# Algebra, Geometry and Number Theory

David Rufino

August 25, 2021

# Contents

# Chapter 1

# Introduction

The main purposes of these notes is to provide a detailed expositions of Galois Theory, Algebraic Number Theory, Algebraic Varieties over non-algebraically closed fields and Schemes, with particular interest in the Weil Conjectures. As such the section on Algebra, whilst broad, doesn't have huge depth, and often straightforward results are stated without proof. I have also tried to be rather explicit in dependence on earlier results, so much use is made of linked references. The section on Algebra largely follows Lang but with some I hope minor improvements in the exposition (e.g. Separability).

For the section on Algebraic Geometry I've tried to simultaneously develop the somewhat "elementary" approach (e.g. Hartshorne I, Kempf, JMilne) alongside the more technically challenging schemes approach (Stacks, Hartshorne II-III, Liu, EGA I) in order to motivate the constructions. I've also tried to adapt the elementary approach to work over non-algebraically closed fields so that it lends itself to talking about the Weil Conjectures at an early stage.

Finally I've included a very small amount of category theory, as it of course a useful language to talk about "universal properties" and helps frame some of the more technical results around schemes.

Some references I found useful

**Set Theory, Lattices**

- Naive Set Theory - Halmos [Hal17]
- Lattice Theory - Birkhoff [Bir40]

**Algebra**

- Algebra - Lang [Lan11]
- Field Theory - Roman [Rom05]
- Introduction to Commutative Algebra - Atiyah, MacDonald [AM69]
- Local Rings - Nagata [Nag75]
- Commutative Algebra II - Zariski-Samuel [ZS76]

**Algebraic Geometry**

- Algebraic Geometry - Hartshorne [Har13]
- Algebraic Geometry - Milne [Mil17]
- Basic Algebraic Geometry - Shafarevich [Sha94]
- Introduction to Algebraic Geometry - Lang [Lan19]
- Elements of Algebraic Geometry (EGA) - Grothendieck

**Geometry**

# Chapter 2

# Foundations

## 2.1 Set Theory

### 2.1.1 Relations

**Definition 2.1.1** (Binary Relation)
*A **binary relation** (or just **relation**) $R$ on a pair of sets $(X, Y)$ is subset of the cartesian product $X \times Y$. We write $xRy$ to mean precisely $(x, y) \in R$.*

**Definition 2.1.2** (Converse Relation)
*Let $R$ be a binary relation on $(X, Y)$ then we the converse relation $R^T$ on $(Y, X)$ given by*

$$yR^T x \iff xRy$$

**Definition 2.1.3** (Domain and Range)
*Let $R$ be a relation on $(X, Y)$. We define the **domain** of $R$ to be*

$$\mathrm{dom}(R) := \{x \in X \mid \exists y \in Y \text{ s.t. } xRy\}$$

*and the **range** of $R$*

$$\mathrm{range}(R) := \{y \in X \mid \exists x \in X \text{ s.t. } xRy\}$$

**Definition 2.1.4** (Equivalence Relation)
*Let $R$ be a binary relation on $(X, X)$. It is said to be*

a) ***reflexive** if $xRx$ for all $x \in X$*

b) ***symmetric** if $xRy \implies yRx$ for all $x, y \in X$*

c) ***transitive** if $xRy \wedge yRz \implies xRz$ for all $x, y, z \in X$*

*A relation which satisfies all these properties is called an **equivalence relation** on $X$. In this case we would write*

$$x \sim y$$

*instead of $xRy$. For an element $x \in X$ denote the **equivalence class** of $x$ by*

$$[x]_R = \{y \mid xRy\}$$

*Note that $R^T = R$.*

**Definition 2.1.5** (Partition)
*Let $X$ be a set an $\mathcal{F}$ a family of subsets of $X$. It is said to be a **partition** if*

a) $X = \bigcup_{A \in \mathcal{F}} A$

b) $A, B \in \mathcal{F} \implies A = B$ *or* $A \cap B = \emptyset$

**Proposition 2.1.6** (Equivalence Classes form a Partition)
*Let $E$ be an equivalence relation on $X$. The family*

$$\mathcal{F} = \{[x]_E \mid x \in X\}$$

*forms a partition of $X$. Denote by $X/E$ the family of equivalence classes, called the **quotient** of $X$ with respect to $E$.*

*Proof.* It's clear that

$$X = \bigcup_{A \in \mathcal{F}} A$$

because by reflexive-ness $x \in [x]_E$ for all $x \in X$.

We claim that for any $z \in [x]_E$ we have $[z]_E = [x]_E$. Suppose $y \in [x]_E$ then $xRz$ and $xRy$. By symmetry and transitivity we then have $zRy$ which implies $y \in [z]_E$. In other words $[x]_E \subseteq [z]_E$. By symmetry of $R$ we have $x \in [z]_E$, so by the same token $[z]_E \subseteq [x]_E$, which shows they are equal.

Therefore it's clear that $[x]_E \cap [y]_E \neq \emptyset \implies [x]_E = [y]_E$ and thus $\mathcal{F}$ forms a partition. □

**Definition 2.1.7** (Composition of Relation)
*Suppose $R$ is a relation on $(X, Y)$ and $S$ a relation on $(Y, Z)$. We define the composition $S \circ R$ on $(X, Z)$*

$$S \circ R = \{(x, z) \mid \exists y \in Y \text{ s.t. } xRy \text{ and } yRz\}$$

### 2.1.2 Functions

**Definition 2.1.8** (Function)
*A **function** $f : X \to Y$ consists of a binary relation $\Gamma(f)$ on $(X, Y)$ such that*

- $\mathrm{dom}(f) = X$
- $\Gamma(f)$ *is* ***single-valued*** *that is $x\Gamma(f)y \wedge x\Gamma(f)y' \implies y = y'$*

*Equivalently for all $x \in X$ there exists precisely one $y \in Y$ such that $x\Gamma(f)y$.*

*We write $f(x) = y$ for the unique element $y \in Y$ such that $x\Gamma(f)y$.*

**Proposition 2.1.9** (Equality of Functions)
*Two functions $f, g : X \to Y$ are equal if and only if $f(x) = g(x)$ for all $x \in X$.*

**Proposition 2.1.10** (Composition of Functions)
*Let $f : X \to Y$ and $g : Y \to Z$ be functions then the composition $\Gamma(g) \circ \Gamma(f)$ is still a function, which we write $g \circ f$, and*

$$(g \circ f)(x) = g(f(x))$$

*Furthermore composition is* ***associative*** *in the sense that*

$$(h \circ g) \circ f = h \circ (g \circ f)$$

**Definition 2.1.11** (Injective, Surjective and Bijective)
*Let $f : X \to Y$ be a function then we say*

- *$f$ is* ***injective*** *if $f(x) = f(x') \implies x = x'$*
- *$f$ is* ***surjective*** *if for all $y$ there exists $x$ such that $f(x) = y$*
- *$f$ is* ***bijective*** *if it is both injective and surjective*

**Definition 2.1.12** (Inverse Function)
*Let $f : X \to Y$ and $g : Y \to X$ be functions. We say*

- *$g$ is a* ***left inverse*** *for $f$ if $g \circ f = 1_X$*
- *$g$ is a* ***right inverse*** *for $f$ if $f \circ g = 1_Y$*
- *$g$ is a* ***two-sided inverse*** *for $f$ if it is both a left and right inverse*

**Proposition 2.1.13**
*Let $f : X \to Y$ be a function then*

- *$f$ is* ***injective*** *if and only if it has a* ***left inverse***
- *$f$ is* ***surjective*** *if and only if it has a* ***right inverse***
- *$f$ is* ***bijective*** *if and only if it has a* ***two-sided inverse***

**Definition 2.1.14** (Idempotent Function)
*A function $p : X \to X$ is* ***idempotent*** *$p \circ p = p$.*

**Lemma 2.1.15** (Idempotent Criterion)
*Let $p : X \to X$ be a function. Then $\mathrm{Fix}(p) \subseteq \mathrm{Im}(p)$ and these are equal if and only if $p$ is idempotent.*

### 2.1.3 Partial Orders

**Definition 2.1.16** (Poset)
*A binary relation $\leq$ on $(X, X)$ is a **partial order** if*

- ***reflexivity*** $x \leq x$
- ***antisymmetry*** $x \leq y$ *and* $y \leq x \implies y = x$
- ***transitivity*** $x \leq y$ *and* $y \leq z \implies x \leq z$

*We may refer to $(X, \leq)$ as a **partially ordered set** or **poset**.*

*Given a poset $(X, \leq)$ denote the set $X$ with the converse relation by $(X, \leq^d)$. This is the **dual poset** to $(X, \leq)$.*

**Example 2.1.17**
*Let $\mathcal{F}$ be a family of subsets of a fixed set $E$. Then $(\mathcal{F}, \subseteq)$ is a poset ordered under inclusion.*

**Definition 2.1.18** (Top and Bottom)
*Let $(X, \leq)$ we say $\top$ (resp. $\bot$) is a **top element** (resp. **bottom element**) if it is greater than (resp. less than) every element of $x$. In this case it is unique.*

**Definition 2.1.19** (Monotone/Antitone Function)
*Let $(X, \leq)$ and $(Y, \leq)$ be posets. A function $f : X \to Y$ is*

- ***monotone / order-preserving*** *if* $x \leq y \implies f(x) \leq f(y)$
- ***antitone / order-reversing*** *if* $x \leq y \implies f(y) \leq f(x)$
- *a **monotone embedding** if* $x \leq y \iff f(x) \leq f(y)$
- *an **order isomorphism** if it is bijective and monotone*
- *a **dual isomorphism** if it is bijective and antitone*

**Proposition 2.1.20**
*Let $f : X \to Y$ be a monotone function. Then it is an embedding if and only if it is injective.*

In what follows the notion of closure and kernel operator will be important.

**Definition 2.1.21** (Closure operator)
*Let $(X, \leq)$ be a partially ordered set. A function $c : X \to X$ is a **closure operator** if it is*

a) ***extensive*** $x \leq c(x)$

b) ***monotone*** $x \leq y \implies c(x) \leq c(y)$

c) ***idempotent*** $c(c(x)) = c(x)$

**Definition 2.1.22** (Kernel operator)
*Let $(X, \leq)$ be a partially ordered set. A function $\kappa : X \to X$ is a **kernel operator** if it is*

- ***co-extensive*** $\kappa(x) \leq x$
- ***monotone*** $x \leq y \implies \kappa(x) \leq \kappa(y)$
- ***idempotent*** $\kappa(\kappa(x)) = \kappa(x)$

Note these definitions are "dual" with respect to the ordering on $X$.

### 2.1.4 Lattices

Certain families of subsets of algebraic structures (e.g. ideals, subgroups, normal subgroups, submodules) form a "sublattice" of the power set. Certain operations on, and results about, these subsets share common features regardless of the type of algebraic structure. Therefore we detail some elements of "Lattice Theory" (see Birkhoff) which may clarify the exposition.

**Definition 2.1.23** (Upper and Lower Bounds)
*Let $(X, \leq)$ be a poset and $S \subseteq X$. Define the set of **upper bounds** for $S$ by*

$$S^{\uparrow} = \{x \in X \mid s \leq x \quad \forall s \in S\}$$

*and the set of **lower bounds** for $S$ by*

$$S^{\downarrow} = \{x \in X \mid x \leq s \quad \forall s \in S\}$$

*Note by convention $\emptyset^{\uparrow} = \emptyset^{\downarrow} = X$. Furthermore*

$$X^{\uparrow} = \begin{cases} \{\top\} & X \text{ has a top element} \\ \emptyset & \text{otherwise} \end{cases}$$

*and*

$$X^{\downarrow} = \begin{cases} \{\bot\} & X \text{ has a bottom element} \\ \emptyset & \text{otherwise} \end{cases}$$

**Lemma 2.1.24** (Upper/Lower bounds are antitone maps)
*Let $(X, \leq)$ be a poset and $S, T$ subsets of $X$ then*

- ***antitone*** $S \subseteq T \implies T^{\uparrow} \subseteq S^{\uparrow}$ *and* $T^{\downarrow} \subseteq S^{\downarrow}$
- ***unit-counit relations*** $S \subseteq S^{\uparrow\downarrow}$ *and* $T \subseteq T^{\downarrow\uparrow}$
- ***triangular identities*** $S^{\uparrow} = S^{\uparrow\downarrow\uparrow}$ *and* $T^{\downarrow} = T^{\downarrow\uparrow\downarrow}$

*Proof.* We prove only the first triangular identity as the others are straightforward consequences of the definitions. Firstly $S \subseteq S^{\uparrow\downarrow} \implies S^{\uparrow\downarrow\uparrow} \subseteq S^{\uparrow}$ by the antitone property. Given the relation $T \subseteq T^{\downarrow\uparrow}$ substitute $T = S^{\uparrow}$ to get the reverse inclusion. □

**Lemma 2.1.25**
*Let $(X, \leq)$ be a poset and $S, T$ subsets of $X$. Then the intersections $S \cap S^{\uparrow}$ and $T \cap T^{\downarrow}$ contain at most one element.* ***When they exist*** *write the elements as $\top_S$ and $\bot_T$ respectively, and are referred to as the* ***maximum*** *and* ***minimum*** *elements respectively.*

*Proof.* Given $x, y \in S \cap S^{\uparrow}$ then by definition $x \leq y$ and $y \leq x$. By anti-symmetry we have $x = y$ as required. □

**Definition 2.1.26** (Supremum and Infimum)
*Let $(X, \leq)$ be a poset and $S \subseteq X$ a subset. We say a* ***supremum*** *of $S$ is the minimal upper bound, i.e. the unique element of*

$$S^{\uparrow} \cap S^{\uparrow\downarrow}$$

*when it exists and write this as* $\sup S$*. Similarly an* ***infimum*** *of $S$ is the maximal lower bound, i.e. the unique element of*

$$S^{\downarrow} \cap S^{\downarrow\uparrow}$$

*when it exists and write this as* $\inf X$*.*

**Lemma 2.1.27** (Maximum = Supremum)
*Let $(X, \leq)$ be a poset and $S \subseteq X$ a subset. Then $\top_S$ exists if and only if* $\sup S$ *exists and is a member of $S$. In this case* $\top_S = \sup S$*.*

**Lemma 2.1.28**
*Let $(X, \leq)$ be a poset. Then $\{\sup S\}^{\uparrow} = S^{\uparrow}$ and $\{\inf T\}^{\downarrow} = T^{\downarrow}$ when these exist.*

**Lemma 2.1.29** (Sup is monotone and Inf is antitone)
*Let $(X, \leq)$ be a poset and $S, T$ subsets of $X$. Then $S \subseteq T \implies \sup S \leq \sup T$ and $\inf T \leq \inf S$ when these exist.*

*Proof.* Note $S \subseteq T \implies T^{\uparrow} \subseteq S^{\uparrow}$ so $\sup T \in S^{\uparrow}$. By definition $\sup S \in S^{\uparrow\downarrow}$ therefore $\sup S \leq \sup T$.

Similarly $S \subseteq T \implies T^{\downarrow} \subseteq S^{\downarrow}$. By definition $\inf T \in T^{\downarrow} \implies \inf T \in S^{\downarrow}$. By definition $\inf S \in S^{\downarrow\uparrow}$ therefore $\inf T \leq \inf S$. □

**Remark 2.1.30**
*Note that $\emptyset^{\uparrow} = X$ and therefore* $\sup \emptyset = \bot$ *when it exists. Similarly* $\inf \emptyset = \top$ *when it exists.*

*When $\top$ exists* $\sup X = \top$*, otherwse it is not defined. Similarly when $\bot$ exists* $\inf X = \bot$*, otherwise it is not defined.*

**Definition 2.1.31** (Lattice)
*A poset $(X, \leq)$ is a* ***lattice*** *if every pair of elements $x, y$ admits both a supremum and infimum. In this case we write*

$$a \vee b := \sup\{a, b\}$$

*and*

$$a \wedge b := \inf\{a, b\}$$

*These are called the **join** and **meet** operations.*

*Similarly it is a **complete lattice** if every subset $S$ admits both a supremum and infimum. This is written*

$$\bigvee S := \sup S$$

*and*

$$\bigwedge S := \inf S$$

*Note a complete lattice has both a top and a bottom element (by considering $\sup \emptyset$ and $\inf \emptyset$), and a lattice admits **finite** joins and meets.*

*Trivially*

$$\bigwedge \{x\} = \bigvee \{x\} = x$$

**Example 2.1.32** (Power Set)
*For a fixed set $E$ the collection of subsets $\mathcal{P}(E)$ is a complete lattice under the union and intersection operator **with the convention that empty intersection is the whole set and empty union is the empty set***

*In this case $\top = E$ and $\bot = \emptyset$.*

Verifying a poset is a lattice is slightly easier than it may first appear.

**Lemma 2.1.33** (Supremum is Infimum of upper bounds)
*Let $(X, \leq)$ be a poset and $S$ a subset of $X$. Then*

$$\sup S = \inf S^{\uparrow}$$

*when either exists. Dually*

$$\inf S = \sup S^{\downarrow}$$

*Proof.* By definition $\sup S$ is the unique element of $S^{\uparrow} \cap S^{\uparrow\downarrow}$ and $\inf S^{\uparrow}$ is the unique element of $S^{\uparrow\downarrow} \cap S^{\uparrow\downarrow\uparrow}$. By (2.1.24) $S^{\uparrow\downarrow\uparrow} = S^{\uparrow}$ so they are equivalent. □

**Proposition 2.1.34** (Criteria to be a Complete Lattice)
*Let $(X, \leq)$ be a poset. Then the following are equivalent*

a) *$X$ is a complete lattice*

b) *$X$ admits arbitrary infimums (and in particular has $\top = \inf \emptyset$)*

c) *$X$ admits arbitrary supremums (and in particular has $\bot = \sup \emptyset$)*

*In this case we have the relationships*

$$\bigvee S = \bigwedge S^{\uparrow}$$
$$\bigwedge S = \bigvee S^{\downarrow}$$

*Proof.* $1 \implies 2, 3$ is clear.

$2, 3 \implies 1$ follows from the previous Lemma. □

**Lemma 2.1.35**
*Let $(X, \leq)$ be a poset and $(Y, \leq)$ a sub-poset. Let $S \subseteq Y$ be a subset. Then $\inf_Y S$ exists if and only if $\inf_X S$ exists and belongs to $Y$. In this case they are equal.*

*Proof.* Note in general that $T^{\downarrow, Y} = T^{\downarrow, X} \cap Y$ and $T^{\uparrow, Y} = T^{\uparrow, X} \cap Y$. Therefore

$$S^{\downarrow, Y} \cap S^{\downarrow\uparrow, Y} = S^{\downarrow, X} \cap S^{\downarrow\uparrow, X} \cap Y$$

Recall $\inf S$ is the unique element of $S^{\downarrow} \cap S^{\downarrow\uparrow}$ if it exists. Then the result follows easily. □

**Definition 2.1.36** (Moore Family)
*Let $(X, \leq)$ be a complete lattice. A sub-poset $(Y, \leq)$ is a **Moore family** over $X$ if it satisfies the following property*

$$S \subseteq Y \implies \bigwedge_X S \in Y$$

*In particular this includes the case $S = \emptyset$ and so $\top \in Y$.*

**Example 2.1.37** (Moore family of sets)
*Given a fixed set $E$, then $\mathcal{P}(E)$ is a complete lattice ordered under inclusion. Then a family of subsets $\mathcal{F}$ is a Moore family precisely when*

- $E \in \mathcal{F}$
- $A_{i\in I} \in \mathcal{F} \implies \bigcap_{i\in I} A_i \in \mathcal{F}$

**Proposition 2.1.38** (Equivalent Formulations of Complete Sub-lattice)
*Let $(X, \leq)$ be a complete lattice and $(Y, \leq)$ a sub-poset. Then the following are equivalent*

a) *$(Y, \leq)$ is a Moore family*

b) *$(Y, \leq)$ is a complete lattice*

c) *$Y$ is the image of some closure operator $c : X \to X$*

*In this case the closure operator is given by*

$$c(x) = \bigwedge_X \{y \in Y \mid x \leq y\}$$

*For $S \subseteq Y$*

$$\bigwedge_Y S = \bigwedge_X S$$

$$\bigvee_Y S = c\left(\bigvee_X S\right)$$

*and for $S \subseteq X$ we have*

$$c(\bigvee_X S) = \bigwedge_X (S^\uparrow \cap Y)$$

*Proof.* $1 \implies 2)$ By (2.1.35) $S \subseteq Y \implies \bigwedge_Y S = \bigwedge_X S$. By (2.1.34) then $Y$ is a complete lattice.

$2 \implies 3)$ Suppose that $(Y, \leq)$ is a complete lattice then define the function $c : X \to X$ by $c(x) = \bigwedge_X \Gamma_x$ where $\Gamma_x = \{y \in Y \mid x \leq y\}$. We need to show that it is a closure operator. Evidently $x \in \Gamma_x^\downarrow$ and $c(x) \in \Gamma_x^{\downarrow\uparrow}$ by definition of infimum. Therefore $x \leq c(x)$ and $c$ is extensive. Note $x \leq y \implies \Gamma_y \subseteq \Gamma_x$. By (2.1.29) we have $\inf \Gamma_x \leq \inf \Gamma_y$, whence $c(x) \leq c(y)$ and $c$ is monotone.

$Y$ is a complete lattice, so by (2.1.35) we have $c(x) \in Y$ so that $\mathrm{Im}(c) \subseteq Y$. We claim that $x \in Y \implies c(x) = x$. In this case $x \in \Gamma_x$ and $c(x) \in \Gamma_x^\downarrow$ whence $c(x) \leq x$ and therefore $x = c(x)$ as required. Therefore $Y \subseteq \mathrm{Fix}(c) \subseteq \mathrm{Im}(c) \subseteq Y$, whence $Y = \mathrm{Im}(c) = \mathrm{Fix}(c)$ and $c$ is idempotent by (2.1.15). As $c$ is extensive, monotone and idempotent it is by definition a closure operator.

$3 \implies 1)$ In order for $Y := \mathrm{Im}(c)$ to be a Moore family, we need to show $S \subseteq Y \implies \bigwedge_X S \in Y$. We claim that by properties of $c$ we have

$$S \subseteq Y \implies c(S^\downarrow) \subseteq S^\downarrow$$
$$T \subseteq X \implies c(T^\uparrow) \subseteq T^\uparrow$$

Therefore $c$ maps the singleton set $S^\downarrow \cap S^{\downarrow\uparrow} = \{\bigwedge_X S\}$ to itself. In otherwords $\bigwedge_X S \in \mathrm{Fix}(c) = \mathrm{Im}(c) = Y$ as required. Define $\Gamma_x := \{y \in Y \mid x \leq y\}$. We wish to show that $c(x) = \bigwedge_X \Gamma_x$. As $x \leq c(x)$ we have $c(x) \in \Gamma_x$. Furthermore $y \in \Gamma_x \implies c(x) \leq c(y) = y$. So $c(x) \in \Gamma_x^\downarrow$. Therefore $c(x) = \bot_{\Gamma_x} = \bigwedge_X \Gamma_x$ as required.

Finally by (2.1.28) $\{\bigvee_X S\}^\uparrow = S^\uparrow$ for any $S \subseteq X$. Therefore, as $c(x) = \bigwedge_X \Gamma_x$ we find

$$c(\bigvee_X S) = \bigwedge_X \left(\left\{\bigvee_X S\right\}^\uparrow \cap Y\right) = \bigwedge_X (S^\uparrow \cap Y)$$

as required. In particular when $S \subseteq Y$ we find by (2.1.38)

$$\bigvee_Y S = \bigwedge_Y S^{\uparrow,Y} = \bigwedge_X S^{\uparrow,Y} = \bigwedge_X (S^\uparrow \cap Y) = c(\bigvee_X S) \tag{2.1}$$

□

**Remark 2.1.39**
*For a given complete lattice $(X, \leq)$ we have established a correspondence between*

$$\Big\{\text{closure operators } c : X \to X\Big\} \longleftrightarrow \Big\{\text{complete sub-lattices } (Y, \leq)\Big\}$$

**Corollary 2.1.40** (Moore family admits a closure operator)
*Let $E$ be a fixed set and $\mathcal{F}$ a Moore family over $(\mathcal{P}(E), \subseteq)$. Then there exists a surjective closure operator $c : \mathcal{P}(E) \to \mathcal{F}$ given by*

$$c(F) = \bigcap_{F \subseteq E_\alpha \in \mathcal{F}} E_\alpha$$

*Any such closure operator $c : \mathcal{P}(E) \to \mathcal{P}(E)$ gives rise to a Moore family $\mathcal{F} := \mathrm{Im}(c)$.*

**Proposition 2.1.41** (Alternative expression for join)
*Let $(X, \leq)$ be a complete lattice and $c : X \to X$ a closure operator with image $Y$. Then for any subset $S \subset X$*

$$c(\bigvee_X S) = c(\bigvee_X c(S)) = \bigvee_Y c(S) = \bigwedge_X \left(S^\uparrow \cap Y\right)$$

*i.e. it's the smallest "closed" set containing each element of $S$.*

*Proof.* By (2.1.38) the expression for $c(\bigvee_X S)$ yields

$$c(\bigvee_X c(S)) = \bigwedge_X \left(c(S)^\uparrow \cap Y\right) = \bigwedge_X \left(S^\uparrow \cap Y\right) = c(\bigvee_X S)$$

where the middle equality follows because if $y \in Y$ then $c(s) \leq y \iff s \leq y$. Furthermore $c(S) \subseteq Y$ so the expression for $\bigvee_Y$ yields

$$c(\bigvee_X c(S)) = \bigvee_Y c(S)\,.$$

as required. □

### 2.1.5 Galois Connections

**Definition 2.1.42** (Galois Connection)
*Let $(X, \leq_X)$ and $(Y, \leq_Y)$ be posets. A pair of functions $(f_\star, f^\star)$*

$$X \underset{f_\star}{\overset{f^\star}{\leftrightarrows}} Y$$

*is called an **antitone Galois connection** if it satisfies the **adjoint property***

- $x \leq_X f^\star(y) \iff y \leq_Y f_\star(x) \quad \forall x \in X, y \in Y$

*We say it is a **monotone Galois connection** if instead*

- $x \leq_X f^\star(y) \iff f_\star(x) \leq_Y y \quad \forall x \in X, y \in Y$

*We will assume that if not otherwise specified the connection is antitone.*

**Proposition 2.1.43** (Equivalent Condition for Galois Connection)
*Let $(X, \leq_X)$ and $(Y, \leq_Y)$ be posets. Consider a pair of functions*

$$X \underset{f_\star}{\overset{f^\star}{\leftrightarrows}} Y$$

*Then this constitutes an **antitone Galois Connection** if and only if*

- *$f_\star$ and $f^\star$ are both antitone*
- *$x \leq_X f^\star(f_\star(x))$ and $y \leq_Y f_\star(f^\star(y))$ for all $x \in X, y \in Y$ (i.e. $f^\star \circ f_\star$ and $f_\star \circ f^\star$ are extensive)*

*Similarly it constitutes a **monotone Galois Connection** if and only if*

- *$f_\star$ and $f^\star$ are both monotone*
- *$x \leq_X f^\star(f_\star(x))$ and $f_\star(f^\star(y)) \leq_Y y$ for all $x \in X, y \in Y$*

*Proof.* We consider only the antitone case, as the monotone follows from duality (flip $\leq_Y$).

Suppose that $(f_\star, f^\star)$ satisfies the adjoint property

$$f_\star(x) = f_\star(x) \implies f_\star(x) \leq_Y f_\star(x) \implies x \leq_X f^\star(f_\star(x))$$
$$f^\star(y) = f^\star(y) \implies f^\star(y) \leq_Y f^\star(y) \implies y \leq_Y f_\star(f^\star(y))$$

whence the extensive property follows. Furthermore

$$x \leq_X x' \implies x \leq_X f^\star(f_\star(x')) \implies f_\star(x') \leq_Y f_\star(x)$$
$$y \leq_Y y' \implies y \leq_Y f_\star(f^\star(y')) \implies f^\star(y) \leq_X f^\star(y')$$

which shows that the functions $f_\star$ and $f^\star$ are antitone.

Conversely suppose they satisfy the given conditions. Then by the antitone and extensive properties in turn

$$x \leq_X f^\star(y) \implies f_\star(f^\star(y)) \leq_Y f_\star(x) \implies y \leq_Y f_\star(x)$$

and

$$y \leq_Y f_\star(x) \implies f^\star(f_\star(x)) \leq_X f^\star(y) \implies x \leq_X f^\star(y)\,.$$

which is the adjoint property as required. □

**Definition 2.1.44** (Closed sets)
*Let $(f_\star, f^\star)$ be a Galois connection. Then define the **closed sets** to be*

$$X^\star := f^\star(Y)$$
$$Y^\star := f_\star(X)$$

**Proposition 2.1.45** (Isomorphism on closed sets)
*Consider an antitone (resp. monotone) Galois connection $X \underset{f_\star}{\overset{f^\star}{\leftrightarrows}} Y$. Then it restricts to a dual isomorphism (resp. order isomorphism) on **closed sets***

$$X^\star \underset{f_\star}{\overset{f^\star}{\leftrightarrows}} X_\star$$

*Furthermore the following properties hold*

- $f_\star \circ f^\star \circ f_\star = f_\star$
- $f^\star \circ f_\star \circ f^\star = f^\star$
- *In the antitone case $f^\star \circ f_\star$ and $f_\star \circ f^\star$ are closure operators.*
- *In the monotone case $f^\star \circ f_\star$ is a closure operator and $f_\star \circ f^\star$ is a kernel operator.*
- $X^\star = \mathrm{Fix}(f^\star \circ f_\star) = \mathrm{Im}(f^\star \circ f_\star)$
- $Y^\star = \mathrm{Fix}(f_\star \circ f^\star) = \mathrm{Im}(f_\star \circ f^\star)$

*Proof.* We detail the antitone case as the monotone case follows by duality. We first prove so-called triangular identities, for by the extensive property (2.1.43)

$$x \leq f^\star(f_\star(x)) \implies f_\star(f^\star(f_\star(x))) \leq f_\star(x)$$

and by the other extensive property

$$f_\star(x) \leq f_\star(f^\star(f_\star(x)))$$

whence they are equal. The other case is similar.

It's immediate that $f^\star \circ f_\star$ and $f_\star \circ f^\star$ are idempotent, and they are extensive by (2.1.43). And the composition of two antitone functions is monotone so $f^\star \circ f_\star$ and $f_\star \circ f^\star$ are closure operators.

Observe

$$\mathrm{Im}(f^\star \circ f_\star) \subseteq \mathrm{Im}(f^\star) \subseteq \mathrm{Fix}(f^\star \circ f_\star)$$

where the first inclusion is trivial and the second inclusion follows from the second triangular identity. However both sides are equal by (2.1.15) and the expression for $X^\star$ follows. The expression for $Y^\star$ follows similarly.

This shows that the maps are mutual inverses as required. □

In certain circumstances we may consider a smaller subset of $X$, by applying a suitable closure operator which is compatible with the Galois correspondence :

**Proposition 2.1.46** (Subordinated Closure Operator)
*Let $X \underset{f_\star}{\overset{f^\star}{\leftrightarrows}} Y$ be a Galois connection and $c : X \to X$ be a closure operator with image $X_c$. Then*

$$c(x) \leq (f^\star \circ f_\star)(x) \quad \forall x \in X \iff \mathrm{Im}(f^\star) \subseteq \mathrm{Fix}(c) \iff X^\star \subseteq X_c$$

*In this case*

$$f_\star(c(x)) = f_\star(x)$$

*Proof.* Suppose $c(x) \leq (f^\star \circ f_\star)(x)$. Substitute $x = f^\star(y)$ then, because $c$ is extensive,

$$f^\star(y) \leq c(f^\star(y)) \leq (f^\star \circ f_\star \circ f^\star)(y) = f^\star(y)\,.$$

Therefore $c(f^\star(y)) = f^\star(y)$ and $\mathrm{Im}(f^\star) \subseteq \mathrm{Fix}(c)$ as required. Conversely suppose this holds, then by the monotone property of $c$ and extensive property of $f^\star \circ f_\star$

$$x \leq (f^\star \circ f_\star)(x) \implies c(x) \leq c((f^\star \circ f_\star)(x)) = (f^\star \circ f_\star)(x)\,.$$

as required. Finally by the extensive property of $c$

$$x \leq c(x) \leq (f^\star \circ f_\star)(x)$$

and by the antitone/monotone property of $f_\star$ and triangular identity

$$f_\star(x) \leq f_\star(c(x)) \leq f_\star(x)$$

whence $f_\star(c(x)) = f(x)$ as required.

□

The meaning of the "adjoint" criterion can be explained by the following rather generic situation

**Example 2.1.47** (Canonical example of an antitone Galois connection)
*Suppose there is a predicate*

$$\psi : X \times Y \to \{0, 1\}$$

*Define a connection*

$$\mathcal{P}(X) \underset{f_\star}{\overset{f^\star}{\leftrightarrows}} \mathcal{P}(Y)$$

*by*

$$f_\star(S) = \{y \in Y \mid \psi(x, y) = 1 \quad \forall x \in S\}$$
$$f^\star(T) = \{x \in X \mid \psi(x, y) = 1 \quad \forall y \in T\}$$

*Then*

$$S \subseteq f^\star(T) \iff \psi(s, t) = 1 \quad \forall s \in S \quad t \in T \iff T \subseteq f_\star(S)$$

**Proposition 2.1.48** (Joins under Galois Correspondence)
*Let $(X, \leq_X)$ and $(Y, \leq_Y)$ be complete lattices with an antitone Galois connection $X \underset{f_\star}{\overset{f^\star}{\leftrightarrows}} Y$. Then for $S \subseteq X$*

$$f_\star\left(\bigvee S\right) = \bigwedge f_\star(S)$$

*Similarly for $T \subseteq Y$ we have*

$$f^\star\left(\bigvee T\right) = \bigwedge f^\star(T)$$

*Proof.* Let $a = \bigvee S$ and $b = \bigwedge f_\star(S)$. Then $s \leq a \implies f_\star(a) \leq f_\star(s)$ for all $s \in S$, which implies $f_\star(a) \leq b$. Similarly $b \leq f_\star(s) \implies s \leq f^\star(b)$ by the adjoint criterion. Therefore $a \leq f^\star(b)$ by definition of join, which implies $b \leq f_\star(a)$ by the adjoint criterion again. Whence $f_\star(a) = b$ as required.

The second statement follows from duality. □

### 2.1.6 Axiom of Choice

**Theorem 2.1.49** (Axiom of choice)
*There are a number of essentially equivalent forrmulations of the axiom of choice*

a) *The Cartesian product of a non-empty family of sets is non-empty*

b) *For any set $X$ of non-empty sets there exists a function $f : X \to \bigcup X$ such that $A \in X \implies f(A) \in A$.*

c) ***Zorn's Lemma*** *Suppose a partially ordered set $(X, \leq)$ is such that every chain in $X$ has an upper bound in $X$. Then $X$ contains at least one maximal element.*

d) *Every surjective function has a right inverse.*

**Corollary 2.1.50** (Choose representatives)
*Let $\pi : X \to Y$ be a surjective function and $T \subseteq Y$ a subset. Then there exists a subset $S \subseteq X$ such that $\pi|_S$ is bijective.*

*When $T$ is finite $\#S = \#T$.*

## 2.2 Matroids (Theory of Bases)

The theory of bases of vector spaces (Section 3.4.8) and transcendence bases of field extensions (Section 3.15.11) have some formal similarities (as noted by ...). Here we abstract the common structure, although the results may be proven in a particular case perhaps more directly

**Definition 2.2.1** (Matroid)
*Consider a set $X$ together with a closure operator $c : \mathcal{P}(X) \to \mathcal{P}(X)$ ("span" operator). Furthermore we say*

- *$S \subset X$ is **independent** if $x \in S \implies x \notin c(S \setminus \{x\})$*
- *$\Gamma \subset X$ is **spanning** if $c(\Gamma) = X$.*

*Note by definition $X$ is spanning and $\emptyset$ is independent.*

*We call the pair $(X, c)$ a **matroid** if it also satisfies the following properties*

a) ***Finitary*** *$x \in c(\Gamma) \implies x \in c(\Gamma')$ for $\Gamma'$ a finite subset of $\Gamma$.*

b) ***Exchange Property*** *If $S \subseteq X$ and $x \in c(S \cup \{y\}) \setminus c(S)$ then $y \in c(S \cup \{x\})$.*

*We say $(X, c)$ has **finite rank** if it has a finite spanning set.*

*Finally we say $\mathcal{B} \subseteq X$ is a **basis** if it is both **spanning** and **independent**.*

We begin with some elementary characterizations of independent sets

**Lemma 2.2.2**
*A set $S \subset X$ is independent if and only no proper subset has the same span.*

*Proof.* □

**Lemma 2.2.3** (Finitary Property)
*Every subset of an independent set is independent. Moreover a set is independent if and only if every finite subset is independent.*

*Proof.* This first statement is immediate from the definition.

Suppose $S$ is such that every finite set is independent and $x \in S$ is such that $x \in c(S \setminus \{x\})$. By the finitary property there is a finite set $S' \subset S \setminus \{x\}$ such that $x \in c(S')$. By assumption $S' \cup \{x\}$ is still independent, a contradiction. □

**Lemma 2.2.4**
*Let $S$ be an independent set and $x \notin S$. Then $S \cup \{x\}$ is independent if and only if $x \notin c(S)$.*

*Proof.* Suppose $S$ is independent and $x \notin c(S)$. We require to prove that $y \in S \cup \{x\} \implies y \notin c(S \cup \{x\} \setminus \{y\})$. If $y = x$ then this is true by hypothesis. Otherwise $y \in S$, whence by independence $y \notin c(S \setminus \{y\})$. Then $y \in c(S \cup \{x\} \setminus \{y\}) \implies x \in c(S)$ by the Exchange Property, contradicting the hypothesis.

Conversely suppose $S$ is independent and $x \in c(S) \setminus S$. By definition $S \cup \{x\}$ is not independent. □

The finite support condition ensures that $\mathcal{E}$ is "inductively ordered"

**Lemma 2.2.5**
*Let $\{S_i\}_{i \in I}$ be a chain of independent subsets. Then $S = \bigcup_{i \in I} S_i$ is also independent.*

*Proof.* By the finite support property (2.2.3) its enough to show that any finite subset is independent. Let $S'$ be a finite subset, then by induction we may show that $S' \subseteq S_i$ for some $i \in I$. By (2.2.3) $S'$ is independent as required. □

**Proposition 2.2.6** (Criteria for bases)
*Let $(X, c)$ be a matroid. Then the following are equivalent*

a) *$\mathcal{B}$ is a basis*

b) *$\mathcal{B}$ is a minimal spanning set*

c) *$\mathcal{B}$ is maximally independent (possibly in some spanning set $\Gamma$)*

*Proof.* *a)* $\iff$ *b)* This follows by definition of independent sets.

*a)* $\implies$ *c)* Suppose $\mathcal{B} \subseteq S$ with $S$ independent. Then $X = c(\mathcal{B}) \subseteq c(S)$ whence $c(\mathcal{B}) = c(S)$. By (2.2.2) $\mathcal{B} = S$ as required.

*c* $\implies$ *a)* Suppose $\mathcal{B}$ is not spanning. Observe $\Gamma \subseteq c(\mathcal{B}) \implies X = c(\Gamma) \subseteq c(\mathcal{B})$ a contradiction. Therefore choose $y \in \Gamma \setminus c(\mathcal{B})$. By (2.2.4) then $\mathcal{B} \cup \{y\}$ is independent, contradicting maximality. □

**Proposition 2.2.7** (Basis exists)
*Let $(X, c)$ be a matroid, $S$ independent and $\Gamma$ spanning such that $S \subseteq \Gamma$. Then there exists a basis $\mathcal{B}$ such that $S \subseteq \mathcal{B} \subseteq \Gamma$.*

*In particular a finitely-generated matroid has a finite basis.*

*Proof.* Consider the collection

$$\mathcal{I} = \{T \text{ independent } \mid S \subseteq T \subseteq \Gamma\}$$

then it's easy to see that this is non-empty and chain-complete by (2.2.5). Therefore it has a maximal element by Zorn's Lemma. By (2.2.6) this is a basis. □

**Proposition 2.2.8** (Exchange Lemma)
*Let $(X, c)$ be a matroid, $S$ finite and independent and $\Gamma$ spanning. Then there exists a subset $T \subset \Gamma$ such that*

- *$\#T = \#S$*
- *$(\Gamma \setminus T) \cup S$ is spanning*

*In particular $\#S \leq \#\Gamma$ when $\Gamma$ is finite.*

*Proof.* We proceed by induction on $n = \#S$. Suppose $S' = S \cup \{x\}$ is independent. Then by assumption we have $\Gamma$ such that $\widetilde{\Gamma} := (\Gamma \setminus T) \cup S$ is spanning and $\#T = \#S$. If $\Gamma = T$ then by hypothesis $S$ is spanning whence $x \in c(S)$, contradicting independence. So choose $y \in \Gamma \setminus T$ then by spanning we have

$$x \in c((\widetilde{\Gamma} \setminus \{y\}) \cup \{y\}) \setminus c(S)$$

whence by the Exchange Property we have

$$y \in c((\widetilde{\Gamma} \setminus \{y\}) \cup \{x\}) \setminus c(S)$$

Then define $T' := T \cup \{y\}$. We claim that $\Gamma' := (\Gamma \setminus T') \cup S'$ is spanning. Note that we have $y \in c(\Gamma')$ which implies $c(\{y\}) \subseteq c(\Gamma')$ by idempotence. Therefore

$$X = c(\widetilde{\Gamma}) \subseteq c(\Gamma' \cup \{y\}) \overset{2.1.41}{=} c(c(\Gamma') \cup c(\{y\})) = c(\Gamma')$$

as required. □

**Corollary 2.2.9**
*Every base of a finite rank matroid is finite and of the same size. Denote this by $r(X)$.*

*Proof.* A simple application of (2.2.8). □

**Definition 2.2.10** (Submatroid)
*A subset $Y \subseteq X$ is a **sub-matroid** if $c(Y) = Y$. In this case $S \subseteq Y \implies c(S) \subseteq Y$ and so we have an induced matroid structure $(Y, c)$.*

**Proposition 2.2.11**
*Let $(X, c)$ be a finite-rank matroid and $S \subseteq X$ an independent subset, then $\#S \leq r(X)$. Similarly a spanning subset $\Gamma$ satisfies $\#\Gamma \leq r(X)$.*

**Proposition 2.2.12**
*Let $\mathcal{B}$ be a subset of a finite-rank matroid $(X, c)$. Then the following are equivalent*

a) $\mathcal{B}$ *is a basis*

b) $\mathcal{B}$ *is independent and* $\#\mathcal{B} \geq r(X)$

c) $\mathcal{B}$ *is spanning and* $\#\mathcal{B} \leq r(X)$

*Proof.* Apply (2.2.7) and counting. □

**Proposition 2.2.13**
*Let* $Y \subseteq X$ *be a sub-matroid of a finite-rank matroid. Then* $Y = X \iff r(Y) = r(X)$.

*Proof.* Let $\mathcal{B}$ be a basis for $Y$ then $\#\mathcal{B} = r(Y) = r(X)$ and is a-fortiori independent in $X$. Therefore by (2.2.12) $\mathcal{B}$ is a basis for $X$ and hence $X = c(\mathcal{B}) = Y$. □

## 2.3 Numbers

Informally we consider the set of integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

and the subset of natural numbers

$$\mathbb{N} = \{0, 1, 2, \ldots, \}$$

Although it's possible to construct the integers painstakingly from a small set of axioms (see ...) we instead for brevity simply state the most commonly used results as axioms.

### 2.3.1 Integers

We suppose the existence of a set $\mathbb{Z}$ with distinguished elements $0 \neq 1$ together with

- A binary operation
$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
and an involution
$$(-) : \mathbb{Z} \to \mathbb{Z}$$
satisfying
  - $-0 = 0$
  - $-(-x) = x$
  - $x + 0 = 0 = 0 + x$
  - $x + y = y + x$
  - $(x + y) + z = x + (y + z)$
  - $x + (-x) = 0 = (-x) + x$
  - $-(x + y) = (-x) + (-y)$
- A subset $\mathbb{N}$ such that
  - $0, 1 \in \mathbb{N}$
  - $x, y \in \mathbb{N} \implies x + y \in \mathbb{N}$
  - $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ and $\{0\} = \mathbb{N} \cap -\mathbb{N}$

  which also satisfies the principle of induction
- Let $S \subseteq \mathbb{N}$ be a set such that
  - $0 \in S$
  - $x \in S \implies x + 1 \in S$

  then $S = \mathbb{N}$

It's possible to use these to show the existence of multiplication

**Proposition 2.3.1** (Multiplication exists)
*There exists a binary operation*
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
*such that*

- $x \cdot 0 = 0 = 0 \cdot x$
- $x \cdot 1 = x = 1 \cdot x$
- $xy = yx$
- $(xy)z = x(yz)$
- $x(y+z) = xy + xz$
- $(y+z)x = yx + zx$
- $(-x)(y) = -(xy) = x(-y)$

We may also show the existence a partial ordering

**Proposition 2.3.2** (Order exists)
*There exists a relation $\leq$ on $\mathbb{Z}$ given by*

$$x \leq y \iff y + (-x) \in \mathbb{N}$$

*which satisfies*

$$x \leq y \vee y \leq x$$

$$x \leq y \wedge y \leq x \implies x = y$$

*Define $x < y$ in the obvious way then it satisfies the usual trichotomy law, namely precisely one of the following holds*

$$x < y,\ x = y,\ y < x$$

*and further*

- *$z > 0$ then $x < y \iff xz < yz$*
- *$z < 0$ then $x < y \iff yz < xz$*
- *$y > 1$ and $x > 0$ then $x < xy$*

Finally we can construct an absolute value function

**Proposition 2.3.3**
*There exists an **absolute value** function*

$$|\cdot| : \mathbb{Z} \to \mathbb{N}$$

*such that*

$$|x| \quad = \quad \begin{cases} x & 0 < x \\ 0 & x = 0 \\ -x & x < 0 \end{cases}$$

*It satisfies*

- $|x| = 0 \iff x = 0$
- $|x| = |y| \iff x = \pm y$
- $|xy| = |x||y|$
- $|x + y| \leq |x| + |y|$

In many cases it may be more convenient to use the following form of induction

**Proposition 2.3.4** (Well-Ordering Principle)
*Let $S \subset \mathbb{N}$ be a non-empty subset. Then it contains a minimal element $d$.*

### 2.3.2 Arithmetic

**Proposition 2.3.5** (Division Algorithm)
*Let $x, y \in \mathbb{Z}$ be non-zero integers then there exists $q, r$ such that*

$$x = yq + r$$

*and*

$$0 \leq r < |y|$$

*Furthermore $(q, r)$ is the unique such pair.*

*Proof.* Suppose first that $x, y > 0$. Let $S = \{x - yn \mid n \in \mathbb{Z}\} \cap \mathbb{N}$. Then $x \in S$ so it is non-empty. By the Well-Ordering principle it has a minimal element $r$. By assumption

$$x = yq + r$$

for some $q \in \mathbb{Z}$ and $r \geq 0$. Suppose $r \geq y$, then $0 \leq x - y(q+1) < r$ contradicting minimality.

The case $x > 0, y < 0$ is then straightforward, as is the case $x < 0$.

For uniqueness suppose $yq' + r' = yq + r$ then $|y||q - q'| = |r' - r| < |y|$ from which it follows $|q - q'| = 0 \implies q = q' \implies r = r'$. □

**Corollary 2.3.6** (Ideals are Principal)
*Let $S \subseteq \mathbb{Z}$ be a non-empty set such that*

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

*Then $S = d\mathbb{Z}$ for a unique $d \geq 0$.*

*Proof.* First we claim that $0 \in S$. For if $x \in S$ then $0 = x - x \in S$ by assumption. Furthermore $x \in S \implies -x = 0 - x \in S$.

Consider the set $S' = (S \cap \mathbb{N}) \setminus \{0\}$. If it's empty then $S = \{0\}$ (for $x \in S \implies -x \in S$) and $d = 0$.

Otherwise it has a minimal element $d > 0$ by the well-ordering principle. Then by induction $d\mathbb{Z} \subseteq S$. Conversely suppose $y \in S$ then by the division algorithm $y = qd + r$ with $0 \leq r < d$. By assumption $r = y - qd \in S$ and by minimality must be equal to 0. Therefore $y \in d\mathbb{Z}$ and $d\mathbb{Z} = S$ as required. □

**Definition 2.3.7** (Divisibility)
*Let $x, y \in \mathbb{Z}$ be two integers. We say that $x$ divides $y$ if there exists $a$ such that $ax = y$. In this case we write*

$$x \mid y$$

*and*

$$\frac{y}{x}$$

*for the unique integer $a$ such that $ax = y$.*

**Lemma 2.3.8**
*Let $x, y \in \mathbb{Z}$ be two integers then*

$$x \mid y \implies |x| \leq |y|$$

*In particular $x \mid y \wedge y \mid x \implies x = \pm y$.*

**Proposition 2.3.9** (Bezout's Theorem)
*Let $x, y$ be non-zero integers. Then there exists a unique positive integer $d$ such that*

- *$d$ is a common divisor of $x, y$*
- *For any other common divisor $e$ we have $e \mid d$.*

*Further there exists integers $a, b$ such that $ax + by = d$. We write this as $(x, y)$.*

*Proof.* Let $S = \{ax + by \mid a, b \in \mathbb{Z}\}$. Then by (2.3.6) we have $S = d\mathbb{Z}$ for a unique $d > 0$. As $x, y \in S$ by definition $d$ is a common divisor, and by definition $d = d \cdot 1 = ax + by$ for some integers $a, b$. Suppose $e$ is a common divisor then $d = ax + by = e(ap + bq)$ and $e \mid d$ as required.

