earlier result $c_i s_i = f^{n_i}$ and $a_i/s_i = a_i c_i / f_i^{n_i}$. As $D(f_i) = D(f_i^{n_i})$ we can assume w.l.o.g. that the compatible sections are of the form $a_i/f_i$. Compatibility means there are elements $s_{ij} \in \Delta(D(f_i f_j))$ such that $s_{ij}\,(f_j a_i - f_i a_j) = 0$. Again we have $c_{ij} s_{ij} = (f_i f_j)^{n_{ij}}$ for some $c_{ij} \in A$ and $n_{ij} \in \mathbb{N}$, which implies $(f_i f_j)^N (f_j a_i - f_i a_j) = 0$, where $N = \max_{i,j} n_{ij}$. Note $\sigma_i = a_i f_i^N / f_i^{N+1} = a_i'/f_i^{N+1}$ and $f_j^{N+1} a_i' = f_i^{N+1} a_j'$. Suppose we have a partition of unity

$$1 = \sum_{j=1}^{n} f_j^{N+1} b_j$$

define

$$\sigma = \sum_{j=1}^{n} a_j' b_j \in A = \mathcal{O}_X(X)$$

then

$$\sigma f_i^{N+1} = \sum_{j=1}^{n} a_j' b_j f_i^{N+1} = \sum_{j=1}^{n} f_j^{N+1} b_j a_i' = a_i'$$

which means precisely that $\sigma|_{D(f_i)} = \sigma_i$.

# 3 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 $\phi(q)$.

## 3.1 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

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

with kernel exactly $\{\pm 1\}$ and image the quadratic residues. Therefore $\psi_2$ 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 $C_1$

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

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

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

**Remark 26.** *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*

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

## 3.2 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 27.** *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* $\epsilon$ *the trivial character. When* $G = \mathbb{F}_q^\star$ *by convention we extend the definition to* $0$ *by*

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

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

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

*Proof.* See below. □

**Example 29.** *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 24.** *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 25.** *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

$$N(X^n = a) \quad := \#\{g \mid g^n = a\} = \begin{cases} |G[n]| & a \in G^n \\ 0 & a \notin G^n \end{cases} \tag{5}$$

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

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

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

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

*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 $\lambda_g$ 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 $\lambda_g^j$ is $\exp\left(\frac{2\pi ij}{N}\right)$. Finally as $\zeta_N$ generates $\mu_N$ as a cyclic group of order $N$, the same statement applies to $\lambda_g$ and $\widehat{G}$. □

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

**Lemma 27.** *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 $\chi$ 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 28.** *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 $\lambda_g$ 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 27.

□

**Proposition 29.** *Orthogonality of characters*
*Let $G$ be a finite cyclic group of order $N$ and $n$ a non-zero integer then*

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

*in particular when $n = N$ we have*

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

*Proof.* When $a \in G^n$ then by Lemma 28, we have $\chi(a)$ for each term in the sum and Proposition 27 gives the order. When $a \notin G^n$ then by Lemma 28 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 23. This follows from combining Proposition 29 and the fact $N(X^n = a) = |G[n]|$ from Proposition 25 □

## 3.3 Gauss and Jacobi Sums

Let $\psi$ be a non-trivial additive character on $\mathbb{F}_q$ and $\chi$ 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 $\chi$ 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 30.** *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 Proofs

We prove Lemma 18

*Proof.* These are essentially straightforward consequences of the universal property of localization.

- $s \in \overline{S} \implies \frac{s}{1}\frac{a}{t} = 1 \implies (as - t)t' = 0 \implies (at')s \in S$. Similarly $as = t \implies \frac{s}{1}\frac{a}{t} = 1$.
- As noted before $\overline{S}$ is saturated because $(S^{-1}A)^\star$ is. Suppose that $S' \supseteq S$ is also saturated. Let $s \in \overline{S}$, then $as \in S \subseteq S' \implies s \in S'$. Therefore $\overline{S} \subseteq S'$ as required. As $\overline{S}$ is saturated, this implies $\overline{\overline{S}} = \overline{S}$.
- Note that $i_T(S) \subseteq \left(T^{-1}A\right)^\star \iff S \subseteq \overline{T}$, so in this case the existence and uniqueness of $i_{ST}$ is guaranteed by the universal property. Conversely if $i_{ST}$ exists then $i_T(S) = i_{ST}i_S(S) \subseteq i_{ST}((S^{-1}A)^\star) \subseteq (T^{-1}A)^\star \implies S \subseteq \overline{T}$. Finally $S \subseteq \overline{T} \implies \overline{S} \subseteq \overline{T}$ by the characterization of $\overline{S}$ as the smallest saturated m.c. set containing $S$.
- $\mathbf{1}$ satisfies the same property as $i_{SS}$ so follows from uniqueness
- Again this follows from uniqueness $(i_{TU} \circ i_{ST}) \circ i_S = i_{TU} \circ i_T = i_U = i_{SU} \circ i_S$
- If $i_{ST}$ is an isomorphism, then $i_{TS}$ exists satisfying the same relation therefore $\overline{S} \subseteq \overline{T}$ and $\overline{T} \subseteq \overline{S}$ by a previous result. Conversely $\overline{S} = \overline{T}$ means there exists $i_{ST}$ and $i_{TS}$, and the previous result implies $i_{ST} \circ i_{TS} = i_{SS} = \mathbf{1}$, so $i_{ST}$ is an isomorphism.
- This follows from previous result and $\overline{S} = \overline{\overline{S}}$

□

# References


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

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

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