Any two such common divisors have $d = \pm d'$ by the previous Lemma. Since they are positive and non-zero we have $d = d'$. □

**Proposition 2.3.10**
*Let $a, x, y$ be non-zero integers then*

$$|a|(x, y) = (ax, ay)$$

*In particular*

$$\left(\frac{x}{(x,y)}, \frac{y}{(x,y)}\right) = 1$$

*Proof.* This follows from the characterization of $(x, y)$ as the minimal positive integer in the set $\{mx + ny\}$. □

### 2.3.3 Prime Factorization

**Definition 2.3.11**
*Let $x \in \mathbb{Z}$ be a non-zero integer. We say that $x$*

- *is a **unit** if it's equal to $1$ or $-1$.*
- *is **prime** if it's not a unit and $x \mid p$ implies $x = \pm 1$ or $x = \pm p$*
- ***composite** otherwise*

**Lemma 2.3.12**
*Let $p$ be a positive prime and $a$ a non-zero integer. Then precisely one of the following holds*

- $(p, a) = 1$
- $(p, a) = p$ *and* $p \mid a$

*Proof.* Note that $(p, a)$ is positive and divides both $p$ and $a$ so the result follows by definition of prime. □

**Proposition 2.3.13** (Euclid's Lemma)
*Suppose $x \mid ab$ then $\frac{x}{(x,a)} \mid b$.*

*In particular if $p$ is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

*Proof.* First suppose that $(x, a) = 1$. Then by assumption $zx = ab$ and by Bezout's Theorem $mx + na = 1$ for some integers $m, n$. Multiply by $z$ to find that $abm + na = a(bm + n) = z$. Therefore $a(bm + n)x = ab$ and cancel $a$ to find $x \mid b$ as required.

For the general case define $x' = x/(x, a)$ and $a' = a/(x, a)$. Then by (2.3.10) $(x', a') = 1$. Furthermore it's clear that $x' \mid a'b$ so we have $x' \mid b$ by the special case just proven.

Finally suppose $p \mid ab$. If $(p, a) = 1$ then $p \mid b$ by the first result. By (2.3.12) if this does not hold then $p \mid a$ as required. □

Using these results we may show that there exists a unique factorization into primes, unique up to multiplication by a unit.

## 2.4 Category Theory

### 2.4.1 Categories

**Definition 2.4.1** (Category)
*A (locally small) **category** $\mathcal{C}$ consists of*

- *a class $\mathrm{ob}(\mathcal{C})$ of objects*
- *for every pair of objects $a, b \in \mathrm{ob}(\mathcal{C})$ a* set *of **morphisms** $\mathrm{Mor}(a, b)$*
- *for every three objects $a, b, c$ a **law of composition***

$$\begin{aligned} \mathrm{Mor}(a,b) \times \mathrm{Mor}(b,c) &\to \mathrm{Mor}(a,c) \\ (g, f) &\to g \circ f \end{aligned}$$

*such that the following conditions hold*

- $h \circ (g \circ f) = (h \circ g) \circ f$ ***associativity***
- *There exists $1_a \in \mathrm{Mor}(a, a)$ such that $1_a \circ f = f$ and $g \circ 1_a = g$.*

**Example 2.4.2**
*The category of sets is* **Set** *with maps in the usual way. Note associativity is automatically satisfied. Most categories are subcategories of this one.*

**Example 2.4.3** ($n$-pointed category)
*Given a category $\mathcal{C}$ where objects are sets, we may consider the pointed category $(\mathcal{C}, \star^n)$ consisting of pairs $(A, a)$ where $A \in \mathrm{ob}(\mathcal{C})$ and $a \in A^n$. We consider only morphisms $f : A \to B$ such that $f(a_i) = b_i$.*

**Definition 2.4.4** (Initial object)
*An **initial object** of a category $\mathcal{C}$ is an object $a$ such that for all objects $b$*

$$\mathrm{Mor}(a, b) = \{\eta_b^a\}$$

*consists of a single element. Clearly in this case we have*

$$f \circ \eta_b^a = \eta_c^a$$

*for all $f : b \to c$ and $\eta_a^a = 1_a$.*

**Example 2.4.5**
*The polynomial ring $A[X]$ is an initial object in the category of pointed $A$-algebras.*

**Definition 2.4.6** (Isomorphism)
*A morphism $f : a \to b$ is an **isomorphism** if there exists $g : b \to a$ such that*

$$g \circ f = 1_a$$

*and*

$$f \circ g = 1_b$$

**Proposition 2.4.7** (Initial objects are unique)
*An initial object is unique up to isomorphism*

*Proof.* First observe by uniqueness $\eta_a^a = 1_a$. Let $a, a'$ be two initial objects with morphisms $\eta_-^a$ and $\eta_-^{a'}$ respectively. Then by definition

$$\eta_a^{a'} \circ \eta_{a'}^a = \eta_a^a = 1_a$$

and vice-versa.

□

**Definition 2.4.8** (Functor)
*A **covariant functor** $F : \mathcal{C} \to \mathcal{D}$ consists of a mapping of objects*

$$F : \mathrm{ob}(\mathcal{C}) \to \mathrm{ob}(\mathcal{D})$$

*together with a mapping of morphisms*

$$F(-) : \mathrm{Mor}(a, b) \to \mathrm{Mor}(F(a), F(b))$$

*which satisfies*

- $F(1_a) = 1_{F(a)}$
- $F(f \circ g) = F(f) \circ F(g)$

*A contravariant functor is the same, except arrows are reversed. A functor will be assumed to be covariant unless otherwise specified.*

**Definition 2.4.9** (Full and faithful)
*A functor $F$ is said to be*

- ***Faithful** if $F(-)$ is injective.*
- ***Full** if $F(-)$ is surjective.*

**Definition 2.4.10** (Concrete Category)
*A **concrete category** is a pair $(\mathcal{C}, U)$ where $\mathcal{C}$ and a "**forgetful functor**" $U : \mathcal{C} \to$ **Set** which is faithful*

**Example 2.4.11** (Forgetful Functor)
*The category of groups (resp. rings, modules, ...) is a concrete category in the obvious way.*

**Definition 2.4.12** (Mor functor)
*For any objects $a, b, c \in \mathrm{ob}(\mathcal{C})$, there is a canonical covariant functor*

$$\begin{aligned} \mathrm{Mor}(a,-) : \mathcal{C} &\longrightarrow \mathbf{Set} \\ b &\longrightarrow \mathrm{Mor}(a,b) \end{aligned}$$

*which acts on a morphism $f : b \to c$ by*

$$\begin{aligned} \mathrm{Mor}(a,f) : \mathrm{Mor}(a,b) &\to \mathrm{Mor}(a,c) \\ g &\to f \circ g \end{aligned}$$

*It's a functor precisely because composition of functions is associative. Similarly there's a canonical contravariant functor* $\mathrm{Mor}(-,b)$.

**Definition 2.4.13** (Natural Transformation)
*Let $F, G : \mathcal{C} \to \mathcal{D}$ be functors. A **natural transformation** $\eta : F \Rightarrow G$ consists of a family of morphisms*

$$\eta_c : F(c) \to G(c) \quad c \in \mathrm{ob}(\mathcal{C})$$

*such that the following diagram commutes holds for all $f : c \to c'$*

$$\begin{array}{ccc} F(c) & \xrightarrow{\eta_c} & G(c) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(c') & \xrightarrow{\eta_{c'}} & G(c') \end{array}$$

*for all $f : c \to c'$.*

**Definition 2.4.14** (Natural isomorphism)
*A natural transformation $\eta : F \Rightarrow G$ is a natural isomorphism if $\eta_c$ is an isomorphism for all $c \in \mathcal{C}$.*

### 2.4.2 Equivalence of categories

**Definition 2.4.15** (Equivalence of categories)
*Let $\mathcal{C}$, $\mathcal{D}$ be categories. An **equivalence of categories** consists of a pair of functors (either both covariant or both contravariant)*

$$\mathcal{C} \underset{F}{\overset{G}{\rightleftarrows}} \mathcal{D}$$

*together with natural isomorphisms*

$$\eta : \mathbf{1} \Rightarrow GF$$
$$\epsilon : FG \Rightarrow \mathbf{1}$$

*We say $F$ is an equivalence of categories if there exists some $G$ satisfying these conditions.*

**Definition 2.4.16**
*We say $F : \mathcal{C} \to \mathcal{D}$ is **essentially surjective** if for all $d \in \mathcal{D}$ there exists $c \in \mathcal{C}$ such that $F(c)$ is isomorphic to $d$.*

**Lemma 2.4.17**
*Let $F : \mathcal{C} \to \mathcal{D}$, $G : \mathcal{D} \to \mathcal{C}$ be functors.*

*If there exists a natural isomorphism $\eta : \mathbf{1} \Rightarrow GF$ then $F$ is faithful. Explicitly $F(-)$ has a left-inverse given by*

$$g \to \eta_{c'}^{-1} \circ G(g) \circ \eta_c$$

*Furthermore $GF(\eta_c) = \eta_{GF(c)}$.*

*Proof.* Consider the sequence of maps

$$\mathrm{Mor}(c,c') \overset{F(-)}{\longrightarrow} \mathrm{Mor}(F(c),F(c')) \overset{G(-)}{\longrightarrow} \mathrm{Mor}(GF(c),GF(c')) \overset{\mathrm{Mor}(\eta_c,\eta_{c'}^{-1})}{\longrightarrow} \mathrm{Mor}(c,c')$$

Note that the composite of this map is given by

$$f \to \eta_{c'}^{-1} \circ GF(f) \circ \eta_c = \eta_{c'}^{-1} \circ \eta_{c'} \circ f = f$$

in other words $F(-)$ has a left inverse and therefore $F$ is faithful.

Note by naturality we have $GF(\eta_c) \circ \eta_c = \eta_{GF(c)} \circ \eta_c$. Since $\eta_c$ is an isomorphism we may cancel to find $GF(\eta_c) = \eta_{GF(c)}$. □

**Proposition 2.4.18** (Equivalence is full and faithful)
*Let $F : \mathcal{C} \to \mathcal{D}$ then the following are equivalent*

- *$F$ is full, faithful and essentially surjective*
- *$F$ is an equivalence of categories*

*In other words $F(-)$ is bijective and hence has a two-sided inverse. Explicitly it is given by*

$$\begin{array}{rcl} \mathrm{Mor}(c, c') & \longleftrightarrow & \mathrm{Mor}(F(c), F(c')) \\ f & \to & F(f) \\ \eta_{c'}^{-1} \circ G(g) \circ \eta_c & \leftarrow & g \end{array}$$

*Proof.* We prove only the second implies the first. By assumption there is an equivalence with $G$ and by the previous Lemma both $F$ and $G$ are faithful by considering $\eta$ and $\epsilon^{-1}$ in turn. Further the given map is already shown to be a left inverse. We claim it's also a right inverse, for consider

$$g' := F(\eta_{c'}^{-1}) \circ FG(g) \circ F(\eta_c)\,.$$

We claim that $G(g') = G(g)$. As $G$ is faithful this would imply $g' = g$ and the given map is a right inverse as required. Observe

$$G(g') = GF(\eta_{c'}^{-1}) \circ GFG(g) \circ GF(\eta_c) = \eta_{GF(c')}^{-1} \circ GFG(g) \circ \eta_{GF(c)} = \eta_{GF(c')}^{-1} \circ \eta_{GF(c')} \circ G(g) = G(g)$$

where we have used the result that $GF(\eta_c) = \eta_{GF(c)}$. Since the maps are mutual inverses we see that $F$ is full and faithful as required.

Given $d \in \mathcal{D}$ then $F(G(d))$ is isomorphic to $d$ via $\epsilon$ so $F$ is essentially surjective. □

**Proposition 2.4.19** (Duality)
*Let $(-)^\star : \mathcal{C} \to \mathcal{C}$ be a (contravariant) functor such that there is a natural isomorphism*

$$\eta : \mathbf{1}_{\mathcal{C}} \Rightarrow (-)^{\star\star}$$

*then $(-)^\star$ is an equivalence of categories and in particular full and faithful.*

*Proof.* Define $\epsilon = \eta^{-1}$ to determine the equivalence of categories. By the previous result then $(-)^\star$ is full and faithful. □

### 2.4.3 Properties of Morphisms

**Definition 2.4.20** (Injective, Surjective and Bijective)
*Let $(\mathcal{C}, U)$ be a concrete category and $f : a \to c$ a morphism. Then we say*

- *$f$ is **injective** if $U(f)$ is injective*
- *$f$ is **surjective** if $U(f)$ is surjective*

**Remark 2.4.21**
*Note if $f$ is both surjective and injective it need not be an isomorphism.*

The concepts of monic/split-monic, epic/split-epic, iso generalize the notion of injective, surjective and bijective to general categories as we shall see.

**Definition 2.4.22** (Monomorphism)
*A morphism $f : a \to b$ is said to be a **monomorphism** (or **monic**) if*

$$f \circ g_1 = f \circ g_2 \implies g_1 = g_2$$

*for all $g_1, g_2 : c \to a$.*

**Definition 2.4.23** (Epimorphism)
*A morphism $f : a \to b$ is said to be an **epimorphism** (or **epic**) if*

$$g_1 \circ f = g_2 \circ f \implies g_1 = g_2$$

*for all $g_1, g_2 : b \to c$.*

**Definition 2.4.24** (Split-monic / Section)
*A morphism $f : a \to b$ is **split-monic** if it has a left inverse, $g : b \to a$*

$$g \circ f = 1_a$$

*We say $g$ is a **section** of $f$.*

**Definition 2.4.25** (Split-epic / Retraction)
*A morphism $f : a \to b$ is **split-epic** if it has a right inverse, $g : b \to a$*

$$f \circ g = 1_b$$

*We say $g$ is a **retraction** of $f$.*

**Proposition 2.4.26** (Split Monic $\implies$ Monic)
*For a general category $\mathcal{C}$ we have*

- *split-monic $\implies$ monic*
- *split-epic $\implies$ epic*

Recall that an isomorphism is a morphism with a two-sided inverse. We can refine the criteria for $f$ to be an isomorphism using the notions just defined

**Proposition 2.4.27** (Isomorphism Criteria)
*Let $f : a \to b$ be a morphism. Then the following are equivalent*

a) *$f$ is an **isomorphism***

b) *$f$ is both **split-epic** and **split-monic***

c) *$f$ is **split-epic** and **monic***

d) *$f$ is **split-monic** and **epic***

*In this case a morphism $g$ is a retraction if and only if it is a section. And such a $g$ is unique, so we denote it by $f^{-1}$*

*Proof.* This is mostly formal
$1 \implies 2)$ Clear.
$2 \implies 3, 4)$ This follows from (2.4.26).
$3 \implies 2)$ Suppose $g$ is a retraction of $f$, that is $fg = 1_b$. Then $f(gf) = (fg)f = 1_b \circ f = f = f \circ 1_a$. As $f$ is monic we conclude that $gf = 1_a$ and $g$ is a section of $f$.
$4 \implies 2)$ Analogous
$2 \implies 1)$ We've shown that any retraction is a section and vice-versa. Furthermore by monic/epic-ness a retraction or section is unique. □

**Proposition 2.4.28**
*For the category* **Set** *we have*

- *split-monic $\iff$ monic $\iff$ injective*
- *split-epic $\iff$ epic $\iff$ surjective*
- *isomorphism $\iff$ bijective*

**Definition 2.4.29** (Preserves/Reflects)
*Let $\mathcal{P}$ be a property of morphisms and $F : \mathcal{C} \to \mathcal{D}$ be a functor then we say*

- *$F$ **preserves** $\mathcal{P}$ if ($f$ satisfies $\mathcal{P} \implies F(f)$ satisfies $\mathcal{P}$)*
- *$F$ **reflects** $\mathcal{P}$ if ($F(f)$ satisfies $\mathcal{P} \implies f$ satisfies $\mathcal{P}$)*

**Proposition 2.4.30**
*Let $F : \mathcal{C} \to \mathcal{D}$ be a covariant functor then*

- *$F$ preserves split-monic, split-epic and iso morphisms.*

*If in addition $F$ is faithful then*

- *$F$ reflects monic and epic morphisms.*

*and if $F$ is full and faithful then*

- *$F$ reflects split-epic, split-monic and isomorphisms.*

*Similar statements apply when $F$ is contravariant.*

*Proof.* The first statement is easy, for example if $gf = 1_a$ then $F(g) \circ F(f) = 1_{F(a)}$.

Suppose $F$ is faithful, $F(f)$ is monic and $fg_1 = fg_2$. Then $F(f)F(g_1) = F(f)F(g_2) \implies F(g_1) = F(g_2)$ by assumption. As $F$ is faithful $g_1 = g_2$ as required. The other statement is similar.

Suppose $F$ is full and faithful and $F(f)$ is split-monic. Then $hF(f) = 1_{F(a)}$. As $F$ is full $h = F(g)$ and $1_{F(a)} = F(gf)$. As $F$ is faithful then $gf = 1_a$. the other statements are similar. □

**Proposition 2.4.31**
*Let $(\mathcal{C}, U)$ be a concrete category then*

- *$f$ split-monic $\implies$ $f$ injective $\implies$ $f$ monic*
- *$f$ split-epic $\implies$ $f$ surjective $\implies$ $f$ epic*
- *$f$ isomorphism $\implies$ $f$ bijective*

*Proof.* Suppose $f$ is split-monic, then $U(f)$ is split-monic by (2.4.30) and so by (2.4.28) $U(f)$ is injective.

Suppose $U(f)$ injective, then by (2.4.28) $U(f)$ is monic. By (2.4.30) $U$ reflects monics and so $f$ is monic.

The other statements are similar. □

We can restate the criteria for split-epic/split-monic

**Proposition 2.4.32**
*Let $f : a \to b$ be a morphism then*

- *$f$ is split-monic if and only if $\mathrm{Mor}(f, c)$ is surjective for all $c \in \mathcal{C}$*
- *$f$ is epic if and only if $\mathrm{Mor}(f, c)$ is injective for all $c \in \mathcal{C}$*

*dually*

- *$f$ is split-epic if and only if $\mathrm{Mor}(c, f)$ is surjective for all $c \in \mathcal{C}$*
- *$f$ is monic if and only if $\mathrm{Mor}(c, f)$ is injective for all $c \in \mathcal{C}$*

*Proof.* $f$ is epic (resp. monic) iff $\mathrm{Mor}(f, c)$ (resp. $\mathrm{Mor}(c, f)$) is injective precisely by the definitions.

Suppose $f$ is split-monic, then $gf = 1_a \implies (hg)f = h$ for any $h$. That is $\mathrm{Mor}(f, c)$ is surjective. Conversely if it's surjective then let $c = b$ and choose $g$ such that $gf = \mathrm{Mor}(f, b)(g) = 1_a$.

A similar statement follows dually for $f$ split-epic, and $f$ monic. □

**Corollary 2.4.33** (Isomorphism Criteria)
*Let $f : a \to b$ be a morphism then TFAE*

- *$f$ is an isomorphism*
- *$\mathrm{Mor}(f, c)$ is bijective for all $c \in \mathcal{C}$*
- *$\mathrm{Mor}(c, f)$ is bijective for all $c \in \mathcal{C}$*

*Proof.* This follows from combining (2.4.32) with (2.4.27). □

**Definition 2.4.34** (Algebraic Category)
*We say a concrete category $(\mathcal{C}, U)$ is an algebraic category if*

- *$U$ reflects (and preserves) isomorphisms*
- *$\mathcal{C}$ has directed limits and $U$ commutes with them*

### 2.4.4 Directed Limits

**Definition 2.4.35** (Directed Category)
*We say a category $I$ is **directed** if*

- *It is small*
- *For any $i, j \in \mathrm{ob}(I)$ we have at most one morphism $i \to j$ (NB bit non-standard)*
- *For any $i, j \in \mathrm{ob}(I)$ there is a $k$ and morphisms $i \to k$ and $j \to k$*

*If there is a morphism $i \to j$ then we write $i \prec j$.*

**Definition 2.4.36** (Direct limit)
*Let $I$ be a directed category and $F : I \to \mathcal{C}$ a functor ("diagram"). We write $A_i := F(i)$ and $\rho_{ij} : A_i \to A_j$ when $i \prec j$. Observe that*

$$\rho_{jk} \circ \rho_{ij} = \rho_{ik} \quad \forall i, j, k \ s.t. \ i \prec j, \ j \prec k.$$

*A **cone** over $F$ is a pair $(A, \{\phi_i^A : A_i \to A\}_{i \in I})$ for $A \in \mathrm{ob}(\mathcal{C})$ which satisfies*

$$\phi_j^A \circ \rho_{ij} = \phi_i^A \quad \forall i, j \ s.t. \ i \prec j \, .$$

*The cones form a category where morphisms consist of morphisms $\psi : A \to B$ such that*

$$\psi \circ \phi_i^A = \phi_i^B$$

*A **directed limit** is a cone $(\varinjlim_i A_i, \{\phi_i : A_i \to \varinjlim_i A\})$ for which given any other cone $(A, \phi_i^A)$ there exists a unique morphism of cones*

$$(\varinjlim_i A_i, \phi_i) \to (A, \phi_i^A) \, .$$

*In otherwords it is an initial object in the category of cones over $F$.*

**Proposition 2.4.37** (Direct limit of sets)
*Let $I$ be a directed category and $F : I \to \mathbf{Set}$ be a diagram of sets. Write $A = F(i)$ and $\rho_{ij} : A_i \to A_j$. We may construct a direct limit as follows*

$$\lim_i A_i = \{(i, x) \mid i \in I \ x \in A_i\} / \sim$$

*where we consider the equivalence relation*

$$(i, x) \sim (j, y)$$

*if for some $k$ we have $\rho_{ik}(x) = \rho_{jk}(y)$.*

### 2.4.5 Adjoint Functors

Some universal constructions may be expressed as an adjoint pair of functors. Using this concept we can simplify the verification of universal properties by appealing to general criteria for adjoint functors as below.

**Definition 2.4.38** (Adjoint Pair)
*Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be functors. We say that $F$ is **left adjoint** to $G$ if there is a bijection*

$$\psi_{c,d} : \mathrm{Mor}(F(c), d) \longrightarrow \mathrm{Mor}(c, G(d))$$

*which is natural in $c$ and $d$ in the following sense. Let $\alpha : c' \to c$, $\beta : d \to d'$, then for all $f : F(c) \to d$ we have*

$$\psi_{c',d'}(\beta \circ f \circ F(\alpha)) = G(\beta) \circ \psi_{c,d}(f) \circ \alpha \tag{2.2}$$

*or equivalently for all $g : c \to G(d)$*

$$\beta \circ \psi_{c,d}^{-1}(g) \circ F(\alpha) = \psi_{c',d'}^{-1}(G(\beta) \circ g \circ \alpha) \tag{2.3}$$

**Proposition 2.4.39** (Adjoint $\implies$ unit, counit)
*Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be adjoint functors with relationship*

$$\psi_{c,d} : \mathrm{Mor}(F(c), d) \longrightarrow \mathrm{Mor}(c, G(d))$$

*Then we have two natural transformations (**unit** and **counit** respectively)*

$$\begin{aligned} \eta : \mathbf{1} &\Rightarrow G \circ F \\ \epsilon : F \circ G &\Rightarrow \mathbf{1} \end{aligned}$$

*defined by*

$$\begin{aligned} \eta_c = \psi_{c,F(c)}(1_{F(c)}) : c &\to G(F(c)) \\ \epsilon_d = \psi^{-1}_{G(d),d}(1_{G(d)}) : F(G(d)) &\to d \end{aligned}$$

*Furthermore we may recover the adjoint relationship via*

$$\begin{aligned} \psi_{c,d}(f) &= G(f) \circ \eta_c \\ \psi^{-1}_{c,d}(g) &= \epsilon_d \circ F(g) \end{aligned}$$

*Proof.* We show that the transformations given are natural. Suppose $\alpha : c \to c'$ athen

$$\begin{aligned} G(F(\alpha)) \circ \eta_c &= G(F(\alpha)) \circ \psi_{c,F(c)}(1_{F(c)}) \\ &= \psi_{c,F(c')}(F(\alpha) \circ 1_{F(c)}) \quad (2.2) \\ &= \psi_{c,F(c')}(1_{F(c')} \circ F(\alpha)) \\ &= \psi_{c',F(c')}(1_{F(c')}) \circ \alpha \quad (2.2) \\ &= \eta_{c'} \circ \alpha \end{aligned}$$

so $\eta$ is a natural transformation. Furthermore

$$\psi_{c,d}(f) = \psi_{c,d}(f \circ 1_{F(c)}) = G(f) \circ \psi_{c,F(c)}(1) = G(f) \circ \eta_c$$

as required. Similarly for $\beta : d \to d'$

$$\begin{aligned} \beta \circ \epsilon_d &= \beta \circ \psi^{-1}_{G(d),d}(1_{G(d)}) \\ &= \psi^{-1}_{G(d),d'}(G(\beta) \circ 1_{G(d)}) \quad (2.3) \\ &= \psi^{-1}_{G(d),d'}(1_{G(d')} \circ G(\beta)) \\ &= \psi^{-1}_{G(d'),d'}(1_{G(d')}) \circ F(G(\beta)) \quad (2.3) \\ &= \epsilon_{d'} \circ F(G(\beta)) \end{aligned}$$

□

Given two natural transformations we may recover a corresponding adjoint

**Proposition 2.4.40** (Adjoint from unit and counit)
*Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be functors with two natural transformations*

$$\begin{aligned} \eta : \mathbf{1} &\Rightarrow G \circ F \\ \epsilon : F \circ G &\Rightarrow \mathbf{1} \end{aligned}$$

*Then TFAE*

a) *$F$ is left adjoint to $G$ with unit and counit $\eta$, $\epsilon$*

b) *The so-called **triangular identities** are satisfied*

$$1_{G(d)} : G(d) \xrightarrow{\eta_{G(d)}} GFG(d) \xrightarrow{G(\epsilon_d)} G(d) \tag{2.4}$$

$$1_{F(c)} : F(c) \xrightarrow{F(\eta_c)} FGF(c) \xrightarrow{\epsilon_{F(c)}} F(c) \tag{2.5}$$

*More precisely the adjunction is given by*

$$\begin{array}{rcl} \mathrm{Mor}(F(c),d) & \underset{\psi}{\overset{\phi}{\leftrightarrows}} & \mathrm{Mor}(c,G(d)) \\ f & \longrightarrow & G(f)\circ\eta_c \\ \epsilon_d\circ F(g) & \longleftarrow & g \end{array}$$

*Proof.* Let $\psi,\phi$ denote the proposed adjunction maps. We will use the triangular identities to show that these are mutually inverse. First observe by naturality of $\eta$ and $\epsilon$ that

$$\psi\phi(g) = G(\epsilon_d\circ F(g))\circ\eta_c = G(\epsilon_d)\circ\eta_{G(d)}\circ g \tag{2.6}$$
$$\phi\psi(f) = \epsilon_d\circ F(G(f)\circ\eta_c) = f\circ\epsilon_{F(c)}\circ F(\eta_c) \tag{2.7}$$

It's then immediate that these are mutually inverse maps if and only if the triangular identities are satisfied (one way is obvious, the other way consider $f=1_{F(c)}$ and $g=1_{G(d)}$).

Further one may easily verify that $\psi,\phi$ so-defined are natural in $c$ and $d$

$$\begin{aligned} \psi(\beta\circ f\circ F(\alpha)) &= G(\beta)\circ G(f)\circ GF(\alpha)\circ\eta_c \\ &= G(\beta)\circ G(f)\circ\eta_{c'}\circ\alpha \\ &= G(\beta)\circ\psi(f)\circ\alpha \end{aligned}$$

□

**Proposition 2.4.41** (Criteria for right adjoint to be full and faithful)
*Let $F:\mathcal{C}\to\mathcal{D}$ and $G:\mathcal{D}\to\mathcal{C}$ be adjoint functors with $\eta,\epsilon$ unit and counit transformations. Then*

- *$G$ is faithful if and only if $\epsilon$ is pointwise epic*
- *$G$ is full if and only if $\epsilon$ is pointwise split-monic*
- *$G$ is full and faithful if and only if $\epsilon$ is a pointwise isomorphism*

*Proof.* Consider the composite map

$$\mathrm{Mor}(d',d) \overset{\mathrm{Mor}(\epsilon_{d'},d)}{\longrightarrow} \mathrm{Mor}(F(G(d')),d) \overset{\psi_{G(d'),d}}{\to} \mathrm{Mor}(G(d'),G(d))$$

which is natural in $d$ and $d'$. Note that image of $\alpha\in\mathrm{Mor}(d',d)$ is

$$\psi_{G(d'),d}(\alpha\circ\epsilon_{d'}) = G(\alpha)\circ\psi_{G(d'),d'}(\epsilon_{d'}) = G(\alpha)$$

so the composite is just $G(-)$. The second map is bijective by the adjoint assumption. Therefore the first map is injective (resp. surjective) if and only if $G$ is faithful (resp. full).

By (2.4.32) $\mathrm{Mor}(\epsilon_{d'},d)$ is injective (resp. surjective) for all $d,d'$ if and only if $\epsilon_{d'}$ is epic (resp. split-monic) for all $d'$.

Then the first two statements follow easily. The last statement follows from the previous two, combined with (2.4.27). □

The following criteria will be useful

**Proposition 2.4.42** (Alternative Characterization)
*Let $F:\mathcal{C}\to\mathcal{D}$ and $G:\mathcal{D}\to\mathcal{C}$ be functors. Suppose that we have natural transformations*

$$\epsilon : F\circ G\Rightarrow \mathbf{1}$$
$$\eta : \mathbf{1}\Rightarrow G\circ F$$

*such that the first **triangular identity** is true*

$$G(\epsilon_d)\circ\eta_{G(d)} = 1_{G(d)}$$

*and one of the following holds*

- *The map $\psi:\mathrm{Mor}(F(c),d)\overset{G(-)\circ\eta_c}{\longrightarrow}\mathrm{Mor}(c,G(d))$ is injective*
- *The map $\phi:\mathrm{Mor}(c,G(d))\overset{\epsilon_d\circ F(-)}{\longrightarrow}\mathrm{Mor}(F(c),d)$ is surjective*

*Then $\eta, \epsilon$ induce an adjoint relationship between $F$ and $G$ as in (2.4.40).*

*Proof.* Recall the proposed adjoint maps from (2.4.40), $\psi$ and $\phi$, where we also demonstrated that

$$\psi(\phi(f)) = G(\epsilon_d) \circ \eta_{G(d)} \circ f$$

Then the first hypothesis clearly implies $\psi\phi = 1$, i.e. $\phi$ has a left-inverse and $\psi$ has a right inverse.

Suppose that the given map $\psi$ is injective, then by (2.4.28) $\psi$ has a left-inverse too. By (2.4.27) $\psi$ is an isomorphism with inverse $\psi^{-1} = \phi$.

The case that $\phi$ is surjective is similar. □

# Chapter 3

# Algebra

## 3.1 Introduction

Follows largely Lang with some Bourbaki.

## 3.2 Magmas and Monoids

**Definition 3.2.1** (Magma)
*Let $X$ be a set. A **law of composition** on $X \times X$ is a function*

$$\cdot : X \times X \to X$$

*and we typically write the composition of $x, y \in X$ as either*

$$x \cdot y$$

*or $xy$, or $x + y$ in the commutative case.*

*A pair $(X, \cdot)$ consisting of a set $X$ and law of composition on $X$ is called a **magma**.*

**Definition 3.2.2** (Magma/Monoid)
*A **magma** $(X, \cdot)$ is said to be*

- ***associative** if $(x \cdot y) \cdot z = x \cdot (y \cdot z)$*
- ***commutative** if $x \cdot y = y \cdot x$ for all $x, y \in X$*
- ***unital** if there exists $e \in X$ such that $e \cdot x = x \cdot e = x$ for all $x \in X$. Such an $e$ is called an **identity**.*
- *a **monoid** if it is both **associative** and **unital***

**Proposition 3.2.3** (Identity is Unique)
*A magma $(X, \cdot)$ has at most one element $e$ such that*

$$x \cdot e = e \cdot x = x$$

*for all $x \in X$.*

**Definition 3.2.4** (Invertible / Monoid)
*Let $(X, \cdot)$ be a unital magma. An element $x \in X$ is **invertible** if there exists $y \in X$ such that*

$$x \cdot y = y \cdot x = e$$

**Proposition 3.2.5** (Inverses are unique)
*Let $(X, \cdot)$ be a monoid. If $x \in X$ is invertible then its inverse is unique and denoted $x^{-1}$.*

*Proof.* Suppose that $xy = xy' = e = yx = y'x$. Then

$$xy = e \implies y'(xy) = y'e = y' \implies (y'x)y = y' \implies y = y'$$

□

**Definition 3.2.6** (Homomorphism)
*Let $(X, \cdot)$, $(Y, \cdot)$ be magmas. Then a function $\phi : X \to Y$ is said to be a **magma homomorphism** if it satisfies*

$$\phi(x_1 \cdot x_2) = \phi(x_1) \cdot \phi(x_2) \quad \forall x_1, x_2 \in X$$

*If $(X, \cdot)$ and $(Y, \cdot)$ are unital then $\phi$ is **unital** if*

$$\phi(e_X) = e_Y$$

*If $(X, \cdot)$ and $(Y, \cdot)$ are monoids then $\phi$ is a **monoid morphism** if it satisfies both these conditions.*

## 3.3 Groups

**Definition 3.3.1** (Group)
*A **group** is a **monoid** $(G, \cdot)$ in which every element is invertible.*

*A group $G$ is said to be **abelian** if the binary operation is **commutative**. In this case we typically write the group operation additively*

$$g + h$$

**Definition 3.3.2** (Subgroup, Normal Subgroup)
*A **subgroup** $H \leq G$ is a subset with the following properties*

- $e_G \in H$
- $x, y \in H \implies xy \in H$
- $x \in H \implies x^{-1} \in H$

*A subgroup $H$ is said to be **normal** in $G$ if in addition it satisfies*

$$gHg^{-1} := \{ghg^{-1} \mid g \in G\} = H$$

*for all $g \in G$. NB it is easily verified that in an abelian group every subgroup is normal.*

**Proposition 3.3.3** (Subgroup is a group)
*Let $H$ be a subgroup of $(G, \cdot)$ then $(H, \cdot|_{H \times H})$ is a group.*

**Example 3.3.4**
*$\mathbb{Z}$ is an abelian group under addition. The subgroups are of the form $n\mathbb{Z}$.*

**Definition 3.3.5**
*Let $(G, \cdot)$ and $(H, \cdot)$ be groups. A function $\phi : G \to H$ is a **group homomorphism** if*

- $\phi(e_G) = e_H$
- $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$

*Define the **image** of $\phi$ to be*

$$\mathrm{Im}(\phi) = \{\phi(g) \mid g \in G\}$$

*and the **kernel** to be*

$$\ker(\phi) := \{g \in G \mid \phi(g) = e_H\}$$

*It may be verified that $\mathrm{Im}(\phi)$ is a subgroup of $H$ and $\ker(\phi)$ is a normal subgroup of $G$.*

**Proposition 3.3.6** (Raise to the $n$-th power)
*Let $g \in G$ be a group element. Then there exist a unique group homomorphism*

$$g^{(-)} : (\mathbb{Z}, +) \to (G, \cdot)$$

*satisfying*

$$g^1 = g$$

*In other words such that*

$$g^0 = e_G$$
$$g^{n+m} = g^n \cdot g^m \quad \forall n, m \in \mathbb{Z}$$

**Proposition 3.3.7**
*Let $g \in G$ be a group element. Then*

$$(g^n)^m = g^{nm}$$

*for all integers $n, m \in \mathbb{Z}$.*

**Definition 3.3.8** (Order of an element)
*For $g \in G$ define the **order** of $g$ to be $o(g) := \inf\{n \geq 0 \mid g^n = e\}$ where $\inf \emptyset = \infty$.*

*We say $g$ has **finite order** if $o(g) \neq \infty$.*

**Definition 3.3.9** (Subgroup generated by an element)
*The **subgroup generated** by an element $g \in G$ is defined to be $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$*

*It may be shown that when $g$ has finite order $n$ we have*

$$\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$$

*and in particular $\#\langle g \rangle = o(g)$.*

**Proposition 3.3.10** (Cosets)
*Let $H$ be a subgroup of $G$. The following is an equivalence relation on $G$*

$$g_1 \sim_H g_2 \iff g_1 g_2^{-1} \in H$$

*and the equivalence classes are precisely the sets of the form*

$$gH = \{gh \mid h \in H\} = [g]_{\sim_H}$$

*for some $g \in G$. Such an equivalence class is called a **coset** and we denote the set of cosets by*

$$G/H$$

*Define the **index** of $H$ in $G$ by $[G : H] := \#G/H$. When $H$ is finite each equivalence class has order $\#H$.*

*We say $\{g_i \in G\}_{i \in I}$ is a set of **coset representatives** for $H$ if the corresponding equivalence classes $\{[g_i]\}_{i \in I}$ are pairwise disjoint and cover $G$.*

*Proof.* It's trivial to show that $\sim_H$ is an equivalence relation (precisely because $H$ is a subgroup). Therefore by (2.1.6) the equivalence classes form a partition which we denote $G/H$.

We claim that $[g_1] = g_1 H$. Then $g_2 \in [g_1] \iff g_1 \sim_H g_2 \iff g_2 \sim_H g_1 \iff g_2 g_1^{-1} \in H \iff g_2 \in g_1 H$, which shows that the sets are equal.

The translation map $\psi_g : G \to G$ given by $g' \to gg'$ is bijective (for it has a two-sided inverse equal to $\psi_{g^{-1}}$). So in particular restricts to a bijective map $H \to gH$. This shows that all the cosets have the same order. □

**Example 3.3.11**
*$d\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ of index $d$. A set of coset representatives are $\{0, 1, \ldots, d-1\}$.*

**Corollary 3.3.12** (Lagrange's Theorem)
*Let $H \leq G$ be a subgroup then*

$$\#G = [G : H] \times \#H$$

*More generally if $K \leq H$ then*

$$[G : K] = [G : H][H : K]$$

**Example 3.3.13**
*$d\mathbb{Z} \subseteq e\mathbb{Z} \iff d \mid e$ and $[e\mathbb{Z} : d\mathbb{Z}] = e/d$.*

**Proposition 3.3.14**
*Let $g \in G$ be an element of finite order. Then*

$$o(g) \mid \#G$$

*Furthermore*

$$g^n = e \iff o(g) \mid n$$

*Proof.* The first statement follows because the order $o(g)$ equals the order of the subgroup $\langle g \rangle$ generated by $g$.

Let $m = o(g)$ then by the division algorithm $n = qm + r$ for some $r < m$. Then $e = g^n = g^{qm}g^r = (g^m)^q g^r = e^q g^r = g^r$. By minimality we have $r = 0$ and $m \mid n$ as required. □

**Proposition 3.3.15** (Quotient Group)
*Let $N$ be a normal subgroup $G$. Then the set of cosets*

$$G/N$$

*forms a group under the binary operation*

$$g_1N \cdot g_2N \to (g_1g_2)N$$

*with identity $eN$.*

a) *There is a canonical surjective group homomorphism*

$$\pi : G \longrightarrow G/N$$

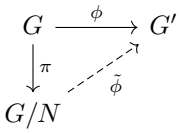
$$g \to gN$$

*with kernel $N$.*

b) *Let $N \subseteq H$ be a subgroup then define the correseponding subgroup of $G/N$*

$$H/N := \pi(H) = \{hN \mid h \in H\}.$$

c) *Let $\phi : G \to G'$ be a homomorphism with $N \subseteq \ker(\phi)$, then there exists a unique homomorphism $\tilde{\phi}$ making the diagram commute*




*such that*

i) $\mathrm{Im}(\phi) = \mathrm{Im}(\tilde{\phi})$

ii) $\ker(\tilde{\phi}) = \ker(\phi)/N$

**Corollary 3.3.16** (Isomorphism Theorem)
*Let $\phi : G \to H$ be a group homomorphism, then there is a canonical isomorphism*

$$G/\ker(\phi) \xrightarrow{\sim} \mathrm{Im}(\phi)$$

**Proposition 3.3.17** (Correspondence Theorem)
*Let $\pi : G \to G'$ be a surjective homomorphism with $\ker(\phi) = N$ then there is a bijective correspondence of subgroups*

$$\begin{array}{rcl} \{H \leq G \mid N \subseteq H\} & \longleftrightarrow & \{H' \leq G'\} \\ H & \longrightarrow & \pi(H) \\ \pi^{-1}(H') & \longleftarrow & H' \end{array}$$

*which preserves index, that is*

$$[G' : H'] = [G : H]$$

*Furthermore $\#H' = [H : N]$.*

### 3.3.1 Cyclic Groups

**Definition 3.3.18**
*A group $G$ is said to be **cyclic** if there is a surjective group homomorphism*

$$(\mathbb{Z}, +) \longrightarrow (G, \cdot)$$

*equivalently if there is $g \in G$ such that $\langle g \rangle = G$. Such a $g$ is called a **generator** for $G$.*

**Proposition 3.3.19**
*Consider the additive group $(\mathbb{Z}, +)$. Then*

a) *Every subgroup is of the form $d\mathbb{Z}$ for $d \geq 0$ and is itself cyclic*

b) *When $d > 0$, then $Z/d\mathbb{Z}$ has a complete set of coset representatives*

$$S := \{0, 1, \ldots, d-1\}$$

c) *In particular $[Z : d\mathbb{Z}] = d$ when $d > 0$*

d) *$d\mathbb{Z} \subseteq e\mathbb{Z} \iff e \mid d$ and in this case $[e\mathbb{Z} : d\mathbb{Z}] = \frac{d}{e}$*

*Proof.* We prove each in turn

a) By (2.3.6) every subgroup is of the form $d\mathbb{Z}$. Multiplication map $[d] : \mathbb{Z} \to d\mathbb{Z}$ shows it is itself cyclic.

b) By the division algorithm (2.3.5) $S$ is a complete set. Given $i, j \in S$ we note that $|i - j| < d$. And $i \sim_d j \implies d \mid |i - j| \implies |i - j| = 0 \implies i = j$. Therefore the set $S$ consists of distinct coset representatives.

c) This is clear from the previous step

d) The first equivalence is clear. By (3.3.12)

$$[\mathbb{Z} : d\mathbb{Z}] = [\mathbb{Z} : e\mathbb{Z}][e\mathbb{Z} : d\mathbb{Z}]$$

and the result follows.

□

**Proposition 3.3.20**
*Let $G$ be a cyclic group. Then*

- *If $G$ is infinite it is isomorphic to $\mathbb{Z}$*
- *If $G$ is finite it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n > 0$*

*Proof.* By the previous Proposition the kernel of the homomorphism $\mathbb{Z} \to G$ is of the form $n\mathbb{Z}$ for $n \geq 0$. By (...) $G$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. When $n = 0$ this is canonically isomorphic to $\mathbb{Z}$.

By the previous Proposition $\mathbb{Z}/n\mathbb{Z}$ is finite for $n > 0$ and therefore if $G$ is not finite we must have $n = 0$. Similarly If $G$ is finite then we must have $n > 0$. □

We analyse the structure of finite cyclic groups in more detail. First recall the definition of **Euler's Totient Function**

**Definition 3.3.21** (Euler Totient Function)
*Define the function*

$$\phi(n) = \#\{0 < d \leq n \mid (d, n) = 1\}$$

**Proposition 3.3.22** (Finite Cyclic Groups)
*Consider a finite cyclic group $G$ of order $n$. Then*

a) *The order of $g^r$ is $\frac{n}{(n,r)}$ where $0 < r \leq n$.*

b) *There are $\phi(n)$ generators*

c) *For every $d \mid n$ there is a unique subgroup of order $n/d$ given by $\langle g^d \rangle$, which is cyclic.*

d) *For $d \mid n$ there are precisely $\phi(d)$ elements of order $d$*

e) *There are precisely $d$ elements of order dividing $d$*

*Proof.* We prove each in turn

a) $(g^r)^s = e_G \iff g^{rs} = e_G \overset{(3.3.14)}{\iff} n \mid rs \overset{(2.3.13)}{\iff} \frac{n}{(n,r)} \mid s$. Therefore $g^r$ has order $\frac{n}{(n,r)}$ as required.

b) Note $h$ is a generator iff $o(h) = n$. So $g^r$ is a generator iff $(n, r) = 1$ by the previous step. As $G = \{g, g^2, \ldots, g^n\}$ the result follows by definition of the totient function.

c) Recall there is a canonical surjective morphism $\pi : \mathbb{Z} \to G$ with kernel $n\mathbb{Z}$ and $\pi(1) = g$. By (3.3.17) the subgroups $H$ of $G$ correspond bijectively to subgroups $H'$ of $\mathbb{Z}$ containing $n\mathbb{Z}$, preserving the index. By (3.3.19) these are of the form $H' = d\mathbb{Z}$ for $d \mid n$, which correspond under $\pi$ to subgroups $H = \langle g^d \rangle$. Further $[G : \langle g^d \rangle] = [\mathbb{Z} : d\mathbb{Z}] = d$ whence $\#\langle g^d \rangle = \frac{n}{d}$. By definition $\langle g^d \rangle$ is cyclic.

d) Let $G[d]$ be the unique (cyclic) subgroup of order $d$. If $h$ has order $d$ then $\langle h \rangle$ has order $d$, and therefore by uniqueness is equal to $G[d]$. In particular $h \in G[d]$. Therefore by the previous part there are $\phi(d)$ elements of order $d$

e) Suppose $h$ has order $e \mid d$. Both $G$ and $G[d]$ contain a unique subgroup of order $e$ and therefore by uniqueness this is simply $G[e] \subseteq G[d]$. Similarly by uniqueness $G[e] = \langle h \rangle$. Therefore $h \in G[d]$. Conversely suppose $h \in G[d]$ then $o(g) \mid d$ by (3.3.14). Therefore $G[d]$ consists of all the elements of order dividing $d$.

□

**Corollary 3.3.23**
*Let $n$ be a positive integer then*

$$n = \sum_{d|n} \phi(d)$$

*Proof.* Consider a cyclic group $G$ of order $n$. Every element has order dividing $n$ so the result follows from the previous Proposition by partitioning the group $G$ into subsets consisting of elements of equal order. □

For an abelian group $G$ define the following subgroup

$$G[d] := \{g \in G \mid g^d = e\}.$$

We have shown for a cyclic group that $\#G[d] = d$ whenever $d \mid n$ and it is empty otherwise. We claim that this can be used to characterize cyclic groups. NB the following is adapted from this stackexchange answer

**Proposition 3.3.24** (Characterization of cyclic group)
*Let $G$ be a finite abelian group such that $\#G[d] \leq d$ for all $d \mid n$. Then $G$ is cyclic.*

*Proof.* Let $n = \#G$ and $G_d$ be the subset of elements of order exactly $d$. Then we wish to show that $G_n$ is non-empty as any element of this set will be a generator. We actually show that $\#G_d = \phi(d) > 0$ whenever $d \mid n$.

Note that $G_d \subseteq G[d]$. If it's non-empty then for any $y \in G_d$, we have $\langle y \rangle$ is a subgroup of $G[d]$ of order $d$. As $\#G[d] \leq d$ we have $G[d] = \langle y \rangle$ is cyclic of order $d$. In other words $G_d$ is equal to the set of generators for $G[d]$. By the previous Proposition $G[d]$ has $\phi(d)$ generators. We conclude that for all $d \mid n$ we have $G_d$ is either empty or of order $\phi(d)$.

Therefore

$$n = \sum_{d|n} \#G_d \leq \sum_{d|n} \phi(d) = n$$

Therefore we must have equality everywhere and $\#G_d = \phi(d)$ as required. □

**Example 3.3.25**
*Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ of order $p^2$. Then $G[p] = G$ so $\#G[p] = p^2 > p$.*

### 3.3.2 Group Actions

**Definition 3.3.26** (Group Action)
*Let $G$ be a group and $S$ a set. A group action of $G$ on $S$ is a map*

$$G \times S \longrightarrow S$$
$$(g, s) \longrightarrow g \cdot s$$

*such that*

- $es = s$
- $g(hs) = (gh)s$

**Definition 3.3.27** (Faithful group action)
*A group action $G$ on $S$ is faithful if*

$$gs = s \quad \forall s \in S \implies g = e$$

**Definition 3.3.28** (Free group action)
*A group action $G$ on $S$ is free if*

$$g \neq e \implies gs \neq s \quad \forall s$$

**Definition 3.3.29** (Orbit/Stabilizer)
*Let $G$ be a group with an action on $S$ and $s \in S$. Define the stabilizer subgroup*

$$G_s := \{g \in G \mid gs = s\}$$

*and the orbit*

$$Gs := \{gs \mid g \in G\}$$

**Proposition 3.3.30** ($S$ is disjoint union of orbits)
*Let $G$ be a group with an action on $S$. Then the following is an equivalence relation*

$$s \sim t \iff gs = t \text{ some } g \in G$$

*and the equivalence classes are precisely the orbits of elements of $S$ under $G$. Further $S$ is the disjoint union of orbits.*

**Remark 3.3.31**
*An action is free if and only if $G_s = \{e\}$ for all $s \in S$.*

**Proposition 3.3.32** (Orbit-Stabilizer Theorem)
*Let $G$ be a group with an action on $S$. Given an element $s \in S$ there is a natural bijection*

$$G/G_s \longrightarrow Gs$$

*between the cosets of $G_s$ and the orbit $Gs$. In particular when $G$ is finite*

$$\#G = \#Gs \times \#G_s$$

*and when the action is free*

$$\#G = \#Gs$$

## 3.4 Rings and Modules

### 3.4.1 Commutative Rings

**Definition 3.4.1** (Ring)
*A ring consists of a triple $(A, +, \cdot)$ where $A$ is a set and $+$ and $\cdot$ are laws of composition ("additive" and "multiplicative" respectively) such that the following holds*

- $(A, +)$ *is an* ***abelian group****, whose identity element we refer to as $0_A$.*
- $(A, \cdot)$ *is a* ***monoid****, whose identity element we refer to as $1_A$*
- $+$ *and* $\cdot$ *satisfy the* ***distributive property****, that is for all $x, y, z \in A$*

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(x + y) \cdot z = x \cdot z + y \cdot z$$

*For $x \in A$ we write the additive inverse as $-x$, and abbreviate multiplication $x \cdot y =: xy$.*

*We say that $A$ is a* ***zero-ring*** *(or trivial) if $0_A = 1_A \iff A = \{0\}$.*

*$A$ is* ***commutative*** *if in addition $xy = yx$ i.e. $(A, \cdot)$ is abelian.*

**Definition 3.4.2** (Subring)
*A* ***subring*** *of a ring $A$ is a subset $B$ such that*

- $0_A, 1_A \in B$
- $x \in B \implies -x \in B$
- $x, y \in B \implies x + y \in B$
- $x, y \in B \implies x \cdot y \in B$

*Then* $(B, +|_{B\times B}, \cdot|_{B\times B})$ *is a ring.*

**Definition 3.4.3** (Multiplicative set)
*A subset* $S \subset A$ *is said to be* ***multiplicative*** *if*

- $1 \in S$
- $x, y \in S \implies xy \in S$

*Further it is said to be* ***saturated*** *if in addition*

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

**Definition 3.4.4** (Integral Domain)
*A commutative ring* $A$ *is said to be an* ***integral domain*** *if it is not a zero-ring and it is* cancellative*, that is*

$$ab = ac, a \neq 0 \implies b = c\,.$$

**Definition 3.4.5** (Reduced)
*A commutative ring* $A$ *is said to be* ***reduced*** *if*

$$x^n = 0 \implies x = 0$$

**Definition 3.4.6** (Unit / Group of Units)
*An element* $0 \neq a$ *of a ring* $A$ *is called a* ***unit*** *if it has a two-sided multiplicative inverse.*

*For* $A$ *not a zero-ring, the set of units* $A^\star$ *forms a group under multiplication, called the* ***group of units****.*

**Definition 3.4.7** (Field)
*A* ***field*** $K$ *is a commutative ring such that every non-zero element is a unit, so that* $K^\star$ *is a group under multiplication.*

Note we have the implications

**Proposition 3.4.8**
*Let* $A$ *be a ring then we have the following implications*

$$\textbf{\textit{field}} \implies \textbf{\textit{integral domain}} \implies \textbf{\textit{reduced}}$$

**Definition 3.4.9** (Ring homomorphism)
*A* ***ring homomorphism*** $\phi : A \to B$ *is a mapping which is both a multiplicative (monoid) and additive (group) homomorphism*

- $\phi(0_A) = 0_B$
- $\phi(1_B) = 1_B$
- $\phi(x + y) = \phi(x) + \phi(y)$
- $\phi(xy) = \phi(x)\phi(y)$

*The* ***kernel*** *of* $\phi$ *is defined to be*

$$\ker(\phi) = \{a \mid \phi(a) = 0_B\}$$

**Definition 3.4.10** (Ideal)
*A (two-sided)* ***ideal*** $\mathfrak{a}$ *of a ring* $A$ *is a subset of* $A$ *which is an additive subgroup and closed under multiplication by* $A$ *:*

- $0_A \in \mathfrak{a}$
- $x, y \in \mathfrak{a} \implies x + y \in \mathfrak{a}$
- $x \in \mathfrak{a} \implies -x \in \mathfrak{a}$
- $x \in \mathfrak{a}, a \in A \implies ax, xa \in \mathfrak{a}$

$\mathfrak{a}$ *is said to be* ***proper*** *if* $\mathfrak{a} \neq A$*.*

**Lemma 3.4.11** (Proper ideal)
*An ideal* $\mathfrak{a}$ *is proper if and only if* $1 \notin \mathfrak{a}$ *if and only if* $\mathfrak{a} \cap A^\star = \emptyset$*.*

*Alternatively* $\mathfrak{a} = A$ *if and only if* $1 \in \mathfrak{a}$ *if and only if* $\mathfrak{a} \cap A^\star \neq \emptyset$*.*

**Proposition 3.4.12**
*Let* $\phi : A \to B$ *be a ring homomorphism, then*

a) *The kernel* $\ker(\phi)$ *is a two-sided ideal of* $A$

b) *The image* $\phi(A)$ *is a subring of* $B$

c) $\phi$ *is injective if and only if* $\ker(\phi) = \{0\}$

**Proposition 3.4.13** (Krull's Theorem)
*Let* $A$ *be a ring and* $\mathfrak{a}$ *a proper ideal. Then it is contained in a proper maximal ideal* $\mathfrak{m}$.

*In particular any non-unit* $a \notin A^\star$ *is contained in a maximal ideal.*

### 3.4.2 Modules I

**Definition 3.4.14** (Module)
*Let* $A$ *be a ring. A* ***left*** $A$***-module*** $(M, +, \cdot)$ *is an abelian group* $(M, +)$ *together with a "multiplication" operation* $A$

$$\cdot : A \times M \to M$$

*which satisfies the* ***distributive*** *properties*

$$(a + b) \cdot x = a \cdot x + b \cdot x$$
$$a \cdot (x + y) = a \cdot x + a \cdot y$$

**Definition 3.4.15** (Submodule)
*Let* $(M, +, \cdot)$ *be a left* $A$*-module. Then a subset* $N \subset M$ *is called an* $A$***-submodule*** *if*

- $N$ *is a subgroup of* $(M, +)$
- $m \in N, a \in A \implies am \in N$

*Then* $(N, +|_{N\times N}, \cdot|_{A\times N})$ *is a left* $A$*-module.*

**Definition 3.4.16** (Module homomorphism)
*Let* $(M, +, \cdot), (N, +, \cdot)$ *be left* $A$*-modules. A function* $f : M \to N$ *is an* $A$*-module homomorphism if*

- *It is an (additive) group homomorphism* $(M, +) \to (N, +)$.
- *It is* $A$*-linear;* $\forall a \in A, m \in M \quad f(a \cdot m) = a \cdot f(m)$

*It may be verified that* $f$ *is bijective if and only if it's an isomorphism.*

**Definition 3.4.17** (Kernel and Image)
*The* ***kernel*** *of a module homomorphism* $f$ *is given by*

$$\ker(f) := \{m \in M \mid f(m) = 0\}$$

*and the* ***image*** *is given by*

$$\mathrm{Im}(f) = f(M)$$

**Example 3.4.18** (Trivial Examples)
*A ring* $A$ *is a left* $A$*-module over itself, denoted* $A_s$.

**Definition 3.4.19** (Restriction of Scalars)
*Let* $\phi : A \to B$ *a ring homomorphism and* $M$ *a* $B$*-module. Then we may consider* $M$ *as an* $A$*-module in the obvious way. Denote this by* $[M]_\phi$.

**Proposition 3.4.20** (Submodules constitute a lattice)
*Let* $M$ *be a left* $A$*-module then the collection* $\mathrm{SubMod}(M)$ *of* $A$*-submodules form a complete sub-lattice of* $\mathcal{P}(M)$ *with meet and join given by*

$$\bigwedge_{i\in I} N_i = \bigcap_{i\in I} N_i$$

*and (the* ***internal sum****)*

$$\bigvee_{i\in I} N_i = \bigcap_{N_i \subseteq N \leq M} N =: \sum_{i\in I} N_i = \left\{ \sum_{j\in J} n_j \mid n_j \in N_j \quad \#J < \infty \right\}$$

*Moreover it is the image of the closure operator* $\langle - \rangle : \mathcal{P}(M) \to \mathcal{P}(M)$ *given by*

$$\langle X \rangle = \bigcap_{X \subseteq N} N = \left\{ \sum_j a_j x_j \mid x_j \in X \right\}$$

*Proof.* The $A$-submodules of $M$ naturally form a Moore family of subsets of $M$. By (2.1.38) they form a complete sub-lattice with the given form of meet and join. Furthermore it is the image of the given closure operator. The only non-trivial statement is the explicit form of $\sum_{i\in I} N_i$ TODO. □

**Lemma 3.4.21**
*Let $M$ be a module. Then*

a) $\langle \bigcup_{i\in I} X_i \rangle = \sum_{i\in I} \langle X_i \rangle$

b) $\langle \bigcup_{i\in I} N_i \rangle = \sum_{i\in I} N_i$

c) $N_1 \subseteq N_2 \implies N_1 + N_2 = N_2$

*Proof.* a) This follows from (2.1.41) applied to the closure operator $\langle - \rangle$

b) This follows from $a$) because $N_i = \langle N_i \rangle$

c) This follows from $b$) because $N_1 \cup N_2 = N_2$

□

**Definition 3.4.22** (External Direct Sum)
*Let $A$ be a ring and $\{M_i\}_{i\in I}$ a family of left $A$-modules. Define the **external direct sum** as the set of ordered tuples indexed over $I$*

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i\}$$

*with the obvious module operations.*

**Definition 3.4.23** (Free Module)
*A left $A$-module $M$ is **free** if it is isomorphic to $\bigoplus_{i\in I} A =: A^I$ for some indexing set $I$. When $I$ may be taken to be finite then $M$ is a **finite free** module.*

**Definition 3.4.24** (Product of ideal and module)
*Let $M$ be a left $A$-module and $\mathfrak{a} \triangleleft A$ an ideal. Define*

$$\mathfrak{a}M = \langle \mathfrak{a} \cdot M \rangle = \{\sum_{i=1}^{n} a_i m_i \mid a_i \in \mathfrak{a} \quad m_i \in M\}$$

### 3.4.3 Operations on Ideals

For this section we assume $A$ is a commutative ring.

**Proposition 3.4.25** (Lattice of Ideals)
*Let $A$ be a ring and $\mathcal{I}(A)$ the set of ideals. Then $\mathcal{I}(A)$ forms a complete lattice ordered by inclusion with join and meets given by*

$$\bigwedge_{i\in I} \mathfrak{a}_i = \bigcap_{i\in I} \mathfrak{a}_i$$

*and*

$$\bigvee_{i\in I} \mathfrak{a}_i = \bigcap_{\mathfrak{a}_i \subseteq \mathfrak{a}} \mathfrak{a} =: \sum_i \mathfrak{a}_i := \{\sum_i a_i \mid a_i \in \mathfrak{a}_i\}$$

*This induces a corresponding closure operator*

$$\langle - \rangle : \mathcal{P}(A) \to \mathcal{I}(A)$$

*given by*

$$\langle X \rangle := \bigcap_{X \subseteq \mathfrak{a}} \mathfrak{a} = \{\sum_j a_j x_j \mid a_j \in A \quad x_j \in X\}$$

**Proposition 3.4.26**
*Let $A$ be a ring and $\mathfrak{a}_i$ a family of ideals. Then*

$$\langle \bigcup_{i\in I} \mathfrak{a}_i \rangle = \sum_{i\in I} \mathfrak{a}_i$$

**Definition 3.4.27** (Product of ideals)
*The product of two ideals* $\mathfrak{ab}$ *is*

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a} \quad b_i \in \mathfrak{b} \right\}$$

*and is itself an ideal.*

**Definition 3.4.28** (Coprime)
*We say two elements* $x, y$ *of a commutative ring* $A$ *are* ***co-prime*** *if* $(x, y) = (1) \iff ax + by = 1$ *for some* $a, b \in A$

*We say a family of ideals* $\{\mathfrak{a}_i\}_{i \in I}$ *are co-prime if* $\sum_{i \in I} \mathfrak{a}_i = A$.

**Definition 3.4.29** (Principal Ideal)
*A* ***principal ideal*** *is an ideal generated by a single element*

$$(a) := \langle \{a\} \rangle = Aa$$

**Lemma 3.4.30**
*A principal ideal* $(a)$ *is proper if and only if* $a \notin A^\star$

**Definition 3.4.31** (Maximal Ideal)
*An ideal* $\mathfrak{m} \triangleleft A$ *is* ***maximal*** *if it is both proper and not contained in another proper ideal.*

**Definition 3.4.32** (Prime Ideal)
*An ideal* $\mathfrak{p} \triangleleft A$ *is* ***prime*** *if it is both proper and satisfies the following property*

$$xy \in \mathfrak{p} \implies x \in \mathfrak{p} \vee y \in \mathfrak{p}$$

**Definition 3.4.33** (Radical Ideal)
*An ideal* $\mathfrak{a} \triangleleft A$ *is* ***radical*** *if it satisfies the following property*

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

**Proposition 3.4.34** (Maximal ideals exist)
*Let* $A$ *be a ring and* $\mathfrak{a} \triangleleft A$ *a proper ideal. Then it is contained in some maximal ideal* $\mathfrak{m}$.

*In particular there always exists a maximal ideal by considering* $\mathfrak{a} = (0)$.

*Proof.* Simple application of Zorn's Lemma. □

**Proposition 3.4.35** (Properties of prime ideals)
*Let* $\mathfrak{p}$ *be a prime ideal and* $\mathfrak{a}$, $\mathfrak{b}$ *be ideals then the following are equivalent*

a) $\mathfrak{a} \subseteq \mathfrak{p}$ *or* $\mathfrak{b} \subseteq \mathfrak{p}$

b) $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$

c) $\mathfrak{ab} \subseteq \mathfrak{p}$

*Proof.* *a)* $\implies$ *b)* Follows because $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$
*b)* $\implies$ *c)* Follows because $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$
*c)* $\implies$ *a)* If $\mathfrak{a} \not\subseteq \mathfrak{p}$, then choose $a \in \mathfrak{a} \setminus \mathfrak{p}$. By hypothesis $a\mathfrak{b} \subseteq \mathfrak{p}$ and since $\mathfrak{p}$ is prime $\mathfrak{b} \subseteq \mathfrak{p}$. □

**Corollary 3.4.36** (Ideal version of primality)
*Let* $\mathfrak{p}$ *be a proper ideal. Then* $\mathfrak{p}$ *is prime if and only if the following condition holds for all ideals* $\mathfrak{a}$, $\mathfrak{b}$

$$\mathfrak{ab} \subseteq \mathfrak{p} \implies \mathfrak{a} \subseteq \mathfrak{p} \text{ or } \mathfrak{b} \subseteq \mathfrak{p}$$

*In particular for all* $k > 0$ *we have*

$$\mathfrak{a} \subseteq \mathfrak{p} \iff \mathfrak{a}^k \subseteq \mathfrak{p}$$

*Proof.* One direction has been shown in (3.4.35). Conversely suppose $fg \in \mathfrak{p}$ then apply the condition to the ideals $(f)$ and $(g)$ we find $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. □

**Lemma 3.4.37** (Generate prime ideals)
*Let* $A$ *be a ring,* $S$ *a multiplicative set and* $\mathfrak{b} \triangleleft A$ *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.* Since $\mathfrak{b} \in \mathcal{I}$ it is non-empty. 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 3.4.38**
*Let $A$ be a ring. Then the set* $\mathrm{Rad}(A)$ *of radical ideals forms a complete sub-lattice of the lattice of ideals $\mathcal{I}(A)$. This induces a closure operator*

$$\sqrt{-} : \mathcal{I}(A) \to \mathrm{Rad}(A)$$

*given by*

$$\sqrt{\mathfrak{a}} := \bigcap_{\mathfrak{a} \subseteq \mathfrak{r}} \mathfrak{r} = \{x \mid x^n \in \mathfrak{a} \quad n > 0\}$$

*The "join" is given by*

$$\bigvee_{i \in I} \mathfrak{a}_i = \sqrt{\sum_i \mathfrak{a}_i}$$

*In particular*

a) $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$

b) $\mathfrak{a} \subseteq \mathfrak{b} \implies \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$

c) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$

*Proof.* The set of radical ideals is closed under arbitrary intersections (which are meets in the lattice $\mathcal{I}(A)$). Therefore by (2.1.38) it forms a complete sub-lattice with meet given by intersection of ideals.

It also shows that $\sqrt{-}$ as defined is a closure operator with image $\mathrm{Rad}(A)$, which demonstrates the required properties.

Finally we just need to show that $I' := \{x \mid x^n \in \mathfrak{a} \quad n > 0\}$ is equal to $\sqrt{\mathfrak{a}}$. Firstly it's an ideal for if $x, y \in I'$ then $x^n \in \mathfrak{a}$ and $y^m \in \mathfrak{a}$, so we may show that $(x+y)^{n+m} \in \mathfrak{a}$ whence $x + y \in I'$. Similarly $a \in A$ and $x \in I'$ implies $(ax)^n = a^n x^n \in I'$. It's radical for suppose $x^m \in I'$ then $x^{mn} = (x^m)^n \in \mathfrak{a}$ by definition whence $x \in I'$. As it contains $\mathfrak{a}$ we find that $\sqrt{\mathfrak{a}} \subseteq I'$. Let $\mathfrak{r}$ be another radical ideal containing $\mathfrak{a}$ then $x \in I' \implies x^n \in \mathfrak{a} \implies x^n \in \mathfrak{r} \implies x \in \mathfrak{r}$. Therefore the reverse inclusion follows. □

**Proposition 3.4.39** (Prime Nullstellensatz)
*The radical of an ideal satisfies*

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

*Proof.* Suppose $x \in \sqrt{\mathfrak{a}}$ and $\mathfrak{p} \supseteq \mathfrak{a}$. Then $x^n \in \mathfrak{p} \implies x \in \mathfrak{p}$. Therefore $\sqrt{\mathfrak{a}} \subseteq \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}$. Conversely suppose $x \notin \sqrt{\mathfrak{a}}$ then $S := \{1, x, x^2, \ldots\}$ is a proper multiplicative set such that $S \cap \mathfrak{a} = \emptyset$. By (3.4.37) there is a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ which does not intersect $S$. Therefore $x \notin RHS$ as required. □

**Proposition 3.4.40** (Properties of Radical Ideals)
*Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals then*

a) $\sqrt{\mathfrak{a}^k} = \sqrt{\mathfrak{a}}$ *for* $k > 0$

b) $\sqrt{\sum_i \mathfrak{a}_i} = \sqrt{\sum_i \sqrt{\mathfrak{a}_i}}$

c) $\sqrt{\mathfrak{a}} = A \iff \mathfrak{a} = A$

d) $\sum_i \mathfrak{a}_i = A \iff \sum_i \sqrt{\mathfrak{a}_i} = A$

e) $\sum_{i=1}^n \mathfrak{a}_i^{k_i} = A \iff \sum_{i=1}^n \mathfrak{a}_i = A \quad k_i > 0.$

*Proof.* a) This may be shown by direct calculation or combining (3.4.39) and (3.4.35).

b) This follows by applying (2.1.41) to the closure operator $\sqrt{-}$.

c) $\sqrt{\mathfrak{a}} = A \iff 1 \in \sqrt{\mathfrak{a}} \iff 1 \in \mathfrak{a} \iff \mathfrak{a} = A$

d) This follows from combining *c*) and *b*)

e) This follows from *d*) and *a*)

□

**Definition 3.4.41** (Extended and contracted ideals)
*Let $\phi : A \to B$ be a homomorphism and $\mathfrak{a}$ (resp. $\mathfrak{b}$) be an ideal of $A$ (resp. $B$). Define the **contraction** (resp. **extension**) ideals as follows*

$$\begin{aligned} \mathfrak{b}^c &:= \phi^{-1}(\mathfrak{b}) \\ \mathfrak{a}^e &:= \phi(\mathfrak{a})B := \langle \phi(\mathfrak{a}) \rangle = \{ \sum_i b_i \phi(a_i) \mid a_i \in \mathfrak{a} \} \end{aligned}$$

*An ideal is said to be **contracted** (resp. **extended**) if it is of the form $\mathfrak{b}^c$ (resp. $\mathfrak{a}^e$)*

**Proposition 3.4.42** (Operations on ideals)
*Let $\phi : A \to B$ a ring homomorphism and $\mathfrak{a} \lhd A$, $\mathfrak{b} \lhd B$ ideals then*

a) $\mathfrak{b}^c \lhd A$ *and* $\mathfrak{a}^e \lhd B$

b) $\mathfrak{b}^c$ *proper if and only if* $\mathfrak{b}$ *is proper*

c) $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ *and* $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$

d) $\mathfrak{a}^{ece} = \mathfrak{a}^e$ *and* $\mathfrak{b}^{cec} = \mathfrak{b}^c$

e) $\mathfrak{b}^{ce} = \mathfrak{b} \iff \mathfrak{b}$ *is an extended ideal* $\iff \mathfrak{b} \subseteq \mathfrak{b}^{ce}$

f) $\mathfrak{a}^{ec} = \mathfrak{a} \iff \mathfrak{a}$ *is a contracted ideal* $\iff \mathfrak{a}^{ec} \subseteq \mathfrak{a}$

g) $\sqrt{\mathfrak{b}^c} = \left(\sqrt{\mathfrak{b}}\right)^c$

h) $(\sqrt{\mathfrak{b}^c})^e \subseteq \sqrt{\mathfrak{b}}$ *with equality when $\phi$ is surjective*

*When $\phi$ is surjective every ideal $\mathfrak{b} \lhd B$ is extended, and the contracted ideals are precisely the ideals containing* $\ker(\phi)$.

*Proof.* We prove each in turn

a-c) Straightforward

d) By the previous step $\mathfrak{b}^{ce} \subseteq \mathfrak{b} \implies (\mathfrak{b}^{ce})^c \subseteq \mathfrak{b}^c$, similarly $\mathfrak{b}^c \subseteq (\mathfrak{b}^c)^{ec}$. The other relation is similar.

e-f) These follow from $c$) and $d$)

g) $x \in \left(\sqrt{\mathfrak{b}}\right)^c \iff \phi(x) \in \sqrt{\mathfrak{b}} \iff \phi(x)^n \in \mathfrak{b} \iff \phi(x^n) \in \mathfrak{b} \iff x^n \in \mathfrak{b}^c \iff x \in \sqrt{\mathfrak{b}^c}$

h) By $c$) and $g$) we find $(\sqrt{\mathfrak{b}^c})^e = \left(\sqrt{\mathfrak{b}}\right)^{ce} \subseteq \sqrt{\mathfrak{b}}$. We will show that when $\phi$ is surjective every ideal is extended, in which case the equality follows from $e$).

Suppose that $\phi$ is surjective. Then by $e$) we only need to show that $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$ for every ideal $\mathfrak{b}$. Let $y \in \mathfrak{b}$ then $y = \phi(x)$, whence $x \in \mathfrak{b}^c$ and $y \in \mathfrak{b}^{ce}$. □

**Corollary 3.4.43**
*Let $\phi : A \to B$ be a ring homomorphism then extension and contraction constitute a monotone Galois connection*

$$\{\mathfrak{a} \lhd A\} \longleftrightarrow \{\mathfrak{b} \lhd B\}$$

*and therefore is order-preserving and satisfies the adjoint property*

$$\mathfrak{a} \subseteq \mathfrak{b}^c \iff \mathfrak{a}^e \subseteq \mathfrak{b}$$

*is satisfied.*

*Proof.* Extension and contraction satisfy conditions of (2.1.43) by (3.4.42).c) and d) □

**Corollary 3.4.44**
*Let $\phi : A \to B$ be a ring homomorphism then there is a order-preserving bijection between "contracted" and "extended ideals"*

$$\{\mathfrak{a} \lhd A \mid \mathfrak{a} \text{ contracted } \} \longleftrightarrow \{\mathfrak{b} \lhd B \mid \mathfrak{b} \text{ extended } \}$$

*which restricts to proper ideals.*

*Proof.* We've shown that $\mathfrak{a}$ (resp. $\mathfrak{b}$) is contracted (resp. extended) if and only if the given maps are mutually inverse. Note that $\mathfrak{b}$ is proper implies $\mathfrak{b}^c$ is proper. Furthermore $\mathfrak{b}^c$ proper implies $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ is proper. Therefore it restricts to proper ideals. □

**Proposition 3.4.45** (Inverse image of maximal / prime ideals)
*Let $\phi : A \to B$ be a morphism then*

- $\mathfrak{q} \lhd B$ *prime* $\implies \phi^{-1}(\mathfrak{q})$ *prime*
- $\mathfrak{n} \lhd B$ *maximal and $\phi$ surjective* $\implies \phi^{-1}(\mathfrak{n})$ *is maximal*

### 3.4.4 Quotient Rings

**Proposition 3.4.46** (Quotient Ring)
*Let $(A,+,\cdot)$ be a ring and $\mathfrak{a}$ an ideal. As $\mathfrak{a}$ is an additive subgroup we may consider the quotient group $(A/\mathfrak{a},+)$. For an element $a \in A$ write $a+\mathfrak{a}$ for the coset $[a]_{\mathfrak{a}} \in A/\mathfrak{a}$. There is a well-defined multiplicative law of composition*

$$\cdot : A/\mathfrak{a} \times A/\mathfrak{a} \to A/\mathfrak{a}$$
$$(a+\mathfrak{a})\cdot(b+\mathfrak{a}) \to (a\cdot b+\mathfrak{a})$$

*which makes $(A/\mathfrak{a},+,\cdot)$ into a ring. Further there is a canonical surjective ring homomorphism*

$$\pi : A \to A/\mathfrak{a}$$

*with the following properties*

- $\ker(\pi)=\mathfrak{a}$
- *Every morphism $\phi : A \to B$ such that $\mathfrak{a} \subseteq \ker(\phi)$, factors uniquely through $\pi$.*

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle \pi} & \nearrow_{\tilde{\phi}} & \\ A/\mathfrak{a} & & \end{array}$$

- $\ker(\tilde{\phi}) = \ker(\phi)/\mathfrak{a}$
- *$\tilde{\phi}$ is injective if and only if* $\ker(\phi)=\mathfrak{a}$
- *$\tilde{\phi}$ is surjective if and only if $\phi$ is surjective*

*For an ideal $\mathfrak{b} \supseteq \mathfrak{a}$ define the corresponding quotient ideal*

$$\mathfrak{b}/\mathfrak{a} := \{b+\mathfrak{a} \mid b \in \mathfrak{b}\} = \pi(\mathfrak{b})$$

*This induces a bijective, order-preserving correspondence of ideals*

$$\{\mathfrak{b}' \lhd A/\mathfrak{a}\} \underset{\pi^{-1}(-)}{\overset{\pi(-)}{\leftrightarrows}} \{\mathfrak{b} \lhd A \mid \mathfrak{a} \subseteq \mathfrak{b}\}$$

*under which maximal (resp. prime) ideals of $A$ containing $\mathfrak{a}$ correspond to maximal (resp. prime) ideals of $A/\mathfrak{a}$.*

**Corollary 3.4.47** (Isomorphism Theorem)
*Let $\phi : A \to B$ be a ring homomorphism. Then this induces a canonical isomorphism*

$$A/\ker(\phi) \cong \phi(A) \subset B$$

**Corollary 3.4.48** (Second Isomorphism Theorem)
*Let $\mathfrak{b}$,$\mathfrak{a}$ be ideals then there is a unique morphism making the diagram commute*

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\mathfrak{a} \\ \downarrow{\scriptstyle \pi} & \swarrow & \downarrow{\scriptstyle \pi} \\ A/(\mathfrak{a}+\mathfrak{b}) & \xrightarrow{\sim} & (A/\mathfrak{a})/((\mathfrak{a}+\mathfrak{b})/\mathfrak{a}) \end{array}$$

*which is in fact an isomorphism. If $\mathfrak{a}+\mathfrak{b} \subseteq \mathfrak{c}$ this restricts to an isomorphism of $A/\mathfrak{b}$-modules*

$$\begin{array}{ccc} \mathfrak{c} & \xrightarrow{\pi} & \mathfrak{c}/\mathfrak{a} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathfrak{c}/(\mathfrak{a}+\mathfrak{b}) & \xrightarrow{\sim} & (\mathfrak{c}/\mathfrak{a})/((\mathfrak{a}+\mathfrak{b})/\mathfrak{a}) \end{array}$$

**Proposition 3.4.49** (Criteria for Maximal, Prime and Reduced)
*Let $\mathfrak{a} \lhd A$ then $\mathfrak{a}$ is*

- ***maximal** if and only if $A/\mathfrak{a}$ is a field*
- ***prime** if and only if $A/\mathfrak{a}$ is an integral domain*
- ***radical** if and only if $A/\mathfrak{a}$ is reduced*

**Corollary 3.4.50**
*Let $\mathfrak{a} \triangleleft A$ be a proper ideal, then the following implications hold*

$$\textbf{\textit{maximal}} \implies \textbf{\textit{prime}} \implies \textbf{\textit{radical}}$$

*Proof.* This follows by comining (3.4.8) and (3.4.49). □

**Corollary 3.4.51**
*Let $A$ be a non-zero ring. Then $A$ is a field if and only if the only proper ideal is $(0)$.*

*Proof.* Let $\mathfrak{a} = (0)$ then $A \to A/(0)$ is an isomorphism. Then it follows by a previous Proposition. □

**Corollary 3.4.52** (Field Morphisms are injective)
*Let $\phi : k \to B$ be a homomorphism from a field to a non-zero ring. Then $\phi$ is injective.*

*Proof.* $\ker(\phi)$ is an ideal. As $\phi(1_k) = 1_B$ and $0_B \neq 1_B$ then $\ker(\phi) \neq k$. Since the only ideals are $(0)$ and $k$ we see $\ker(\phi) = \{0\}$ and $\phi$ is injective. □

### 3.4.5 Irreducible and Reduced rings

We say an element $x$ is nilpotent if $x^n = 0$. By (3.4.38) these form an ideal.

**Definition 3.4.53** (Nilradical)
*Define the **nilradical** to be the set (ideal) of nilpotents*

$$\mathfrak{N}(A) := \sqrt{(0)} \overset{(3.4.39)}{=} \bigcap_{\mathfrak{p}} \mathfrak{p}$$

*Clearly $A$ is reduced if and only if $\mathfrak{N}(A) = \{0\}$.*

We also make the following definition

**Definition 3.4.54** (Irreducible)
*Let $A$ be a ring. We say $A$ is **irreducible** if $\mathfrak{N}(A)$ is prime.*

**Lemma 3.4.55** (Integral Domain $\iff$ 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 $\mathfrak{N}(A)$ 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. □

### 3.4.6 Algebra over a Commutative Ring

For what follows let $A$ be a commutative ring.

**Definition 3.4.56** (Algebra (over a commutative ring))
*An algebra over $A$ (or an $A$-algebra) is a pair $(i_B, B)$ where $B$ is a (not necessarily commutative) ring and $i_B : A \to B$ is a ring homomorphism.*

*We call $i_B$ the structural morphism and write $a \cdot b := i_B(a)b$*

*Morphisms of $A$-algebras are the ring homomorphisms $\phi : B \to C$ such that $\phi \circ i_B = i_C$. This then constitutes a category $\mathbf{Alg}_A$.*

*If $k$ is a field an algebra over $k$ is referred to as a $k$-algebra.*

**Definition 3.4.57** (Sub-algebra)
*Let $(i_B, B)$ be an $A$-algebra. A sub-algebra $C$ is a subring $C$ of $B$ for which*

$$a \in A \quad c \in C \implies i_B(a)c \in C$$

**Example 3.4.58** (Algebra over commutatve sub-ring)
*If $A \subset B$ is a commutative sub-ring, then $B$ is naturally a $A$-algebra.*

*The polynomial ring $A[X]$ is naturally an $A$-algebra*

**Definition 3.4.59** (Algebra generated by a set)
*Let $B$ be an $A$-algebra. The collection of $A$-subalgebras forms a Moore family. Therefore by (2.1.38) there is a canonical closure operator*

$$A[-] : \mathcal{P}(B) \to \mathrm{SubAlg}_A(B)$$

*which we denote by $A[S]$ for $S \subset B$. A more explicit characterization when $S$ is finite is given in Section Section 3.7. More generally we have*

$$A[S] = \bigcup_{S' \subset S | S' \text{ finite}} A[S']$$

### 3.4.7 Modules II

**Definition 3.4.60** (Faithful Module)
*We say an $A$-module $M$ is **faithful** if*

$$am = 0 \quad \forall m \in M \implies a = 0$$

**Definition 3.4.61** (Linearly Independent, Spanning and Basis)
*Let $M$ be an $A$-module and $S \subset M$ a set. We say $S$ is*

- ***spanning** if $\langle S \rangle = M$*
- ***linearly independent** if for every finite subset $\{s_1, \ldots, s_n\} \subseteq S$ with $s_i$ distinct we have*

$$\sum_{i=1}^{n} a_i s_i = 0 \implies a_i = 0 \quad 1 \leq i \leq n$$

- *a **basis** if it is both spanning and linearly independent*

**Definition 3.4.62** (Finite Module)
*An $A$-module $M$ is **finite** if there exists a finite spanning set.*

**Definition 3.4.63** (Minimal spanning set)
*Let $M$ be an $A$-module. Then $S \subset M$ is a **minimal spanning set** if it generates $M$ and no proper subset does so.*

**Definition 3.4.64** (Free Module)
*Let $M$ be an $A$-module. We say that $M$ is a **free module** over $A$ if it has a basis.*

**Proposition 3.4.65** (Free $A$-module is an external sum of $A$)
*An $A$-module $M$ is free if and only if it is isomorphic to $\bigoplus_{i \in I} A$ for some $I$. The isomorphism is given by*

$$\sum_{i \in I} a_i m_i \to (a_i)_{i \in I}$$

**Definition 3.4.66** (Vector space)
*If $k$ is a field and $V$ a $k$-module, then we say $V$ is a **vector space** over $k$.*

**Definition 3.4.67** (Module homomorphism)
*A **module homomorphism** $\phi : M \to N$ is an additive group homomorphism which commutes with the $A$ action*

$$\phi(am) = a\phi(m) \quad \forall a \in A \, m \in M$$

*Denote the $A$-module of morphisms*

$$\mathrm{Mor}_A(M, N)$$

*and the $A$-algebra of endomorphisms*

$$\mathrm{End}_A(M) := \mathrm{Mor}_A(M, M)$$

**Proposition 3.4.68** (Kernel)
*Let $\phi : M \to N$ be an $A$-module homomorphism, then the **kernel** of $\phi$*

$$\ker(\phi) := \{m \in M \mid \phi(m) = 0\}$$

*is an $A$-submodule of $M$. Observe $\phi$ is injective iff $\ker(\phi) = 0$.*

**Proposition 3.4.69** (Image)
*Let $\phi : M \to N$ be an $A$-module homomorphism then the image*

$$\mathrm{Im}(\phi) = \{\phi(m) \mid m \in M\}$$

*is an $A$-submodule of $N$.*

**Definition 3.4.70** (Quotient Module)
*Let $N \subseteq M$ be an $A$-submodule then define the* ***quotient module*** *$M/N$ to be the quotient group with an action of $A$ given by*

$$a(m+N) = (am+N)$$

*When $N \subseteq P \subseteq M$ is a sequence of submodules then define the $A$-submodule $P/N$ of $M/N$ by*

$$P/N := \{p+N \mid p \in P\}$$

**Proposition 3.4.71** (Quotient Module Properties)
*Let $N \subseteq M$ be an $A$-submodule then there is a canonical surjective morphism*

$$\pi : M \to M/N$$

*with the following properties*

a) $\pi(m) = m+N$

b) $\ker(\pi) = N$

c) *Every homomorphism $\psi : M \to P$ such that $N \subseteq \ker(\psi)$, factors uniquely through $\pi$*

$$\begin{array}{ccc} M & \xrightarrow{\psi} & P \\ \downarrow{\scriptstyle \pi} & \nearrow_{\tilde{\psi}} & \\ M/N & & \end{array}$$

*Furthermore there is a bijection of $A$-submodules*

$$\{P' \subseteq M/N\} \longleftrightarrow \{P \mid N \subseteq P \subseteq M\}$$

*given by $P' = P/N$. In the situation above $\ker(\tilde{\psi}) = \ker(\psi)/N$. In particular if $\ker(\psi) = N$ then $\tilde{\psi}$ is injective.*

**Corollary 3.4.72**
*Let $\psi : M \to N$ be an $A$-module homomorphism, then this induces an isomorphism*

$$M/\ker(\psi) \cong \mathrm{Im}(\psi)$$

**Definition 3.4.73** (Exact Sequence)
*Let $N \xrightarrow{\phi} M \xrightarrow{\psi} P$ be an sequence of $A$-module homomorphisms. We say it is* ***exact*** *if*

$$\mathrm{Im}(\phi) = \ker(\psi)$$

*It is equivalent to the following two conditions*

a) $\psi \circ \phi = 0$

b) $\psi(m) = 0 \implies m = \phi(n)$ *for some $n \in N$.*

*An exact sequence of the form*

$$0 \to N \to M \to P \to 0$$

*is said to be* ***short-exact****.*

**Remark 3.4.74**
*There are a few trivial observations*

- $0 \to M \to N$ *is exact if and only if the map $M \to N$ is injective*
- $M \to N \to 0$ *is exact if and only if the map $M \to N$ is surjective.*

**Proposition 3.4.75** (Isomorphism induced by short-exact sequence)
*Let $N \subseteq M$ be a $A$-submodule then there is a canonical short-exact sequence*

$$0 \to N \to M \to M/N \to 0$$

*Conversely suppose we have a short exact sequence*

$$0 \to N \xrightarrow{i} M \xrightarrow{\pi} P \to 0$$

*then this induces an isomorphism*

$$M/i(N) \cong P$$

*If $N$ is a submodule of $M$ then we would simply write $M/N \cong P$.*

**Proposition 3.4.76** (Second Isomorphism Theorem)
*Let $N \subseteq N' \subseteq M$ be a chain of modules then there is a short-exact sequence*

$$0 \to N'/N \to M/N \to M/N' \to 0$$

*which then induces an isomorphism*

$$(M/N)/(N'/N) \cong M/N'$$

**Proposition 3.4.77** (Product of ideal and quotient module)
*Let $N$ be a submodule of $M$ and $\mathfrak{a} \triangleleft A$ an ideal. Then*

$$\mathfrak{a}(M/N) = (N + \mathfrak{a}M)/N$$

**Proposition 3.4.78** (Induced module)
*Let $M$ be an $A$-module and $\mathfrak{a}$ an ideal such that $\mathfrak{a}M = 0$, then $M$ is naturally an $A/\mathfrak{a}$-module with action given by*

$$\bar{a} \cdot m := a \cdot m$$

### 3.4.8 Vector Spaces

**Definition 3.4.79** (Vector Space)
*A **vector space** $V$ over $k$ is simply a $k$-module.*

*A $k$-submodule is referred to as a **subspace***

*A $k$-module homomorphism is referred to as a **linear map***

*A vector space is finite-dimensional if it is finite as a $k$-module.*

The main result on vector spaces is that bases exist and all have the same cardinality. Recall that $\langle\cdot\rangle$ is a closure operator. We show that $(V, \langle\cdot\rangle)$ determines a matroid so that we may appeal to results in Section 2.2. First we need to show that the notions of independence coincide

**Proposition 3.4.80** (Equivalent definitions of linear independence)
*Let $V$ be a vector space and $S \subset V$. Then the following are equivalent*

a) *$S$ is linearly independent*

b) *No proper subset $S' \subset S$ satisfies $\langle S' \rangle = \langle S \rangle$*

c) ***Matroid Independence*** $x \in S \implies x \notin \langle S \setminus \{x\} \rangle$

*Proof.* *b* $\iff$ *c*) This is (2.2.2).

*a* $\implies$ *c*). If $x \in \langle S \setminus \{x\} \rangle$ then it's clear that $S$ is not linearly independent.

*c* $\implies$ *a*). Suppose we have a linear relationship

$$0 = \sum_{i=1}^{n} \lambda_i v_i \quad v_i \in S$$

Assume wlog that $\lambda_1 \neq 0$, then rearrange to show $v_1 \in \langle S \setminus \{v_1\} \rangle$, contradicting the hypothesis. □

We show that $(V, \langle\cdot\rangle)$ satisfies the Exchange Property and therefore constitutes a matroid.

**Proposition 3.4.81** (Exchange Property)
*Let $V$ be a vector space and $S \subset V$. Then*

$$y \in \langle S \cup \{x\} \rangle \setminus \langle S \rangle \implies x \in \langle S \cup \{y\} \rangle$$

*Proof.* Suppose $y$ is as given, then

$$y = \lambda x + \sum_i \lambda_i s_i \quad s_i \in S$$

Assume wlog that $x \notin S$, then by assumption we must have $\lambda \neq 0$. Therefore we may rearrange to find

$$x = \lambda^{-1} y - \sum_i \lambda^{-1} \lambda_i s_i$$

whence $x \in \langle S \cup \{y\} \rangle$. □

Finally we show $(V, \langle\cdot\rangle)$ is finitary

**Proposition 3.4.82** (Modules are finitary)
*If $v \in \langle S\rangle$ then there exists some finite subset $S' \subset S$ such that $v \in \langle S'\rangle$.*

Therefore we have the following

**Proposition 3.4.83** (Vector Spaces are Free)
*Every vector space has a basis, and in the finite-dimensional case every basis is finite of the same size. We denote this by* $\dim_k V$.

*Proof.* Follows from (2.2.7) and (2.2.9). □

**Proposition 3.4.84**
*A vector space $V = \{0\}$ if and only if* $\dim_k V = 0$

**Proposition 3.4.85** (Image of a basis)
*Let $\phi : V \to W$ be a linear map*

a) *If $S$ is linearly-independent and $\phi$ is injective, then $\phi(S)$ is linearly-independent*

b) *If $\Gamma$ is spanning then ($\phi$ is surjective $\iff$ $\phi(\Gamma)$ is spanning)*

c) *If $\mathcal{B}$ is a basis then ($\phi$ is an isomorphism $\iff$ $\phi(\mathcal{B})$ is a basis and $\phi$ injective on $\mathcal{B}$)*

*Proof.* a) Suppose $\sum_i \lambda_i \phi(s_i) = 0 \implies \phi(\sum_i \lambda_i s_i) = 0$. As $\phi$ is injective this implies $\sum_i \lambda_i s_i = 0 \implies \lambda_i = 0$.

b) If $\phi$ is surjective then for $w \in W$ we have $\phi(v) = w$ for some $v \in V$. By hypothesis $v = \sum_i \lambda_i \gamma_i$ and $w = \sum_i \phi(\lambda_i)$. Conversely given $w \in W$ by hypothesis $w = \sum_i \lambda_i \phi(\gamma_i) = \phi(\sum_i \lambda_i \gamma_i)$ and $\phi$ is surjective as required.

c) Suppose $\phi$ is isomorphism, hence bijective, then it's surely injective on $\mathcal{B}$ and by the previous two points $\phi(\mathcal{B})$ is a basis. Conversely if $\phi(\mathcal{B}) = \mathcal{B}'$ is a basis then by the previous point $\phi$ is surjective. Suppose $\phi(v) = 0$. Then by hypothesis $v = \sum_i \lambda_i v_i$ for $v_i \in \mathcal{B}$ and $0 = \phi(v) = \sum_i \lambda_i \phi(v_i)$. By hypothesis $\phi(v_i)$ are distinct elements of the basis $\mathcal{B}'$ and therefore $\lambda_i = 0$ and $v = 0$. Therefore $\phi$ is injective and therefore bijective.

□

**Corollary 3.4.86** (Dimension is an invariant)
*Dimension is preserved under isomorphism. More generally for $\phi : V \to W$ we have*

$$\phi \text{ injective} \implies \dim_k V \leq \dim_k W$$

$$\phi \text{ surjective} \implies \dim_k V \geq \dim_k W$$

**Proposition 3.4.87**
*Let $W \subseteq V$ be finite-dimensional vector spaces then the dimension of the quotient module satisfies*

$$\dim_k V/W = \dim_k V - \dim_k W$$

*Proof.* Let $\{v_1, \ldots, v_m\}$ be a basis of $W$, then there exists a basis $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ of $V$ containing the first by **??**. We claim that

$$\{[v_{m+1}], \ldots, [v_n]\}$$

is a basis for $V/W$, and the result follows. For given $[v] \in V/W$ then

$$v = \sum_{i=1}^{n} \lambda_i v_i$$

since the basis is spanning. We have

$$v - \sum_{i=m+1}^{n} \lambda_i v_i \in W$$

therefore

$$[v] = [\sum_{i=m+1}^{n} \lambda_i v_i] = \sum_{i=m+1}^{n} \lambda_i [v_i]$$

and the given set is spanning. Similarly suppose

$$\sum_{i=m+1}^{n} \lambda_i [v_i] = 0$$

then by definition $\sum_{i=m+1}^{n} \lambda_i v_i \in W$. Therefore

$$\sum_{i=m+1}^{n} \lambda_i v_i = \sum_{i=1}^{m} \lambda_i v_i$$

and since $v_i$ are linearly independent we must have $\lambda_i = 0$. □

**Proposition 3.4.88** (Injective Criteria)
*Let $\phi : V \to W$ be a linear map then*

$$\phi \text{ injective} \iff \ker(\phi) = \{0\} \iff \dim_k \ker(\phi) = 0$$

*Proof.* Note for any linear map $\phi$ we have $\phi(0) = 0$. Therefore $\phi$ injective clearly shows $\ker(\phi) = \{0\}$. Conversely suppose $\ker(\phi) = 0$ and $\phi(v) = \phi(w)$. Then $\phi(v - w) = 0 \implies v - w = 0 \implies v = w$ as required. □

**Definition 3.4.89** (Rank)
*Let $\phi : V \to W$ be a linear map then define*

$$\operatorname{rank}_k(\phi) := \dim_k(\operatorname{Im}(\phi))$$

**Proposition 3.4.90** (Surjective Criteria)
*Let $\phi : V \to W$ be a linear map with $W$ finite-dimensional then*

$$\phi \text{ surjective} \iff \operatorname{rank}_k(\phi) = \dim_k W$$

*Proof.* This follows directly from (2.2.13). □

**Proposition 3.4.91** (Isomorphism Theorem / Rank-Nullity)
*Let $\phi : V \to W$ be a linear map then this induces an isomorphism*

$$V/\ker(\phi) \longrightarrow \operatorname{im}(\phi)$$

*in particular when $V$ is finite-dimensional*

$$\dim_k V = \dim_k \ker(\phi) + \operatorname{rank}_k(\phi)$$

**Corollary 3.4.92** (Isomorphism Criteria)
*Let $V, W$ vector spaces with $W$ finite-dimensional. A linear map $\phi : V \to W$ is an isomorphism if and only if any* two *of the following are satisfied*

a) $\dim_k \ker(\phi) = 0 \iff \phi$ *injective*

b) $\dim_k V = \dim_k W$

c) $\operatorname{rank}_k(\phi) = \dim_k W \iff \phi$ *surjective*

*Proof.* The rank-nullity equation ensures that if any two hold the third is automatically satisfied. In this case $\phi$ is isomorphism as required. □

**Corollary 3.4.93** (Endomorphism Isomorphism Criteria)
*Let $V$ be a finite-dimensional vector space and $\phi : V \to V$ then TFAE*

a) *$\phi$ is injective*

b) *$\phi$ is surjective*

c) *$\phi$ is an isomorphism*

*Proof.* Use the previous result with $W = V$ and note $\dim_k W = \dim_k V$ is automatically satisfied. □

**Proposition 3.4.94** (Internal Direct Sum)
*Let $U_1, U_2$ be two subspaces of $V$ then TFAE*

a) *$U_1 \cap U_2 = \{0\}$ and $V = U_1 + U_2$*

b) *Every $v \in V$ may be written uniquely as $u_1 + u_2$ for $u_i \in U_i$.*

*and we say $V = U_1 \oplus U_2$ is an **internal direct sum** and $U_2$ is a **supplementary subspace** for $U_1$.*

**Proposition 3.4.95**
*Every subspace $U$ has a supplementary subspace $U'$ such that*

$$V = U \oplus U'$$

*Proof.* Let $\mathcal{B}_1$ be a basis for $U$ and extend to a basis $\mathcal{B}$ and define $\mathcal{B}_2 := \mathcal{B} \setminus \mathcal{B}_1$. Then it's easy to show that $U' = \langle \mathcal{B}_2 \rangle$ is a supplementary subspace. □

**Proposition 3.4.96** (Dimension formula for direct sums)
*Suppose $V = U_1 \oplus U_2$, $\mathcal{B}_1$ is a basis for $U_1$ and $\mathcal{B}_2$ is a basis for $U_2$. Then $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$ and $\mathcal{B}_1 \cup \mathcal{B}_2$ is a basis for $V$. In particular*

$$\dim_k V = \dim_k U_1 + \dim_k U_2$$

#### 3.4.8.1 Vector Space Hom

**Definition 3.4.97**
*Let $V, W$ be two $k$-vector spaces. Define the $k$-vector space*

$$\mathrm{Hom}_k(V, W) := \mathrm{Mor}(V, W)$$

*with the obvious module operations*

$$(\phi + \psi)(v) = \phi(v) + \phi(w)$$
$$(\lambda\phi)(v) = \lambda\phi(v)$$

*For every $V$ this yields a covariant functor*

$$\mathrm{Hom}_k(V, -) : \mathbf{Vect_k} \to \mathbf{Vect_k}$$

*and a contravariant functor*

$$\mathrm{Hom}_k(-, W) : \mathbf{Vect_k} \to \mathbf{Vect_k}$$

**Proposition 3.4.98** (Basis for Hom-Set)
*Let $V, W$ be finite-dimensional vector spaces. Then*

$$\dim_k \mathrm{Hom}_k(V, W) = \dim_k V \times \dim_k W$$

*More precisely if $\{v_1, \ldots, v_n\}$ is a basis for $V$ and $\{w_1, \ldots, w_m\}$ is a basis for $W$, then $\{F_{ij}\}_{i=1\ldots n, j=1\ldots m}$ is a basis for $\mathrm{Hom}_k(V, W)$ where*

$$F_{ij}\left(\sum_{p=1}^{n} \lambda_p v_p\right) := \lambda_i w_j$$

#### 3.4.8.2 Dual Space

**Definition 3.4.99** (Dual Space)
*Let $V$ be a $k$-vector space and define the **dual space** to be*

$$V^\star := \mathrm{Hom}_k(V, k)$$

*This is an abelian group and even a $k$-vector space under the obvious operations. The construction $V \to V^\star$ determines a contravariant functor*

$$(-)^\star : \mathbf{Vect}_k \to \mathbf{Vect}_k$$

**Proposition 3.4.100** (Double Dual)
*There is a natural transformation $\eta : \mathbf{1} \Rightarrow (-)^{\star\star}$ given by*

$$\begin{aligned} \eta_V : V &\to V^{\star\star} && (3.1)\\ v &\to (\theta \longrightarrow \theta(v)) && (3.2)\end{aligned}$$

*which is injective. When $V$ is finite-dimensional then it is an isomorphism.*

*Proof.* It's clearly linear. Suppose the image of $v$ is 0, by definition $\theta(v) = 0$ for all $\theta \in V^\star$. Suppose $v$ is non-zero, then $\{v\}$ is linearly independent and so may be extended to a basis $\mathcal{B} = \{v_i\}_{i \in I}$ with $v_{i0} = v$. Define

$$\theta(\sum_i \lambda_i v_i) = \lambda_{i_0}$$

clearly $\theta(v) \neq 0$ a contradiction. Therefore $\ker(\psi) = \{0\}$ and $\psi$ is injective. We show in (3.4.102) that $\dim_k V^\star = \dim_k V$ whence $\dim_k V^{\star\star} = \dim_k V$. By (3.4.92) it's an isomorphism. □

**Corollary 3.4.101**
*The contravariant functor $(-)^\star : \mathbf{FdVect}_k \to \mathbf{FdVect}_k$ is an equivalence of categories and therefore full and faithful.*

*Proof.* Use the dual isomorphism $\eta$ together with (2.4.19) and (2.4.18). □

**Proposition 3.4.102** (Dual Basis)
*Let $V$ be a finite-dimensional $k$-vector space, then $\dim_k V = \dim_k V^\star$. In particular if $v_1, \ldots, v_n$ be a basis for $V$ then there are elements $v_1^\star, \ldots, v_n^\star \in V^\star$ such that*

$$v_i^\star(v_j) = \delta_{ij} \tag{3.3}$$

*and these form a basis for $V^\star$. Each $v_i^\star$ is uniquely defined by this condition. Similarly given any basis $v_1^\star, \ldots, v_n^\star \in V^\star$ then there exists a basis $v_1, \ldots, v_n$ such that (3.3) holds.*

*Proof.* Note that $k$ as a $k$-vector space has basis $\{1\}$. So apply (3.4.98) to obtain the required dual basis. For the reverse direction suppose $v_1^\star, \ldots, v_n^\star$ be a basis of $V^\star$. By the same token there is a basis $v_1^{\star\star}, \ldots, v_n^{\star\star} \in V^{\star\star}$ such that

$$v_i^{\star\star}(v_j^\star) = \delta_{ij}$$

Let $v_1, \ldots, v_n$ be the unique inverse image under the dual isomorphism $V \to V^{\star\star}$ from (3.4.100). These clearly satisfy (3.3) and furthermore by (3.4.85) is a basis for $V$ as required. □

**Definition 3.4.103** (Annihilator)
*Let $V$ be a vector space and $U \subseteq V$ a subspace. Define the **annihilator** of $U$ by*

$$U^\circ = \{\theta \in V^\star \mid \theta(u) = 0 \quad \forall u \in U\}$$

*This is a linear subspace of $V^\star$.*

**Proposition 3.4.104** (Dimension formula for annihilators)
*There is a canonical isomorphism by restriction*

$$V^\star / U^\circ \longrightarrow U^\star$$

*In particular when $V$ is a finite-dimensional vector space then*

$$\dim_k V = \dim_k U + \dim_k U^\circ$$

*Proof.* Let $W$ be a supplementary subspace and consider the morphism $V = U \oplus W \xrightarrow{\pi_U} U$. Then $(\theta \circ \pi_U)|_U = \theta$ so the restriction map is surjective. Clearly the kernel is $U^\circ$. The dimension formula follows from (3.4.91) and (3.4.102). □

**Corollary 3.4.105** (Dual rank = rank)
*Let $\phi : V \to W$ be a linear map and $\phi^\star : W^\star \to V^\star$ then*

$$\begin{aligned} \ker(\phi^\star) &= \operatorname{im}(\phi)^\circ \\ \operatorname{im}(\phi^\star) &\subseteq \ker(\phi)^\circ \end{aligned}$$

*In the finite-dimensional case, the last is equal and*

$$\begin{aligned} \dim_k \ker(\phi^\star) &= \dim_k W - \operatorname{rank}_k(\phi) \\ \operatorname{rank}_k(\phi^\star) &= \operatorname{rank}_k(\phi) \end{aligned}$$

*Proof.* Note $\ker(\phi^\star) = \operatorname{im}(\phi)^\circ$ and $\operatorname{im}(\phi^\star) \subseteq \ker(\phi)^\circ$ by the definitions.

Consider the finite-dimensional case. By (3.4.104)

$$\dim_k \ker(\phi^\star) = \dim_k \operatorname{im}(\phi)^\circ = \dim_k W - \operatorname{rank}_k(\phi)$$

By rank-nullity applied to $\phi^\star$ and $\dim_k W = \dim_k W^\star$ we deduce

$$\operatorname{rank}_k(\phi^\star) = \operatorname{rank}_k(\phi)\,.$$

By (3.4.104) and rank-nullity applied to $\phi$

$$\dim_k \ker(\phi)^\circ = \dim_k V - \dim_k \ker(\phi) = \operatorname{rank}_k(\phi)\,.$$

Finally by (2.2.13) $\operatorname{im}(\phi^\star) = \ker(\phi)^\circ$.

□

From this it follows that taking duals reflects and preserve isomorphisms

**Corollary 3.4.106** ($(-)^\star$ reflects isomorphisms)
*Let $\phi : V \to W$ be a linear map of finite-dimensional spaces then*

a) *$\phi$ is injective if and only if $\phi^\star$ is surjective*

b) *$\phi$ is surjective if and only if $\phi^\star$ is injective*

c) *$\phi$ is iso if and only if $\phi^\star$ is iso*

*Proof.* Note by (3.4.105) we have $\operatorname{rank}_k(\phi) = \operatorname{rank}_k(\phi^\star)$ and by (3.4.102) $\dim_k V^\star = \dim_k V$.

$\phi$ is surjective $\iff \operatorname{rank}_k(\phi) = \dim_k W = \operatorname{rank}_k(\phi^\star) \overset{(3.4.91)}{\iff} \dim_k \ker(\phi^\star) = 0 \iff \ker(\phi^\star) = \{0\}$

$\phi$ is injective $\iff \dim_k \ker(\phi) = 0 \overset{(3.4.91)}{\iff} \operatorname{rank}_k(\phi) = \dim_k V \iff \dim_k V^\star = \operatorname{rank}_k(\phi^\star) \iff \phi^\star$ is surjective.

The last point may be deduced from the first two, or the fact that $(-)^\star$ is full and faithful (3.4.101) and category-theoretic result (2.4.30). □

### 3.4.8.3 Bilinear Pairings

**Definition 3.4.107** (Bilinear maps)
*Let $V, W$ be vector spaces a bilinear map $\psi$ is a map*

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

*which is $k$-linear in each variable. We denote the set of bilinear maps as*

$$\operatorname{Bilin}_k(V, W)$$

**Proposition 3.4.108** (Dual maps)
*Let $V$ and $W$ be vector spaces, then there is a natural bijection*

$$\begin{array}{ccccc} \operatorname{Mor}_k(V, W^\star) & \longleftrightarrow & \operatorname{Bilin}_k(V, W) & \longleftrightarrow & \operatorname{Mor}_k(W, V^\star) \\ \psi_L & \longleftarrow & \psi & & \\ & & \psi & \longrightarrow & \psi_R \end{array}$$

*where*

$$\psi_L(v)(w) = \psi(v, w) = \psi_R(w)(v)$$

*When $V, W$ are finite-dimensional then $\psi_L$ is an isomorphism if and only if $\psi_R$ is an isomorphism. In this case we say $\psi$ is a perfect pairing. More generally*

$$\operatorname{rank}_k(\psi_L) = \operatorname{rank}_k(\psi_R)$$

*Proof.* The bijections stated are obvious. One may show that $\psi_L = \psi_R^\star \circ \eta_V$ where $\eta_V$ is the dual isomorphism. Therefore $\psi_L$ is an isomorphism if and only if $\psi_R^\star$ is an isomorphism, and by (3.4.106) if and only if $\psi_R$ is an isomorphism. Since $\eta_V$ is surjective we have $\operatorname{rank}_k(\psi_L) = \operatorname{rank}_k(\psi_R^\star) = \operatorname{rank}_k(\psi_R)$, by (3.4.105). □

**Definition 3.4.109** (Orthogonal Complement)
*Let $\psi : V \times W \to k$ be a perfect pairing of finite-dimensional vector spaces. Suppose $U \subset V$ is a subspace then define the* ***orthogonal complement***

$$U^\perp := \{w \in W \mid \psi(v, w) = 0 \quad \forall v \in U\}$$

**Proposition 3.4.110**
*Let $\psi : V \times W \to k$ be a perfect pairing of finite-dimensional vector spaces and $U \subset V$ a subspace. Then*

$$\dim_k U + \dim_k U^\perp = \dim_k V$$

*Indeed $\psi_R$ induces an isomorphism $U^\perp \to U^\circ$.*

*Proof.* We claim that $\psi_R(U^\perp) = U^\circ$. For if $w \in U^\perp$ then $\psi_R(w)(v) = \psi(w, v) = 0$ for all $v \in U$, and so $\psi_R(w) \in U^\circ$. Conversely given $\theta \in U^\circ$, as $\psi_R$ is surjective, there is $w \in W$ such that $\psi_R(w) = \theta$. By definition $w \in U^\perp$ as required.

As $\psi_R$ is injective then $\dim_k U^\perp \overset{(3.4.86)}{=} \dim_k U^\circ \overset{(3.4.104)}{=} \dim_k V/U = \dim_k V - \dim_k U$. □

**Remark 3.4.111**
*In the case $V = W$, then it's not necessarily true that $U \cap U^\perp = \{0\}$, and so $U^\perp$ is not necessarily a complementary subspace.*

*The classic example is the perfect pairing on $\mathbb{R}^n$ induced by $vDv^T$ for a real diagonal matrix $D$. Then it's true in general if and only if $D$ is positive-definite.*

**Proposition 3.4.112** (Quotients are dual to subspaces)
*Let $\psi : V \times W \to k$ be a perfect pairing of finite-dimensional vector spaces. Suppose $U \subset V$ is a subspace, then there is a canonical perfect pairing*

$$\psi' : V/U \times U^\perp \to k$$

*given by*

$$\psi'(v + U, w) = \psi(v, w)$$

*Proof.* The given map is well defined, for suppose $v_1 + U = v_2 + U$ then $v_1 - v_2 \in U \implies \psi(v_1 - v_2, w) = 0 \quad \forall w \in U^\perp \implies \psi(v_1, w) = \psi(v_2, w)$ as required. It's clearly $k$-bilinear.

It's clear that $\psi'_R$ is injective, because $\psi'_R(w) = 0_{V/U} \implies \psi_R(w) = 0_V \implies w = 0$.

By the previous Proposition $\dim_k U^\perp = \dim_k V/U$. Therefore by (3.4.92) $\psi'_R$ is an isomorphism and $\psi'$ is perfect.

□

## 3.5 Localization

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.

Recall the definition of multiplicative set. Some rather canonical examples are as follows

**Example 3.5.1**
*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 3.5.2**
*If $\mathfrak{p} \lhd A$ is a prime ideal, then $A \setminus \mathfrak{p}$ is a saturated multiplicative set. More generally, we show later that $S$ is a saturated multiplicative set if and only if it's of the form*

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

*for some family of prime ideals.*

### 3.5.1 Rings

**Definition 3.5.3** (Localization of a ring)
*Let $A$ be a ring and $S$ a multiplicative set. Define the set*

$$S^{-1}A = \left\{ \frac{a}{s} \mid a \in A \, s \in S \right\}$$

*under the equivalence relation*

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

*then this is a ring in the obvious way*

**Definition 3.5.4** (Localization of an ideal)
*Let $A$ be a ring and $S$ a multiplicative set and $\mathfrak{a} \lhd A$ define*

$$S^{-1}\mathfrak{a} := \left\{ \frac{a}{s} \mid a \in \mathfrak{a} \right\}$$

*then this is an ideal of $S^{-1}A$.*

**Proposition 3.5.5**
*The set $S^{-1}A$ is a ring under the obvious ring operations. It is non-zero precisely when $S$ is proper. There is a canonical homomorphism*

$$\begin{aligned} i_S : A &\to S^{-1}A \\ a &\to \left[\frac{a}{1}\right] \end{aligned}$$

a) $i_S(a) = 0 \iff sa = 0$ *for some* $s \in S$

b) $S^{-1}A$ *is the zero-ring if and only if* $0 \in S$ *if and only if there exists* $s, t \in S$ *such that* $st = 0$.

c) $i_S(s)$ *is invertible for all* $s \in s$

d) $i_S$ *is injective if and only if* $S$ *has no zero-divisors*

e) *This is an isomorphism if and only if* $S \subseteq A^\star$ *already consists only of invertible elements (e.g.* $S = \{1\}$*).*

*Proof.* a) This follows by the definitions

b) $1/1 = 0/0 \iff s = 0$ for some $s \in s$ by the definitions

c) $\frac{s}{1}\frac{1}{s} = \frac{s}{s} = \frac{1}{1}$

d) This follows from the first part.

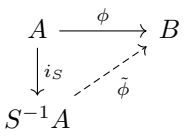
e) If $S \subseteq A^\star$ then it contains no zero-divisors and $i_S$ is injective. Further it's clear that $\frac{a}{s} = \frac{as^{-1}}{1}$ so that the map is surjective. Similarly if the map is bijective $S$ does not contain zero-divisors and $\frac{1}{s}$ is in the image. Therefore there is $a$ such that $tas = 1$ for some $t$, which implies $s$ is invertible.

□

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

**Proposition 3.5.6** (Universal Property)
*Let $\phi : A \to B$ be a ring homomorphism and $S$ a multiplicative set. Then*

a) *There is a unique morphism $\tilde{\phi}$ making the diagram commute*




*if and only if $\phi(S) \subseteq B^\star$. In this case it's given by*

$$\tilde{\phi}\left(\frac{a}{s}\right) = \phi(a)\phi(s)^{-1}$$

b) $\ker(\tilde{\phi}) = S^{-1}\ker(\phi)$

*Proof.* a) If $\tilde{\phi}$ exists then $1 = \tilde{\phi}(1) = \tilde{\phi}(\frac{s}{1}\frac{1}{s}) = \tilde{\phi}(\frac{s}{1})\tilde{\phi}(\frac{1}{s}) = \phi(s)\tilde{\phi}(\frac{1}{s})$. Which shows that $\phi(S) \subseteq B^\star$ and $\phi(s)^{-1} = \tilde{\phi}(\frac{1}{s})$.

Conversely suppose $\phi(S) \subseteq B^\star$ then we claim that the given mapping is well-defined. For

$$\frac{a}{s} = \frac{a'}{s'} \implies s''(s'a - sa') = 0 \implies \phi(s'')\phi(s')\phi(a) = \phi(s'')\phi(s)\phi(a')$$

Multiply by the appropriate inverses to find

$$\phi(a)\phi(s)^{-1} = \phi(a')\phi(s')^{-1}$$

It's clearly a multiplicative homomorphism. Further it's additive because

$$\begin{aligned} \tilde{\phi}\left(\frac{a}{s} + \frac{b}{t}\right) &= \tilde{\phi}\left(\frac{at + bs}{st}\right) \\ &= \phi(at + bs)\phi(st)^{-1} \\ &= \phi(a)\phi(t)\phi(s)^{-1}\phi(t)^{-1} + \phi(b)\phi(s)\phi(s)^{-1}\phi(t)^{-1} \\ &= \phi(a)\phi(s)^{-1} + \phi(b)\phi(t)^{-1} \\ &= \tilde{\phi}\left(\frac{a}{s}\right) + \tilde{\phi}\left(\frac{b}{t}\right) \end{aligned}$$

b) Suppose $\tilde{\phi}(\frac{a}{s}) = 0$ then clearly $a \in \ker(\phi) \implies \frac{a}{s} \in S^{-1}\ker(\phi)$. The converse is clear.

□

In the case that $A$ is an integral domain then generally everything becomes a lot simpler.

**Example 3.5.7** (Field of fractions)
*Let $A$ be an integral domain then $A \setminus 0 = A^\star$ and we define the field of fractions*

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

**Proposition 3.5.8** (Field of fractions contains all localization)
*Let $A$ be an integral domain, and $\mathrm{Frac}(A)$ the field of fractions. Define another model for $S^{-1}A$ as follows*

$$S^{-1}A := \left\{ \frac{a}{s} \in \mathrm{Frac}(A) \mid a \in A \, s \in S \right\}$$

*The canonical map $A \to S^{-1}A \subset \mathrm{Frac}(A)$ is injective, and satisfies the universal property for localization.*

*Proof.* It's injective because $A$ has no zero-divisors. That it satisfies the universal property is very similar as before. □

**Proposition 3.5.9** (Directed Limit)
*Let $S_i$ be a family of multiplicatively closed sets directed by inclusion, such that $S = \bigcup_i S_i$ is multiplicatively closed. Then there is a canonical isomorphism*

$$\varinjlim_i S_i^{-1}A \to S^{-1}A$$

*induced by the canonical maps*

$$S_i^{-1}A \to S^{-1}A$$

*Proof.* The canonical maps $i_{S_i S}$ induce a unique morphism

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

$$[a_i/s_i] \longrightarrow a_i/s_i$$

by the universal property. An element on the right hand side is written $a/s$ for some $s \in S$. By hypothesis $s \in S_i$ for some $i$, therefore it is surjective. Suppose we have two elements $[a_i/s_i]$ and $[a_j/s_j]$ on the left hand side which become equal in $S^{-1}A$. Then by definition $s_k(s_j a_i - a_j s_i) = 0$ for some $s_k \in S_k$. Since it's a directed system we can find $S_l$ containing $S_i, S_j, S_k$. Then by definition $a_i/s_i = a_j/s_j$ in $S_l^{-1}A$ and we see that $[a_i/s_i] = [a_j/s_j]$. Therefore the given morphism is also injective as required. □

### 3.5.2 Modules

**Definition 3.5.10** (Localization of a module)
*Let $A$ be a ring with $S$ multiplicative set and $M$ an $A$-module. Then we define*

$$S^{-1}M = \left\{ \frac{m}{s} \mid m \in M \right\}$$

*under the obvious equivalence relation. This is then an $S^{-1}A$-module in the obvious way.*

**Definition 3.5.11** (Localization of a sub-module)
*Let $M$ be an $A$-module and $N \subseteq M$ a sub-$A$-module then define*

$$S^{-1}N = \left\{ \frac{n}{s} \mid n \in M \, s \in S \right\} \subseteq S^{-1}M$$

**Proposition 3.5.12**
*$S^{-1}(-)$ constitutes a functor $A-\mathbf{Mod} \to S^{-1}A-\mathbf{Mod}$. More precisely there is a unique morphism $\psi$ making the following diagram commute as $A$-module morphisms*

$$\begin{array}{ccc} N & \xrightarrow{\psi} & M \\ \downarrow{\scriptstyle i_S} & & \downarrow{\scriptstyle i_S} \\ S^{-1}N & \xrightarrow{S^{-1}(\psi)} & S^{-1}M \end{array}$$

*where $S^{-1}(\psi)$ is in fact an $S^{-1}A$-module morphism.*

*It is an exact functor; for an exact sequence*

$$N \to M \to P$$

*the corresponding sequence of $S^{-1}A$-module morphisms*

$$S^{-1}N \to S^{-1}M \to S^{-1}P$$

*is exact. If $N$ is a submodule of $M$ then we may regard $S^{-1}N$ as a submodule of $S^{-1}M$.*

**Proposition 3.5.13** (Localization commutes with quotients)
*There is a commutatiee diagram of $A$-module morphisms*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{i} & M & \xrightarrow{\pi} & M/N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i_S} & & \downarrow{\scriptstyle i_S} & & \downarrow & & \\ 0 & \longrightarrow & S^{-1}N & \longrightarrow & S^{-1}M & \xrightarrow{S^{-1}(\pi)} & S^{-1}(M/N) & \longrightarrow & 0 \end{array}$$

*with exact rows and the bottom row consists of $S^{-1}A$-module morphisms. This induces an isomorphism of $S^{-1}A$-modules.*

$$S^{-1}M/S^{-1}N \cong S^{-1}(M/N)$$

**Proposition 3.5.14**
*Suppose $N \subseteq N' \subseteq M$ then there is a canonical short-exact sequence of $S^{-1}A$-modules*

$$0 \to S^{-1}(N'/N) \to S^{-1}(M/N) \to S^{-1}(M/N') \to 0$$

*which induces an isomorphism*

$$S^{-1}(M/N)/S^{-1}(N'/N) \cong S^{-1}(M/N')$$

**Proposition 3.5.15**
*Let $M$ be a finitely-generated $A$-module. Then*

$$S^{-1}M = 0 \iff sM = 0 \text{ some } s \in S$$

### 3.5.3 Ideals

Recall the notion of extended and contracted ideals in Definition (3.4.41).

**Definition 3.5.16** (Localization of an ideal)
*Let $A$ be a ring, $S$ a multiplicative set and $\mathfrak{a}$ an ideal. Then define*

$$S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} \mid a \in \mathfrak{a} \right\}$$

*an ideal of $S^{-1}A$.*

**Proposition 3.5.17** (Extension and Contraction)
*Let $A$ be a ring with multiplicative set $S$ and canonical morphism $i_S : A \to S^{-1}A$.*

a) $\mathfrak{a}^e = i_S(\mathfrak{a})S^{-1}A = \left\{ \frac{a}{s} \mid a \in \mathfrak{a}, s \in S \right\} = S^{-1}\mathfrak{a}$

b) $\mathfrak{b}^c = \left\{ a \mid \frac{a}{1} \in \mathfrak{b} \right\}$

c) *An ideal $\mathfrak{a}$ in $A$ satisfies*

$$\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : s) = \{ a \in A \mid as \in \mathfrak{a} \text{ some } s \in S \}$$

*In particular $\mathfrak{a}$ is contracted if and only if*

$$as \in \mathfrak{a} \wedge s \in S \implies a \in \mathfrak{a}$$

d) $\mathfrak{b}$ *proper* $\iff$ $\mathfrak{b}^c$ *proper* $\iff$ $\mathfrak{b}^c \cap S = \emptyset$

e) $\mathfrak{a}^e$ *proper* $\iff$ $\mathfrak{a} \cap S = \emptyset$

f) *Every ideal $\mathfrak{b} \lhd S^{-1}A$ is extended (equiv. $\mathfrak{b} = \mathfrak{b}^{ce} = S^{-1}\mathfrak{b}^c$).*

g) *A prime ideal $\mathfrak{p}$ is contracted if and only if $\mathfrak{p} \cap S = \emptyset$. In this case $\mathfrak{p}^e$ is prime. Similarly $\mathfrak{q}$ prime $\implies \mathfrak{q}^c$ is prime and satisfies $\mathfrak{q}^c \cap S = \emptyset$.*

*Proof.* .

a) $S^{-1}\mathfrak{a}$ is an additive subgroup because $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$. It contains $i_S(\mathfrak{a})$ and is closed under multiplication by $A$, therefore $\mathfrak{a}^e \subseteq S^{-1}\mathfrak{a}$. Similarly as $\mathfrak{a}^e$ is an ideal containing $i_S(\mathfrak{a})$, we have $\frac{a}{s} = \frac{1}{s}\frac{a}{1} \in \mathfrak{a}^e$, i.e. $S^{-1}\mathfrak{a} \subseteq \mathfrak{a}^e$ as required.

b) This is clear

c) Observe that

$$\begin{aligned} \mathfrak{a}^{ec} &= \left\{ a \in A \mid \frac{a}{1} \in \mathfrak{a}^e \right\} \\ &= \left\{ a \in A \mid \frac{a}{1} = \frac{a'}{s} \quad a' \in \mathfrak{a}\, s \in S \right\} \\ &= \{ a \in A \mid sa \in \mathfrak{a} \text{ some } s \in S \} \end{aligned}$$

By (3.4.42) an ideal $\mathfrak{a}$ is contracted if and only if $\mathfrak{a} = \mathfrak{a}^{ec}$. Furthermore it always satisfies $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$. The reverse inclusion is precisely the condition given.

d) This first equivalence is true in general, see (3.4.42). Clearly $\mathfrak{b}^c = A \implies \mathfrak{b}^c \cap S \neq \emptyset$. Similarly if $S \cap \mathfrak{b}^c \neq \emptyset$ then $s \in \mathfrak{b}^c \implies \frac{s}{1} \in \mathfrak{b} \implies 1 \in \mathfrak{b} \implies 1 \in \mathfrak{b}^c$.

e) By 4. $\mathfrak{a}^e$ is proper if and only if $\mathfrak{a}^{ec}$ is proper. By 3. we see $1 \in \mathfrak{a}^{ec}$ if and only if $S \cap \mathfrak{a} \neq \emptyset$ and the result follows.

f) By (3.4.42) we need only show $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$. Note $\frac{a}{s} \in \mathfrak{b}^{ce} \implies \frac{a}{s} = \frac{a'}{s'}$ with $a' \in \mathfrak{b}^c$. By 2. $\frac{a'}{1} \in \mathfrak{b}$ and therefore so is $\frac{a}{s} = \frac{a'}{s'} = \frac{a'}{1}\frac{1}{s'} \in \mathfrak{b}$ as required.

g) If $\mathfrak{p} \cap S = \emptyset$ then by primality it automatically satisfies the conditions in 3. and is therefore contracted. Conversely if a prime ideal $\mathfrak{p}$ is contracted then $\mathfrak{p} = \mathfrak{q}^c$. It is by definition proper so by 4. it satisfies $\mathfrak{p} \cap S = \emptyset$ as required.

Suppose $\frac{a}{s}\frac{b}{t} \in \mathfrak{p}^e$ then $\frac{ab}{st} = \frac{x}{u}$ for $x \in \mathfrak{p} \implies v(abu - xst) = 0 \implies uvab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Therefore $\frac{a}{s} \in \mathfrak{p}^e$ or $\frac{b}{t} \in \mathfrak{p}^e$ as required.

Generically $\mathfrak{q}^c$ is a contracted prime ideal and we've already shown in 4. that $\mathfrak{q}^c \cap S = \emptyset$.

□

**Corollary 3.5.18** (Ideal Structure Localization)
*Let $A$ be a ring and $S$ a multiplicative set then there is an order-preserving bijection of proper ideals*

$$\{ \mathfrak{a} \lhd A \mid \mathfrak{a} \text{ contracted } \} \longleftrightarrow \{ \mathfrak{b} \lhd S^{-1}A \}$$

*which restricts to a bijection of prime ideals*

$$\{ \mathfrak{p} \lhd A \mid \mathfrak{p} \cap S = \emptyset \} \longleftrightarrow \{ \mathfrak{q} \lhd S^{-1}A \}$$

*Proof.* From (3.5.17) every ideal of $S^{-1}A$ is extended. Therefore the bijection of proper ideals follows from (3.4.44). For prime ideals each direction is well-defined by (3.5.17) g). □

### 3.5.4 Change of Rings

For what follows it is useful to have the concept of saturation of a multiplicatively closed set. Essentially taking the saturation $\bar{S}$ of $S$ doesn't change the ring $S^{-1}A$.

**Proposition 3.5.19** (Saturation)
*Let $A$ be a ring and $S$ a multiplicatively closed set. Then the following sets are equal*

- $(i_S)^{-1}((S^{-1}A)^\star)$
- $\{ t \mid at \in S \text{ for some } a \in A \}$
- $\bigcap_{T \supseteq S : T \text{ saturated}} T$

*which we denote by $\overline{S}$. We have the following properties*

- *$\overline{S}$ is saturated.*
- *$S$ is saturated if and only if $S = \overline{S}$*

- $\overline{\overline{S}} = \overline{S}$.

*Proof.* TODO □

We also give another characterization of saturated multiplicatively closed subsets

**Proposition 3.5.20**
*Let $A$ be a ring and $S$ a multiplicatively closed subset. 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 (3.5.19)). Therefore by (3.4.37) 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. □

**Proposition 3.5.21** (Change of Rings)
*Let $\phi : A \to B$ be a ring homomorphism, $S, T$ corresponding multiplicative subsets. Then*

- *There exists a unique morphism $\tilde{\phi}$ making the diagram commute*

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

  *if and only if $\phi(S) \subseteq \overline{T}$. In this case it's given by*

$$\tilde{\phi}\left(\frac{a}{s}\right) = \frac{\phi(a)b'}{\phi(s)b'}$$

  *where $b' \in B$ is any $b'$ such that $\phi(s)b' \in T$.*

- *If in addition $T \subseteq \phi(\overline{S})$ then $\phi$ injective (resp. surjective, bijective) implies $\tilde{\phi}$ is injective (resp. surjective, bijective)*
- *Further $\phi$ surjective $\implies \ker(\tilde{\phi}) = S^{-1}\ker(\phi)$.*

*Proof.*
- If $\tilde{\phi}$ is well-defined, then $i_T(\phi(S)) = \tilde{\phi}(i_S(S)) \subseteq \tilde{\phi}((S^{-1}A)^\star) \subseteq (T^{-1}B)^\star$, which implies $\phi(S) \subseteq i_T^{-1}((T^{-1}B)^\star) = \overline{T}$.

  Conversely if $\phi(S) \subseteq \overline{T}$ then $(i_T \circ \phi)(S) \subseteq (T^{-1}B)^\star$ therefore by the previous Proposition the morphism exists making the diagram commute.

  Note that

$$\tilde{\phi}\left(\frac{a}{s}\right) = \tilde{\phi}\left(i_S(a)i_S(s)^{-1}\right) = \tilde{\phi}(i_S(a))\tilde{\phi}(i_S(s))^{-1}$$

  so it is uniquely defined by the commutativity condition. Note that given $s \in S$ by (...) there exists $b' \in B$ such that $\phi(s)b' \in T$. In this case it's clear that $i_T(\phi(s))^{-1} = \frac{b'}{\phi(s)b'}$ from which the explicit form results.

- Suppose $T \subseteq \phi(\overline{S})$ and $\phi$ is injective. Then $\tilde{\phi}\left(\frac{a}{s}\right) = 0 \implies t\phi(a) = 0$ for $t \in T$. Then there exists $s' \in \overline{S}$ and $x \in A$ such that $xs' \in S$ and $\phi(s') = t$. Therefore $\phi(as') = 0 \implies as' = 0 \implies a(xs') = 0 \implies \frac{a}{s} = 0$ as required.

  Similary if $\phi$ is surjective and given $\frac{b}{t} \in T^{-1}B$ there exists $a \in A$ such that $\phi(a) = b$ and $s \in \overline{S}$ such that $\phi(s) = t$. Then $xs \in S$, $\phi(xs) \in \overline{T}$ and $\phi(yxs) \in T$ for some $x, y \in A$. Finally

$$\tilde{\phi}\left(\frac{axy}{sxy}\right) = \frac{\phi(axy)}{\phi(sxy)} = \frac{b}{t}$$

  as required.

- TODO

□

**Corollary 3.5.22**
*Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be a sequence of homomorphisms and $S, T, U$ be multiplicative sets such that $\phi(S) \subseteq \overline{T}$ and $\psi(T) \subseteq \overline{U}$, then in the notation of the previous Proposition*

$$\tilde{\psi} \circ \tilde{\phi} = \widetilde{\psi \circ \phi}$$

*Proof.* This follows from the uniqueness condition in the previous Proposition. □

**Corollary 3.5.23** (Localization Maps)
*Let $A$ be a ring and $S, T$ two multiplicative sets. Then TFAE*

- *There exists $i_{ST} : S^{-1}A \to T^{-1}A$ such that $i_{ST} \circ i_S = i_T$*
- *$S \subseteq \overline{T}$*

*In this case $i_{ST}$ is the unique such map. We have the transitivity relationships*

$$i_{TU} \circ i_{ST} = i_{SU}$$
$$i_{SS} = \mathbf{1}_{S^{-1}A}$$

*and furthermore $i_{ST}$ is an isomorphism if and only if $\overline{S} = \overline{T}$. In particular $i_{S\overline{S}}$ is an isomorphism.*

*Proof.* This largely follows from the previous Proposition when considering the map $\phi = 1_A$. The transitivity and reflexive relationships follow from the uniqueness condition. □

**Corollary 3.5.24** (Localization commutes with quotient)
*Let $A$ be a ring, $\mathfrak{a}$ an ideal and $S$ a multiplicative set. Then there exists a unique morphism making the diagram commute*

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\mathfrak{a} \\ \downarrow{\scriptstyle i_S} & & \\ S^{-1}A & & \downarrow{\scriptstyle i_{\pi(S)}} \\ \downarrow{\scriptstyle \pi} & & \\ S^{-1}A/S^{-1}\mathfrak{a} & \xrightarrow{\sim} & \pi(S)^{-1}(A/\mathfrak{a}) \end{array}$$

*which is an isomorphism, and determined by*

$$\frac{a}{s} + S^{-1}\mathfrak{a} \longrightarrow \frac{a+\mathfrak{a}}{s+\mathfrak{a}}$$

*Note that $S \cap \mathfrak{a} \neq \emptyset \iff S^{-1}A/S^{-1}\mathfrak{a} = 0 \iff \pi(S)^{-1}(A/\mathfrak{a}) = 0$.*

*When $\mathfrak{b} \supseteq \mathfrak{a}$ this restricts to a commutative diagram of $A$-modules*

$$\begin{array}{ccc} \mathfrak{b} & \xrightarrow{\pi} & \mathfrak{b}/\mathfrak{a} \\ \downarrow{\scriptstyle i_S} & & \\ S^{-1}\mathfrak{b} & & \downarrow{\scriptstyle i_{\pi(S)}} \\ \downarrow{\scriptstyle \pi} & & \\ S^{-1}\mathfrak{b}/S^{-1}\mathfrak{a} & \xrightarrow{\sim} & \pi(S)^{-1}(\mathfrak{b}/\mathfrak{a}) \end{array}$$

*and the bottom arrow is still an isomorphism of $S^{-1}A/S^{-1}\mathfrak{a}$-modules.*

**Corollary 3.5.25** (Localization commutes with quotient II)
*Let $A$ be a ring, $\mathfrak{a}$ an ideal and $S$ a multiplicative set. Then there exists a unique morphism making the diagram commute*

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\mathfrak{a} \\ \downarrow{\scriptstyle i_S} & & \vdots \\ S^{-1}A & \xrightarrow{\pi} & S^{-1}A/S^{-1}\mathfrak{a} \end{array}$$

*given by*

$$a + \mathfrak{a} \to \frac{a}{1} + S^{-1}\mathfrak{a}$$

*and it is an isomorphism precisely when every $s \in S$ is co-prime to $\mathfrak{a}$, i.e.*

$$(s) + \mathfrak{a} = A \quad \forall s \in S.$$

*When $\mathfrak{b} \supseteq \mathfrak{a}$ this restricts to a commutative diagram*

$$\begin{array}{ccc} \mathfrak{b} & \xrightarrow{\pi} & \mathfrak{b}/\mathfrak{a} \\ \downarrow{\scriptstyle i_S} & & \vdots \\ S^{-1}\mathfrak{b} & \xrightarrow{\pi} & S^{-1}\mathfrak{b}/S^{-1}\mathfrak{a} \end{array}$$

*which is an $A/\mathfrak{a}$-module morphism, and is an isomorphism when the condition (...) holds.*

*Proof.* □

**Proposition 3.5.26** (Transitivity)
*Let $S \subset T$ be multiplicative subsets of $A$ and let*

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

*be the localization at $S$. Define $T_S := i_S(T)$. Then $T_S$ is multiplicative and there is a canonical isomorphism*

$$T^{-1}A \longrightarrow (T_S)^{-1}(S^{-1}A) \longrightarrow (\overline{T_S})^{-1}(S^{-1}A)$$

*Furthermore if $T \subseteq U$ then $T_S \subseteq U_S$ there is a commutative diagram*

$$\begin{array}{ccccc} & & S^{-1}A & & \\ & \swarrow^{i_{ST}} & \downarrow{\scriptstyle i_{T_S}} & \searrow^{i_{\overline{T_S}}} & \\ T^{-1}A & \xrightarrow{\sim} & (T_S)^{-1}(S^{-1}A) & \xrightarrow{\sim} & \left(\overline{T_S}\right)^{-1}(S^{-1}A) \\ \downarrow{\scriptstyle i_{TU}} & & \downarrow & & \downarrow \\ U^{-1}A & \xrightarrow{\sim} & (U_S)^{-1}(S^{-1}A) & \xrightarrow{\sim} & \left(\overline{U_S}\right)^{-1}(S^{-1}A) \end{array}$$

### 3.5.5 Localization at an element

**Definition 3.5.27** (Localization at an element)
*Let $A$ be a ring and $f \in A$. Then define*

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

*and*

$$A_f := \left(\overline{S_f}\right)^{-1} A$$

*where we have canonical map*

$$i_f : A \to A_f$$

*given by $i_f = i_{\overline{S_f}}$.*

**Proposition 3.5.28** (Transition maps for localization at an element)
*Let $A$ be a ring and $f, g \in A$ then*

$$\overline{S_f} \subseteq \overline{S_g} \iff f \mid g^N \text{ some } N > 0$$

*in this case define $i_{fg} = i_{\overline{S_f}\,\overline{S_g}}$ to be the unique morphism such that $i_{fg} \circ i_f = i_g$. In addition if $h \in A$ and $\overline{S_g} \subseteq \overline{S_h}$ we have a commutative diagram*

$$\begin{array}{ccccc} & & A & & \\ & \swarrow^{i_f} & \downarrow{\scriptstyle i_g} & \searrow^{i_h} & \\ A_f & \xrightarrow[i_{fg}]{} & A_g & \xrightarrow[i_{gh}]{} & A_h \\ & & \underset{i_{fh}}{\smile} & & \end{array}$$

*Furthermore $\overline{S_1} = A^\star$ and $i_1$ is an isomorphism.*

**Proposition 3.5.29** (Transitivity of localizing at elements)
*Let $A$ be a ring and $f, g \in A$ such that $\overline{S_f} \subseteq \overline{S_g}$. Then $\overline{i_f(\overline{S_g})} = \overline{S_{g/1}}$ as multiplicatively closed subsets of $A_f$. Therefore there is a canonical isomorphism*

$$(A_f)_{g/1} \longrightarrow A_g$$

*Furthermore $\overline{S_g} \subseteq \overline{S_h} \iff \overline{S_{g/1}} \subseteq \overline{S_{h/1}}$ and there is a commutative diagram*

$$\begin{array}{ccc}
(A_f)_1 & \xrightarrow{\sim} & A_f \\
\downarrow{\scriptstyle i_{1(g/1)}} & & \downarrow{\scriptstyle i_{g/1}} \\
(A_f)_{g/1} & \xrightarrow{\sim} & A_g \\
\downarrow & & \downarrow{\scriptstyle i_{gh}} \\
(A_f)_{h/1} & \xrightarrow{\sim} & A_h
\end{array}$$

*with the horizontal arrows isomorphisms and the vertical arrows are well-defined.*

*Proof.* Firstly let $S'_g := \overline{i_f(\overline{S_g})}$, which is a saturated multiplicatively closed set containing $g/1$, whence $S_{g/1} \subseteq S'_g$ and $\overline{S_{g/1}} \subseteq S'_g$ by (3.5.19). Suppose $h \in S'_g$ then $ah = b/1$ for $b \in \overline{S_g}$ whence $a'h = g^N/1$ and $h \in \overline{S_{g/1}}$. Therefore $\overline{i_f(\overline{S_g})} = \overline{S_{g/1}}$ as required.

Suppose we have $\overline{S_f} \subseteq \overline{S_g}$ and $\overline{S_f} \subseteq \overline{S_h}$. We claim that $\overline{S_g} \subseteq \overline{S_h} \iff \overline{S_{g/1}} \subseteq \overline{S_{h/1}}$. Note the former implies $g \mid h^N \implies g/1 \mid (h/1)^N$ which implies the latter. Conversely suppose $g/1 \mid h^N/1$ then $ag/f^r = h^N/1 \implies f^s(ag - f^r h^N) = 0$. But similarly $f \mid h^M$ so we find $g \mid h^N$ for some suitably large $N$ and $\overline{S_g} \subseteq \overline{S_h}$.

The required isomorphisms and commutative diagrams follow from (3.5.26). □

### 3.5.6 Localization at a prime ideal

**Definition 3.5.30** (Localization at a prime ideal)
*Let $A$ be a ring and $\mathfrak{p} \lhd A$ a prime ideal. Then $S := A \setminus \mathfrak{p}$ is a saturated multiplicatively closed subset, and we define*

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} A$$

*For an ideal $\mathfrak{a} \lhd A$ write the extended ideal*

$$\mathfrak{a}A_{\mathfrak{p}} := \mathfrak{a}^e = S^{-1}\mathfrak{a}\,.$$

**Definition 3.5.31** (Relative localization at a prime ideal)
*Let $\phi : A \to B$ be a ring homomorphism and $\mathfrak{p} \lhd A$ a prime ideal. Define*

$$B_{\mathfrak{p}} := \phi(A \setminus \mathfrak{p})^{-1} B$$

*For an ideal $\mathfrak{a} \lhd A$ write*

$$\mathfrak{a}B_{\mathfrak{p}} := (\phi(\mathfrak{a})B)B_{\mathfrak{p}}$$

*Observe $B_{\mathfrak{p}} = 0 \iff \mathfrak{p} \subsetneq \ker(\phi)$, so we would typically assume $\ker(\phi) \subseteq \mathfrak{p}$.*

**Proposition 3.5.32**
*Let $A$ be a ring and $\mathfrak{p}$ a prime ideal. Consider the localization $A \to A_{\mathfrak{p}}$. Then there is a bijection between (prime) ideals contained in $\mathfrak{p}$ and (prime) ideals of $A_{\mathfrak{p}}$*

$$\begin{array}{ccc}
\{\mathfrak{q} \lhd A \mid \mathfrak{q} \subseteq \mathfrak{p}\} & \longleftrightarrow & \{\mathfrak{q} \lhd A_{\mathfrak{p}}\} \\
\mathfrak{q} & \longrightarrow & \mathfrak{q}A_{\mathfrak{p}}
\end{array}$$

*In particular $A_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.*

*Proof.* Clearly $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset \iff \mathfrak{q} \subseteq \mathfrak{p}$, so the result follows from from (3.5.18). □

**Proposition 3.5.33** (Localization at prime is direct limit of localization at an element)
*Let $A$ be a ring and $\mathfrak{p}$ a prime ideal then*

$$S_{\mathfrak{p}} := A \setminus \mathfrak{p} = \bigcup_{f \in A \setminus \mathfrak{p}} \overline{S_f}$$

*Therefore there are canonical morphisms (for $f \notin \mathfrak{p}$)*

$$i_{\overline{S_f} S_{\mathfrak{p}}} : A_f \longrightarrow A_{\mathfrak{p}}$$

*Furthermore the family of multiplicatively closed sets $\{\overline{S_f}\}_{f \notin \mathfrak{p}}$ (resp. rings $\{A_f\}_{f \notin \mathfrak{p}}$) form a directed system. Therefore we have a canonical morphism*

$$\varinjlim_{f \notin \mathfrak{p}} A_f \longrightarrow A_{\mathfrak{p}}$$

*which is an isomorphism.*

*Proof.* As $A \setminus \mathfrak{p}$ is a saturated multiplicatively closed set we have $f \in A \setminus \mathfrak{p} \iff S_f \subseteq A \setminus \mathfrak{p} \iff \overline{S_f} \subseteq A \setminus \mathfrak{p}$. Therefore the expression for $S_{\mathfrak{p}}$ follows.

The family of multiplicatively closed subsets is a directed system because $\overline{S_f} \subseteq \overline{S_{fg}}$. To see this note $fg \in \overline{S_{fg}} \implies f \in \overline{S_{fg}} \implies S_f \subseteq \overline{S_{fg}} \implies \overline{S_f} \subseteq \overline{S_{fg}}$.

The final isomorphism follows from (3.5.9), by considering the directed system of multiplicative sets $\{S_f\}_{f \notin \mathfrak{p}}$ whose union we have shown is $S_{\mathfrak{p}}$. □

## 3.6 Polynomial Rings in One Variable

**Definition 3.6.1**
*Let $A$ be a ring. The polynomial ring $A[X]$ is an $A$-algebra consisting of formal sums*

$$f(X) = \sum_{i=0}^{\infty} a_i X^i$$

*such that only finitely many $a_i$ are non-zero. Define degree in the obvious way*

$$\deg(f) = \inf\{n \mid m > n \implies a_m = 0\} < \infty$$

*and the leading coefficient to be $c(f) := a_{\deg(f)}$. By convention $\deg(0) = -\infty$. We say $f$ is* monic *if the leading coefficient is $1$.*

*Addition is defined in the obvious way and multiplication is defined by*

$$f(X)g(X) = \sum_{d=0}^{\infty} \left( \sum_{i+j=d} a_i b_j \right) X^d$$

*It's associative because*

$$f(X)g(X)h(X) = \sum_{d=0}^{\infty} \left( \sum_{i+j+k=d} a_i b_j c_k \right) X^d$$

**Lemma 3.6.2**
*If $A$ is an integral domain then for elements $f, g \in A[X]$*

$$\deg(fg) = \deg(f) + \deg(g)$$

$$c(fg) = c(f)c(g)$$

*Further $A[X]$ is an integral domain.*

**Proposition 3.6.3** (Nilpotent and Invertible Polynomials)
*Let $A$ be a ring then*

a) $\mathfrak{N}(A[X]) = \mathfrak{N}(A)[X] \subset A[X]$

b) $A[X]^\star = A^\star + X\mathfrak{N}(A)[X]$

*Proof.* Suppose $a \in \mathfrak{N}(A)$ then clearly $aX^i$ is nilpotent. Therefore $\mathfrak{N}(A)[X] \subseteq \mathfrak{N}(A[X])$ since the nilradical is an ideal. Conversely suppose $f \in A[X]$ is nilpotent, i.e. $f^n = 0$. For any prime ideal $\mathfrak{p} \lhd A$ we find that $\bar{f}^n = 0$ as an element of $(A/\mathfrak{p})[X]$. As $A/\mathfrak{p}$ is an integral domain we have by the previous Lemma $\bar{f} = 0$. As $\mathfrak{p}$ is arbitrary and $\mathfrak{N}(A) = \bigcap \mathfrak{p}$ we see that $f \in \mathfrak{N}(A)[X]$ as required.

Suppose $f \in A[X]^\star$ and $fg = 1$, then clearly the constant term of $f$ must be invertible. Reduce modulo $\mathfrak{p}$ to find $\deg(\bar{f}) + \deg(\bar{g}) = 0 \implies \deg(\bar{f}) = \deg(\bar{g}) = 0$, which means $\bar{f}$ is a constant polynomial. As $\mathfrak{p}$ was arbitrary we see again that the other coefficients of $f$ must be nilpotent as required. Therefore $A[X]^\star \subseteq A^\star + X\mathcal{N}(A)[X]$. Conversely it's a general fact that $B^\star + \mathfrak{N}(B) \subseteq B^\star$, for if

$$f = a + g$$

with $g^r = 0$ and $a \in B^\star$ then one may check that

$$f^{-1} = (a^{-1} - a^{-2}g + a^{-3}g^2 + \ldots + (-1)^{r-1}a^{-r}g^{r-1})$$

□

It satisfies the following universal property

**Proposition 3.6.4** (Evaluation at a point)
*Consider an $A$-algebra $B$ and $b \in B$. Then there exists a unique $A$-algebra homomorphism*

$$\mathrm{ev}_b : A[X] \to B$$

*such that $\mathrm{ev}_b(X) = b$. We write $p(b) = \mathrm{ev}_b(p)$. It is given by*

$$p(b) = \sum_{k=0}^{\deg(p)} i_B(a_k) b^k$$

*The image of $\mathrm{ev}_p$ is equal to $A[b]$ the smallest sub-$A$-algebra generated by $b$. For any morphism $\phi : B \to C$ such that $\phi(b) = c$ we have*

$$\phi \circ \mathrm{ev}_b = \mathrm{ev}_c$$

**Remark 3.6.5**
*In categorical jargon $A[X]$ is an initial object in the category of pointed $A$-algebras.*

**Proposition 3.6.6** (Evaluation commutes with algebra homomorphism)
*Let $\phi : B \to C$ be a homomorphism of $A$-algebras and $p \in A[X]$ then*

$$\phi(p(b)) = p(\phi(b))$$

**Definition 3.6.7** (Conjugate polynomial)
*Let $\phi : A \to B$ be a homomorphism and $f \in A[X]$, then define*

$$f^\phi(X) := \sum_{i=0}^{n} \phi(a_i) X^i$$

*It induces a ring homomorphism*

$$A[X] \to B[X]$$

*and has the property that*

$$f^\phi(\phi(a)) = \phi(f(a))$$

**Proposition 3.6.8** (Division Algorithm I)
*Let $A$ be an integral domain and $f(X) \in A[X]$ a polynomial and $g(X) \in A[X]$ a non-zero monic polynomial. Then there exists $q(X)$ and $r(X)$ such that*

$$f(X) = q(X)g(X) + r(X)$$

*and $\deg(r) < \deg(g)$. In particular when $\deg(g) = 1$ then $r \in A$.*

*Proof.* If $\deg(f) < \deg(g)$ then $q = 0$ and $r = f$. Otherwise assume $n = \deg(f) \geq \deg(g) = m$ and proceed by induction on $n$. Note that since $g$ is monic then we have $f - c(f)gX^{n-m}$ has degree $n - 1$, so by induction

$$f - c(f)gX^{n-m} = q'g + r$$

with $\deg(r) < \deg(g)$. Therefore

$$f = (q' + c(f)X^{n-m})g + r$$

as required. □

## 3.7 Polynomial Rings in Many Variables

**Definition 3.7.1**
*Let $A$ be a ring then the polynomial ring $A[X_1, \ldots, X_n]$ consists of formal sums of monomials*

$$f(X_1, \ldots, X_n) = \sum_{v \in \mathbb{N}^n} f_v X_1^{v_1} \ldots X_n^{v_n}$$

*where $f_v \in A$ and only finitely many coefficients are non-zero. Addition is defined in the obvious way. Multiplication is defined as*

$$\left(\sum_v f_v X^v\right)\left(\sum_w g_w X^w\right) := \sum_z \left(\sum_{v,w : v+w=z} f_v g_w\right) X^z$$

*We may canonically regarding $A$, $A[X_i]$ and $A[X_1, \ldots, X_i]$ as subrings in the obvious way.*

*Define* $\deg(f, i)$ *to be the maximal power of* $X_i$ *with a non-zero coefficient.*

**Remark 3.7.2**
*It may be useful for certain induction arguments to write*

$$A[X_1, \ldots, X_n] = A$$

*when* $n = 0$.

**Proposition 3.7.3** (Universal Property)
$A[X_1, \ldots, X_n]$ *satisfies the following universal property. Given any* $A$*-algebra* $B$ *and points* $(b_1, \ldots, b_n)$ *there exists morphism*

$$\phi_b : A[X_1, \ldots, X_n] \to B$$

*such that*

$$\phi_b(X_i) = \phi(b_i)$$

*given by*

$$\phi_b(\sum_v a_v X_1^{v_1} \ldots X_n^{v_n}) = \sum_v i_B(a_v)\phi(b_1)^{v_1} \ldots \phi(b_n)^{v_n}$$

*In otherwords it is an initial object in the category of* $n$*-pointed* $A$*-algebras. Furthermore*

$$\mathrm{Im}(\phi_b) = A[b_1, \ldots, b_n]$$

**Lemma 3.7.4** (Iterated polynomial ring)
*Given* $f \in A[X_1, \ldots, X_n]$ *and let* $N = \deg(f, n)$ *then there exist unique polynomials* $g_i \in A[X_1, \ldots, X_{n-1}]$ *such that*

$$f = \sum_{i=0}^{N} g_i X_n^i$$

*in other words there is a canonical isomorphism*

$$\psi : A[X_1, \ldots, X_{n-1}][X_n] \to A[X_1, \ldots, X_n]$$

*under which* $\deg(f) = \deg(\psi(f); n)$.

*Proof.* Define $g_i = \sum_{v : v_n = i} f_v X_1^{v_1} \ldots X_{n-1}^{v_{n-1}}$ □

**Proposition 3.7.5** (Homogenous grading)
*Consider* $R = k[X_1, \ldots, X_n]$ *and* $x \in k^n$. *Then there is a direct sum of* $k$*-submodules*

$$R = \bigoplus_{n \geq 0} R^{n,x}$$

*where*

$$R^{n,x} = \Big\{ \sum_{|\alpha|_1 = n} \lambda_\alpha (X_1 - x_1)^{\alpha_1} \ldots (X_n - x_n)^{\alpha_n} \mid \lambda_\alpha \in k \quad \alpha \in \mathbb{N}^n \Big\}$$

*and every* $F \in R$ *may be written uniquely as*

$$F(X) = F(x) + F^{(1,x)}(X) + \ldots + F^{(n,x)}(X) + \ldots$$

*with* $F^{(n,x)} \in R^{n,x}$. *Note that*

$$\ker(\mathrm{ev}_x) =: M_x = \bigoplus_{n \geq 1} R^{n,x} = (X_1 - x_1, \ldots, X_n - x_n)$$

*and*

$$M_x^k = \bigoplus_{n \geq k} R^{n,x}$$

*Finally there is a canonical isomorphism*

$$k[X_1, \ldots, X_n]^{(1,x)} \cong M_x / M_x^2$$

*Proof.* By Proposition (...) there is $k$-algebra homomorphism $\rho_x : R \to R$ given by $X_i \to X_i + x_i$. It is an isomorphism with two-sided inverse $\rho_{-x}$. Let $F \in R$ then

$$\rho_x(F) = \sum_{n=0}^{\infty} \left( \sum_{|\alpha|_1 = n} \lambda_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n} \right)$$

whence applying $\rho_{-x}$

$$\begin{aligned} F(X) &= \sum_{n=0}^{\infty} F^{(n)}(X) \\ F^{(n)}(X) &= \sum_{|\alpha|_1 = n} \lambda_\alpha (X_1 - x_1)^{\alpha_1} \dots (X_n - x_n)^{\alpha_n} \end{aligned}$$

as required. The coefficients $\lambda_\alpha$ are seen to be uniquely determined by applying $\rho_x$. Therefore the internal sum is direct. Finally evaluate at $x$ to find $F^{(0)} = F(x)$. The statement regarding $M_x$ is straightforward. And because $R^{n,x} \cdot R^{m,x} \subseteq R^{n+m,x}$ the statement regarding $M_x^k$ follows by induction. □

**Proposition 3.7.6**
*Using the notation of the previous Proposition then*

$$F^{(1,x)}(X) = \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(x)(X_i - x_i)$$

**Definition 3.7.7** (Projection to linear terms)
*Given $\mathfrak{a} \lhd k[X_1, \dots, X_n]$ and $x \in k^n$ define*

$$\mathfrak{a}^{(i,x)} = \{F^{(i,x)} \mid F \in \mathfrak{a}\}$$

## 3.8 Chain Conditions

**Definition 3.8.1** (Noetherian / Artinian / Finite Modules)
*We say an $A$-module $M$ is **Noetherian** if it satisfies the **ascending chain condition**, namely any ascending chain of submodules*

$$M_0 \subseteq M_1 \subseteq \dots \subseteq M$$

*eventually stabilizes, i.e $M_n = M_{n+1} \quad \forall n \geq N$.*

*Similarly we say an $A$-module $M$ is **Artinian** if it satisfies the **descending chain condition**, namely any descending chain of submodules*

$$M \supseteq M_0 \supseteq M_1 \supseteq \dots$$

*eventually stabilizes.*

**Definition 3.8.2** (Noetherian / Artinian Ring)
*We say a ring $A$ is **Noetherian** (resp. Artinian) if every it is Noetherian (resp. Artinian) as an $A$-module.*

The following is useful

**Proposition 3.8.3** (Noetherian criterion)
*Let $M$ be an $A$-module. The following are equivalent*

a) *$M$ is Noetherian*

b) *Every submodule $N \subseteq M$ is finitely-generated*

c) *Every set of submodules has a maximal element*

**Proposition 3.8.4** (Restriction of Scalars preserves finiteness)
*Let $\phi : A \to B$ be a finite $A$-algebra and $M$ a finite $B$-module. Then $[M]_\phi$ is a finite $A$-module.*

*Proof.* We suppose that $M$ is generated by $m_1, \dots, m_n$, and $B$ is generated by $b_1, \dots, b_m$. Then we claim that the elements $b_i m_j$ generate $[M]_\phi$. □

## 3.9 Unique Factorization

For this section we assume $A$ is a commutative integral domain.

**Definition 3.9.1** (Associates)
*We say two non-zero elements $x$ and $y$ are **associates** if $x = uy$ for some $u \in A^\star$. We write $x \sim y$.*

**Lemma 3.9.2**
*The associate relation $x \sim y$ is an equivalence relation on $A \setminus \{0\}$.*

**Definition 3.9.3** (Irreducible element)
*We say $0 \neq x$ is **irreducible** if $x = ab \implies a$ a unit or $b$ a unit.*

**Definition 3.9.4** (Prime element)
*We say $0 \neq p$ is prime if $p \mid ab \implies p \mid a$ or $p \mid b$.*

**Example 3.9.5**
*The units of $\mathbb{Z}$ are $\{-1, 1\}$ so each equivalence class is of the form $\{n, -n\}$.*

**Lemma 3.9.6**
*Suppose $A$ is an integral domain. Then $x \mid y \wedge y \mid x \iff x \sim y$.*

*Proof.* We have $y = ax = aby \implies y(1 - ab) = 0$. Since $A$ is an integral domain $1 = ab$, i.e. $a$ is a unit as required. The converse is clear. □

**Example 3.9.7**
*A number $p \in \mathbb{Z}$ is prime in the traditional sense exactly when it is irreducible. It is of course also prime in the ring-theoretic sense but this requires proof (see (2.3.13)).*

The concept of associates is important to unique factorization, because we may only hope to have unique factorization upto multiplication by a unit.

**Lemma 3.9.8**
*If $x \sim y$ are associates then $x$ is irreducible iff $y$ is*

*Proof.* Suppose $x \sim y$ and $x$ irreducible. If $y = ab$ then $x = abu \implies a$ a unit and $bu$ a unit $\implies b$ a unit. Therefore $y$ is irreducible as required. □

**Example 3.9.9**
*The units of $\mathbb{Z}$ are $\{-1, 1\}$. Therefore $n$ is irreducible (i.e. prime) iff $-n$ is.*

**Lemma 3.9.10** (Criterion for primality)
*$p$ is prime if and only if $(p)$ is a prime ideal*

*Proof.* Note $x \mid y \iff y \in (x)$. So in particular if $p$ is prime then $xy \in (p) \implies p \mid xy \implies p \mid x$ or $p \mid y \implies x \in (p)$ or $y \in (p)$, whence $(p)$ is prime.

Conversely if $(p)$ is prime, then $p \mid xy \implies xy \in (p) \implies x \in (p)$ or $y \in p \implies p \mid x$ or $p \mid y$, so that $p$ is prime. □

**Lemma 3.9.11** (Criterion for irreducibility)
*Let $A$ be an integral domain. Then $f$ is irreducible if and only if $(f)$ is maximal amongst principal ideals.*

*Proof.* Suppose $f$ is irreducible and $(f) \subseteq (g)$. Then $f = ag$ with either $a$ a unit or $g$ a unit. If $a$ is a unit then $(f) = (g)$, and if $g$ is a unit $(g) = A$. So the result follows.

Conversely TODO □

**Proposition 3.9.12** (Primes are Irreducible)
*Let $A$ be an integral domain then $p$ prime $\implies p$ irreducible*

*Proof.* Suppose $b \mid p$ then $p = ab$ and $a \mid p$. By hypothesis $p \mid a$ or $p \mid b$. If $p \mid a$ (resp. $b$) then by (3.9.6) $p \sim a$ (resp. $b$) as required. □

**Definition 3.9.13** (Unique Factorization Domain (UFD) or Factorial Ring)
*We say an integral domain $A$ is factorial (or a UFD) if every element $0 \neq a$ may be represented as*

$$a = u \prod_{i=1}^{n} p_i$$

*for $u$ a unit and $p_i$ irreducible, and moreover this is unique in the sense that given another factorization*

$$a = u' \prod_{i=1}^{m} p_i'$$

*we have* $n = m$ *and* $p_i \sim p'_{\psi(i)}$*, for* $\psi$ *a permutation on* $\{1, \ldots, n\}$*.*

**Definition 3.9.14** (Atomic Ring)
*We say that* $A$ *is* ***atomic*** *if it has a (not necessarily unique) decomposition into irreducible elements.*

**Proposition 3.9.15**
*A Noetherian ring is atomic.*
*In fact we need only the weaker condition that any ascending chain of* principal *ideals terminates (ACCP).*

*Proof.* □

We show a simple criterion for a ring to be a UFD.

**Proposition 3.9.16** (Atomic + AP $\iff$ UFD)
*The following are equivalent*

- *A is a UFD*
- *A is integral, atomic and (p irreducible* $\implies$ *p prime)*

*NB a ring satisfying irreducible* $\implies$ *prime is referred to as an AP-domain.*

*Proof.* Suppose $A$ is a UFD. Then by definition it is atomic. Suppose $p$ is an irreducible element and $p \mid ab$, then by uniqueness it must appear in the irreducible factorization of either $a$ or $b$, so we are done.

Conversely suppose $A$ is integral and atomic. We wish to show uniqueness of factorization, that is if

$$\prod_{i=1}^{n} p_i \sim \prod_{j=1}^{m} p_j'$$

then $n = m$ and $p_i \sim p'_{\sigma(i)}$ for some permutation $\sigma$. By convention an empty product is 1 and by hypothesis all the elements are in fact prime. If $n = 0$, then since $p_j'$ is irreducible, it is not a unit and hence $m = 0$. Otherwise consider $p_1$, then $p_1 \mid$ RHS , so by definition of prime we must have $p_1 \mid p_j'$ for some $j$. Since $p_j'$ is irreducible and $p_1$ is not a unit, we have $p_1 \sim p_j'$. Since $A$ is integral we may cancel these two to obtain an equivalence of smaller degree and we may proceed by induction. □

Furthermore it may be convenient in applications to count the multiplicities

**Proposition 3.9.17** (Factorization with multiplicities)
*Let* $A$ *be a unique factorization domain, then for every element* $0 \neq a \in A$ *there is a factorization of the form*

$$a = u \prod_{i=1}^{n} p_i^{r_i}$$

*where* $r_i > 0$ *and none of the* $p_i$ *are associate to each other. Furthermore this is essentially unique in the sense that given another such factorization we have* $n = n'$*,* $r_i = r'_{\sigma(i)}$ *and* $p_i \sim p'_{\sigma(i)}$ *for some permutation* $\sigma \in S_n$*.*

*Proof.* Given a factorization into irreducible elements

$$a = u \prod_{i=1}^{n} p_i$$

Consider a representative set of irreducibles $q_1, \ldots, q_m$ (under the equivalence relation $x \sim y$). Then we have $p_i = q_{\pi(i)} u_i$ for some units $u_i$ and mapping $\pi : \{1, \ldots, n\} \to \{1, \ldots, m\}$. Let $r_j = \#\pi^{-1}(j)$. Then we have that the set of irreducibles $\{p_1, \ldots, p_n\}$ is the *disjoint* union of the set of equivalence classes with representatives $q_j$. Therefore

$$a = u \prod_{j=1}^{m} \prod_{p \sim q_j} p = u \prod_{j=1}^{m} \prod_{i:\pi(i)=j} u_i q_j = \left( u \prod_{j=1}^{m} \prod_{i:\pi(i)=j} u_i \right) \prod_{j=1}^{m} q_j^{r_j}$$

as required. Suppose we have two factorizations

$$u \prod_{i=1}^{n} p_i^{r_i} = u' \prod_{i=1}^{m} (p_i')^{r_i'}$$

Let $I$ be the indexing set of $p_i$ and $J$ the set of $p'_j$. By unique factorization there must be mappings $\sigma : I \to J$ such that $p_i \sim p'_{\sigma(i)}$, and $\tau : J \to I$ such that $p'_j \sim p_{\tau(j)}$. Which means that $p_i \sim p_{\tau(\sigma(i))}$ and $p'_j \sim p_{\sigma(\tau(i))}$. Since none are associate to each other we see that $\tau$ and $\sigma$ are mutual inverses, whence $m = n$ and we may regard $\sigma \in S_n$. In the unique factorization $p_i$ appears $r_i$ times and $p'_{\sigma(i)}$ appears $r'_{\sigma(i)}$ times. Since $p_i$ is associate to $p'_{\sigma(i)}$ it is not associate to any $p'_j$ for $j \neq \sigma(i)$. Unique factorization shows that $r_i = r'_{\sigma(i)}$.

□

If we take a suitable fixed set of irreducible elements we can obtain completely unique factorization

**Definition 3.9.18**
*Let $A$ be a ring we say $\mathcal{P}$ is a **representative set of irreducible elements** if*

- *No two elements $p, q \in \mathcal{P}$ are associate*
- *Every irreducible element $p \in A$ is associate to one in $\mathcal{P}$*

**Example 3.9.19**
*For $\mathbb{Z}$ the* positive *primes are a canonical set of irreducible elements.*

**Corollary 3.9.20** (Canonical Factorization)
*Let $A$ be a UFD and let $\mathcal{P}$ be a set of representative irreducible elements, then we may define a valuation function*

$$v_{(-)}(-) : \mathcal{P} \times A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$$

*such that for all $0 \neq a \in A$ we have*

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

*This factorization is totally unique, and so $v_p$ is additive in the sense that for a fixed irreducible $p \in \mathcal{P}$*

$$v_p(ab) = v_p(a) + v_p(b)$$

**Lemma 3.9.21** (Divisibility)
*Suppose $A$ is a UFD with a canonical factorization function $v_p$. Then $f \mid g$ iff $v_p(f) \leq v_p(g)\ \forall p$ iff $(g) \subseteq (f)$*

## 3.10 Principal Ideal Domains

**Definition 3.10.1** (Principal Ideal Domain)
*An integral domain $A$ is a **principal ideal domain** (or **PID**) if every ideal $\mathfrak{a}$ is principal.*

**Proposition 3.10.2**
*Let $A$ be a PID. An element $a \in A$ is irreducible if and only if $(a)$ is maximal.*

*Proof.* This follows from the definition of a PID and (3.9.11). □

**Proposition 3.10.3**
*A PID is a Noetherian UFD.*

*Furthermore ($f$ is irreducible $\iff$ $f$ is prime), and every prime ideal is maximal.*

*Proof.* Suppose we have an ascending chain of ideals

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_n \ldots$$

Clearly the union is again an ideal, which is also principal of the form $(a)$. We must have $a \in \mathfrak{a}_n$ for some $n$, whence it terminates after $n$. Therefore $A$ is Noetherian by (3.8.3) and atomic by (3.9.15). By (3.9.16) it's enough to show that an irreducible element is prime.

Note that from previous results, and by hypothesis, we have

$$p \text{ irreducible} \overset{(3.10.2)}{\iff} (p) \text{ maximal} \overset{(3.4.50)}{\implies} (p) \text{ prime} \overset{(3.9.10)}{\iff} p \text{ is prime}$$

Finally $p$ prime $\implies$ $p$ irreducible by (3.9.12) to complete the equivalences.

Every prime ideal is principal of the form $(p)$ and we've already shown it's maximal.

□

**Proposition 3.10.4**
*$\mathbb{Z}$ is a PID.*

*In particular an integer $m$ is irreducible $\iff$ it is prime and every prime ideal is maximal.*

*Proof.* This follows from the well-ordering principle. Let $\mathfrak{a}$ be an ideal with minimal positive element $d$. We claim $\mathfrak{a} = (d)$. By the division algorithm (or apply well-ordering principle to the coset $x + (d)$), for every $x \in \mathfrak{a}$ there is $0 \leq r < d$ and $q \in \mathbb{Z}$ such that

$$x = qd + r\,.$$

Clearly $r \in \mathfrak{a}$, whence by minimality $r = 0$ as required. □

**Example 3.10.5**
*Let $k$ be a field, then the ring of polynomials $k[X]$ is a PID, as shown in later.*

**Lemma 3.10.6** (Co-prime elements in a PID)
*Let $A$ be a PID, then $x, y$ are coprime if and only if they have no non-invertible common divisors.*

*Proof.* First suppose $(x, y) = A$, then $ax + by = 1$ and any common divisor $d$ must divide 1 and therefore be invertible.

Conversely suppose $(x, y) \neq (1)$, since A is a PID it must equal $(d)$ for some non-invertible $d$ which is then a common divisor. □

## 3.11 Matrix Rings

**Definition 3.11.1**
*Let $A$ be a non-zero commutative ring. Define the set of matrices*

$$\mathrm{Mat}_{m,n}(A) = \{(E_{ij})_{i=1\ldots n\, j=1\ldots m}\}$$

*There is the standard multiplication operator*

$$\mathrm{Mat}_{m,n}(A) \times \mathrm{Mat}_{n,p}(A) \to \mathrm{Mat}_{m,p}(A)$$

*If $\phi : A \to B$ is a ring homomorphism, then there is a pointwise map*

$$\begin{array}{rcl} \mathrm{Mat}_{m,n}(A) & \to & \mathrm{Mat}_{m,n}(B) \\ E & \to & E^{\phi} \end{array}$$

Matrices are concrete realisations of linear maps of finite free $A$-modules, as demonstrated in the next two Propositions.

**Proposition 3.11.2** (Matrix by vector multiplication)
*There is a canonical bijection of $A$-modules*

$$\begin{array}{rcl} \mathrm{Mat}_{m\times n}(A) & \longrightarrow & \mathrm{Hom}_A(A^n, A^m) \\ E & \longrightarrow & \widehat{E} : (v_j)_{j=1\ldots n} \to \left(\sum_{j=1}^{n} E_{ij} v_j\right)_{i=1\ldots m} \end{array}$$

*under which matrix multiplication corresponds to composition of functions, that is*

$$\widehat{E} \circ \widehat{F} = \widehat{EF}$$

**Corollary 3.11.3** (Algebra of matrices)
*The set of square matrices $\mathrm{Mat}_{n,n}(A)$ forms an $A$-algebra under multiplication, with the structural morphism given by*

$$a \longrightarrow aI_n$$

Similarly

**Proposition 3.11.4** (Matrix representation of a morphism)
*Let $M, N$ be two finite free $A$-modules with bases $\mathcal{B}$, $\mathcal{B}'$ of order $p$ and $q$ respectively. Let $\phi \in \mathrm{Mor}_A(M, N)$, then there is a unique matrix $[\phi]^{\mathcal{B}}_{\mathcal{B}'} \in \mathrm{Mat}_{q\times p}(A)$ such that*

$$\phi(m)_{\mathcal{B}'} = [\phi]^{\mathcal{B}}_{\mathcal{B}'} m_{\mathcal{B}}\,.$$

*Explicitly it is characterized by the relationship*

$$\phi(m_i) = \sum_{j=1}^{q} [\phi]_{ji} n_j \quad i = 1 \ldots p$$

*where* $\mathcal{B} = \{m_1, \ldots, m_p\}$ *and* $\mathcal{B}' = \{n_1, \ldots, n_q\}$.

*In addition of* $L$ *is a finite free* $A$*-module with basis* $\mathcal{B}''$ *and* $\psi \in \mathrm{Mor}_A(N, L)$*, then*

$$[\psi \circ \phi]^{\mathcal{B}}_{\mathcal{B}''} = [\psi]^{\mathcal{B}'}_{\mathcal{B}''}[\phi]^{\mathcal{B}}_{\mathcal{B}'}$$

*In particular we induce an* $A$*-module isomorphism*

$$\mathrm{End}_A(M, N) \longrightarrow \mathrm{Mat}_{n\times m}(A)$$
$$\phi \longrightarrow [\phi]^{\mathcal{B}}_{\mathcal{B}'}$$

*for every pair of bases (which is an* $A$*-algebra isomorphism when* $N = M$*) and*

$$[1_M]^{\mathcal{B}}_{\mathcal{B}} = I_n$$

*is the identity matrix.*

**Corollary 3.11.5**
*Let* $M$ *be a finite free* $A$*-module with bases* $\mathcal{B}, \mathcal{B}'$ *and* $\phi \in \mathrm{End}_A(M)$*. Then* $\phi$ *is an isomorphism if and only if* $[\phi]^{\mathcal{B}}_{\mathcal{B}'}$ *is invertible.*

**Corollary 3.11.6** (Change of basis)
*Let* $M$ *be a finite free* $A$*-module and* $\mathcal{B}, \mathcal{B}'$ *bases then*

$$[1_M]^{\mathcal{B}}_{\mathcal{B}'} = \left([1_M]^{\mathcal{B}'}_{\mathcal{B}}\right)^{-1}$$

*and*

$$[\phi]^{\mathcal{B}'}_{\mathcal{B}'} = P[\phi]^{\mathcal{B}}_{\mathcal{B}}P^{-1}$$

*where*

$$P := [1_M]^{\mathcal{B}}_{\mathcal{B}'}$$

*is invertible.*

We may define determinants as follows

**Definition 3.11.7** (Determinant of a Matrix)
*Let* $A$ *be a ring, then define the determinant of a square matrix* $E \in \mathrm{Mat}_{n\times n}(A)$ *as follows*

$$\det(E) := \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} E_{i\sigma(i)}$$

**Proposition 3.11.8**
*The determinant satisfies a number of properties*

- $\det(EF) = \det(E)\det(F)$
- $\det(I_n) = 1$
- $\det(PEP^{-1}) = \det(E)$

*Proof.* TODO

□

**Proposition 3.11.9**
*Let* $\phi : A \to B$ *be a ring homomorphism and* $E \in \mathrm{Mat}_{n,n}(A)$*, then*

$$\det(E^{\phi}) = \phi(\det(E))$$

**Definition 3.11.10**
*Let* $M$ *be a finite free* $A$*-module and* $\phi \in \mathrm{End}_A(M)$*, then define*

$$\det(\phi) := \det([\phi]_{\mathcal{B}})$$

*This is independent of the basis* $\mathcal{B}$.

**Proposition 3.11.11** (Adjoint Matrix)
*Let $E \in \mathrm{Mat}_n(A)$ then there exists an adjoint matrix $E^{\mathrm{ad}}$ such that*

$$EE^{\mathrm{ad}} = E^{\mathrm{ad}}E = \det(E)I_n$$

*Explicitly*

$$E^{\mathrm{ad}}_{ij} = (-1)^{i+j}\det(E_{(ji)})$$

*where $E_{(ij)}$ is formed from $E$ by removing the $i$-th row and $j$-th column.*

**Corollary 3.11.12** (Existence of an Inverse)
*Let $E \in \mathrm{Mat}_n(A)$ then $E$ is invertible if and only if $\det(E) \neq 0$.*

## 3.12 Polynomial ring over a field

Consider polynomials over a field $k$.

**Proposition 3.12.1**
*Degree is multiplicative in the sense $0 \neq f, g$ we have*

$$\deg(fg) = \deg(f) + \deg(g)$$

*In particular $f \mid g \implies \deg(f) \leq \deg(g)$.*

**Proposition 3.12.2**
*The units of $k[X]$ are precisely the non-zero polynomials of degree 0.*

**Proposition 3.12.3** (Associate polynomials)
*The following are equivalent for $0 \neq f, g$*

- $f \sim g$
- $f = \lambda g$ *for* $\lambda \neq 0$
- $f \mid g$ *and* $g \mid f$

**Proposition 3.12.4**
*A polynomial $f \in k[X]$ is associate to precisely one monic polynomial $g$. If $f$ is irreducible so is $g$.*

*Proof.* **TODO** □

**Proposition 3.12.5** (Division Algorithm over a field)
*For $k$ a field consider the polynomial ring $k[X]$. For every pair of polynomials $f(X)$, $g(X)$ there exists unique polynomials $q(X)$ and $r(X)$ such that*

$$f(X) = q(X)g(X) + r(X)$$

*and* $\deg(r) < \deg(g)$.

*Proof.* Apply (3.6.8) to $g/c(g)$, and multiply by $c(g)$ again. □

**Proposition 3.12.6** (Polynomial ring is a PID)
*Let $k$ be a field, then $k[X]$ is a PID, and therefore a Noetherian UFD.*

*Proof.* Let $(0) \neq \mathfrak{a}$ be an ideal and let $f \in \mathfrak{a}$ be a polynomial of minimal degree. We may assume it is monic. Any $g \in \mathfrak{a}$ may be represented as $f = qg + r$ by the division algorithm. Clearly $r \in \mathfrak{a}$, therefore by minimality $r = 0$, whence $g \in (f)$. □

**Proposition 3.12.7** (Unique Factorization of Polynomials)
*For the ring $k[X]$ the set of irreducible monic polynomials constitutes a representative set (Definition (3.9.18)). Therefore we have a unique factorization*

$$f = c(f) \prod_{p \text{ irreducible monic}} p^{v_p(f)}$$

*such that*

$$v_p(fg) = v_p(f) + v_p(g)$$

*Proof.* (3.12.4) shows that the irreducible monic polynomials constitute a representative set. Therefore the result follows from (3.9.20). Let $u$ be the unit appearing in the factorization, it must be an element of $k$. Compare leading coefficients to see that $u = c(f)$. □

**Lemma 3.12.8** (Roots and Multiplicity)
*For $f \in k[X]$ a non-constant polynomial and $\alpha \in k$ we have*

$$f(\alpha) = 0 \iff (X-\alpha) \mid f \iff v_{(X-\alpha)}(f) > 0$$

*In this case $r := v_{(X-\alpha)}(f)$ is the multiplicity of the root $\alpha$, and observe*

$$f(X) = c(f)(X-a)^r g(X)$$

*with $g(\alpha) \neq 0$ (equivalently $v_{(X-\alpha)}(g) = 0$).*

*Proof.* The right to left implication is obvious. Conversely by the division algorithm we may write

$$f(X) = f(\alpha) + (X-\alpha)Q(X)$$

Then if $f(\alpha) = 0$ we clearly have $v_{(X-\alpha)}(f) > 0$. Finally we may construct

$$g(X) = \prod_{p \neq (X-\alpha)} p^{v_p(f)}$$

It's clear that for every $p$ appearing in the product $p(\alpha) \neq 0$ because otherwise we would have $(X-\alpha) \mid p$ and by irreducibility $(X-\alpha) = p$. Therefore $g(\alpha) \neq 0$ as required. □

**Definition 3.12.9** (Splitting Polynomial)
*Let $K/k$ be a field extension and $f \in k[X]$. We say a polynomial $f$ splits completely in $K$ if the irreducible factorization of $f^i$ in $K[X]$ is*

$$f^i(X) = c(f^i)\prod_{i=1}^{n}(X-\alpha_i)^{r_i}$$

*where $\alpha_i$ are the distinct roots of $f(X)$ in $K$ and $r_i := v_{(X-\alpha_i)}(f^i)$ are the multiplicities. Equivalently $f$ splits in $K$ if*

$$p \in K[X] \text{ irreducible } \wedge \deg(p) > 1 \implies v_p(f^i) = 0 \tag{3.4}$$

*Observe that the number of roots counting multiplicities is* $\deg(f)$

$$\deg(f) = \sum_{i=1}^{n} v_{(X-\alpha_i)}(f^i)$$

**Corollary 3.12.10**
*A polynomial $f$ has at most* $\deg(f)$ *roots*

**Corollary 3.12.11**
*Let $K/k$ be a field extension and $f \in k[X]$. Suppose $g \mid f$ and $f$ splits completely in $K$. Then so does $g$.*

*Proof.* By assumption the irreducible factorization of $f$ consists of polynomials of degree 1. Consider the irreducible factorization of $g = \prod_{i=1}^{n} g_i$, then by unique factorization ((3.12.7)) each $g_i$ must be appear in the factorization of $f$, that is to say $g$ splits completely. □

### 3.12.1 Separable Polynomials

We are interested in characterizing polynomials $f \in k[X]$ which do not have multiple roots in any extension field $K/k$. These are exactly the separable polynomials, and it useful to consider the formal derivative $f'(X)$ as follows

**Proposition 3.12.12** (Criteria for Multiple Roots)
*Let $f(X) \in k[X]$ be a polynomial and either $char(k) = 0$ or $r < char(k)$. Then $\alpha \in k$ is a root of multiplicity $r$ precisely when*

$$f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(r-1)}(\alpha) = 0$$

*and $f^{(r)}(\alpha) \neq 0$.*
*Therefore the multiple roots are precisely the common roots of $f(X)$ and $f'(X)$ (irrespective of the characteristic).*

*Proof.* Note that by (3.12.8)

$$f^{(1)}(X) = (X-\alpha)^{r-1}[rg(X) + (X-\alpha)g'(X)]$$

with $g(\alpha) \neq 0$ and $r$ the multiplicity of the root. If $r = 1$, then $f^{(1)}(\alpha) = g(\alpha) \neq 0$ as required. If $r > 1$, then $f^{(1)}(X)$ has $\alpha$ as a root of multiplicity $r-1$, so it follows by induction.
The second statement is simply the case $r = 1$. □

**Definition 3.12.13** (Separable Polynomial)
*A polynomial $f \in k[X]$ is separable if $f$ and $f'$ are coprime.*

**Proposition 3.12.14** (Separable Polynomial)
*A separable polynomial $f \in k[X]$ has no multiple roots in any extension field $K/k$*

*Proof.* Since $(f, f') = 1$ we have $af + bf' = 1$. Clearly $f$ and $f'$ have no common roots, and therefore $f$ has no multiple roots by (3.12.12). □

**Proposition 3.12.15**
*Suppose $f, g \in k[X]$, $g$ is separable and $f \mid g$, then $f$ is separable.*

*Proof.* Suppose $f$ is not separable then by (3.10.6) $f$ and $f'$ have a common divisor $d$ such that $\deg(d) > 0$. Since $g = fh$, so $g' = f'h + fh'$. Therefore $d$ is also a non-trivial common divisor of $g$ and $g'$ contradicting (3.10.6). □

We can provide a partial converse to (3.12.14) by working in a large enough extension field

**Proposition 3.12.16** (Separability)
*Let $K/k$ be a field extension and $f \in k[X]$ a polynomial which splits completely in $K$. Then TFAE*

a) *$f$ is separable*

b) *$f$ has no multiple roots in $K$*

c) *$f$ has $\deg(f)$ distinct roots in $K$*

*Proof.* Using the formula

$$\deg(f) = \sum_{i=1}^{n} v_{(X-\alpha_i)}(f)$$

we see easily that 3 $\iff$ 2. The previous Proposition shows that 1 $\implies$ 2.

Conversely suppose $f$ is not separable, then by (3.10.6) $f$ and $f'$ must have a non-trivial common divisor $h$. By (3.12.11) we see that $h$ splits in $K$. Any root of $h$ is a common root of $f$ and $f'$ in $K$, which by (3.12.12) is a multiple root of $f$ in $K$. □

## 3.13 Cayley-Hamilton Theorem

**Definition 3.13.1** (Characteristic Polynomial of a Matrix)
*For a matrix $E \in \mathrm{Mat}_n(A)$ define the characteristic polynomial by*

$$P_E(X) := \det(X \cdot I_n - E^T)$$

*working in $\mathrm{Mat}_n(A[X])$. This is a monic polynomial in $A[X]$.*

**Definition 3.13.2** (Characteristic Polynomial of an endomorphism of a free module)
*Let $M$ be a finite free $A$-module. Define the characteristic polynomial of $\phi \in \mathrm{End}_A(M)$ by*

$$P_\phi(X) := P_{[\phi]}(X)$$

*This is independent of the basis $\mathcal{B}$.*

**Lemma 3.13.3**
*Suppose $M = \langle m_1, \ldots, m_n \rangle$ is a finitely generated $A$-module then*

$$\mathfrak{a}M = \mathfrak{a}m_1 + \ldots + \mathfrak{a}m_n$$

*That is every $m \in \mathfrak{a}M$ may be written as*

$$m = \sum_i a_i m_i \quad a_i \in \mathfrak{a}$$

*Proof.* By hypothesis

$$m = \sum_i a_i m_i' \quad m_i' \in M \, a_i \in \mathfrak{a}$$

Furthermore by finite-generation hypothesis

$$m_i' = \sum_j b_{ij} m_j \quad b_{ij} \in A \, .$$

Therefore

$$m = \sum_j (\sum_i a_i b_{ij}) m_j$$

as required. □

**Theorem 3.13.4** (Cayley-Hamilton)
*Let $M$ be a finitely generated $A$-module and $\phi \in \mathrm{End}_A(M)$. Then there exists a monic polynomial $P(X) \in A[X]$ such that*

$$P(\phi) = 0$$

*Furthermore this result may be strengthened in two orthogonal ways*

a) *If $M$ is a finite free $A$-module then $P$ may be taken to be the characteristic polynomial $P_\phi(X)$.*

b) *If $\phi(M) \subseteq \mathfrak{a}M$ for some ideal $\mathfrak{a} \triangleleft A$, then the non-leading coeffients of $P(X)$ may be chosen to be in $\mathfrak{a}$.*

*Proof.* First since $\mathrm{End}_A(M)$ is an $A$-algebra there is a canonical evaluation morphism

$$\mathrm{ev}_\phi : A[X] \to \mathrm{End}_A(M)$$

and the meaning of $P(\phi)$ is simply $\mathrm{ev}_\phi(P)$.

Let $\{m_1, \dots, m_n\}$ be a generating set, then by definition

$$\phi(m_i) = \sum_j E_{ij} m_j$$

for some $E \in \mathrm{Mat}_n(A)$. Consider the matrix

$$B(X) = XI_n - E \in \mathrm{Mat}_n(A[X])$$

Then we may define $B(\phi) := B(X)^{\mathrm{ev}_\phi} \in \mathrm{Mat}_n(\mathrm{End}_A(M))$ pointwise, so given by

$$B(\phi)_{ij} = \delta_{ij}\phi - E_{ij}1_M \,.$$

By definition

$$\sum_j B(\phi)_{ij} m_j = \phi(m_i) - \sum_{ij} E_{ij} m_j = 0$$

Formally we have a group action

$$\mathrm{Mat}_n(\mathrm{End}_A(M)) \times M^n \to M^n$$

$$F \cdot (x_1, \dots, x_n)^T \to \left( \sum_j F_{ij}(x_j) \right)_i$$

such that $(EF)v = E(Fv)$ (check).
And we have shown that

$$B(\phi)\,(m_1, \dots, m_n)^T = \mathbf{0}$$

Using (3.11.11), premultiply by the adjoint to show that

$$\det(B(\phi)) I_n\,(m_1, \dots, m_n)^T = \mathbf{0}$$

and $\det(B(\phi)) \in \mathrm{End}_A(M)$ annihilates $m_1, \dots, m_n$ and therefore $M$.

Finally we claim that $P(X) := \det(B(X)) \in A[X]$ is a suitable monic polynomial. We see that

$$P(\phi) := \mathrm{ev}_\phi(\det(B(X))) \overset{(3.11.9)}{=} \det(B(X)^{\mathrm{ev}_\phi}) = \det(B(\phi)) = 0$$

When $M$ is a finite free $A$-module then we may choose $\{m_1, \dots, m_n\}$ to be a basis, and then the matrix $E$ equals $[\phi]^T$ as required.

Finally when $\phi(M) \subseteq \mathfrak{a}M$ then Lemma 3.13.3 shows we may choose the coefficients $E_{ij}$ to be in $\mathfrak{a}$. It's clear that $P(X)$ then has non-leading coefficients in $\mathfrak{a}$. □

## 3.14 Finite-type Algebras

**Definition 3.14.1** (Finite algebra)
*An $A$-algebra $B$ is* finite *if it is finite as an $A$-module.*

**Definition 3.14.2** (Finitely generated algebra)
*An $A$-algebra $B$ is finitely generated (or of finite type) if there exists an integer $n \in \mathbb{N}$ and a surjection of $A$-algebras*

$$A[X_1, \dots, X_n] \to B$$

*the images of $X_i$ are the generators.*

## 3.15 Fields and Galois Theory

This largely follows Lang's Algebra, where extensive use of an algebraic closure $\bar{k}$ is central. However many results may be shown in the finite case without recourse to $\bar{k}$, and so I attempt to present the results with respect to an arbitrary normal overfield $L$, so that the use of $\bar{k}$ *may* be avoided.

### 3.15.1 Algebraic Extensions

**Definition 3.15.1** (Field Extension)
*Let $k$ be a field. A field extension $K/k$ is a $k$-algebra $K$ which is also a field. Every field $K$ is an extension over its prime subfield ($\mathbb{Q}$ or $\mathbb{F}_p$).*

*We typical denote the structural morphism by $i_{kK} : k \to K$, and it is automatically injective ((3.4.52)). We may write $(K/k, i_{kK})$ if we need to stress the relevance of the structural morphism to the argument.*

*These objects form a category $\mathbf{Field}_k$ in the obvious way. The morphisms may be called $k$-embeddings and we denote them by*

$$\mathrm{Mor}_k(K, L)$$

*and the set of automorphisms by*

$$\mathrm{Aut}(K/k)\,.$$

*Observe every extension $K/k$ may be viewed as a $k$-vector space so we define the degree of an extension field to be the vector space dimension*

$$[K : k] := \dim_k K$$

**Definition 3.15.2** (Finite field extension)
*A field extension $K/k$ is finite if $[K : k] < \infty$*

**Definition 3.15.3** (Tower of Field Extensions)
*We may also consider a "tower" of extensions*

$$K_n/\ldots/K_0 = k$$

*with embeddings $i_{K_iK_{i+1}} : K_i \to K_{i+1}$, with the picture that these usually correspond to inclusions. We may consider an extension $K_i/K_j$ for $j < i$. Typically if we have a family of morphisms*

$$\sigma_i : K_i \to M$$

*they would commute with these embeddings. In particular we may abuse notation by defining $\sigma_i|_{K_j} = \sigma_i \circ i_{K_{i-1}K_i} \circ \ldots \circ i_{K_jK_{j+1}}$.*

**Proposition 3.15.4**
*Let $L/K$ and $K/k$ be two finite extensions with basis $\{l_1, \ldots, l_n\}$ and $\{k_1, \ldots, k_m\}$. Then $L/k$ has basis $\{l_ik_j\}_{i,j}$. In particular*

$$[L : k] = [L : K][K : k]$$

**Corollary 3.15.5**
*Let $K = K_n/\ldots/K_0 = k$ be a tower of finite extensions then*

$$[K : k] = \prod_{i=1}^{n} [K_i : K_{i-1}]$$

**Definition 3.15.6** (Evaluation homomorphism)
*Let $K/k$ be a field extension and $\alpha \in K$. There is a canonical homomorphism*

$$\mathrm{ev}_\alpha : k[X] \to K$$
$$\sum_{i=0}^{n} a_iX^i \to \sum_{i=0}^{n} i_{kK}(a_i)\alpha^i$$

*which we write as $f(\alpha)$. We say $\alpha \in K$ is a root of $f(X)$ if $f(\alpha) = 0$.*

**Proposition 3.15.7** (Morphisms commute with evaluation)
*Let $\sigma : K/k \to L/k$ be a morphism of field extensions then*

$$\sigma(p(\alpha)) = p(\sigma(\alpha))$$

*for all $p \in k[X]$. In particular $\alpha$ is a root of $p \iff \sigma(\alpha)$ is a root of $p$.*

*Proof.* This is just a specific case of (3.6.6), The last statement is obvious, because $\sigma$ is injective ((3.4.52)). □

**Definition 3.15.8** (Subalgebra generated by a set)
*Let $K/k$ be a field extension and $S \subset K$ a finite subset. Recall $k[S]$ is the smallest sub-algebra containing $S$. When $S = \{\alpha_1, \dots, \alpha_n\}$ is finite then*

$$k[\alpha_1, \dots \alpha_n] = \text{im}(\text{ev}_\alpha) = \{p(\alpha_1, \dots, \alpha_n) \mid p \in k[X_1, \dots, X_n]\}$$

*from the characterization from (3.7.3). In general then*

$$k[S] = \bigcup_{S' \subset S \text{ finite}} k[S']$$

**Lemma 3.15.9** (Trivial result)
*For $S, T \subset K/k$ finite*

- $S \subset T \implies k[S] \subseteq k[T]$
- $k[S][T] = k[S \cup T]$

*Proof.* The first is obvious. For the second we wish to show

$$k[S][t] = k[S \cup \{t\}]$$

This essentially follows from (3.7.4). By induction it's true in general. □

**Definition 3.15.10** (Subfield generated by a set)
*Let $K/k$ be a field extension and $S \subset K$ a subset. When $S = \{\alpha_1, \dots, \alpha_n\}$ is finite define*

$$k(S) := \left\{ \frac{p(\alpha_1, \dots, \alpha_n)}{q(\alpha_1, \dots, \alpha_n)} \mid p, q \in k[X_1, \dots, X_n] \right\}$$

*Clearly this is independent of the ordering om $S$. And in general*

$$k(S) := \bigcup_{S' \subset S \text{ finite}} k(S')$$

*It is the smallest subfield of $K$ containing $S$.*

**Lemma 3.15.11** (Trivial result)
*For $S, T \subset K/k$ finite*

- $S \subset T \implies k(S) \subseteq k(T)$
- $k(S)(T) = k(S \cup T)$

**Lemma 3.15.12**
*If $S \subset K$ and $k[S]$ is a field then $k[S] = k(S)$*

*Proof.* This follows from the characterization of $k(S)$ and $k[S]$ when $S$ is finite. The infinite case then follows easily. □

**Lemma 3.15.13** (Image of f.g. field extension)
*Let $K/k$ be a field extension and $S \subset K$ a subset. If $\sigma : K/k \to L/k$ is a morphism them*

$$\sigma(k(S)) = k(\sigma(S))$$

**Proposition 3.15.14** (Uniqueness of morphisms on a generating set)
*Let $K/k$ be a field extension and $S \subset K$ a finite set. If $\sigma, \sigma' : k(S)/k \to L/k$ are morphisms of field extensions such that $\sigma|_S = \sigma'|_S$. Then $\sigma = \sigma'$.*

**Definition 3.15.15** (Simple (Algebraic) Extension)
*A field extension $K/k$ is simple if $K = k(\{\alpha\}) =: k(\alpha)$ for some $\alpha \in K$. It is a simple algebraic extension if $\alpha$ is also algebraic over $k$.*

**Definition 3.15.16** (Algebraic Element)
*We say an element $\alpha \in K/k$ is algebraic if it is a root of a polynomial $f \in k[X]$ (i.e. $\alpha$ is integral, since we can always ensure $f$ is monic)*
*We say an extension $K/k$ is algebraic if every element $\alpha \in K$ is algebraic over $k$.*

**Proposition 3.15.17** (Finite $\implies$ algebraic)
*A finite extension $K/k$ is algebraic.*

*Proof.* Suppose $n = \dim_k K$. The set $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ is linearly dependent by (2.2.11). Therefore there is a non-zero polynomial with $\alpha$ as a root. □

**Proposition 3.15.18** (Endomorphisms are automorphisms)
*Let $\sigma \in \mathrm{Mor}_k(K,K)$ be an endomorphism of an algebraic extension. Then it is an isomorphism. In other words*

$$\mathrm{Mor}_k(K,K) = \mathrm{Aut}(K/k)$$

*Proof.* As field morphisms are injective (3.4.52) we only need to show that $\sigma$ is surjective. Given $\alpha \in K$ let $T$ denote the set of roots of $m_\alpha \in k[X]$ in $K$. Note by (3.12.10) $T$ is finite. Further by (3.15.7) $\sigma$ maps $T$ to itself. Since $\sigma$ is injective it is also surjective on $T$. In particular $\alpha$ is in the image of $\sigma$ as required. □

**Proposition 3.15.19** (Minimal Polynomial)
*If $\alpha \in K/k$ is algebraic then there is a unique monic, irreducible polynomial $m_{\alpha,k}(X) \in k[X]$ such that $m_{\alpha,k}(\alpha) = 0$. This is called the minimal polynomial of $\alpha$ over $k$ and $(m_{\alpha,k}) = \ker(\mathrm{ev}_\alpha)$.*

*Proof.* Let $\mathfrak{a} = \ker(\mathrm{ev}_\alpha)$. Since $k[X]$ is a PID it is of the form $(m_{\alpha,k})$. As $\alpha$ is algebraic it is non-zero. $m_{\alpha,k}(X)$ cannot be a constant, and therefore is not a unit.

We claim $m_{\alpha,k}$ is irreducible. If $m_{\alpha,k}(X) = p(X)q(X)$ then $p, q$ are non-zero and either $p(\alpha) = 0$ or $q(\alpha) = 0$. If $p(\alpha) = 0$ then $m_{\alpha,k} \mid p$. As $p \mid m_{\alpha,k}$ by (3.12.3) $m_{\alpha,k} = \lambda p$. In particular $\deg(m_{\alpha,k}(X)) = \deg(p(X))$ so $\deg(q(X)) = 0$ and $q(X)$ is a unit (3.12.2). Therefore by definition $m_{\alpha,k}(X)$ is irreducible.

Dividing by the leading coefficient we may assume that this polynomial is monic. Suppose $m'(X)$ is another such irreducible monic polynomial. Then $m_\alpha \mid m'$. Since $m_\alpha$ is not a unit, by definition of irreducible $m' \sim m_\alpha$ whence $m' = \lambda m_\alpha$. Compare leading coefficients to find $\lambda = 1$ and $m' = m_\alpha$. □

**Definition 3.15.20** (Conjugate elements)
*Two elements $\alpha, \beta \in K$ are said to be conjugate if they have the same minimal polynomial.*

*NB it's necessary and sufficient that $m_{\alpha,k}(\beta) = 0$.*

**Proposition 3.15.21**
*Let $\sigma : K/k \to L/k$ be a field morphism and $\alpha \in K$. Then $m_{\alpha,k}(X) = m_{\sigma(\alpha),k}(X)$.*

*Proof.* This follows from (3.15.7). □

Given an irreducible polynomial $f \in k[X]$ it's possible to construct an extension field $K/k$ which has at least one root, as follows.

**Proposition 3.15.22** (Construct simple extension)
*Let $f \in k[X]$ be an irreducible polynomial. Then $(f)$ is maximal and $K := k[X]/(f)$ is a field extension with canonical structural morphism. Define $\alpha := X + (f)$*

- $f(\alpha) = 0$
- *$K = k(\alpha)$ is a simple field extension and $k(\alpha) = k[\alpha]$*
- *$m_\alpha = f/c(f)$ and $\deg(m_\alpha) = \deg(f) =: n$*
- *$K$ is a finite-dimensional $k$-vector space with basis*

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

**Example 3.15.23**
*Take $k = \mathbb{R}$, $f(X) = X^2 + 1$, then $\mathbb{C}/\mathbb{R} = \mathbb{R}[i] = \mathbb{R}[X]/(X^2+1)$.*

*Proof.* Consider the structural morphism $i : k \to k[X]$ and canonical surjective homomorphism

$$\pi : k[X] \to k[X]/(f)$$

and $\alpha = X + (f) = \pi(X)$. As $k[X]$ is a PID, $f$ irreducible implies $(f)$ maximal by (3.10.2) so $K$ is a field by (3.4.49). The composition $\pi \circ i$ makes $K$ into a $k$-algebra and hence a field extension. Furthermore $\pi$ is then by definition a $k$-algebra homomorphism.

Since $\pi$ is surjective every $\beta \in K$ is represented as $\pi(p(X)) \overset{(3.15.7)}{=} p(\pi(X)) = p(\alpha)$. By (3.15.8) we see $K = k[\alpha]$. Since $K$ is a field then $K = k[\alpha] = k(\alpha)$ is simple by (3.15.12).

Similarly $f(\alpha) = f(\pi(X)) \overset{(3.15.7)}{=} \pi(f(X)) = 0$, so $\alpha$ is a root of $f$. By (3.12.3) $f/c(f)$ is irreducible and by uniqueness in (3.15.19) we have $m_\alpha = f/c(f)$.

Given $\beta = p(\alpha)$, the division algorithm (...) yields

$$p(X) = q(X)f(X) + r(X)$$

with $\deg(r) < \deg(f) = n$. Therefore $\beta = r(\alpha)$ and the given set is spanning. A non-trivial linear dependence yields a non-zero polynomial $g(X)$ such that $g(\alpha) = 0$ and $\deg(g) < \deg(f)$. But by definition of the minimal polynomial $m_\alpha \mid g$ a contradiction by comparing degrees. Therefore the given set is linearly independent and hence a basis. □

Conversely any simple algebraic extension is obtained in this way, as follows

**Proposition 3.15.24** (Simple extension)
*Let $k(\alpha)/k$ be a simple extension. Then there is a canonical isomorphism of $k$-algebras*

$$k[X]/(m_\alpha) \longrightarrow k(\alpha)$$

*under which $X + (m_\alpha) \to \alpha$. Further $k(\alpha)$ is a finite-dimensional vector space with basis*

$$\{1, \alpha, \dots, \alpha^{n-1}\}$$

*where $n = \deg(m_\alpha) = [k(\alpha) : k]$ and $k(\alpha) = k[\alpha]$.*

*Proof.* By (3.15.19), Definition (3.15.8) and (3.4.47) there is a canonical isomorphism $k[X]/(m_\alpha) \to k[\alpha]$ of $k$-algebras induced by the evaluation homomorphism $\mathrm{ev}_\alpha : k[X] \to K$. (3.15.22) shows that the image of this isomorphism, $k[\alpha]$, is a field, whence $k[\alpha] = k(\alpha)$ by (3.15.12). Since a $k$-algebra isomorphism is a-fortiori a $k$-vector space isomorphism it maps a basis to a basis. The result follows from (3.15.22) as the basis thus defined is the image of the basis in the proposition under the specified isomorphism. □

**Definition 3.15.25** (Degree of an algebraic element)
*Let $K/k$ be an algebraic extension and $\alpha \in K$. Then define*

$$\deg_k(\alpha) := \deg m_{\alpha,k} = [k(\alpha) : k]$$

We may show the following

**Proposition 3.15.26** (Finitely generated by algebraic $\implies$ finite and algebraic)
*Let $K = k(\alpha_1, \dots, \alpha_n)/k$ be a field extension such that $\alpha_i$ is algebraic. Then $K/k$ is a finite algebraic extension. Furthermore*

$$k[\alpha_1, \dots, \alpha_n] = k(\alpha_1, \dots, \alpha_n)$$

*In particular a finitely-generated algebraic extension is finite.*

*Proof.* We write $K_i = k(\alpha_1, \dots, \alpha_i)$. Then we have a tower

$$K = K_n/\dots/K_0 = k$$

such that $K_i = K_{i-1}(\alpha_i)$ is a simple algebraic extension. By (3.15.24) $K_i/K_{i-1}$ is finite. Therefore by (3.15.5) $K/k$ is finite. By (3.15.17) it's also algebraic. For the second statement we may proceed inductively. Note we have

$$k[\alpha_1, \dots, \alpha_{i+1}] \overset{(3.15.9)}{=} k[\alpha_1, \dots, \alpha_i][\alpha_{i+1}] = k(\alpha_1, \dots, \alpha_i)[\alpha_{i+1}] \overset{(3.15.24)}{=} k(\alpha_1, \dots, \alpha_i)(\alpha_{i+1}) \overset{(3.15.11)}{=} k(\alpha_1, \dots, \alpha_{i+1})$$

The second equality is simply the inductive hypothesis. □

**Corollary 3.15.27**
*Let $K/k$ be a field extension then the algebraic elements form a subfield.*

*Proof.* For any two algebraic elements $\alpha, \beta \in K$ we have $k(\alpha, \beta)$ is an algebraic extension. □

The following is useful for reducing to cases of finite extensions where counting arguments work.

**Lemma 3.15.28** (Reduce to finite extensions)
*Let $K/E/k$ be a tower with $E$ algebraic over $k$. For every $\alpha \in K$ algebraic over $E$, there is some subfield $E_0 \subset E$ such that*

- *$E_0/k$ is finite*
- *$\alpha$ is algebraic over $E_0$*
- *$m_{\alpha,E} = m_{\alpha,E_0}$*

*Furthermore $\alpha$ is algebraic over $k$ and $m_{\alpha,E_0} \mid m_{\alpha,k}^{i_{kE}}$.*

*Proof.* Suppose

$$m_{\alpha,E}(X) = a_0 + a_1 X + \dots a_n X^n$$

Then define $E_0 = i_{kE}(k)(a_0, \dots, a_n)$. By (3.15.26) $E_0/k$ is finite. Clearly $\alpha$ is algebraic over $E_0$ as it is a root of $m_{\alpha,E}$. By (3.15.19) $m_{\alpha,E_0} \mid m_{\alpha,E}$ as elements of $E_0[X]$ and $m_{\alpha,E} \mid m_{\alpha,E_0}$. Therefore $m_{\alpha,E_0} = m_{\alpha,E}$.

By (3.15.24) $E_0(\alpha)/E$ is finite, therefore $E_0(\alpha)/k$ is finite. By (3.15.17) $E_0(\alpha)/k$ is algebraic, whence $\alpha$ is algebraic over $k$. The last statement follows from (3.15.19) again. □

**Corollary 3.15.29**
*$K/E$ and $E/k$ are both algebraic if and only if $K/k$ is.*

*Proof.* One direction is obvious. The converse follows from the previous result. □

We may prove the first lifting theorem

**Proposition 3.15.30** (Lifting to simple extensions)
*Let $k(\alpha)/k$ be a simple algebraic extension and $L/k$ a field extension such that $m_{\alpha,k}$ has a root in $L$. Then there exists a morphism $\sigma : k(\alpha)/k \to L/k$.*

*More precisely there is a bijective mapping*

$$\mathrm{Mor}_k(k(\alpha), L) \longrightarrow \{\beta \in L \mid m_{\alpha,k}(\beta) = 0\}$$

*where*

$$\sigma \to \sigma(\alpha)$$

*and $\sigma(k(\alpha)) = k(\sigma(\alpha))$. In particular if $m_{\alpha,k}$ is separable and splits completely in $L$ then there are precisely* $\deg(m_\alpha) \overset{(3.15.24)}{=} [k(\alpha) : k]$ *such extensions.*

*Proof.* Observe $m_{\alpha,k}(\sigma(\alpha)) \overset{(3.15.7)}{=} \sigma(m_{\alpha,k}(\alpha)) = 0$. Therefore the mapping is well-defined. By (3.15.14) it is injective. We claim it is also surjective. By (3.15.24) there is a $k$-algebra isomorphism

$$k[X]/(m_{\alpha,k}) \longrightarrow k(\alpha)$$

Similarly for $\beta \in T$ there is a $k$-algebra isomorphism

$$k[X]/(m_{\beta,k}) \longrightarrow k(\beta)$$

We are done if $m_{\alpha,k} = m_{\beta,k}$. But $m_{\alpha,k}$ is monic, irreducible and has $\beta$ as a root. So this follows from uniqueness of the minimal polynomial in (3.15.19). The final statement follows from (3.12.16) □

We may use this to generalize to arbitrary extensions, but we require that the minimal polynomials split completely in order for the inductive step to work.

**Proposition 3.15.31** (Generic Lifting Theorem)
*Let $K/k$ be an algebraic field extension such that $K = k(\{\alpha_i\}_{i \in I})$ and $L/k$ a field extension such that $m_{\alpha_i,k}(X)$ splits completely in $L$ for all $i \in I$.*

*Then there exists a morphism $\sigma : K/k \to L/k$.*

*Furthermore given $\alpha \in K$ and $\beta \in L$ any root of $m_{\alpha,k}(X)$ we may choose $\sigma$ such that $\sigma(\alpha) = \beta$.*

*Proof.* If $K/k$ is finite then we may proceed by induction on $[K : k]$, using (3.15.30) and applying a similar argument to below.

For the general case we may consider the poset of morphisms $\sigma : K'/k \to L/k$ for subfields $K'/k \subset K/k$ ordered by consistency. It is non-empty by considering $K' = i_{kK}(k)$. By Zorn's Lemma it has a maximal element, $(K', \sigma')$. It's enough to show that $K' = K$.

If $\alpha_i \in K'$ for all $i \in I$ then $K' = K$ and we are done. Otherwise choose $\alpha = \alpha_i \notin K'$. By (...) $m_{\alpha,K'}(X) \mid m_{\alpha,k}(X)$. By (3.12.11) $m_{\alpha,K'}(X)$ splits in $L$ (because $m_{\alpha,k}(X)$ does). Therefore by (3.15.30) there is a morphism $\sigma : K'(\alpha)/K' \to (L/K', \sigma')$. Note that by definition $\sigma|_{K'} = \sigma'$ and $K' \subsetneq K'(\alpha)$, contradicting maximality.

For the final part we may consider the poset consisting only of morphisms such that $\sigma(\alpha) = \beta$. As we observed this poset is also non-empty, and the same argument works. □

### 3.15.2 Galois Theory Summary

**Definition 3.15.32** (Separable, Normal and Galois)
*Let $K/k$ be an algebraic extension. We say that $K/k$ is*

- Normal *if every minimal polynomial $m_{\alpha,k} \in k[X]$ splits completely in $K$ (iff every irreducible polynomial $f \in k[X]$ with at least one root in $K$ splits completely in $K$)*
- Separable *if every minimal polynomial $m_{\alpha,k} \in k[X]$ is separable.*
- Galois *if it is both normal and separable (iff $m_{\alpha,k}$ has $\deg(m_{\alpha,k})$ distinct roots in $K$, see (3.12.16)).*

*In the case of a Galois extension we denote the group of automorphisms by $\mathrm{Gal}(K/k)$.*

To summarize the main results

a) The group of automorphism of a normal extension $K/k$ acts transitively on the roots of a given irreducible polynomial.

b) For $K/k$ finite we have $\#\operatorname{Aut}(K/k) \leq [K:k]$ with equality if and only if $K/k$ is Galois.

c) An algebraic extension $K/k$ is automatically separable whenever either $\mathrm{char}(k) = 0$ or $k$ is finite.

d) When $K/k$ is finite and Galois then we have an order-reversing bijection between subfields and subgroups

$$\begin{array}{rcl} \{H \leq \mathrm{Gal}(K/k)\} & \longleftrightarrow & \{F \subseteq K\} \\ \phi : H & \longrightarrow & K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \psi : \mathrm{Gal}(K/F) & \longleftarrow & F \end{array}$$

### 3.15.3 Splitting Fields and Algebraic Closure

In this section we discuss splitting fields, which are the "smallest" extensions in which a given set of polynomials split completely. The fundamental result is that splitting fields are precisely the Normal extensions. Further we discuss the algebraic closure, in which every polynomial splits and in which every algebraic extension (normal or otherwise) may be embedded.

**Definition 3.15.33** (Splitting field)
*Let $S \subset k[X]$ a family of polynomials. We say that $K/k$ is a **splitting field** for $S$ if*

- *Every polynomial $f \in S$ splits completely in $K$*
- *$K$ is generated by the roots of all the polynomials in $S$*

*Note that by (3.15.26) $K/k$ is necessarily algebraic, and if $S$ is finite then so is $K/k$.*

**Definition 3.15.34** (Set of roots)
*Let $K/k$ be a field extension and $f \in k[X]$. Then define*

$$T_{f,K} := \{\beta \in K \mid f(\beta) = 0\}$$

**Proposition 3.15.35** (Splitting field is minimal)
*Let $S \subset k[X]$ be a family of polynomials which split completely in $K/k$. Then the following are equivalent*

- *$K$ is a splitting field for $S$ i.e.*

$$K = k\left(\bigcup_{f \in S} T_{f,K}\right)$$

- *Any subfield $K' \subset K$ in which $S$ splits completely is equal to $K$*

*Proof.* Let $f_i \in S$ be the polynomials and

$$f_i = \prod_j (X - \alpha_{ij})$$

Suppose $K = k(\alpha_{ij})$. Let $K'$ be a subfield in which all $f_i$ split completely. Then by unique factorization in $K[X]$ we have $\alpha_{ij} \in K'$ for all $i, j$ and therefore $K' = K$.

Conversely it's clear that $S$ splits completely in $k(\alpha_{ij})$, therefore by hypothesis $K = k(\alpha_{ij})$. □

**Lemma 3.15.36**
*Let $\sigma : K/k \to L/k$ be a morphism and $f(X) \in k[X]$ a polynomial. Then*

- *$\sigma$ induces an injective map on the roots $T_{f,K} \to T_{f,L}$*
- *$f$ splits completely in $K \iff f$ splits completely in $\sigma(K)$. In this case the above map is a bijection*

**Proposition 3.15.37** (Image of a splitting field is fixed)
*Let $K/k$ be a splitting field for $S$ and $\sigma : K/k \to L/k$ a morphism. Then $S$ splits completely in $L$. Any such $\sigma$ satisfies*

$$\sigma(K) = k(\bigcup_{f \in S} T_{f,L})$$

*Proof.* Clearly by (3.15.36) $S$ splits completely in $L$.

By the same result $\sigma$ induces a bijection $T_{f,K} \longleftrightarrow T_{f,L}$. Therefore $\sigma(K) = \sigma(k\left(\bigcup_{f\in S} T_{f,K}\right)) = k\left(\sigma\left(\bigcup_{f\in S} T_{f,K}\right)\right) = k\left(\bigcup_{f\in S} T_{f,L}\right)$ by (3.15.13). □

**Proposition 3.15.38** (Uniqueness of Splitting Fields)
*Let $S \subset k[X]$ be a family of polynomials. Let $K/k$ be a splitting field for $S$ and $L/k$ an extension in which $S$ splits completely.*

*Then there exists a morphism $\sigma : K/k \to L/k$. Let $\alpha \in K$ and $\beta \in L$ be conjugate elements, then we may choose $\sigma$ such that $\sigma(\alpha) = \beta$.*

*Furthermore any two splitting fields are isomorphic.*

*Proof.* By assumption $K$ is generated by the roots $\alpha_{ij}$ of $f_i \in S$. For each $\alpha_{ij}$ we therefore have $m_{\alpha_{ij},k}(X) \mid f_i(X)$ and $m_{\alpha_{ij},k}(X)$ splits completely in $L$ by (3.12.11). Therefore the morphism $\sigma : K/k \to L/k$ exists by (3.15.31).

Note by (3.15.37) $S$ splits in $\sigma(K) = k(\bigcup_{f\in S} T_{f,L})$. If $L$ is also a splitting field for $S$ then $L = \sigma(K)$ by (3.15.35) and therefore $\sigma$ is an isomorphism as required. □

**Proposition 3.15.39** (Algebraically Closed)
*A field $M$ is algebraically closed if one of the following equivalent conditions holds*

- *Every algebraic extension $M'/M$ is trivial*
- *Every non-constant polynomial in $M[X]$ has a root in $M$*
- *Every non-constant polynomial in $M[X]$ splits in $M$*

*NB in this case $M$ is also normal.*

**Definition 3.15.40** (Algebraic Closure)
*An **algebraic closure** $\bar{k}$ of $k$ is a field extension $\bar{k}/k$ which is algebraic and for which $\bar{k}$ is algebraically closed.*

The following result shows that it's sufficient for polynomials in the base field to split completely (rather than all polynomials).

**Proposition 3.15.41** (Existence of Algebraic Closure)
*Given a field $k$ there exists an algebraic closure $\bar{k}/k$*

**Proposition 3.15.42** (Algebraic extensions embed into Algebraic Closure)
*Let $K/k$ be an algebraic extension and $M/k$ be an algebraically closed field (e.g. $M = \bar{k}$) then there exists a morphism $\sigma : K/k \to M/k$.*

*Proof.* A straightforward application of (3.15.31) since every $m_{\alpha,k}(X)$ splits in $M$. □

**Corollary 3.15.43** (Uniqueness of algebraic closure)
*An algebraic closure $\bar{k}$ of $k$ is unique up to (non-unique) isomorphism.*

More generally we may show the existence of smaller splitting fields

**Proposition 3.15.44** (Existence of Splitting Field)
*Given a field $k$ and family of polynomials $S \subset k[X]$ then there exists a splitting field $K$.*

*When $S = \{f\}$ then this can be chosen such that $[K : k] \leq n!$ where $n = \deg(f)$.*

*Proof.* We may take the subfield of $\bar{k}$ generated by the roots of polynomials in $S$.

In the case $S$ is finite it is possible to avoid the use of $\bar{k}$. First reduce to the case of a single polynomial $S = \{f\}$ and proceed by induction on $\deg(f)$. The inductive step may be demonstrated using (3.15.22). □

**Remark 3.15.45**
*Note if $K/k$ is an algebraic extension then (3.15.42) shows that we may construct an embedding $K \to \bar{k}$ commuting with $k \to \bar{k}$.*

*In general given a tower of algebraic extensions*

$$K = k_n/\dots/k_0 = k$$

*we will assume the existence of compatible embeddings $i_{k_i} : k_i \to \bar{k}$ such that $i_{k_{i+1}} \circ i_{k_i,k_{i+1}} = i_{k_i}$.*

### 3.15.4 Normal Extensions

Recall that an algebraic extension $K/k$ is normal if all minimal polynomials split completely. They are in some sense "closed". Furthermore $\bar{k}/k$ is clearly normal and results about $\bar{k}$ can often be generalized to normal fields $L/k$. We also show that an extension is normal iff it is a splitting field.

**Lemma 3.15.46**
*Let $L/K/k$ be a tower of algebraic extensions then*

$$L/k \text{ normal} \implies L/K \text{ normal}$$

*Proof.* $m_{\alpha,K}(X) \mid m_{\alpha,k}^{i_{kK}}(X)$ as elements of $K[X]$. □

**Proposition 3.15.47** (Morphisms into Normal fields are conjugate)
*Suppose $K/k$ is algebraic and $L/k$ normal (e.g. $L = \bar{k}$). Then for any pair of morphisms*

$$\alpha, \beta : K/k \to L/k$$

*there is $\sigma \in \mathrm{Aut}(L/k)$ such that*

$$\beta = \sigma \circ \alpha$$

*Proof.* Note that we have two algebraic extensions $(L/K, \alpha)$ and $(L/K, \beta)$. By (3.15.31) there is a morphism

$$\sigma : (L/K, \alpha) \to (L/K, \beta)$$

which is an isomorphism on $L$ by (...). Note that $\sigma \circ i_{kL} = \sigma \circ \alpha \circ i_{kK} = \beta \circ i_{kK} = i_{kL}$, whence $\sigma \in \mathrm{Aut}(L/k)$. □

**Corollary 3.15.48** (Extension to normal overfield)
*Let $L/K/k$ be a tower of algebraic field extensions with $L/k$ normal (e.g. $L = \bar{k}$) then there is a canonical surjection of monoids*

$$\begin{aligned} \mathrm{Mor}_k(i_{KL}, L) : \mathrm{Aut}(L/k) &\to \mathrm{Mor}_k(K, L) \\ \sigma &\to \sigma \circ i_{KL} \end{aligned}$$

*When $i_{KL}$ is inclusion then this is simply the restriction to $K$. The kernel is precisely $\mathrm{Aut}(L/K)$.*

*Proof.* Use the previous corollary with $\alpha := i_{KL}$. □

**Corollary 3.15.49** (Lifting inside normal overfield)
*Let $L/K/F/k$ be a tower of field extensions with $L/k$ normal, then there is a surjection*

$$\mathrm{Mor}_k(i_{FK}, L) : \mathrm{Mor}_k(K, L) \to \mathrm{Mor}_k(F, L)$$

*Proof.* Note that $\mathrm{Mor}_k(i_{FK}, L) \circ \mathrm{Mor}_k(i_{KL}, L) = \mathrm{Mor}_k(i_{FL}, L)$. By the previous Corollary this composition is surjective, whence the result follows. □

**Proposition 3.15.50** (Conjugate elements in Normal Extensions)
*Let $L/k$ be a* normal *extension (e.g. $L = \bar{k}$) and $\alpha, \beta \in L$ elements with the same minimal polynomial $m_\alpha(X) = m_\beta(X)$. Then there exists $\sigma \in \mathrm{Aut}(L/k)$ such that*

$$\sigma(\alpha) = \beta$$

*Proof.* Apply (3.15.31) with $K = L$. It satisfies the hypothesis because every $m_\alpha(X)$ splits completely in $L$. □

**Proposition 3.15.51** (Normal Criteria)
*Let $L/K/k$ be a tower of extensions such that $L/k$ is normal (e.g. $L = \bar{k}$). Then the following are equivalent*

**NOR1a** *For any $\sigma \in \mathrm{Aut}(L/k)$ we have $(\sigma \circ i_{KL})(K) = i_{KL}(K)$*

**NOR1b** *For any $\sigma \in \mathrm{Mor}_k(K, L)$ we have $\sigma(K) = i_{KL}(K)$.*

**NOR2** *$K/k$ is the splitting field of some family of polynomials $f_i \in k[X]$.*

**NOR3** *$K/k$ is normal*

*Proof.* $1b \implies 1a$ is clear.

For $1a \implies 1b$ we may use (3.15.48) to lift to $\tilde{\sigma} \in \mathrm{Aut}(L/k)$.

Clearly $3 \implies 2$, for $K$ is the splitting field of all the minimal polynomials of elements in $K$.

$2 \implies 1b$. This is (3.15.37).

Finally we show $1b \implies 3$. Consider any $\alpha \in K$ with minimal polynomial $m_{\alpha,k}(X)$. By definition $m_{\alpha,k}(X)$ splits completely in $L$ because it has a root $\alpha_1 = i_{KL}(\alpha)$. Denote the roots by $\alpha_1, \ldots, \alpha_r$. By (3.15.50) there is $\sigma_j \in \mathrm{Aut}(L/k)$ such that $\sigma_j(\alpha_1) = \alpha_j$. By hypothesis we have $\alpha_j \in (\sigma \circ i_{KL})(K) = i_{KL}(K)$ whence there exists $\alpha_j' \in K$ such that $i_{KL}(\alpha_j') = \alpha_j$. By (3.15.36) $m_{\alpha,k}(X)$ splits completely in $K$. Therefore $K/k$ is normal as required. □

**Corollary 3.15.52** (Splitting fields are normal)
*An algebraic extension $K/k$ is normal if and only if it is a splitting field.*

*Proof.* We may apply the previous Proposition with $L = \bar{k}$.

We may prove a splitting field is normal more directly (without recourse to $\bar{k}$ or Zorn's Lemma in the finite case). Suppose $K/k$ is a splitting field for $S \subset k[X]$. Consider $\alpha \in K$ with minimal polynomial $m_{\alpha,k}(X)$. Let $(L/K, i_{KL})$ be a splitting field for $m_{\alpha,k}(X)$ (as a polynomial in $K[X]$, NB may not be irreducible).

Let $\beta \in L$ be another root of $m_{\alpha,k}(X)$. Observe that $S$ splits in $L$, so by (3.15.38) there is a morphism $\sigma : K/k \to L/k$ with $\sigma(\alpha) = \beta$. By (3.15.37) we have $i_{KL}(K) = \sigma(K)$ whence $\beta \in i_{KL}(K)$. As $\beta$ was an arbitrary root of $m_{\alpha,k}(X)$ we see it splits completely in $i_{KL}(K)$. Finally by (3.15.36) $m_{\alpha,k}(X)$ splits completely in $K$. As $\alpha$ was arbitrary then $K/k$ is normal. □

**Corollary 3.15.53** (Quotient of automorphism group)
*Let $L/K/k$ be a tower of extensions such that $L/k$ and $K/k$ are normal. Then $L/K$ is normal and there is an isomorphism of groups.*

$$\begin{array}{rcl} \mathrm{Aut}(L/k)/\mathrm{Aut}(L/K) & \longrightarrow & \mathrm{Aut}(K/k) \\ \sigma & \to & i_{KL}^{-1} \circ \sigma \circ i_{KL} \end{array}$$

*Proof.* The given map is well-defined by the previous Proposition since $(\sigma \circ i_{KL})(K) = i_{KL}(K)$, and $\sigma$ fixes $K$ precisely when $\sigma \circ i_{KL} = i_{KL}$, that is $\sigma \in \mathrm{Aut}(L/k)$. Given $\tau \in \mathrm{Aut}(K/k)$, by (3.15.48) there exists $\sigma \in \mathrm{Aut}(L/k)$ such that $\sigma \circ i_{KL} = i_{KL} \circ \tau$. This shows the given map is surjective. The result follows from the group isomorphism theorem. □

**Definition 3.15.54** (Normal Closure)
*Let $K/k$ be an algebraic extension. Then an algebraic extension $L/K$ is a **normal closure** for $K/k$ if*

- *$L/k$ is normal*
- *No proper subfield $i_{KL}(K) \subseteq L' \subsetneq L$ is normal over $k$*

**Proposition 3.15.55** (Existence and Uniqueness of Normal Closure)
*Let $K/k$ be an algebraic extension. Then a normal closure $L/K$ exists and is unique up to isomorphism. Indeed it is the splitting field for all the minimal polynomials $\{m_{\alpha,k}(X) \mid \alpha \in K\}$ over $k$.*

*Furthermore if $K/k$ is finite then so is $L/k$*

*Proof.* Suppose $K = k(\{\alpha_i\}_{i \in I})$. Let $L/k$ be the splitting field for $S = \{m_{\alpha_i,k}(X)\}_{i \in I}$. By (3.15.52) $L/k$ is normal and by (3.15.31) there is a morphism $\sigma : K/k \to L/k$, so we may consider it as an extension $(L/K, \sigma)$. Suppose $i_{KL}(K) \subset L' \subset L$ is normal. As $i_{KL}(\alpha_i) \in L'$, by definition $S$ splits in $L'$ and therefore $L' = L$ by (3.15.35). Therefore $L/K$ is a normal closure as required.

If $K/k$ is finite then we may choose $I$ to be finite, and therefore $L/k$ is finite.

Let $L/K$ be an arbitrary normal closure, then we claim $L/k$ is a splitting field for $S' := \{m_{\alpha,k}(X) \mid \alpha \in K\}$. Clearly $S'$ splits in $L/k$, because each has a root in $L$. Let $L'/k$ be the subfield generated by roots of $S'$. Then it is a splitting field and therefore normal by (3.15.52). By assumption $L' = L$ and therefore $L/k$ is the splitting field for $S'$. Uniqueness follows from the uniqueness of splitting fields (3.15.38). □

### 3.15.5 Separability

We follow Lang and not only characterize separability but define a "separability degree" which equals the extension degree if and only if it's separable. The proofs are somewhat technical, especially in light of the fact most base fields will be perfect.

**Definition 3.15.56** (Separable element)
*We say $\alpha \in K/k$ is separable over $k$ if $m_{\alpha,k}(X)$ is a separable polynomial.*

*We say $K/k$ is separable if every $\alpha \in K$ is separable.*

**Lemma 3.15.57**
*$\alpha \in K/k$ is separable if and only if it is a root of a separable polynomial in $k[X]$.*

*In particular $\alpha$ separable over $k$ implies it is separable over any subfield $E \subset K$.*

*Proof.* One direction is obvious. Conversely suppose $f(\alpha) = 0$ with $f$ separable. Then $m_{\alpha,k} \mid f$ so the result follows from (3.12.15). □

**Proposition 3.15.58** (Separability Degree)
*Let $K/k$ be an algebraic extension and $L/K$ an extension such that $L/k$ is normal (e.g. $L = \bar{k}$ or $L$ is a normal closure). Then define the **separability degree***

$$[K : k]_s := \#\operatorname{Mor}_k(K, L)$$

*This is independent of the choice of $L/K$.*

*Proof.* Given such an $L$, let $L'/K$ be the intersection of all subfields of $L/K$ normal over $k$. This is a normal closure of $K/k$. Let $\sigma \in \operatorname{Mor}_k(K, L)$ and $\alpha \in K$. Then $\sigma(\alpha)$ is a root of $m_{\alpha,k}(X)$ along with $i_{KL}(\alpha) \in L'$. As $L'$ is normal we have $\sigma(\alpha) \in L'$. Therefore without loss of generality we may replace $L$ with $L'$. As the normal closure is unique up to isomorphism the degree is well-defined. □

First we prove a key lemma regarding simple extension

**Lemma 3.15.59** (Separability degree of simple extension)
*If $k(\alpha)/k$ is a simple extension then*

$$[k(\alpha) : k]_s = \#\{ \text{ roots of } m_\alpha \text{ in } \bar{k}\} \leq \deg(m_\alpha) = [k(\alpha) : k]$$

*Furthermore equality holds iff $\alpha$ is separable over $k$.*

*Proof.* The first equality follows from (3.15.30), the final equality from (3.15.24). The inequality follows from (3.12.10). The final statement follows from (3.12.16). □

The main results of this section are the following

**Proposition 3.15.60** (Separability Degree)
*Let $K/F/k$ be a tower of finite extensions*

a) *Then $[K : k]_s = [K : F]_s[F : k]_s$*

b) *$[K : k]_s \leq [K : k]$ with equality if and only if $K/k$ is separable*

*Proof.* For a tower $L/K/F/k$ with $L/k$ normal, consider the restriction map

$$\psi := \operatorname{Mor}_k(i_{FK}, L) : \operatorname{Mor}_k(K, L) \to \operatorname{Mor}_k(F, L)$$

It is surjective by (3.15.49). Consider $\sigma \in \operatorname{Mor}_k(F, L)$ and the fibre $\psi^{-1}(\sigma) = \operatorname{Mor}_F(K, (L/F, \sigma))$. This has order equal to $\#\psi^{-1}(\sigma) = [K : F]_s$ for all $\sigma$, because as we noted it does not depend on the embedding $i_{FL}$. As $\operatorname{Mor}_k(K, L)$ is equal to the disjoint union of all the fibres, then the multiplicativity result follows.

It's possible to decompose $K/k$ as a tower of simple extensions

$$K = K_n/\ldots/K_0 = k$$

with $K_i = K_{i-1}(\alpha_i)$. By (3.15.59) we have

$$[K_i : K_{i-1}]_s \leq [K_i : K_{i-1}]$$

with equality iff $\alpha_i$ separable over $K_{i-1}$. By multiplicativity the inequality follows.

If $K/k$ is separable then by (3.15.57) $\alpha_i$ is separable over $K_{i-1}$ and we have $[K_i : K_{i-1}]_s = [K_i : K_{i-1}]$ and $[K : k]_s = [K : k]$ by multiplicativity. Conversely if $[K : k]_s = [K : k]$ then $[K_i : K_{i-1}]_s = [K_i : K_{i-1}]$ and $\alpha_i$ is separable over $K_{i-1}$. Since the choice of $\alpha_1$ was arbitrary we see that $K/k$ is separable. □

**Proposition 3.15.61**
*Consider a tower of algebraic extensions $K/E/k$. Then $K/E$ and $E/k$ is separable iff $K/k$ is.*

*Proof.* $K/k$ separable $\implies$ $K/E$ and $E/k$ separable follows from (3.15.57).

Conversely the finite case follows from (3.15.60) by multiplicativity. We delay the proof of the general case until later in the section, as we don't need it for subsequent results. □

**Proposition 3.15.62**
*An algebraic extension $K = k(\alpha_1, \ldots, \alpha_n)/k$ is separable iff $\alpha_i$ are.*

*Proof.* Let $K = k(\alpha_1, \ldots, \alpha_n)$. Then we may construct a tower of finite (simple) extensions

$$K = K_n/\ldots/K_0 = k$$

with $K_i = k(\alpha_1, \ldots, \alpha_i)$ and $K_i = K_{i-1}(\alpha_i)$. By (3.15.57) $\alpha_i$ is separable over $K_{i-1}$. Therefore $[K_i : K_{i-1}]_s = [K_i : K_{i-1}]$ by (3.15.59) and $[K : k]_s = [K : k]$ by multiplicativity. (3.15.60) shows that $K/k$ is separable. □

**Proposition 3.15.63** (Equivalent definition of separability)
*An algebraic extension $K/k$. TFAE*

a) *$K/k$ is separable*

b) *$E/k$ is separable for every finite sub-extension*

c) *$[E : k]_s = [E : k]$ for every finite sub-extension*

NB 3) is Lang's definition of separability which makes it a lot easier to prove certain results.

*Proof.* *a)* $\implies$ *b)* is trivial and *b)* $\iff$ *c)* follows from (3.15.60). We need only show *b)* $\implies$ *a)*.

Consider $\alpha \in K$. Then by (3.15.28) there exists a finite sub-extension $E/k$ such that $\alpha$ is algebraic over $E$. Therefore $E(\alpha)/k$ is finite, and by assumption $E(\alpha)/k$ separable as required. □

*Proof.* Proof of (3.15.61) general case

Assume $K/E$ and $E/k$ are separable. Take $\alpha \in K$. Then (3.15.28) shows the existence of a finite sub-extension $E_0/k$ of $E$ such that $m_{\alpha,E} = m_{\alpha,E_0}$. Therefore $\alpha$ is separable over $E_0$. By (3.15.59) we see that $[E_0(\alpha) : E_0]_s = [E_0(\alpha) : E_0]$. As $E/k$ is separable a-fortiori $E_0/k$ is separable so by (3.15.60) $[E_0 : k]_s = [E_0 : k]$. By multiplicativity $[E_0(\alpha) : k]_s = [E_0(\alpha) : k]$ and the same result again shows that $E_0(\alpha)/k$ is separable. In particular $\alpha$ is separable over $k$ as required. □

### 3.15.6 Perfect Fields

For large classes of base fields all algebraic extensions are separable :

**Proposition 3.15.64** (Perfect field)
*Let $k$ be a field. Then TFAE*

- *Every irreducible polynomial in $k[X]$ is separable*
- *Every algebraic extension $K/k$ is separable*
- *$\bar{k}$ is separable*

*In this case we say $k$ is **perfect**.*

**Proposition 3.15.65** (Criteria for perfectness)
*$k$ is perfect if and only if one of the following holds*

- *$k$ has characteristic 0*
- *$k$ has characteristic $p$ and every element is a $p$-th power*

*In particular finite fields are perfect.*

### 3.15.7 Applications of Separability

**Definition 3.15.66** (Bounds on $\mathrm{Aut}(K/k)$)
*Let $K/k$ be an algebraic extension and $L/K$ an extension such that $L/k$ is normal. Then there is a natural injection*

$$\begin{aligned} \mathrm{Mor}_k(K, i_{KL}) : \mathrm{Aut}(K/k) &\to \mathrm{Mor}_k(K, L) \\ \sigma &\to i_{KL} \circ \sigma \end{aligned}$$

*In particular in the case $[K:k] < \infty$*

$$\#\,\mathrm{Aut}(K/k) \leq [K:k]_s \leq [K:k] < \infty$$

*If $i_{KL}$ is inclusion, then we may regard $\mathrm{Aut}(K/k)$ as a subset of $\mathrm{Mor}_k(K, L)$*

As an application of the concept of separability degree we prove

**Proposition 3.15.67** (Primitive Element Theorem)
*Let $K/k$ be a finite separable extension of $k$ then $K = k(\alpha)$ is simple.*

*Proof.* We only prove the case $k$ is infinite. The finite case can be proven separately by showing that the $K^\star$ is cyclic.

Consider the set $\mathrm{Mor}_k(K, \bar{k}) = \{\sigma_1, \ldots, \sigma_n\}$ which by (3.15.63) has order $n = [K:k]$. By induction we can assume that $K = k(\alpha, \beta)$. We claim that there exists $0 \neq c \in k$ such that $\sigma_i(\alpha + c\beta)$ are all distinct. In this case we clearly have $\#\,\mathrm{Mor}_k(k(\alpha + c\beta), \bar{k}) \geq n$ so by the same result $[k(\alpha + c\beta) : k] \geq [k(\alpha + c\beta) : k]_s \geq n$ whence $k(\alpha + c\beta) = K$ (by (2.2.13)).

We have $\sigma_i(\alpha + c\beta) = \sigma_j(\alpha + c\beta) \iff c(\sigma_i(\beta) - \sigma_j(\beta)) = (\sigma_i(\alpha) - \sigma_j(\alpha))$. Therefore consider the polynomial

$$f(X) = \prod_{i \neq j} (X(\sigma_i(\beta) - \sigma_j(\beta)) - (\sigma_i(\alpha) - \sigma_j(\alpha)))$$

Then the embeddings are distinct precisely when $f(c) \neq 0$. Since $f(X)$ has at most finitely many roots and $k$ is infinite, there must exist such a $c$. □

### 3.15.8 Normal Extensions II

We provide some more straightforward criteria based on $[K:k]_s$

**Proposition 3.15.68** (Normal Criteria II)
*Let $L/K/k$ be a tower of algebraic extensions such that $L/k$ is normal (e.g. $L = \bar{k}$). Then $K/k$ is normal if and only if the embedding*

$$\mathrm{Mor}_k(K, i_{KL}) : \mathrm{Aut}(K/k) \to \mathrm{Mor}_k(K, L)$$

*is a bijection. In particular if $K/k$ is finite, then it is normal if and only if*

$$\#\,\mathrm{Aut}(K/k) = [K:k]_s$$

*Proof.* Suppose $K/k$ is normal and consider $\sigma \in \mathrm{Mor}_k(K, L)$. Then by NOR1b $\sigma(K) = i_{KL}(K)$ and we may define $\tau := i_{KL}^{-1} \circ \sigma$ with $\tau \in \mathrm{Aut}(K/k)$. The converse is similar.

For the final part we've already observed (3.15.66) that in the finite case $\#\,\mathrm{Aut}(K/k) \leq [K:k]_s = \#\,\mathrm{Mor}_k(K, L) \leq [K:k] < \infty$. Therefore the embedding $\mathrm{Mor}_k(K, i_{KL})$ is a bijection precisely when the orders are the same. □

**Corollary 3.15.69** (Galois Criteria)
*Let $K/k$ be a finite extension. Then*

$$\#\,\mathrm{Aut}(K/k) \leq [K:k]_s \leq [K:k]$$

*with equalities if and only if $K/k$ is Galois.*

*Proof.* We've seen the inequalities (3.15.66)

$$\#\,\mathrm{Aut}(K/k) \leq [K:k]_s \leq [K:k] < \infty$$

with equality if and only if $K/k$ is both normal (3.15.68) and separable (3.15.60) □

### 3.15.9 Finite Fields

A finite field $K$ necessarily has positive characteristic $p$, and therefore the prime subfield is isomorphic to the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. We list some necessary properties of a finite field

**Proposition 3.15.70** (Properties of finite fields)
*Every finite field $K$ is a finite-dimensional vector space over its prime subfield $\mathbb{F}_p$. Define $n = [K : \mathbb{F}_p]$.*

- $\#K = p^n$
- *$K$ is a splitting field for $X^{p^n} - X \in \mathbb{F}_p[X]$, and indeed is equal to the set of roots*
- *The multiplicative group of units $K^\star$ is cyclic.*
- *$K/\mathbb{F}_p$ is simple*

*Proof.* Since $K/\mathbb{F}_p$ is a finite-dimensional vector space it must have order $p^n$.

The group of units has order $p^n - 1$, so by Lagrange's theorem every non-zero element satisfies $X^{p^n-1} - 1 = 0$, so therefore every element satisfies $X^{p^n} - X = 0$. Since this polynomial can have at most $p^n$ roots ((3.12.10)) it shows that the roots are exactly all the elements of $K$.

We note again that $X^d - 1$ has at most $d$ roots by (3.12.10). Therefore the fact $K^\star$ is cyclic follows from (3.3.24). □

**Proposition 3.15.71** (Frobenius morphism)
*Given any field $K/\mathbb{F}_p$ the Frobenius map*

$$\phi : x \to x^p$$

*is an injective field homomorphism. In particular when $K$ is finite (or even algebraic) it is an automorphism over $\mathbb{F}_p$.*

*Proof.* The only non-trivial step is showing

$$(x + y)^p = x^p + y^p$$

which follows from elementary calculations on binomial coefficients.

For the final statement use (3.15.18). □

Further we can show existence and uniqueness of finite fields.

**Proposition 3.15.72** (Existence and uniqueness of finite fields)
*Consider the algebraic closure $\overline{\mathbb{F}_p}$ and let $\mathbb{F}_{p^n}$ denote the splitting field of $f(X) = X^{p^n} - X$ in $\overline{\mathbb{F}_p}$. Then*

- *$\mathbb{F}_{p^n}$ is equal to the set of roots of $X^{p^n} - X$*
- *It is the unique subfield of order $p^n$ and every finite field of order $p^n$ is isomorphic to this.*
- $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$

*Proof.* By the previous Proposition the set of roots of $f(X)$ forms a subfield of $\overline{\mathbb{F}_p}$.

Furthermore $f'(X) = -1$ so $f(X)$ is separable because clearly $(f, f') = 1$. Therefore by (3.12.16) $f(X)$ has $p^n$ distinct roots and the splitting field of $f(X)$ is exactly the set of roots.

Furthermore every subfield of order $p^n$ must satisfy this polynomial by Lagrange's (3.3.12), so it is the unique such subfield.

Since every algebraic extension of $\mathbb{F}_p$ is isomorphic to a subfield of $\overline{\mathbb{F}_p}$ it's also the unique algebraic extension of order $p^n$ up to isomorphism.

Clearly if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ we see that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p]$, so we must have $m \mid n$. Conversely if $\alpha \in \mathbb{F}_{p^m}$ then $\alpha^{p^m} = \alpha \implies \alpha^{p^{rm}} = \alpha$ for all $r > 0$, so $\alpha \in \mathbb{F}_{p^n}$. □

It is usually most convenient to work in $\overline{\mathbb{F}_p}$ and consider the finite fields of the form $\mathbb{F}_{p^n}$ as in the Proposition. We've seen in (3.15.65) that every finite field $\mathbb{F}_q := \mathbb{F}_{p^n}$ is perfect and therefore every algebraic extension is separable. In fact we may show that every finite extension is Galois.

**Proposition 3.15.73**
*The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle$$

*cyclic of order $n$ generated by the Frobenius automorphism.*

*Proof.* Let $G = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. We've observed that $\phi \in G$. Let $d = o(\phi)$, and we wish to prove that $n = d$. Certainly Lagrange's theorem applied to the multiplicative group $\mathbb{F}_{p^n}^\star$ implies $\phi^n = 1$. Therefore $d \mid n$ by (3.3.12) applied to $G$. By definition $\phi^d = e$, so every $\alpha \in \mathbb{F}_{p^n}$ satisfies the polynomial $X^{p^d} - X = 0$. This has at most $p^d$ roots ((3.12.10)) so we must have $d \geq n$, and therefore $d = n$. Clearly $\phi$ generates a cyclic subgroup of order $n$. However by (3.15.69) $G$ has at most order $n$, whence $G = \langle \phi \rangle$ as required. Furthermore by the same result $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. □

**Proposition 3.15.74** (Subfields of $\mathbb{F}_{p^n}$)
*Consider the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. Then it has a unique subfield of order $p^m$ if and only if $m \mid n$. In this case $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois and*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \phi^m \rangle$$

*and in particular has order $n/m$.*

*Proof.* We've already shown that $\mathbb{F}_{p^n}$ has a unique subfield of order $p^m$, by assuming an embedding in $\overline{\mathbb{F}_p}$. Let $H = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$. Note $\phi^m$ has order $n/m$. Furthermore from (3.15.72) every element of $\mathbb{F}_{p^m}$ satisfies $X^{p^m} - X$. In other words $\phi^m$ fixes $\mathbb{F}_{p^m}$ and $\phi^m \in H$. Therefore $\langle \phi^m \rangle \leq H$ and $\#H \geq n/m$. By (3.15.69) $\#H \leq [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$, whence we have equality and so the extension is Galois and $H = \langle \phi^m \rangle$. □

The following is quite straightforward but also fundamental.

**Corollary 3.15.75** (Finite fields are fixed points of Frobenius)
*Let $\alpha \in \overline{\mathbb{F}_p}$ then*

$$\deg(\alpha) \mid d \iff \alpha \in \mathbb{F}_{p^d} \iff \phi^d(\alpha) = \alpha$$

*where $\phi$ is the Frobenius automorphism.*

*Proof.* Recall by Definition (3.15.25) that $\deg(\alpha) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$. Then $\alpha \in \mathbb{F}_{p^d} \iff \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^d}$. The first equivalence then follows from the tower law and uniqueness of subfields.

Define $K = \mathbb{F}_p(\alpha)$ and $G = \mathrm{Gal}(K/\mathbb{F}_p)$. Then by (3.15.73) $G = \langle \phi \rangle$ is cyclic of order $m = \deg(\alpha)$.

In particular Lagrange's theorem shows $\phi^m = e$. Then $m = \deg(\alpha) \mid d \implies \phi^d = e$ and in particular $\phi^d(\alpha) = \alpha$.

Conversely suppose $\phi^d(\alpha) = \alpha$. As $\alpha$ generates $K$ we see $\phi^d = e$ (by (3.15.14)), and by (3.3.14) we have $\deg(\alpha) = m = o(\phi) \mid d$. □

## 3.15.10 Galois Theory

We've seen that for $K/k$ a finite extension

$$\#\,\mathrm{Aut}(K/k) \leq [K : k]_s \leq [K : k]$$

with equality if and only if $K/k$ is Galois, by (3.15.69).

**Remark 3.15.76**
*If $k$ is perfect then $\bar{k}/k$ is Galois.*

The main result of Galois Theory is

**Proposition 3.15.77**
*Let $K/k$ be a finite Galois extension then there is an order-reversiing bijection between subgroups and subfields*

$$\begin{aligned} \{H \leq \mathrm{Gal}(K/k)\} &\longleftrightarrow \{F \subseteq K\} \\ \phi : H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \psi : \mathrm{Gal}(K/F) &\longleftarrow F \end{aligned}$$

*Proof.* This is proved in a series of Propositions in the rest of this section. Firstly we show it is well-defined in (3.15.78). The maps are mutual inverses by (3.15.79) and (3.15.80). □

Such an order reversing map is usually called an (antitone) Galois connection, as the first such type arose from Galois Theory. Note it is well-defined because of the following proposition.

**Proposition 3.15.78**
*If $K/k$ is Galois and $F \subset K$ then $K/F$ is Galois.*

*Proof.* This follows from (3.15.46) and (3.15.61). □

**Proposition 3.15.79** (Fixed field of Galois group)
*If $K/k$ is Galois and $F \subset K/k$ a subfield then*

$$K^{\mathrm{Gal(K/F)}} = F$$

*Proof.* Clearly $F \subseteq K^{\mathrm{Gal(K/F)}}$. Conversely given $\alpha \in K \setminus F$, then $\deg m_{\alpha,F} > 1$. Since $\alpha$ is separable it must have another root $\beta \in K$. By (3.15.50) there is an element $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\alpha) = \beta$. In other words $\alpha \notin K^{\mathrm{Gal}(K/F)}$, which shows the reverse inclusion. □

**Proposition 3.15.80**
*Let $K/k$ be a field extension and $H \subseteq \mathrm{Aut}(K/k)$ a finite subgroup then $K/K^H$ is finite Galois with*

$$H = \mathrm{Gal}(K/K^H)$$

*and order equal to $[K : K^H]$. When $K/k$ is finite then $H$ is automatically finite.*

*Proof.* Firstly observe that trivially $H \subseteq \mathrm{Aut}(K/K^H)$. If we know that $[K : K^H] < \infty$, then by (3.15.69) we have

$$\#H \leq \#\,\mathrm{Aut}(K/K^H) \leq [K : K^H]_s \leq [K : K^H]$$

We can prove equality everywhere if we show that $[K : K^H] \leq \#H$, which is shown either by (3.15.81) or (3.15.82). Note equality also shows that $K/K^H$ is finite Galois by the same result.

Finally when $K/k$ is finite, then $\#\,\mathrm{Aut}(K/k) < \infty$. So in this case $H$ is always finite. □

We present two approaches to showing the inequality $[K : K^H] \leq \#H$. The first uses independence of characters style argument (see Garling, JMilne), and the second which is more straightforward uses the action of $H$ to show that every element has degree at most $\#H$ (Artin).

**Lemma 3.15.81** (Bound degree of fixed field I)
*Let $K/k$ be a field extension and $H \subset \mathrm{Aut}(K/k)$ a finite subgroup. Then $[K : K^H] \leq \#H$*

*Proof.* Let $H = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}$ and $\alpha_1, \ldots, \alpha_m$ a $K^H$-basis for $K$.

Consider the vector space $K^n$ and the elements $\hat{\alpha}_j = (\sigma_1(\alpha_j), \ldots, \sigma_n(\alpha_j))$ for $j = 1 \ldots m$. It's enough to show that these are linearly independent over $K$, as that implies $m \leq n$ by **??**.

Let $S(K) := \{v \in K^m \mid \sum_{j=1}^m v_j \hat{\alpha}_j = 0\}$, we aim to show that $S(K) = \{0\}$. If we also consider $S(K^H)$, any non-zero elements will be a $K^H$ linear-dependence for $\alpha_1, \ldots, \alpha_m$ by considering the first component ($\sigma_1 = \mathrm{id}$). Therefore by linear independence of $\alpha_i$ we see $S(K^H) = \{0\}$. So it's enough to show that $S(K) \neq \{0\} \implies S(K^H) \neq \{0\}$, to prove $S(K) = \{0\}$ by contradiction.

First observe that $K^\star$ and $H$ both act on $S(K)$ component-wise. The first by multiplication and the second by application. This is well-defined because $v \in S(K)$ if and only if

$$\sum_j v_j \sigma(\alpha_j) = 0 \quad \forall \sigma \in H\,.$$

Apply $\tau$ to obtain

$$\sum_j \tau(v_j)(\tau \circ \sigma)(\alpha_j) = 0 \quad \forall \sigma \in H$$

and since multiplication by $\tau$ permutes $H$ we see $\tau(v) \in S(K)$ as required.

If there exists $0 \neq v \in S(K)$, consider $v$ with a minimal number of non-zero components. By scaling we can assume $\lambda v$ has at least one component in $K^H$. The vector $\tau(\lambda v) - \lambda v$ then has at least one fewer non-zero components, so by minimality must be zero. Since $\tau$ was arbitrary we see $0 \neq \lambda v \in S(K^H)$ as required.

□

**Lemma 3.15.82** (Bound degree of fixed field II)
*Let $K/k$ be a field extension and $H$ a finite subgroup of $\mathrm{Aut}(K/k)$. Then $K/K^H$ is finite separable, and simple, with $[K : K^H] \leq \#H$*

*Proof.* We show that $K/K^H$ is separable and every element has degree at most $\#H$. For any $\alpha \in K$, consider the orbit $H(\alpha) = \{\sigma(\alpha) \mid \sigma \in H\}$, which is of order at most $\#H$. Then the polynomial

$$f(X) = \prod_{\beta \in H(\alpha)} (X - \beta)$$

has $\alpha$ as a root and is separable by (3.12.16). Furthermore $f^\tau = f$ because $\tau$ permutes $H(\alpha)$ (it's injective and hence bijective). Therefore $f \in K^H[X]$ and $m_{\alpha,K^H} \mid f$. We see that $\alpha$ has degree at most $\#H$ and is separable by (3.12.15).

If $K/k$ is finite, then a-fortiori $K/K^H$ is finite, so we may apply the Primitive Element (3.15.67) directly to show the result.

More generally let $K^H(\alpha)$ be a simple subfield of $K$ of maximal degree. This exists because the degree of $\alpha$ is bounded above by $\#H$. We claim $K^H(\alpha) = K$, for if not then $K^H \subseteq K^H(\alpha) \subsetneq K^H(\alpha, \beta)$ is a finite separable extension of $K^H$, whence it must be simple by the Primitive Element (3.15.67), contradicting maximality. Finally the degree of $[K : K^H]$ is the degree of $\alpha$, which we've seen is bounded above by $\#H$. □

Now we may demonstrate straightforward criteria for subfield to be normal

**Proposition 3.15.83**
*Let $K/k$ be a finite Galois extension and $k \subset F \subset K$ a subfield.*

*Then $F/k$ is Galois if and only if $\mathrm{Gal}(K/F) \triangleleft \mathrm{Gal}(K/k)$ is normal. In this case we have a canonical isomorphism*

$$\mathrm{Gal}(K/k)/\mathrm{Gal}(K/F) \to \mathrm{Gal}(F/k)$$

*Proof.* Recall from (3.15.51) we have $F/k$ is normal iff $\sigma(F) = F$ for all $\sigma \in \mathrm{Gal}(K/k)$. Recall $K/F$ is normal for all subfields $F$. Furthermore, we observe that

$$\mathrm{Gal}(K/\sigma(F)) = \sigma\,\mathrm{Gal}(K/F)\sigma^{-1}$$

By the correspondence (3.15.77) $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/F') \iff F = F'$. Therefore

$$\begin{aligned} F/k \text{ normal} &\iff \sigma(F) = F \quad \forall \sigma \in \mathrm{Gal}(K/k) \\ &\iff \mathrm{Gal}(K/\sigma(F)) = \mathrm{Gal}(K/F) \quad \forall \sigma \in \mathrm{Gal}(K/k) \\ &\iff \sigma\,\mathrm{Gal}(K/F)\sigma^{-1} = \mathrm{Gal}(K/F) \quad \forall \sigma \in \mathrm{Gal}(K/k) \\ &\iff \mathrm{Gal}(K/F) \triangleleft \mathrm{Gal}(K/k) \end{aligned}$$

The result then follows from (3.15.53). □

### 3.15.11 Transcendental Extensions

**Definition 3.15.84** (Algebraic Independence)
*Let $K/k$ be a field extension and $S \subset K$. We say $S$ is **algebraically independent** if for every finite subset of distinct elements $x_1, \ldots, x_n \in S$ we have*

$$f(x_1, \ldots, x_n) = 0 \implies f = 0$$

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

*For a subset $S \subset K$ define the closure operator*

$$c(S) := \overline{k(S)} \cap K := \{x \in K \mid x \text{ algebraic over } k(S)\}$$

*We say $\Gamma$ is **algebraically spanning** if $c(\Gamma) = K$, equivalently if $K/k(\Gamma)$ is algebraic.*

Essentially we show that $(K, c)$ satisfies the properties of a matroid, in analogy with vector spaces, so that we can use the results of Section 2.2.

**Proposition 3.15.85** (Exchange Property for field extensions)
*Let $K/k$ be a field extension, $S \subseteq K$ and $x, y \in K$. Suppose $x$ is algebraic over $k(S \cup \{y\})$ and transcendental over $k(S)$. Then $y$ is algebraic over $k(S \cup \{x\})$.*

Further we show the notion of matroid independence and algebraic independence coincide.

**Proposition 3.15.86** (Equivalent form of independence)
*Let $K/k$ be a field extension and $S \subset K$. Then $S$ is algebraically independent if and only if $x$ is transcendental over $k(S \setminus \{x\})$ for all $x \in S$.*

*Proof.* Suppose $S$ is algebraically dependent. Then

$$f(x_1, \ldots, x_n) = 0$$

for $f \in k[X_1, \ldots, X_n]$ non-constant and $x_i \in S$ distinct. Choose $i \in \{1, \ldots, n\}$ such that $X_i^k$ has a non-zero coefficient for some $k > 0$. Rearranging we find that $x_i$ is algebraic over $k(S \setminus \{x_i\})$. The converse is similar. □

**Proposition 3.15.87** (Transcendence Base)
*Let $K/k$ be a field extension and $\mathcal{S} \subset K$ a subset. Then the following are equivalent*

a) $\mathcal{S}$ *is algebraically independent and* $K/k(\mathcal{S})$ *is algebraic*

b) $\mathcal{S}$ *is a maximal algebraically independent set*

c) $\mathcal{S}$ *is minimal under the condition* $K/k(\mathcal{S})$ *is algebraic*

*In this case we say* $\mathcal{S}$ *is a* ***transcendence base****.*

*A transcendence base always exists, and when* $K/k$ *is finitely-generated then bases are finite and of the same size (****transcendence degree****). Write this as* $\operatorname{trdeg}(K/k)$*.*

*Proof.* The equivalent criteria follow from (3.15.86) and (2.2.6).

The final statements follow from (2.2.7) and (2.2.9). □

## 3.16 Local Rings

Local rings arise quite naturally when localizing at a prime ideal (see (3.5.32) and Example Example 3.16.4) so we recall some basic properties here.

**Definition 3.16.1** (Local Ring)
*A ring* $A$ *is a* ***local ring*** *if it has a unique maximal ideal* $\mathfrak{m}$*. The field* $A/\mathfrak{m}$ *is called the* ***residue field*** *of* $A$*.*

**Definition 3.16.2** (Local Homomorphism)
*Let* $(A, \mathfrak{m}_A)$ *and* $(B, \mathfrak{m}_B)$ *be local rings. A ring homomorphism* $\phi : A \to B$ *is said to be a* local homorphism *if*

$$\phi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$$

Recall that the group of units $A^\star$ of a ring is a saturated multiplicative set, that is

$$xy \in A^\star \iff x \in A^\star \wedge y \in A^\star$$

**Proposition 3.16.3** (Criteria for Local Rings)
*Let* $A$ *be a ring. Then the following are equivalent*

a) $A$ *is a local ring*

b) $A \setminus A^\star$ *is an additive subgroup of* $A$

*In this case* $\mathfrak{m} = A \setminus A^\star$ *is the unique maximal ideal of* $A$*.*

*Proof.* 1 $\implies$ 2) Let $\mathfrak{m}$ be the unique maximal ideal then, because it's proper, $\mathfrak{m} \cap A^\star = \emptyset \implies \mathfrak{m} \subseteq A \setminus A^\star$ by (3.4.11). Conversely given $x \in A \setminus A^\star$ then $(x)$ is a proper ideal by (3.4.30), and therefore contained in a maximal ideal (3.4.13) which by uniqueness means $x \in \mathfrak{m}$.

2 $\implies$ 1) Define $\mathfrak{m} = A \setminus A^\star$ it's a (prime) ideal because it is an additive subgroup and $A^\star$ is a saturated multiplicative set. Let $\mathfrak{a}$ be a proper ideal then $\mathfrak{a} \cap A^\star = \emptyset \implies \mathfrak{a} \subseteq \mathfrak{m}$. Therefore $\mathfrak{m}$ is the unique maximal ideal. □

**Example 3.16.4**
*Let* $A$ *be a ring and* $\mathfrak{p} \lhd A$ *a prime ideal. Then* $A_\mathfrak{p}$ *is a local ring with unique maximal ideal* $\mathfrak{p}A_\mathfrak{p}$*.*

*When* $A \subset K$ *is a subring of a field then* $A \subset A_\mathfrak{p} \subset K$ *in a natural way.*

We may use this to provide another criteria

**Lemma 3.16.5** (Criteria for Local Domain)
*Let* $A \subset K$ *be a subring of a field with a prime ideal* $\mathfrak{p} \lhd A$*. Then* $A \subset A_\mathfrak{p}$*.*

$A$ *is a local ring with unique maximal ideal* $\mathfrak{p}$ *if and only if* $A = A_\mathfrak{p}$*,*

*Proof.* We've observed that $A_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$.

If $A = A_\mathfrak{p}$ then it is a local ring and $\mathfrak{p} \subset \mathfrak{p}A_\mathfrak{p}$. For $y \notin \mathfrak{p}$, then $\frac{1}{y} \in A_\mathfrak{p} \implies \frac{1}{y} \in A$. So we see that $x \in \mathfrak{p}, y \notin \mathfrak{p}$ we have $\frac{x}{y} \in \mathfrak{p}$ and $\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$.

Conversely suppose $A$ is a local ring with unique maximal ideal $\mathfrak{p}$. Then $y \notin \mathfrak{p} \implies y \in A^\star$ and $A_\mathfrak{p} = A$ as required. □

## 3.17 Modules over Local Rings (Nakayama's Lemma)

The main result of this section (Theorem 3.17.7) is that every finitely-generated module over a local ring has a minimal spanning set. Recall in the vector space case a minimal spanning set is precisely a basis **??**. Analogously we may also show that (in the local case) every minimal spanning set has the same order. The crucial result is Nakayama's Lemma, which we develop here.

**Definition 3.17.1** (Jacobson Radical)
*Let $A$ be a commutative ring. Define the **Jacobson Radical** to be the intersection of all maximal ideals*

$$J(A) := \bigcap_{\mathfrak{m} \lhd A} \mathfrak{m}$$

**Proposition 3.17.2**
*The Jacobson Radical $J(A)$ is a proper ideal*

**Example 3.17.3**
*When $(A, \mathfrak{m}_A)$ is a local ring then $J(A) = \mathfrak{m}_A$.*

**Lemma 3.17.4** (Characterization of Jacobson Radical)
*For an ideal $\mathfrak{a}$ and $\mathfrak{m}$ a maximal ideal*

a) $\mathfrak{a} \not\subseteq \mathfrak{m} \iff \mathfrak{a} + \mathfrak{m} = A \iff (1 + \mathfrak{a}) \cap \mathfrak{m} \neq \emptyset$

b) $\mathfrak{a} \subseteq J(A) \iff 1 + \mathfrak{a} \subseteq A^\star$

c) $x \in J(A) \iff 1 + (x) \subseteq A^\star$

*Proof.* We prove each in turn.

a) Clearly $\mathfrak{a} \subseteq \mathfrak{m} \implies \mathfrak{a} + \mathfrak{m} = \mathfrak{m}$. Conversely $\mathfrak{a} \not\subseteq \mathfrak{m} \implies \mathfrak{a} + \mathfrak{m} = A$ by maximality. Suppose $\mathfrak{a} + \mathfrak{m} = A$ then $1 = a + m$ whence $(1 - a) \in \mathfrak{m}$. The converse is similar.

b) By a) $\mathfrak{a} \subseteq J(A) \implies (1 + \mathfrak{a}) \cap \mathfrak{m} = \emptyset$ for all maximal ideals $\mathfrak{m}$. By (3.4.13) this implies $(1 + \mathfrak{a}) \subseteq A^\star$.

Conversely if $(1 + \mathfrak{a}) \subseteq A^\star$ then $(1 + \mathfrak{a}) \cap \mathfrak{m} = \emptyset$ for any maximal ideal $\mathfrak{m}$ by (3.4.11). Again by a) $\mathfrak{a} \subseteq \mathfrak{m}$ as required.

c) This follows from b) and noting $x \in J(A) \iff (x) \subseteq J(A)$.

□

**Proposition 3.17.5** (Nakayama's Lemma)
*Let $M$ be a finitely generated $A$-module and $\mathfrak{a} \lhd A$ an ideal. Then the following holds*

a) *If $M = \mathfrak{a}M$ then there exists $a \in \mathfrak{a}$ such that $m = am$ for all $m \in M$*

*Suppose in addition that $\mathfrak{a} \subseteq J(A)$ (e.g. if $A$ is local and $\mathfrak{a}$ is proper) then*

b) $M = \mathfrak{a}M \implies M = 0$

c) *$N \leq M$ and $M = N + \mathfrak{a}M \implies M = N$.*

*Proof.* We prove each in turn

a) Apply Theorem 3.13.4 with $\phi := \mathbf{1}_M$ to find a monic polynomial $P(X) \in A[X]$ with non-leading coefficients in $\mathfrak{a}$ such that $P(\phi)(m) = 0$ for all $m \in M$. Then we see that $(1 + a_{n-1} + \ldots a_0)m = 0$ for all $m \in M$ whence $a := -(a_{n-1} + \ldots + a_0)$ is the required element.

More directly, suppose $m_1, \ldots, m_n$ is a generating set for $M$. By Lemma 3.13.3 (and $M = \mathfrak{a}M$) there is a matrix $E$ with coefficients in $\mathfrak{a}$ such that

$$(I_n - E)\mathbf{m} = 0$$

where $\mathbf{m}$ is the column vector consisting of $m_1, \ldots, m_n$. By Proposition 3.11.11 we see $\det(I_n - E)m_i = 0$ for all $i = 1 \ldots n$. It's enough to show $a := \det(I_n - E) \in 1 + \mathfrak{a}$. Observe

$$\det(I_n - E) = \prod_i (1 - E_{ii}) + \sum_{\sigma \neq id} \epsilon(\sigma) \prod_j E_{j\sigma(j)}$$

The second term lies in $\mathfrak{a}$ and

$$\prod_i (1 - E_{ii}) = 1 - \sum_{i=1}^{n} E_{ii} \prod_{j>i} (1 - E_{jj}) \in 1 + \mathfrak{a}$$

b) Consider any $m \in M$. By a) we have $(1-a)m = 0$ for some $a \in \mathfrak{a}$, and by (3.17.4) $(1-a)$ is invertible, whence $m = 0$ as required.

c) Observe $\mathfrak{a}(M/N) \overset{(3.4.77)}{=} (N + \mathfrak{a}M)/N = M/N$ whence $M/N = 0$ by b). Therefore $N = M$ as required.

We may show b) more directly. Suppose $M \neq 0$, and let $\{m_1, \dots, m_n\}$ be a non-zero generating set for $M$ of minimal size. Then by Lemma 3.13.3

$$m_1 = \sum_j a_j m_j \quad a_j \in \mathfrak{a}$$

whence

$$(1-a_1)m_1 = \sum_{j \geq 2} a_j m_j$$

As $a_1 \in J(A)$ we have $1 - a_1 \in A^\star$ by (3.17.4). Then $\{m_2, \dots, m_n\}$ is a smaller generating set, a contradiction. Therefore $M = 0$.

a) may be deduced from b) as follows. Observe $S := 1 + \mathfrak{a}$ is a multiplicatively closed subset, so we may consider $S^{-1}M$ as an $S^{-1}A$-module. It's easy to verify that $1 + S^{-1}\mathfrak{a} \subseteq (S^{-1}A)^\star$ so by Lemma 3.17.4 $S^{-1}\mathfrak{a} \subseteq J(S^{-1}A)$. Clearly $\mathfrak{a}M = M \implies (S^{-1}\mathfrak{a})S^{-1}M = S^{-1}M$ so by the weaker form $S^{-1}M = 0$. By (3.5.15) there exists $s \in S$ such that $sM = 0$, which is the required result as $s = 1 + a$ for some $a \in \mathfrak{a}$. □

Recall (3.4.78) in the case of a local ring $(A, \mathfrak{m})$ that $\widetilde{M} := M/\mathfrak{m}M$ is a vector space over $k := A/\mathfrak{m}$. We may use Nakayama's Lemma to exhibit a correspondence between minimal spanning sets of $M$ and bases of $M/\mathfrak{m}M$ as a $k$-vector space. First we prove a simpler form

**Lemma 3.17.6**
*Let $(A, \mathfrak{m})$ be a local ring with residue field $k = A/\mathfrak{m}$, $M$ a finite $A$-module and $S \subset M$ a subset. Then*

$$S \text{ spans } M \iff \widetilde{S} \text{ spans } \widetilde{M}$$

*where $\widetilde{\cdot}$ denotes reduction modulo $\mathfrak{m}M$.*

*Proof.* One direction is obvious. Conversely suppose $\widetilde{S}$ spans $\widetilde{M}$. Define $N := \langle S \rangle$, then this means precisely that $N + \mathfrak{m}M = M$, so $N = M$ by (3.17.5).c) as required. □

Recall from (2.1.50) that every subset of $T$ of $M/\mathfrak{m}M$ may be written in the form $\widetilde{S}$ for $S \subset M$ and $\widetilde{\cdot}$ injective on $S$.

**Theorem 3.17.7** (Structure theorem for modules over a local ring)
*Let $(A, \mathfrak{m})$ be a local ring with residue field $k = A/\mathfrak{m}$, $M$ a finite $A$-module. Then*

a) *$\widetilde{M} := M/\mathfrak{m}M$ is a finite-dimensional $k$-module (of dimension $n$ say)*

b) *If $\widetilde{S}$ is a $k$-basis for $\widetilde{M}$ (for which $\widetilde{\cdot}$ is injective) then $S$ is a minimal spanning set for $M$ and $\#S = \#\widetilde{S} = n$*

c) *If $S$ is a minimal spanning set then $\widetilde{S}$ is a basis for $\widetilde{M}$ (and $\widetilde{\cdot}$ is injective on $S$ so $\#S = \#\widetilde{S} = n$).*

*Proof.* a) By (3.4.78) $\widetilde{M}$ is a $k$-module, and it's clearly finite.

b) By the (3.17.6) $S$ spans $M$. Suppose $S' \subset S$ spans $M$, then by the same result $\widetilde{S'}$ spans $\widetilde{M}$. Recall (2.2.6) that a vector space basis is precisely a minimal spanning set, so $\widetilde{S'} = \widetilde{S}$. As $\widetilde{\cdot}$ is injective this means $S' = S$. Therefore $S$ is a minimal spanning set.

c) Let $S$ be a minimal spanning set. Then by (3.17.6) $\widetilde{S}$ spans $\widetilde{M}$. Suppose $\widetilde{T} \subset \widetilde{S}$ also spans $\widetilde{M}$. Then it corresponds to a set $T \subset S$. By (3.17.6) $T$ spans $M$, and by hypothesis $T = S$. Therefore $\widetilde{T} = \widetilde{S}$. As $\widetilde{T}$ was arbitrary we see that $\widetilde{S}$ is a minimal spanning set for $\widetilde{M}$, which by (2.2.6) is a basis.

Finally suppose $\widetilde{\cdot}$ is not injective on $S$, that is $\widetilde{s_1} = \widetilde{s_2}$. Then $S' := S \setminus \{s_1\}$ satisfies $\widetilde{S'} = \widetilde{S}$. Therefore by the Lemma $S'$ spans $M$, contradicting minimality.

□

## 3.18 Lying over, Incomparability, Going Up and Going Down

**Definition 3.18.1** (Lying over / Going up)
*Let $\phi : A \to B$ be a ring map and $\mathfrak{p}$ and $\mathfrak{q}$ primes of $A$ and $B$ respectively*

a) *$\mathfrak{q}$ **lies over** $\mathfrak{p}$, or $\mathfrak{p}$ **lies under** $\mathfrak{q}$ if $\mathfrak{p} = \phi^{-1}(\mathfrak{q}) = \mathfrak{q}^c$. When $A \subseteq B$ and $\phi$ is the identity then this is equivalent to saying $\mathfrak{p} = \mathfrak{q} \cap A$.*

**Definition 3.18.2** (Lying Over / Going Up / Incomparability)
*Let $\phi : A \to B$ be a ring map. We say that it has the*

a) ***lying over property*** *if every prime ideal $\mathfrak{p} \supseteq \ker(\phi)$ has a prime $\mathfrak{q}$ lying over it. NB $\ker(\phi) \subseteq \mathfrak{p}$ is a necessary condition for $\mathfrak{p}$ to be a contraction and is equivalent to $B_{\mathfrak{p}} \neq 0$.*

b) ***going up property*** *if for every pair of prime ideals $\mathfrak{p} \subsetneq \mathfrak{p}'$ in $A$ and $\mathfrak{q} \triangleleft B$ lieing over $\mathfrak{p}$, there exists a prime ideal $\mathfrak{q}'$ such that $\mathfrak{q} \subsetneq \mathfrak{q}'$ and $\mathfrak{q}'$ lies over $\mathfrak{p}'$.*

c) ***incomparability property*** *if for every pair of prime ideals $\mathfrak{q}, \mathfrak{q}' \triangleleft B$ then $\mathfrak{q} \subsetneq \mathfrak{q}' \implies \phi^{-1}(\mathfrak{q}) \subsetneq \phi^{-1}(\mathfrak{q}')$*

The main result of this section is the correspondence between primes lieing over $\mathfrak{p}$ and primes of the ring $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ Proposition 3.18.4. As a preliminary result we consider conditions under which we can strengthen $\mathfrak{p} \subseteq \mathfrak{q}^c$ to $\mathfrak{p} = \mathfrak{q}^c$, as the former condition is somewhat easier to satisfy.

**Lemma 3.18.3** (Lieing over criteria)
*Let $\phi : A \to B$ be a ring map, $\mathfrak{p} \triangleleft A$ prime and $\mathfrak{q} \triangleleft B$. Then*

$$\mathfrak{p} = \mathfrak{q}^c \iff \mathfrak{p}^e \subseteq \mathfrak{q} \text{ and } \mathfrak{q} \cap \phi(A \setminus \mathfrak{p}) = \emptyset$$

*In particular*

$$\mathfrak{p} = \mathfrak{p}^{ec} \text{ is contracted} \iff \mathfrak{p}^e \cap \phi(A \setminus \mathfrak{p}) = \emptyset$$

*Proof.* Recall (3.4.43) that in general $\mathfrak{p} \subseteq \mathfrak{q}^c \iff \mathfrak{p}^e \subseteq \mathfrak{q}$. The first equivalence is then clear because $x \in \mathfrak{q}^c \setminus \mathfrak{p} \iff \phi(x) \in \mathfrak{q} \cap \phi(A \setminus \mathfrak{p})$.

The final statement follows by considering $\mathfrak{q} = \mathfrak{p}^e$. □

**Proposition 3.18.4** (Lieing over correspondence)
*Let $\phi : A \to B$ be a ring map and $\mathfrak{p} \triangleleft A$ a prime ideal. Then there is a order-preserving correspondence of prime ideals*

$$\begin{array}{ccccc} \{\mathfrak{q} \mid \mathfrak{q} \text{ lies above } \mathfrak{p}\} & \longleftrightarrow & \{\mathfrak{q}' \triangleleft B_{\mathfrak{p}} \mid \mathfrak{p}B_{\mathfrak{p}} \subseteq \mathfrak{q}'\} & \longleftrightarrow & \{\mathfrak{q}'' \triangleleft B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}\} \\ \mathfrak{q} & \longrightarrow & \mathfrak{q}B_{\mathfrak{p}} & & \\ & & & \longrightarrow & \mathfrak{q}B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \end{array}$$

*In particular TFAE*

a) *$\mathfrak{p}$ lies under a prime $\mathfrak{q}$*

b) *$B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \neq 0$*

c) *$\mathfrak{p} = \mathfrak{p}^{ec}$ is contracted*

*NB c) is a-priori weaker than a).*

*Proof.* Recall $B_{\mathfrak{p}} := S^{-1}B$ and $\mathfrak{p}B_{\mathfrak{p}} := \mathfrak{p}^e B_{\mathfrak{p}} = S^{-1}\mathfrak{p}^e$ where $S := \phi(A \setminus \mathfrak{p})$.

By Lemma 3.18.3 $\mathfrak{q}$ lies above $\mathfrak{p}$ if and only if $\mathfrak{p}^e \subseteq \mathfrak{q}$ and $\mathfrak{q} \cap S = \emptyset$. The first correspondence then follows from (3.5.18) and the second from (3.4.46).

*a)* $\iff$ *b)* This follows from the correspondence.
*b)* $\iff$ *c)* Follows by noting $\mathfrak{p} = \mathfrak{p}^{ec} \overset{3.18.3}{\iff} \mathfrak{p}^e \cap S = \emptyset \overset{3.5.17}{\iff} \mathfrak{p}B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$ and $B_{\mathfrak{p}} \neq 0$ □

**Remark 3.18.5**
*Geometrically this is an explicit representation of the fiber as a prime spectrum*

$$\mathrm{Spec}(\phi)^{-1}(\mathfrak{p}) \longleftrightarrow \mathrm{Spec}(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}})$$

## 3.19 Integral Ring Extensions

**Definition 3.19.1** (Integral Element)
*Let $\phi : A \to B$ be a ring map and $\alpha \in B$. Then we say $\alpha$ is integral over $A$ if $m^{\phi}(\alpha) = 0$ for some* monic *polynomial $m(X) \in A[X]$.*

*Note often we assume $A \subseteq B$ and $\phi$ is the identity.*

**Definition 3.19.2** (Ring Extensions)
*Let $\phi : A \to B$ be a ring map (so that $B$ is an $A$-algebra). Then we say $\phi$ is*

- ***finite*** *if $B$ is finite as an $A$-module*

- ***finite-type*** *if $B$ is finitely generated as an $A$-algebra*
- ***integral*** *if every element of $B$ is integral over $A$*

*When $A \subseteq B$ and $\phi$ is the identity then we say that $B$ is respectively finite over $A$, finite-type over $A$ or integral over $A$.*

We note the trivial implication

$$\text{finite} \implies \text{finite type}$$

For example $k[X]$ is a ring of finite type over $k$, but certainly not finite. The follow criterion for integrality is fundamental.

**Proposition 3.19.3**
*Let $\phi : A \to B$ be a ring map and $b \in b$. Then the following are equivalent*

a) *$b$ is integral over $A$*

b) *$\phi(A)[b]$ is a finite $A$-module*

c) *$\phi(A)[b]$ is contained in a subring $C$ of $B$ which is a finite $A$-module*

d) *There exists a $\phi(A)[b]$-module $M$ which is faithful and finite as an $A$-module*

*Proof.* Note that the subring $C$ in $c$) is a faithful $A$-module, so the only non-trivial step is $d \implies a$. This is the usual "determinant trick". We apply Theorem 3.13.4 by considering $\psi_b \in \mathrm{End}_A(M)$ to be multiplication by $b$. Then we have some monic polynomial $P(X) \in A[X]$ such that $P(\psi_b) = 0$, whence $P^\phi(b)m = 0$ for all $m \in M$. Since $M$ is faithful, then we have $P(b) = 0$ as required. □

**Proposition 3.19.4** (Finite $\iff$ finite-type and integral)
*Let $\phi : A \to B$ be a ring map and $b_1, \ldots, b_n \in B$ over $A$. Then the ring homorphism $\phi : A \to \phi(A)[b_1, \ldots, b_n]$ is finite and integral.*

*In particular if $\phi$ is integral and of finite type if and only if it is finite.*

*Proof.* We assume without loss of generality that $A \subseteq B$ and $\phi$ is the identity map. Consider a tower

$$A \subset A[b_1] \subset \ldots \subset A[b_1, \ldots, b_n] = B$$

We proceed inductively on $n$. Namely we assume that $A[b_1, \ldots, b_i]$ is a finite $A$-module. Then a-fortiori $A[b_1, \ldots, b_{i+1}]$ is integral over $A[b_1, \ldots, b_i]$. Therefore by the previous Proposition it is a finite $A[b_1, \ldots, b_i]$-module and therefore a finite $A$-module (by (3.8.4)).

For any $b \in A[b_1, \ldots, b_n]$ we have $A[b] \subset A[b_1, \ldots, b_n]$ so by (3.19.3) we have $b$ is integral over $A$.

It then follows that $B$ integral and finite type $\implies$ $B$ is finite (as an $A$-module). Conversely if $B$ is finite then it is clearly finitely-generated. Further for any $b \in B$ then $A[b]$ is contained in the ring $B$ which is finite as an $A$-module, and therefore is $b$ is integral by (3.19.3). □

**Proposition 3.19.5** (Transitivity property)
*Let $\phi : A \to B$ and $\psi : B \to C$ be ring maps.*

*If $c \in C$ is integral over $B$, then it is integral over $A$ (with respect to the ring map $\psi \circ \phi : A \to C$)*

*In particular if $\phi, \psi$ integral $\implies$ $\psi \circ \phi$ integral.*

*Proof.* Suppose $c \in C$ is integral over $B$. Let $b_0, \ldots, b_{n-1}$ be the coefficients of the integral relation then clearly $c$ is integral over $B' := A[b_0, \ldots, b_{n-1}]$. By (3.19.3) $B'$ is a finite $A$-module and $B'[c]$ is a finite $B'$-module. Therefore $B'[c]$ is a finite $A$-module and by (3.19.3) we have $c$ is integral over $A$. □

**Definition 3.19.6** (Integrally Closed)
*Let $A \subset B$ be a subring, then we say that $A$ is* ***integrally closed*** *in $B$ if*

$$b \in B \text{ integral over } A \implies b \in A\,.$$

*We say that an integral domain $A$ is* ***integrally closed*** *if it is integrally closed in its field of fractions.*

**Proposition 3.19.7** (Integral Closure)
*Let $A$ be a subring of a ring $B$. Then the set of elements of $B$ integral over $A$ (the* ***integral closure****) is a subring of $B$. Denote this by $\bar{A}$.*

*Further $\bar{A}$ is* ***integrally closed*** *in $B$.*

*Proof.* Let $\alpha, \beta \in B$ be integral over $A$. Then by (3.19.4) the subring $A[\alpha, \beta]$ is a finite $A$-module containing $\alpha \pm \beta$ and $\alpha\beta$. Therefore by (3.19.3) they are also integral over $A$.

Clearly $\bar{A}$ is integral over $A$ so by (3.19.5) it is integrally closed. □

The following criterion is also useful :

**Lemma 3.19.8** (Integral Criterion II)
*Let $\phi : A \to B$ be a ring map. Suppose $x \in B$ is invertible, then $x$ is integral over $A$ if and only if $x \in \phi(A)[x^{-1}]$*

*Proof.* Suppose $x \in \phi(A)[x^{-1}]$ then

$$x = \phi(a_0) + \phi(a_1)x^{-1} + \ldots + \phi(a_n)x^{-n}$$

Multiply by $x^n$ to deduce an integral equation. Conversely suppose $x \in B$ is integral over $A$ then by definition

$$x^n + \phi(a_{n-1})x^{n-1} + \ldots + \phi(a_0) = 0$$

Multiply by $x^{-(n-1)}$ to deduce $x \in \phi(A)[x^{-1}]$ □

**Proposition 3.19.9** (Integral extension preserves field property)
*Let $\phi : A \hookrightarrow B$ be an injective, integral ring map. Then $B$ is a field if and only if $A$ is a field.*

*Proof.* As $\phi$ is injective, it induces an isomorphism between $A$ and $\phi(A)$. So we may assume without loss of generality that $A \subseteq B$ and $\phi$ is the identity.

Suppose $B$ is a field and $x \in A$. Then $x^{-1} \in B$ is integral over $A$ by hypothesis, so by the previous Lemma $x^{-1} \in A[x] \subseteq A$. Therefore $A$ is a field.

Conversely suppose $A$ is a field and $0 \neq x \in B$. Then by hypothesis $x$ is integral over $A$, that is

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

Choose the degree $n$ to be minimal. We claim $a_0 \neq 0$, for if $a_0 = 0$ we may cancel $x$ to obtain an integral relation of smaller degree. Therefore

$$-x(x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1)a_0^{-1} = 1$$

and in particular $x$ is invertible. □

**Proposition 3.19.10**
*Let $\phi : A \to B$ be an integral ring map. Then*

a) *If $\phi^{-1}(\mathfrak{b}) \subseteq \mathfrak{a}$ then the induced ring map $A/\mathfrak{a} \to B/\mathfrak{b}$ (see (3.4.46)) is integral.*

b) *If $S$ is a multiplicatively closed subset of $A$ and $T := \phi(S)$, then the induced ring map $S^{-1}A \to T^{-1}B$ is also integral.*

**Proposition 3.19.11** (Maximal ideals under integral extension)
*Let $\phi : A \to B$ be an integral ring map. Suppose $\mathfrak{q}$ lies above $\mathfrak{p}$. Then*

$$\mathfrak{p} \text{ is maximal} \iff \mathfrak{q} \text{ is maximal}$$

*Proof.* The map $\phi : A \to B$ induces an injective map $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ of integral domains by (3.4.46). By (3.19.10) this map is also integral. Note $A/\mathfrak{p}$ (resp. $B/\mathfrak{q}$) is a field if and only if $\mathfrak{p}$ (resp. $\mathfrak{q}$) is a maximal ideal by (3.4.49). Then we may apply (3.19.9) to show the equivalence. □

**Proposition 3.19.12** (Properties of integral extensions)
*Let $\phi : A \to B$ be an integral ring map then it has*

a) *the **Lying Over** property*

b) *the **Incomparability** property*

c) *the **Going up** property*

*Proof.* For any prime ideal $\mathfrak{p} \triangleleft A$ we have the commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle i_S} & & \downarrow{\scriptstyle i_T} \\ A_{\mathfrak{p}} & \xrightarrow{\tilde{\phi}} & B_{\mathfrak{p}} \end{array}$$

where $S := A \setminus \mathfrak{p}$ and $T := \phi(S)$. By (3.5.6) there exists a morphism $\tilde{\phi}$, and by (3.19.10) it is integral. Define $\mathfrak{m} := \mathfrak{p}A_{\mathfrak{p}}$ to be the unique maximal ideal of $A_{\mathfrak{p}}$.

a) As we assume $\ker(\phi) \subseteq \mathfrak{p}$ we know $B_{\mathfrak{p}} \neq 0$ (3.5.31). Let $\mathfrak{n}$ be a maximal (and hence prime) ideal of $B_{\mathfrak{p}}$. Then $\mathfrak{q} := i_T^{-1}(\mathfrak{n})$ is a prime ideal of $B$ such that $\mathfrak{q} \cap T = \emptyset$. In addition by (3.19.11) $\widetilde{\phi}^{-1}(\mathfrak{n})$ is a maximal ideal, and therefore by uniqueness $\mathfrak{m} = \widetilde{\phi}^{-1}(\mathfrak{n})$. By commutativity of the diagram we then have $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ as required.

(Stacks) As an alternative argument to show existence of $\mathfrak{q}$ by (3.18.4) it's enough to show that $\mathfrak{p}B_{\mathfrak{p}}$ is proper (by assumption $\ker(\phi) \subseteq \mathfrak{p}$ so $B_{\mathfrak{p}} \neq 0$). By the diagram above $\mathfrak{p}B_{\mathfrak{p}} = \tilde{\phi}(\mathfrak{p}A_{\mathfrak{p}})B_{\mathfrak{p}}$. Therefore it's enough to consider the case $(A, \mathfrak{m})$ local and to show $\phi(\mathfrak{m})B$ is proper. Suppose $1 \in \phi(\mathfrak{m})B$ then

$$1 = \sum_{i=1}^{n} \phi(a_i)b_i \quad a_i \in \mathfrak{m}_A \, b_i \in B \, .$$

By (3.19.4) the subring $B' := \phi(A)[b_1, \ldots, b_n] \subset B$ is a finite $A$-module. Furthermore $1 \in \mathfrak{m}B'$ whence $\mathfrak{m}B' = B'$ and by Nakayama's Lemma (3.17.5) $B' = 0$, a contradiction.

b) Suppose $\mathfrak{p} = \phi^{-1}(\mathfrak{q}) = \phi^{-1}(\mathfrak{q}')$ and $\mathfrak{q} \subseteq \mathfrak{q}'$. Let $\mathfrak{n} = \mathfrak{q}B_{\mathfrak{p}}$ and $\mathfrak{n}' = \mathfrak{q}'B_{\mathfrak{p}}$. Clearly $\mathfrak{n} \subseteq \mathfrak{n}'$. By commutativity of the diagram $i_S^{-1}(\tilde{\phi}^{-1}(\mathfrak{n})) = \phi^{-1}(\mathfrak{q}) = \mathfrak{p}$. By (3.5.17) extending the ideals to $A_{\mathfrak{p}}$ shows $\tilde{\phi}^{-1}(\mathfrak{n}) = \mathfrak{m}$, and similarly for $\mathfrak{n}'$. By (3.19.11) both $\mathfrak{n}$, $\mathfrak{n}'$ are maximal so $\mathfrak{n} = \mathfrak{n}'$. By (3.5.18) $\mathfrak{q} = \mathfrak{q}'$.

c) Suppose we have prime ideals $\mathfrak{p} \subsetneq \mathfrak{p}'$ and $\mathfrak{q}$ is a prime ideal lieing above $\mathfrak{p}$. Consider the commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow & & \downarrow \\ A/\mathfrak{p} & \xhookrightarrow{\tilde{\phi}} & B/\mathfrak{q} \end{array}$$

The induced map $\tilde{\phi}$ is integral (3.19.11). By a) there is a prime ideal of $B/\mathfrak{q}$ lieing above $\mathfrak{p}'/\mathfrak{p}$, which is of the form $\mathfrak{q}'/\mathfrak{q}$ for $\mathfrak{q} \subseteq \mathfrak{q}'$ prime (3.4.46). Then from the diagram we see $\phi^{-1}(\mathfrak{q}') = \mathfrak{p}'$ as required.

□

**Remark 3.19.13**
*In other words given a homomorphism $A \to B$ there is a mapping*

$$\operatorname{Spec}(B) \to \operatorname{Spec}(A)$$

*When the homomorphism is injective and integral then this mapping is surjective, and restricts to a surjective mapping*

$$\operatorname{Specm}(B) \to \operatorname{Specm}(A)$$

## 3.20 Valuation Rings and Places

**Definition 3.20.1** (Valuation Ring)
*A subring $A \subset K$ of a field $K$ is a **valuation ring for** $K$ if for every $0 \neq x \in K$ either $x \in A$ or $x^{-1} \in A$ (or both). Such a ring is an integral domain and $K$ is necessarily a field of fractions for $A$.*

*An integral domain $A$ is a **valuation ring** if it is a valuation ring for its field of fractions.*

**Proposition 3.20.2** (Properties of valuation rings)
*Let $A$ be a valuation ring and $K$ its field of fractions then the following properties hold*

a) *$A$ is local ring*

b) *$x^{-1} \notin A \iff x \in \mathfrak{m}$*

c) *$A$ is integrally closed in $K$*

*Proof.* We prove each in turn

a) By (3.16.3) we need to show that $\mathfrak{m} := A \setminus A^\star$ is an additive subgroup of $A$. Given $x, y \in \mathfrak{m}$, without loss of generality we may assume that $x, y$ are non-zero, and $x/y \in A$. Then $x + y = y(1 + x/y)$. If $(x + y) \in A^\star$ then $y \in A^\star$ a contradiction. Therefore $(x + y) \in \mathfrak{m}$ as required.

b) Note $x^{-1} \notin A \iff x \notin A^\star \iff x \in \mathfrak{m}$.

c) Suppose $0 \neq x \in K$ is integral over $A$. If $x \in A$ we are done. If $x^{-1} \in A$ then by (3.19.8) $x \in A[x^{-1}] \subseteq A$ as required.

□

**Definition 3.20.3** (Place (Zariski-Samuel 1960 / Lang 1972))
*Let $K$ be a field. A **place** of $K$ consists of a valuation ring $(A, \mathfrak{m}_A)$ for $K$ and a homomorphism to a field $F$*

$$\phi : A \to F$$

*such that* $\ker(\phi) = \mathfrak{m}_A$.

*Furthermore if $x \in K \setminus A$ then we may write $\phi(x) = \infty$. Note that the second part of the previous Proposition then may be reinterpreted as saying*

$$\phi(x) = \infty \iff \phi(x^{-1}) = 0 \quad \forall x \in K$$

*which motivates the alternative definition below.*

*We say it is a **semi-place** of $K$ if $(A, \mathfrak{m}_A)$ is simply a local ring.*

**Remark 3.20.4** (Alternative definition of place)
*Lang defines it slightly differently namely a function $\phi : K \to F \cup \{\infty\}$ such that for all $x, y \in K$*

- $\phi(0) = 0$ *and* $\phi(1) = 1$
- $\phi(x) + \phi(y) = \phi(x) + \phi(y)$
- $\phi(xy) = \phi(x)\phi(y)$
- $\phi(x^{-1}) = \phi(x)^{-1}$

whenever these are well-defined. *Note that the relations hold over $K$ rather than just $A$. This means we extend the usual algebraic operations in $F$ as follows*

$$x\infty = \infty \quad 0 \neq x$$
$$x \pm \infty = \infty$$
$$0^{-1} = \infty$$
$$\infty^{-1} = 0$$

*noting that $(-)^{-1}$ is still an involution, and excluding terms of the form*

$$\infty \pm \infty, 0 \cdot \infty$$

*Define $A := \{x \in K \mid \phi(x) \neq \infty\}$. Then the final condition naturally implies $x \notin A \implies v(x) = 0$ and $x \in A$, so $A$ is a valuation ring and $\phi|_A$ constitutes a place. One may conversely show relatively easily that a place satisfies the algebraic relations over $K$ as above, being careful about the exceptional cases.*

**Lemma 3.20.5**
*Let $A \subset K$ be a subring of a field and $\mathfrak{a} \triangleleft A$ a proper ideal. Then at least one of $\mathfrak{a}A[x]$ or $\mathfrak{a}A[x^{-1}]$ is a proper ideal.*

*Proof.* Suppose neither are proper then we can write

$$1 = \sum_{j=0}^{n} a_j x^j$$
$$1 = \sum_{j=0}^{m} b_j x^{-j}$$

for $a_j, b_j \in \mathfrak{a}$. Choose $n, m$ to be minimal and assume wlog that $m \leq n$. Observe that $a_0 \neq 1 \implies m > 0$. Multiply the second equation by $x^n a_n$ to find

$$x^n a_n (1 - b_0) = a_n b_1 x^{n-1} + \ldots a_n b_m x^{n-m}$$

and multiply the first by $(1 - b_0)$ to find

$$(1 - b_0) = a_0(1 - b_0) + \ldots + a_n(1 - b_0)x^n$$

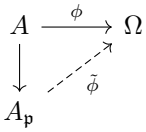
consequently cancelling the $x^n$ term and we obtain a relation of smaller degree a contradiction. □

We prove the first extension theorem

**Proposition 3.20.6** (Extension to localization)
*Let $A$ be a ring and $\phi : A \to \Omega$ a homomorphism into a field. Let $\mathfrak{p} := \ker(\phi)$. Then*

- $\mathfrak{p}$ *is prime*

- *There is a unique extension $\tilde{\phi}$ making the diagram commute*




*Furthermore* $\ker(\tilde{\phi}) = \mathfrak{p}A_{\mathfrak{p}}$ *and* $\tilde{\phi}$ *constitutes a* ***semi-place****.*

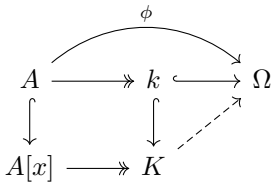
*Proof.* Clearly $\mathfrak{p}$ is prime because $\phi(A)$ is an integral domain. We may extend $\phi$ to the ring $A_{\mathfrak{p}}$ in the obvious way. The extension has kernel $\mathfrak{p}A_{\mathfrak{p}}$, the unique maximal ideal of $A_{\mathfrak{p}}$. □

**Proposition 3.20.7** (Places as maximal extensions)
*Let $A$ be a subring of a field $K$ and $\phi : A \to \Omega$ a homomorphism into an algebraically closed field. Then*

- *For all $x \in K$, $\phi$ may be extended to at least one of $A[x]$ and $A[x^{-1}]$.*
- *There exists a maximal extension $\tilde{\phi} : B \to \Omega$, and any such maximal extension constitutes a place on $K$ with valuation ring $B$ (and $\ker(\tilde{\phi}) = \mathfrak{m}_B$). Furthermore $\mathfrak{m}_B \cap A = \ker(\phi)$.*

*Proof.* We prove each in turn.

- By (3.20.6) we may assume wlog that $A$ is a local ring with unique maximal ideal $\mathfrak{m} = \ker(\phi)$. By (3.20.5) we may suppose without loss of generality that $\mathfrak{m}A[x]$ is proper. Then it's contained in a maximal ideal $\mathfrak{B} \lhd A[x]$. Furthermore $\mathfrak{m} = \mathfrak{B} \cap A$ by maximality of $\mathfrak{m}$. Let $k = A/\mathfrak{m}$ and $K = A[x]/\mathfrak{B}$, then there is a commutative diagram




  Then $K = k[\bar{x}]$ is a field and by (...) $\bar{x}$ is algebraic over $k$. Therefore $K/k$ is algebraic and, because $\Omega$ is algebraically closed, by (3.15.42) there is an extension to $K$, which gives the required extension to $A[x]$.

- It's easy to show that the poset of extensions to subrings of $K$ ordered by consistency is chain complete. Therefore by Zorn's Lemma there is a maximal extension $\tilde{\phi} : B \to \Omega$. By the previous part for any $x \in K$ any such maximal element $B$ must satisfy either $B[x] = B$ or $B[x^{-1}] = B$, i.e. $B$ is a valuation ring for $K$. Consider $\mathfrak{B} := \ker(\tilde{\phi})$ a prime ideal contained in $\mathfrak{m}_B$. Then by (3.20.6) may extend $\tilde{\phi}$ to $B_{\mathfrak{B}}$ and so by maximality $B = B_{\mathfrak{B}}$. Finally (3.16.5) shows that $B$ is a local ring with maximal ideal $\mathfrak{B} = \mathfrak{m}_B$. Clearly $\ker(\tilde{\phi}) \cap A = \ker(\phi)$, so the final statement follows easily.

□

**Corollary 3.20.8**
*Let $A \subset K$ be a subring of a field and $\mathfrak{a} \lhd A$ a proper ideal. Then there exists a valuation ring $(B, \mathfrak{m}_B)$ such that $A \subset B$ and $\mathfrak{a} \subset \mathfrak{m}_B \cap A$. In particular if $\mathfrak{a} = \mathfrak{m}_A$ is maximal then $\mathfrak{m}_A = \mathfrak{m}_B \cap A$.*

*Proof.* By (...) there is a maximal ideal $\mathfrak{m}_A \lhd A$ containing $\mathfrak{a}$. Let $k = A/\mathfrak{m}_A$ and $\Omega = \bar{k}$. Then the canonical homomorphism $\phi : A \to \Omega$ has kernel $\mathfrak{m}_A$. It has an extension to a valuation ring $(B, \mathfrak{m}_B)$ by (3.20.7), such that $\mathfrak{m}_B \cap A = \ker(\phi) = \mathfrak{m}_A$. □

**Corollary 3.20.9**
*Let $A \subset K$ be a subring of a field then the integral closure of $A$ in $K$ (denoted $\bar{A}$) satisfies*

$$\bar{A} = \bigcap_{A \subset V} V$$

*where the intersection is taken over all valuation rings $V$ of $K$ containing $A$.*

*Alternatively the integral elements over $A$ are precisely the elements which are finite at all places of $K$, which are finite over $A$.*

*Proof.* First if $x \in \bar{A}$ then by (3.19.8) we have $x \in A[x^{-1}] \subseteq V[x^{-1}]$. If $x \notin V$ then by hypothesis $x^{-1} \in V$, whence $x \in V$ a contradiction. Therefore $x \in V$ as required.

Conversely suppose $x \notin \bar{A}$, then $x \notin A[x^{-1}]$. That is to say $(x^{-1})$ is a proper ideal in $A[x^{-1}]$. Therefore by (3.20.8) there is a valuation ring $(V, \mathfrak{m}_V)$ such that $x^{-1} \in \mathfrak{m}_V$ which implies $x \notin V$ by (3.20.2). □

## 3.21 Noether Normalisation

The following normalisation result can be seen as a refinement of results on transcendence bases (Section 3.15.11). The proof is adapted from [Mil17].

**Proposition 3.21.1** (Noether Normalisation Lemma)
*Let $A = k[x_1, \dots, x_n]$ be a finitely-generated $k$-algebra such that $k$ is infinite. Then there exists elements $y_1, \dots, y_d \in A$ such that*

- *Each $y_i$ is a $k$-linear combination of $x_1, \dots, x_n$*
- *$A$ is finite (i.e. integral and finitely generated) over $k[y_1, \dots, y_d]$*

*Furthermore if $A$ is an integral domain and $K := \mathrm{Frac}(A)$ then $d = \mathrm{trdeg}(K/k)$ and in particular is unique.*

*Proof.* Suppose $A = k[x_1, \dots, x_n]$. Choose a maximally algebraically independent subset of $\{x_1, \dots, x_n\}$ and renumber so that $x_1, \dots, x_d$ are algebraically independent and $x_{d+1}, \dots, x_n$ are each algebraic over $k[x_1, \dots, x_d]$.

Note if each $x_j$ were actually integral over $k[x_1, \dots, x_d]$, then we would be done by (3.19.4). The substance of the proof is to show this can be arranged after a simple linear change of variables.

If $n = d$ we're done, otherwise assume $n > d$. By assumption then $\{x_1, \dots, x_d, x_n\}$ is algebraically dependent therefore there is a polynomial $f \in k[X_1, \dots, X_d, T]$ such that

$$f(x_1, \dots, x_d, x_n) = 0$$

As $x_1, \dots, x_d$ are algebraically independent, then $T$ appears in $f$ and we have

$$f(X_1, \dots, X_d, T) = a_m T^m + a_{m-1} T^{m-1} + \dots + a_0 \quad a_j \in k[X_1, \dots, X_d]$$

If $a_m \in k$ is constant then $x_n$ is integral over $k[x_1, \dots, x_d]$, which shows that $A$ is finite over $k[x_1, \dots, x_{n-1}]$ (since it's generated by the integral element $x_n$).

We may write $f$ in terms of homogenous polynomials

$$f(X_1, \dots, X_d, T) = f_n(X_1, \dots, X_d, T) + f_{n-1}(X_1, \dots, X_d, T) + \dots + f_0$$

where $f_j$ are homogenous in all variables of degree $j$, $f_n \neq 0$ and $n > 0$. Note that the monomial $T^n$ only appears in $f_n$, and it clearly has coefficient $f_n(0, \dots, 0, 1)$ (since the other monomials have another factor of $X_k$). Actually if this coefficient was non-zero we would be done. Define

$$g(X_1, \dots, X_d, T) = f(X_1 + c_1 T, \dots, X_d + c_d T, T)$$

then we can see that (since $(X + Y)^r$ consists of monomials of degree $r$)

$$g_n(X_1, \dots, X_d, T) = f_n(X_1 + c_1 T, \dots, X_d + c_d T, T)$$

whence the coefficient of $T^n$ in $g$ is $g(0, \dots, 0, 1) = f_n(c_1, \dots, c_d, 1)$. As $f_n \neq 0$ and $k$ is infinite we see that there is a choice of $c_i$ such that the leading coefficient of $T$ in $g$ is constant and non-zero.

Therefore $x_n$ is integral over $k[z_1, \dots, z_d]$ where $z_i = x_i - c_i x_n$. Therefore $A = k[z_1, \dots, z_d, x_{d+1}, \dots, x_n]$ is integral over $B := k[z_1, \dots, z_d, x_{d+1}, \dots, x_{n-1}]$ and of finite-type, and therefore module-finite (3.19.4).

By induction on the number of generators we have that $B$ is finite over $C := k[y_1, \dots, y_r]$ for some algebraically independent $y_j$, and where $y_i$ are $k$-linear combinations of $z_1, \dots, z_d, x_{d+1}, \dots, x_{n-1}$, and therefore $k$-linear combinations of $x_1, \dots, x_n$. By transitivity (3.8.4) we have that $A$ is finite over $C$ as required.

□

**Remark 3.21.2**
*This is really a geometric result, namely there is a linear map $\bar{k}^n \to L(\bar{k})$ onto a linear subspace, which restricts to a surjective mapping $X(\bar{k}) \to L(\bar{k})$.*

*To illustrate why simply taking a maximally algebraically independent subset of generators doesn't always work, consider the canonical example of a parabola*

$$A := k[X, Y]/(XY - 1)$$

*with corresponding zero locus $X(k) := \{(x, x^{-1}) \mid x \in k^\star\}$. The projection map $X(k) \to k$ has non-empty discrete fibres everywhere except at 0, which is an artifact of the ring map $k[X] \to k[X, Y]/(XY - 1)$ not being integral (at $Y$).*

## 3.22 Nullstellensatz

**Definition 3.22.1** (Zeros of an ideal)
*Let $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$ be an ideal and $K/k$ a field extension. Then a point $(x) \in K^n$ is a **zero** of $\mathfrak{a}$ if*

$$f \in \mathfrak{a} \implies f(x) = 0$$

The follow observation is useful

**Proposition 3.22.2** (Zeros are homomorphisms)
*Let $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$ be an ideal then there is a bijection*

$$\begin{aligned} \mathrm{AlgHom}_k(k[X_1, \dots, X_n]/\mathfrak{a}, K) &\longleftrightarrow \{ \text{ zeros of } \mathfrak{a} \text{ in } K^n \} \\ \phi &\longrightarrow (\phi(\bar{X}_1), \dots, \phi(\bar{X}_n)) \end{aligned}$$

Generally we are interested in the relationship between ideals of $k[X_1, \dots, X_n]$ and corresponding zeros in an extension field $K/k$. The following proposition is fundamental

**Proposition 3.22.3** (Correspondence between ideals and zeros)
*Let $K/k$ be a field extension and $(x) \in K^n$. Define $\mathfrak{p}_x$ to be the kernel of the homomorphism*

$$\mathrm{ev}_x : k[X_1, \dots, X_n] \to K$$

*Then*

- *$\mathfrak{p}_x$ is a prime ideal*
- *If $x_i$ are algebraic over $k$ then $\mathfrak{p}_x$ is maximal*
- *If $K/k$ is an algebraically closed field of transcendence degree $\geq n$ then every prime ideal is of this form.*
- *If $\bar{k} \subset K$ then every maximal ideal is of the form $\mathfrak{p}_x$ for $x \in \bar{k}^n$ an algebraic point.*

*In this case we have a canonical isomorphism*

$$k[X_1, \dots, X_n]/\mathfrak{p}_x \xrightarrow{\sim} k[x_1, \dots, x_n] \subset K$$

*Proof.* The canonical isomorphism follows from (3.7.3). Any subring of a field is an integral domain, which means $\mathfrak{p}_x$ is prime by (3.4.49).

By (3.15.26) $x_i$ are algebraic over $k$ if and only if $k(x_1, \dots, x_n)/k$ is algebraic. By the same result $k[x_1, \dots, x_n] = k(x_1, \dots, x_n)$ and therefore $\mathfrak{p}_x$ is maximal by (3.4.49).

Let $\mathfrak{p}$ be a prime ideal and define $k(x) := \mathrm{Frac}(k[x])$ and $k[x] := k[X_1, \dots, X_n]/\mathfrak{p}$. If $K$ has transcendence degree $\geq n$ then there is an embedding $k(x)/k \to K/k$ by (3.15.42). This restricts to an isomorphism $k[x] \xrightarrow{\sim} k[\bar{x}]$ for some $\bar{x}_i \in K$. It's clear that $\mathfrak{p} = \mathfrak{p}_x$.

The proof of the final part we defer to Section 3.22.1. □

The final part is what is usually known as the **Weak Nullstellensatz**. It can be rephrased in multiple forms

**Proposition 3.22.4** (Weak Nullstellensatz I)
*Let $k$ be a field, then the following are trivially equivalent*

a) *Every proper / prime / maximal ideal in $k[X_1, \dots, X_n]$ has a zero in $\bar{k}^n$*

b) *Every maximal ideal $\mathfrak{m} \triangleleft k[X_1, \dots, X_n]$ is of the form $\mathfrak{p}_x$ for $x \in \bar{k}^n$*

c) *For every maximal ideal $\mathfrak{m}$, the field extension $K := k[X_1, \dots, X_n]/\mathfrak{m}$ is algebraic over $k$*

d) ***Zariski's Lemma** If $A$ is a finitely generated $k$-algebra which is a field then $A$ is finite ($\implies$ algebraic, integral) over $k$.*

*Further it's sufficient to consider the case $k$ is infinite.*

*Proof.* Observe for a) it's enough to prove just for maximal ideals because any proper / prime ideal is contained in a maximal ideal.

*a)* $\implies$ *b)* We have $\mathfrak{m} \subseteq \mathfrak{p}_x$ by assumption, and by maximality $\mathfrak{m} = \mathfrak{p}_x$.

*b)* $\implies$ *c)* Observe $\mathfrak{m} = \mathfrak{p}_x$ for $x \in \bar{k}^n$ so $K$ is isomorphic to $k[x_1, \dots, x_n]$ which is an algebraic field extension by (3.15.26).

*c)* $\implies$ *a)* By (3.15.42) there is an embedding $K \to \bar{k}$. Therefore by (3.22.2) every maximal ideal has a root.

*c)* $\implies$ *d)* Every finitely generated $k$-algebra $A$ is of the form $k[X_1, \ldots, X_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$. If $A$ is a field then $\mathfrak{a}$ is maximal by (3.4.49) and so by assumption $A/k$ is a finitely-generated algebraic field extension and therefore finite by (3.15.26).

*d)* $\implies$ *c)*. This is clear.

Finally even if $k$ is finite, it's always the case that $\bar{k}$ is infinite, so we can reduce to the case $k$ is infinite by considering $\mathfrak{a}\bar{k}[X_1, \ldots, X_n]$ in part 1. □

When $K = \bar{k}$ is an algebraic closure we may use these results to make the connection more precise

**Proposition 3.22.5** (Weak Nullstellensatz II)
*There is a bijective map*

$$\begin{array}{rcl} \bar{k}^n / \operatorname{Aut}(\bar{k}/k) & \longrightarrow & \{\mathfrak{m} \lhd k[X_1, \ldots, X_n] \text{ maximal } \} \\ x & \longrightarrow & \mathfrak{p}_x \end{array}$$

*When* $x \in k^n$ *then*

$$\mathfrak{p}_x = (X_1 - x_1, \ldots, X_n - x_n)$$

*Proof.* The map is surjective by (3.22.4). It's well-defined because $\mathfrak{p}_{\sigma(x)} = \mathfrak{p}_x$.

By (3.22.3) we have an isomorphism $k[X_1, \ldots, X_n]/\mathfrak{p}_x \xrightarrow{\sim} k[x_1, \ldots, x_n] \subset \bar{k}$. If $\mathfrak{p}_x = \mathfrak{p}_y$ then these compose to yield an isomorphism $\sigma : k[x_1, \ldots, x_n] \xrightarrow{\sim} k[y_1, \ldots, y_n] \subset \bar{k}$ such that $\sigma(x_i) = y_i$. By (3.15.48) this extends to $\sigma \in \operatorname{Aut}(\bar{k}/k)$. Therefore the given mapping is injective. □

### 3.22.1 Proof of Weak Nullstellensatz

This section uses approaches from [ZS76], [Lan19].

*Proof of Nullstellensatz using normalisation.* For any ideal $\mathfrak{a}$ the Normalisation Lemma shows $A := k[X_1, \ldots, X_n]/\mathfrak{a}$ is integral over $B := k[z_1, \ldots, z_d]$ where $z_1, \ldots, z_d$ are algebraically independent.

If $\mathfrak{a}$ is maximal then $A$ is a field and by (3.19.9) $B = k$ is a field. Therefore $d = 0$ and $A/k$ is a finite extension which is one form of the Weak Nullstellensatz.

Alternatively if $\mathfrak{a}$ is not necessarily maximal, then $B$ has a maximal ideal $\mathfrak{p}_z$ for any $\bar{z} \in \bar{k}^d$ (except maybe when $d = 0$). By (3.19.12) there is a maximal ideal $\mathfrak{m} \lhd A$ lieing above. Then we have a diagram

$$\begin{array}{ccccc} A & \longrightarrow & A/\mathfrak{m} & \dashrightarrow & \bar{k} \\ \uparrow & & \uparrow & \nearrow & \\ B & \longrightarrow & B/\mathfrak{p}_z & & \end{array}$$

which may be completed because $A/\mathfrak{m}$ is algebraic over $B/\mathfrak{p}_z$. By (3.22.2) this yields a zero of $\mathfrak{a}$. □

*Proof of Nullstellensatz avoiding normalisation.* Consider only the case $\mathfrak{a} = \mathfrak{p}$ is prime.

Define $A := k[X_1, \ldots, X_n]/\mathfrak{p}$ an integral domain and $k(x) = k(x_1, \ldots, x_n) := \operatorname{Frac}(A)$.

Let $z_1, \ldots, z_d$ be a transcendence basis for $k(x)$. Then $k(x)/k(z_1, \ldots, z_d)$ is algebraic and therefore there exist polynomials $g_{ij} \in k[Z_1, \ldots, Z_d]$ such that

$$g_{im}(z)x_i^m + \ldots g_{i0} \quad = \quad 0 \tag{3.5}$$

(by clearing denominators). Because $\bar{k}$ is infinite it's possible to choose $\bar{z} \in \bar{k}^d$ such that $g_{im}(\bar{z}) \neq 0$ for all $i = 1 \ldots n$. Then evaluation gives a homomorphism

$$\phi : k[z_1, \ldots, z_d] \to k[\bar{z}_1, \ldots, \bar{z}_d] \subset \bar{k}$$

This extends to a place $\tilde{\phi}$ of $k(x)$ by (3.20.7). We claim this place must be finite on $x_i$, for otherwise divide (3.5) by $x_i^m$ and evaluate at $\tilde{\phi}$ to find a contradiction. This then restricts to a morphism

$$\tilde{\phi} : k[x_1, \ldots, x_n] \to \bar{k}$$

which yields a zero of $\mathfrak{p}$ by (3.22.2) as required. □

## 3.23 Jacobson Rings

**Definition 3.23.1** (Jacobson Radical)
*Let $\mathfrak{a} \triangleleft A$ be an ideal. Define the **Jacobson Radical** of $\mathfrak{a}$ to be*

$$\sqrt{\mathfrak{a}}^J := \bigcap_{\mathfrak{a} \subseteq \mathfrak{m}} \mathfrak{m}$$

*Note by (3.4.39) and (3.4.50)*

$$\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}}^J$$

**Proposition 3.23.2** (Jacobson Ring)
*Let $A$ be a ring the following are equivalent*

a) *For any ideal $\mathfrak{a}$, $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}}^J$*

b) *For any radical ideal $\mathfrak{a} = \sqrt{\mathfrak{a}}^J$*

c) *For any prime ideal $\mathfrak{p} = \sqrt{\mathfrak{p}}^J$*

*We say such a ring is a **Jacobson ring**.*

*Proof.* a) $\implies$ b) This clear because in this case $\mathfrak{a} = \sqrt{\mathfrak{a}}$.
b) $\implies$ c) This is clear because a prime ideal is radical.
c) $\implies$ a) By (3.4.39)

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

as required □

We prove later that the Weak Nullstellensatz implies the following result

**Proposition 3.23.3** (Strong Nullstellensatz)
*$k[X_1, \ldots, X_n]$ is a Jacobson ring.*

## 3.24 Dimension Theory

**Definition 3.24.1** (Krull Dimension)
*Let $A$ be a commutative ring. We say that a chain of distinct prime ideals*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

*has **length** $n$.*

a) *The **Krull dimension** $\dim A$ of $S$ is the maximum length of all chains of prime ideals.*

b) *The **height** or **codimension** of a prime ideal $\mathfrak{p} \triangleleft A$, denoted $\operatorname{codim}(\mathfrak{p})$, is the maximum length of chains of prime ideals contained in $\mathfrak{p}$.*

c) *The **dimension** of an ideal $\mathfrak{a} \triangleleft A$, denoted $\dim \mathfrak{a}$, is the maximum length of chains of prime ideals containing $\mathfrak{a}$.*

**Proposition 3.24.2** (Simple properties)
*The following properties of Krull dimension hold*

a) $\dim A = \dim A/N(A)$

b) $\operatorname{codim}(\mathfrak{p}) = \dim A_{\mathfrak{p}}$

c) $\dim \mathfrak{a} = \dim A/\mathfrak{a}$

d) $\dim A = \sup_{\mathfrak{p}} \dim A_{\mathfrak{p}}$

e) $\dim A \geq \dim \mathfrak{p} + \operatorname{codim} \mathfrak{p}$

f) $\dim k = 0$ *for any field $k$*

g) *A principal ideal domain $A$ which is not a field has dimension* 1

*Proof.* a) By (3.4.46) there is an order-isomorphism between prime ideals of $A$ containing $N(A)$ and prime ideals of $A/N(A)$. However by (3.4.39) all prime ideals of $A$ contain $N(A)$, so there is a bijection between chains of $A$ and chains of $A/N(A)$, and the result follows.

b) This follows similarly from (3.5.32).

c) This follows similarly from (3.4.46).

d) This is clear

e) Join two chains together to find the given lower bound on $\dim A$.

f) The only (prime) ideal is (0)

g) By (...) every prime ideal (besides (0)) is maximal so every chain has length at most 1.

□

**Proposition 3.24.3** (Krull Dimension is preserved under integral maps)
*Let $\phi : A \to B$ be a ring map.*

a) *Going Up* $\implies \dim B \geq \dim(A/\ker(\phi))$

b) *Incomparability* $\implies \dim B \leq \dim(A/\ker(\phi))$

*In particular $\phi$ integral and injective implies $\dim A = \dim B$.*

*Proof.* Without loss of generality we can assume that $\phi$ is injective. The two cases follow by lifting chains of prime ideals from $A$ (resp. $B$) to $B$ (resp. $A$), checking that properness is maintained.

The final statement follows from (3.19.12). □

# Chapter 4

# Topology and Differential Geometry

Many of the constructions in algebraic geometry are analogues of constructions in topology and differential geometry. Therefore we review these, but slanted from the point of view of algebraic geometry.

## 4.1 Topological Spaces

Topology is useful in algebraic geometry, but often the natural topologies are usually much coarser so the theory looks rather different.

**Definition 4.1.1** (Topological Space)
*A topological space $(X, \mathcal{T}_X)$ consists of a set $X$ and family of open sets $\mathcal{T}_X \subseteq \mathcal{P}(X)$ satisfying the following properties*

- $X, \emptyset \in \mathcal{T}_X$
- $U_i \in \mathcal{T}_X \implies \bigcup_{i \in I} U_i \in \mathcal{T}_X$
- $U, V \in \mathcal{T}_X \implies U \cap V \in \mathcal{T}_X$

*A subset $Z \subset X$ is said to be closed iff $X \setminus Z$ is open. We may equivalently define the topology in terms of closed sets.*

**Definition 4.1.2** (Continuous)
*A map $f : X \to Y$ is continuous if the inverse image of an open (closed) set is open (closed).*

**Remark 4.1.3**
*In the case of $\mathbb{R}^n$ this can be shown to be equivalent to the usual $\delta - \epsilon$ definition.*

**Definition 4.1.4** (Subspace topology)
*Let $Y \subset X$, then we may define the subspace topology on $Y$ by*

$$\mathcal{T}_Y := \{U \cap Y \mid U \in \mathcal{T}_X\}$$

*when $Y$ is open then this is given by*

$$\mathcal{T}_Y = \{U \subseteq Y \mid U \in \mathcal{T}_X\}$$

**Definition 4.1.5** (Base)
*We say $\mathcal{B} \subseteq \mathcal{P}(X)$ is a base (of open sets) on $X$ if*

- *For every $x \in X$ there is a $U \in \mathcal{B}$ such that $x \in U$*
- *Suppose $U, V \in \mathcal{B}$ and $x \in U \cap V$ then there exists $W \in \mathcal{B}$ such that $x \in W \subseteq U \cap V$*

**Proposition 4.1.6** (Topology generated by a base)
*Let $\mathcal{B}$ be a base, then the following is a topology on $X$*

$$\mathcal{T}_{\mathcal{B}} := \{\bigcup_{U_i \in I} U_i \mid I \subseteq \mathcal{B}\}$$

*i.e. the set of arbitrary unions of sets in $\mathcal{B}$.*

**Proposition 4.1.7** (Base generating topology)
*A base $\mathcal{B}$ satisfies $\mathcal{T}_{\mathcal{B}} = \mathcal{T}_X$ if and only if for every $x \in U$ and $U \in \mathcal{T}_X$ there exists $V \in \mathcal{B}$ such that $x \in V \subseteq U$.*

*In this case we say $\mathcal{B}$ is a base* for *$X$.*

**Definition 4.1.8** (Limit point)
*For $Y \subset X$ we say $x$ is a limit point of $Y$ if $(x \in U \implies Y \cap U \neq \emptyset)$. NB every point of $Y$ is necessarily a limit point.*

**Remark 4.1.9**
*In the case of $\mathbb{R}^n$ this is equivalent to $x$ being the limit of a convergent sequence $x_n \in Y$.*

**Proposition 4.1.10** (Topological Closure)
*Let $Y \subset X$ then the following sets are equal*

$$\mathrm{cl}_X(Y) := \overline{Y} := \bigcap_{\substack{Z \supseteq Y \\ Z \text{ closed}}} Z = \{x \in X \mid x \text{ limit point of } Y\}$$

*Furthermore*

a) *$Y \subseteq \overline{Y}$ and $\overline{Y}$ is closed*

b) *$Y = \overline{Y}$ if and only if $Y$ is closed*

c) *$(Y \cap U \neq \emptyset \iff \overline{Y} \cap U \neq \emptyset)$ for any $U$ open*

*Proof.* Suppose $Z$ is a closed set containing $Y$ and $x$ is a limit point of $Y$. Then $x \notin Z \implies x \in X \setminus Z \implies (X \setminus Z) \cap Y \neq \emptyset$ a contradiction. Conversely assume $x \notin \overline{Y}$ then there exists $Z \supseteq Y$ closed such that $x \notin Z \implies x \in X \setminus Z$. This means $x$ is not a limit point.

a) An arbitrary intersection of closed sets is closed

b) This follows because $\overline{Y}$ is the smallest closed superset.

c) One implication is clear because $Y \subseteq \overline{Y}$. Conversely if $x \in \overline{Y} \cap U$ then $x$ must be a limit point of $Y$ hence $U \cap Y \neq \emptyset$ as required.

□

**Remark 4.1.11**
*In $\mathbb{R}^n$ this is simply adjoining limit points, e.g. $[a,b] \setminus T \to [a,b]$ where $T$ is a finite set.*

**Proposition 4.1.12** (Dense subset)
*Let $Y \subset X$ then the following are equivalent*

a) *$\overline{Y} = X$*

b) *$Y \cap U \neq \emptyset$ for any $U$ open*

*and we say $Y$ is dense.*

*Proof.* $1 \implies 2)$ Follows from (4.1.10) criteria 3.
$2 \implies 1)$. Suppose $Y \subseteq \overline{Y} \subsetneq X$ then $X \setminus \overline{Y}$ is an open set not intersecting $Y$ a contradiction. □

**Proposition 4.1.13** (Closed point)
*Let $x \in X$ then TFAE*

- *$\{x\}$ is closed*
- *For every $y \neq x$ there is $U \ni y$ such that $x \notin U$.*

**Definition 4.1.14**
*For a topological space $X$ let $X^\circ$ denote the subset of closed points.*

### 4.1.1 Continuous Maps

### 4.1.2 Irreducible Topological Spaces

**Proposition 4.1.15** (Irreducible space)
*Let $X$ be a topological space. Then the following are equivalent*

a) *$X = Z_1 \cup Z_2$ closed implies either $Z_1 = X$ or $Z_2 = X$*

b) *$U, V \neq \emptyset \implies U \cap V \neq \emptyset$ for open sets $U, V$*

c) *$U \neq \emptyset \implies \overline{U} = X$ i.e. every non-empty open set is dense*

*and we say $X$ is irreducible.*

*Proof.* $1 \implies 2)$ Suppose $U, V$ are open sets such that $U \cap V = \emptyset$. Then $X = U^c \cup V^c$. By hypothesis $X = U^c$ or $X = V^c$ whence either $U$ or $V$ is empty.
$2 \implies 1)$ Similar.
$3 \iff 2)$ Follows directly from (4.1.12) □

**Proposition 4.1.16** (Irreducible Subset)
*Let $Y \subset X$ be a subset of a topological space. Then the following conditions on $Y$ are equivalent*

a) $Y$ *is irreducible in the subspace topology.*

b) $Y \subseteq Z_1 \cup Z_2$ *closed implies either* $Y \subseteq Z_1$ *or* $Y \subseteq Z_2$

c) $U \cap Y \neq \emptyset, V \cap Y \neq \emptyset \implies (U \cap V) \cap Y \neq \emptyset$ *for* $U, V$ *open*

*and we say* $Y$ *is an irreducible subset.*

*Proof.* This follows by applying (4.1.15) along with the definition of the subspace topology. □

**Remark 4.1.17**
*Singletons* $\{x\}$ *are always irreducible.*

**Definition 4.1.18** (Irreducible Component)
*We say that* $Y$ *is an irreducible component if it is a maximal irreducible subset.*

https://stacks.math.columbia.edu/tag/004W

**Proposition 4.1.19** (Decomposition into Irreducible Components)
*A topological space* $X$ *may be decomposed into irreducible components. More precisely*

- $Y$ *irreducible* $\implies \overline{Y}$ *irreducible*
- $Y$ *irreducible component* $\implies Y$ *is closed*
- *Every irreducible subset is contained in an irreducible component*
- $X$ *is the union of irreducible components*

*Proof.* We prove each in turn

- Suppose $\overline{Y} \subseteq Z_1 \cup Z_2$ then by irreducibility $Y_1 \subseteq Z_1$ say. By (4.1.10) then $\overline{Y} \subseteq Z_1$ as required.
- Since an irreducible component is maximal and $\overline{Y}$ is irreducible we see that for $Y$ irreducible and maximal we must have $Y = \overline{Y}$. (4.1.10) implies that such a $Y$ is closed.
- By Zorn's Lemma it's enough to show that if $T_i$ is a chain (i.e. $I$ is totally ordered and $i \leq j \implies T_i \subseteq T_j$) of irreducible subsets then $T := \cup_i T_i$ is irreducible. Suppose $T \subseteq Z_1 \cup Z_2$. Then for every $i$ we have $T_i \subseteq Z_1$ or $T_i \subseteq Z_2$. Suppose for some $i$, $T_i \not\subseteq Z_1$, then for $j \geq i$ we have $T_j \not\subseteq Z_1$ whence $T_j \subseteq Z_2$ which implies $T \subseteq Z_2$ as required.
- As $\{x\}$ is irreducible every element is contained in an irreducible component by the previous step.

□

**Corollary 4.1.20**
*Let* $x \in X$ *be a point then the closure* $\overline{\{x\}}$ *is an irreducible closed subset.*

**Corollary 4.1.21**
$X$ *is irreducible if and only if it has a single irreducible component.*

**Definition 4.1.22** (Generic Point)
*Let* $Z$ *be an irreducible closed subset of* $X$*, then we say* $\eta \in X$ *is a generic point of* $Z$ *if*

$$Z = \overline{\{\eta\}}$$

**Definition 4.1.23** (Sober)
*A topological space is said to be sober if the mapping*

$$x \longrightarrow \overline{\{x\}}$$

*is bijective mapping from the set of points to irreducible closed subsets.*

## 4.2 Sheaves

For what follows we assume $\mathcal{C}$ is an algebraic category.

**Definition 4.2.1** (Sheaf [War13, Defn 5.7] [For81, Defn 6.3])
*A* $\mathcal{C}$*-valued sheaf* $\mathcal{F}$ *on a topological space* $X$ *is a mapping*

$$U \longrightarrow \mathcal{F}(U) \in \mathrm{ob}(\mathcal{C})$$

*together with a collection of restriction morphisms* $\rho_{UV} \in \mathrm{Mor}(F(U), F(V))$*, for any pair of open sets* $V \subset U$ *satisfying the following properties*

a) $\rho_{VW} \circ \rho_{UV} = \rho_{UW}$. *Write*

$$\sigma|_V := \rho_{UV}(\sigma)$$

b) *For any open set* $U$, *open cover* $U = \bigcup_{i \in I} U_i$ *and* $\sigma, \tau \in \mathcal{O}_X(U)$ *satisfying*

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

*then* $\sigma = \tau$.

c) *Consider any open set* $U$ *and any open covering* $U = \bigcup_{i \in I} U_i$ *and 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* $\sigma$ *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 4.2.2** ($\mathcal{B}$-sheaf)
*Let* $\mathcal{B}$ *be a base for* $X$, *which is closed under finite intersection. We say a* $\mathcal{B}$*-sheaf is a mapping*

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

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

**Definition 4.2.3** (Morphism of sheaves)
*Let* $\mathcal{F}, \mathcal{G}$ *be (pre)-sheaves on a topological space* $X$. *The a morphism* $\phi : \mathcal{F} \to \mathcal{G}$ *consists of a family of morphisms*

$$\phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$$

*such that* $\rho_{UV} \circ \phi_U = \phi_V \circ \rho_{UV}$ *for all* $V \subseteq U$ *open. We say that*

- $\phi$ *is injective if* $\phi_U$ *is injective for all* $U$
- $\phi$ *is an isomorphism if* $\phi_U$ *is an isomorphism for all* $U$ *(iff it has a two-sided inverse)*

**Definition 4.2.4** (Category of sheaves)
*Let* $X$ *be a topological space and* $\mathcal{B}$ *a base for* $X$. *Then we denote the category of presheaves by*

$$\mathrm{PSh}(X; \mathcal{B})$$

*and the (full subcategory) of sheaves by*

$$\mathrm{Sh}(X; \mathcal{B})$$

*When* $\mathcal{B} = \mathcal{T}_X$ *we may omit* $\mathcal{B}$.

**Definition 4.2.5** (Stalk of a (pre)sheaf)
*Let* $\mathcal{F}$ *be a (*$\mathcal{B}$*-)presheaf 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* $\{\mathcal{F}(U) \to \mathcal{F}(V)\}_{V \subseteq U}$. *Explicitly this may be constructed as*

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

*where* $(U, \sigma) \sim (V, \tau)$ *if there is an open set* $x \in W \subset U \cap V$ *such that* $\sigma|_W = \tau|_W$. *It comes equipped with a family of morphisms* $\rho_{Ux} : \mathcal{F}(U) \to \mathcal{F}_x$ *such that*

$$\rho_{Vx} \circ \rho_{UV} = \rho_{Ux}$$

*Moreover for any open set* $U$ *and family of morphisms* $\{\phi_V : \mathcal{F}(V) \to A\}_{V \subseteq U}$ *there is a unique morphism* $\phi_x : \mathcal{F}_x \to A$ *such that* $\phi_U = \phi_x \circ \rho_{Ux}$.

**Lemma 4.2.6** (Lifting Stalks)
*Let* $\mathcal{F}$ *be a* $\mathcal{B}$*-presheaf and* $\sigma \in \mathcal{F}(U)$ *and* $\tau \in \mathcal{F}(V)$ *be sections such that* $x \in U \cap V$.

- *Then $\sigma_x = \tau_x$ if and only if there is a neighbourhood $x \in W \subseteq U \cap V$ such that $\sigma|_W = \tau|_W$.*
- *If $\sigma_x = \tau_x$ for all $x \in U \cap V$, then there is an open cover $U \cap V = \bigcup_i U_i$ such that $\sigma|_{U_i} = \tau|_{U_i}$*
- *If in addition $\mathcal{F}$ is separated then $\sigma|_{U\cap V} = \tau|_{U\cap V}$.*

**Proposition 4.2.7**
*Let $\mathcal{F}$ be a $\mathcal{B}_1$-presheaf on $X$, and $\mathcal{B}_2 \subseteq \mathcal{B}_1$ another base for the topology on $X$. Then there is a well-defined, canonical, isomorphism*

$$\rho_x : (\mathcal{F}|_{\mathcal{B}_2})_x \quad \to \quad \mathcal{F}_x$$

*It satisfies*

$$[(U, \sigma)]_{x,\mathcal{B}_2} \to [(U, \sigma)]_{x,\mathcal{B}_1}$$

*for all $U \in \mathcal{B}_2$ and $\sigma \in \mathcal{F}(U)$.*

*Proof.* The given map is clearly well-defined because $\mathcal{B}_2 \subseteq \mathcal{B}_1$

Suppose $[(U, \sigma)] = [(V, \tau)]$ in $\mathcal{F}_x$ then by definition there exists an open set $W \in \mathcal{B}_1$ such that $x \in W$, $W \subset U \cap V$ such that $\sigma|_W = \tau|_W$. By (4.1.7) there is $W' \in \mathcal{B}_2$ such that $x \in W'$ and $W' \subseteq W$. As $\sigma|_{W'} = \tau|_{W'}$, this shows that $(U, \sigma) \sim (V, \tau)$ in $(\mathcal{F}|_{\mathcal{B}_2})_x$, and therefore $\rho_x$ is injective.

Similarly consider $[(U, \sigma)] \in \mathcal{F}_x$ with $U \in \mathcal{B}_1$. By (4.1.7) there is $V \in \mathcal{B}_2$ such that $x \in V$ and $V \subseteq U$. Therefore $[(U, \sigma)] = [(V, \sigma|_V)]$ and the map is surjective. □

**Proposition 4.2.8**
*Let $\phi : \mathcal{F} \to \mathcal{G}$ be a morphism of ($\mathcal{B}$-)pre-sheaves then there exists a unique map on stalks*

$$\phi_x : \mathcal{F}_x \to \mathcal{G}_x$$

*such that $\phi(\sigma)_x = \phi_x(\sigma_x)$ for all $\sigma \in \mathcal{F}(U)$ and $U$ neighbourhoods of $x$. Furthermore if $\psi : \mathcal{G} \to \mathcal{H}$ is another morphism of (pre-)sheaves then*

$$\psi_x \circ \phi_x = (\psi \circ \phi)_x$$

**Definition 4.2.9** (Push-forward sheaf)
*Let $f : X \to Y$ be a continuous map and $\mathcal{F}$ a sheaf on $X$. Then we may define the push-forward sheaf on $Y$ by*

$$(f_\star \mathcal{F})(V) = \mathcal{F}(f^{-1}V)$$

**Proposition 4.2.10** (Stalks on a push-forward sheaf)
*Let $f : X \to Y$ be a continuous map and $\mathcal{F}$ a sheaf on $X$. Then for $x \in X$ there is a unique morphism*

$$\rho_x : (f_\star \mathcal{F})_{f(x)} \to \mathcal{F}_x$$

*such that $\rho_x(\sigma_{f(x)}) = \sigma_x$ for all $\sigma \in \mathcal{F}(f^{-1}V)$ and $V$ nbhds of $f(x)$.*

**Proposition 4.2.11** (Sheafification)
*Given a $\mathcal{B}$-presheaf $\mathcal{F}$ define the sheafification $\mathcal{F}^+$ on $\mathcal{T}_X$ by*

$$\mathcal{F}^+(U) := \{(s_x)_{x\in U} \mid s_x \in \mathcal{F}_x\}$$

*where we only consider "sections" $(s_x)$ such that there is an open cover $U = \cup_i U_i$ with $U_i \in \mathcal{B}$ and sections $\sigma_i \in \mathcal{F}(U_i)$ such that $s_y = (\sigma_i)_y$ for all $y \in U_i$. We say the section $s$ is determined by the sections $(U_i, \sigma_i)$. This constitutes a functor*

$$(-)^+ : \mathrm{PSh}(X; \mathcal{B}) \to \mathrm{Sh}(X)$$

*Furthermore there is a natural transformation $\eta : \mathbf{1} \Rightarrow (-)^+|_{\mathcal{B}}$ given by*

$$\eta_{\mathcal{F}} : \mathcal{F} \to (\mathcal{F}^+)|_{\mathcal{B}}$$
$$\sigma \to (\sigma_x)$$

*which is an isomorphism if and only if $\mathcal{F}$ is a sheaf. It satisfies a natural universal property, which may be formalised as saying that $(-)^+$ is left-adjoint to $(-)|_{\mathcal{B}}$, namely there is a natural bijection*

$$\begin{array}{rcl} \mathrm{Mor}(\mathcal{F}^+, \mathcal{G}) & \longrightarrow & \mathrm{Mor}(\mathcal{F}, \mathcal{G}|_{\mathcal{B}}) \\ \alpha & \longrightarrow & \alpha|_{\mathcal{B}} \circ \eta_{\mathcal{F}} \\ \epsilon_{\mathcal{G}} \circ \beta^+ & \longleftarrow & \beta \end{array}$$

*where we have used the counit natural transformation, which is infact an isomorphism,*

$$\begin{array}{rcl} \epsilon_{\mathcal{G}} : (\mathcal{G}|_{\mathcal{B}})^{+} & \longrightarrow & \mathcal{G} \\ (\rho_x(\sigma_x)) & \longleftarrow & \sigma \end{array}$$

*Finally there is an isomorphisms of stalks which commutes with restrictions, namely for all $U \in \mathcal{B}$ and $x \in U$ there is a commutative diagram*

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\eta_U} & \mathcal{F}^{+}(U) \\ {\scriptstyle \rho_x}\downarrow & & \downarrow{\scriptstyle \rho_x} \\ \mathcal{F}_x & \xrightarrow{\eta_x} & (\mathcal{F}^{+})_x \end{array}$$

*where the bottom arrow is uniquely determined by this condition.*

*Proof.* $\mathcal{F}^{+}$ is clearly a sheaf. The fact $(-)^{+}$ is functorial follows from (4.2.8), namely $\alpha^{+}((s_x)) = (\alpha_x(s_x))$. It's well-defined for suppose $s$ is determined by sections $(U_i, \sigma_i)$ then $\alpha^{+}((s_x))$ is determined by the sections $(U_i, \alpha_{U_i}(\sigma_i))$.

In order to define $\eta$ and $\epsilon$ first consider the following. Let $\mathcal{B}_2 \subseteq \mathcal{B}_1$ be bases for $X$, $\mathcal{F}$ a $\mathcal{B}_1$-presheaf and $U \in \mathcal{B}_1$ an open subset. Then define the morphism

$$\begin{array}{rcll} \Phi^{\mathcal{B}_2}_{\mathcal{F},U} : \mathcal{F}(U) & \to & (\mathcal{F}|_{\mathcal{B}_2})^{+}(U) & U \in \mathcal{B}_1 \\ \sigma & \to & (\rho_x^{-1}(\sigma_x))_{x \in U} & \end{array}$$

where we have used the isomorphism from (4.2.7) $\rho_x : (\mathcal{F}|_{\mathcal{B}_2})_x \longrightarrow \mathcal{F}_x$.

We claim $\Phi$ is well-defined. For if $U \in \mathcal{B}_1$ there is an open cover $U = \bigcup_{i \in I} U_i$ with $U_i \in \mathcal{B}_2$. For any $\sigma \in \mathcal{F}(U)$ define $\sigma_i := \sigma|_{U_i}$. Then $x \in U_j$ for some $j$ and $\sigma_x = [(U, \sigma)]_{x,\mathcal{B}_1} = [(U_j, \sigma_j)]_{x,\mathcal{B}_1}$ and therefore $\rho_x^{-1}(\sigma_x) = [(U_j, \sigma_j)]_{x,\mathcal{B}_2}$. In other words the given section is supported by $\{(U_i, \sigma_i)\}_{i \in I}$ as required.

We claim $\Phi_{\mathcal{F},U}$ is an isomorphism for all $U$ if and only if $\mathcal{F}$ is a sheaf. Suppose $\mathcal{F}$ is a sheaf, and $\rho_x^{-1}(\sigma_x) = \rho_x^{-1}(\tau_x)$ for all $x \in U$, then $\sigma_x = \tau_x$. By (4.2.6) we see $\sigma = \tau$. Therefore the mapping is injective.

Similarly let $(s_x) \in (\mathcal{F}|_{\mathcal{B}_2})^{+}(U)$ be determined by sections $(U_i, \sigma_i)$ with $\sigma_i \in \mathcal{F}(U_i)$ and $U_i \in \mathcal{B}_2$. Then $s_x = [(U_i, \sigma_i)]_{x,\mathcal{B}_2} = [(U_j, \sigma_j)]_{x,\mathcal{B}_2}$ for all $x \in U_i \cap U_j$ so, applying $\rho_x$, $(\sigma_i)_x = (\sigma_j)_x$ for all $x \in U_i \cap U_j$. By (4.2.6) we see that $\sigma_i|_{U_i \cap U_j} = \sigma_j|_{U_i \cap U_j}$, so by hypothesis there is an element $\sigma$ such that $\sigma|_{U_i} = \sigma_i$. In particular $\sigma_x = (\sigma_i)_x$ and $\rho_x^{-1}(\sigma_x) = \rho_x^{-1}((\sigma_i)_x) = s_x$ and the mapping is surjective as required.

Conversely suppose $\Phi_{\mathcal{F},U}$ is an isomorphism for all $U$ - TODO.

Finally we may define the unit and counit natural transformations as follows

$$\begin{array}{rcll} \epsilon_{\mathcal{G},U} := & \left(\Phi^{\mathcal{B}}_{\mathcal{G},U}\right)^{-1} & U \in \mathcal{T}_X \\ \eta_{\mathcal{F},U} := & \Phi^{\mathcal{B}}_{\mathcal{F},U} & U \in \mathcal{B} \end{array}$$

By abstract nonsense (2.4.42) we may show an adjoint relationship arising from $\eta, \epsilon$ if

- $\epsilon_{\mathcal{G}}|_{\mathcal{B}} \circ \eta_{\mathcal{G}|_{\mathcal{B}}} = 1_{\mathcal{G}|_{\mathcal{B}}}$
- The following map is injective

$$\begin{array}{rcl} \mathrm{Mor}(\mathcal{F}^{+}, \mathcal{G}) & \longrightarrow & \mathrm{Mor}(\mathcal{F}, \mathcal{G}|_{\mathcal{B}}) \\ \alpha & \longrightarrow & \alpha|_{\mathcal{B}} \circ \eta_{\mathcal{F}} \end{array}$$

The first follows by definition of $\eta$ and $\epsilon$. The second is essentially because $\mathcal{G}$ is separated. For suppose $\alpha_1$ and $\alpha_2$ are two morphisms such that $\alpha_1|_{\mathcal{B}} \circ \eta = \alpha_2|_{\mathcal{B}} \circ \eta$. Consider a section $s(x) \in \mathcal{F}^{+}(U)$. Then it is supported by sections $(\sigma_i, U_i)$ for $U_i \in \mathcal{B}$ and $\sigma_i \in \mathcal{F}(U_i)$. This means precisely that $s|_{U_i} = \eta(\sigma_i)$. Then the assumption on $\alpha_1$, $\alpha_2$ shows that

$$\alpha_1(s)|_{U_i} = \alpha_{1,U_i}(s|_{U_i}) = \alpha_{2,U_i}(s, |_{U_i}) = \alpha_2(s)|_{U_i}$$

Finally by the separatedness condition we have $\alpha_1 = \alpha_2$ and the given map is injective. This completes the requirements to show the adjoint relationship.

By the universal property of direct limits, the maps $\mathcal{F}(U) \to \mathcal{F}^+(U) \to (\mathcal{F}^+)_x$ induce a map $\eta_x$ making the diagram commute, given by $\eta_x(\sigma_x) = \eta(\sigma)_x$. If $\eta_x(\sigma_x) = \eta(\sigma)_x = \eta(\tau)_x = \eta_x(\tau_x)$ then by (4.2.6) there is a nbhd $x \in W$ such that $\eta(\sigma)|_W = \eta(\tau)|_W$ and in particular $\sigma_x = \eta(\sigma)(x) = \eta(\tau)(x) = \tau_x$ so the map is injective. Given $s_x \in (\mathcal{F}^+)_x$ then by (4.2.6) there is $x \in U$ and a corresponding section $s \in (\mathcal{F}^+)(U)$. By assumption there exists $x \in U_i \in \mathcal{B}$ and $\sigma \in \mathcal{F}(U_i)$ such that $s(y) = \sigma_y$ for all $y \in U_i$. In otherwords $s|_{U_i} = \eta_{U_i}(\sigma)$ and therefore $s_x = (s|_{U_i})_x = \eta_{U_i}(\sigma)_x = \eta_x(\sigma_x)$. Therefore the map is surjective. □

**Remark 4.2.12**
*This motivates the term "sheaf" namely we view it as a "bundle" of "stalks" and sections are "slices" through the sheaf. It's possible to impose a topology on $\coprod_{x\in X} \mathcal{F}_x$ such the sections of $\mathcal{F}^+$ are precisely the continuous maps $\sigma : U \to \coprod_{x\in U} \mathcal{F}_x$ with $\sigma(x) \in \mathcal{F}_x$.*

We note a corollary, which may be proved more directly

**Corollary 4.2.13**
*The functor*

$$(-)|_{\mathcal{B}} \colon \mathrm{Sh}(X) \to \mathrm{PSh}(X; \mathcal{B})$$

*is full and faithful.*

*Proof.* This follows because it is a right-adjoint with a counit isomorphism by (2.4.41). □

**Corollary 4.2.14**
*There is an equivalence of categories*

$$\mathrm{Sh}(X; \mathcal{B}) \underset{(-)^+}{\overset{(-)|_{\mathcal{B}}}{\rightleftarrows}} \mathrm{Sh}(X)$$

## 4.3 Spaces with $k$-functions

Often sheaves arise in a very concrete way (for example the class of smooth functions on a manifold, see Section 4.4).

**Definition 4.3.1** (Space with $k$-functions)
*Let $X$ be a topological space and $k$ a field. We say $(X, \mathcal{O}_X)$ is a space with $k$-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*

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

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

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

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

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

**Proposition 4.3.2** (Stalks are local)
*Let $(X, \mathcal{O}_X)$ be a space with $k$-functions. For every $x \in X$ there is a well-defined evaluation map*

$$\mathcal{O}_{X,x} \longrightarrow k$$
$$[(U, \sigma)] \longrightarrow \sigma(x)$$

*Define*

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

*Then $\mathfrak{m}_x$ is the unique maximal ideal making $\mathcal{O}_{X,x}$ a local ring.*

**Definition 4.3.3** (Morphisms of spaces with $k$-functions)
*Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be spaces of $k$-functions. A morphism is a continuous mapping $f : X \to Y$ such that*

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

*This determines a category*

$$\mathfrak{Fns}/k$$

*and every such morphism $f$ determines a morphism of sheaves*

$$f^\sharp : \mathcal{O}_Y \to f_\star \mathcal{O}_X$$

**Proposition 4.3.4** (Morphisms are local on stalks)
*Let $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of spaces of $k$-functions. Then the composite*

$$\mathcal{O}_{Y,f(x)} \xrightarrow{f_x^\sharp} (f_\star \mathcal{O}_X)_{f(x)} \xrightarrow{4.2.10} \mathcal{O}_{X,x}$$

*is given by*

$$[(f^{-1}U, \sigma)] \to [(U, \sigma \circ f)]$$

*and is a local homomorphism.*

## 4.4 Differentiable Manifolds

We consider two types of manifold in parallel

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

**Definition 4.4.1** (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 $\mathbf{E}$. Such a homeomorphism is a pair $(U, \phi : U \to \mathbf{E})$, which we call a coordinate system. The functions $x_i = \pi_i \circ \phi$ are the "local coordinates" relative to this coordinate system.*

**Definition 4.4.2** (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 $\phi_\alpha \circ \phi_\beta^{-1} : \phi_\beta(U_\alpha \cap U_\beta) \to \phi_\alpha(U_\alpha \cap U_\beta)$ are $\mathcal{C}^\infty$ for all $\alpha, \beta$*
- *$\mathcal{F}$ is maximal with respect to these properties, namely if there is a $(U, \phi)$ which is compatible in the sense of the above, then it is already in $\mathcal{F}$.*

**Example 4.4.3** (Euclidean space)
**E** *is a canonical example of smooth manifold, where the differentiable structure is the maximal one containing the identity map on* **E**.

**Definition 4.4.4** (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 4.4.5** (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 $\phi$.*

**Definition 4.4.6** (Coordinate functions)
*Let $X$ be a smooth manifold and $(U, \phi)$ be a coordinate chart then the local coordinates $x_i$ are functions*

$$x_i : U \to k$$

*given by*

$$x_i(y) = \phi(y)_i \quad \forall y \in U$$

**Proposition 4.4.7** (Manifold = Space of $k$-functions)
*Let $X$ be a smooth manifold over $k$ then the pair $(X, \mathcal{O}_X)$ is a space of $k$-functions.*

*In particular $\mathcal{O}_{X,p}$ is a local ring with unique maximal ideal*

$$\mathfrak{m}_p := \{f_p \mid f(p) = 0\}$$

*such that $k \to \mathcal{O}_{X,p} \to \mathcal{O}_{X,p}/\mathfrak{m}_p =: k(p)$ is an isomorphism.*

**Definition 4.4.8** (Smooth maps)
*Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be smooth manifolds, then a smooth map is simply a morphism of a space of $k$-functions. That is a continuous map $f : X \to Y$ which induces a sheaf morphism*

$$f^\sharp : \mathcal{O}_Y \longrightarrow f_\star \mathcal{O}_X$$

*By (...) this induces a local homomorphism*

$$f_p^\sharp : \mathcal{O}_{Y,f(p)} \longrightarrow \mathcal{O}_{X,p}$$

Given a point $p \in X$, a chart $(U, \phi)$ and a vector $v \in k^n$ we may determine a directional derivative

$$D_{v,p} : \mathcal{O}_{X,p} \longrightarrow k$$

$$D_{v,p}(f_p) = \frac{d}{dt}(f \circ \phi^{-1})(\phi(p) + tv)|_{t=0} = \nabla(f \circ \phi^{-1})(\phi(p))v$$

A different chart and vector may determine the same functional on $\mathcal{O}_{X,p}$. So we define an equivalence relation which (we will show) still makes this correspondence well-defined and indeed injective.

**Definition 4.4.9** (Tangent Space)
*Let $X$ be a smooth manifold define the tangent space at $p \in X$ to be $T_pX$ the set of triples $(U, \phi, v)$ where $(U, \phi)$ is a chart and $v \in \mathbf{E}$, under the equivalence relation*

$$(U, \phi, v) \sim (V, \psi, w)$$

*if*

$$\nabla(\psi \circ \phi^{-1})(\phi p)v = w$$

*Proof.* This follows relatively easily from the multivariate version of the chain rule. □

If we fix coordinates then there is a canonical basis for $T_pX$

**Proposition 4.4.10** (Tangent Vectors as derivatives of germs)
*Each coordinate chart $(U, \phi)$ induces a bijection*

$$\begin{aligned} \mathbf{E} &\xrightarrow{\sim} T_pX \\ v &\xrightarrow{\sim} [(U, \phi, v)] \end{aligned}$$

*In particular $T_pX$ inherits the structure of a $k$-vector space and the given map is an isomorphism, and $\dim_k T_pX = n$. Let $x_i$ denote the coordinates for this chart, and denote the image of the standard basis as*

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

*Furthermore there is a canonical $k$-linear map*

$$\begin{aligned} T_pX &\to \mathcal{D}_pX \\ [(U, \phi, v)] &\to D_{v,p} \end{aligned}$$

*where $\mathcal{D}_pX$ is the set of $k$-linear functionals $D : \mathcal{O}_{X,p} \to k$ satisfying the Liebniz rule*

$$D(fg) = f(p)D(g) + g(p)D(f)$$

*Under this map*

$$\left.\frac{\partial}{\partial x_i}\right|_p f = \left.\frac{\partial(f \circ \phi^{-1})}{\partial x_i}\right|_p$$

*in the usual calculus sense, motivating the terminology.*

*Proof.* We show that the map $\mathbf{E} \to T_pX$ is surjective. Given a tangent vector $(V, \psi, w)$ and a coordinate chart $(U, \phi)$. Define $v = \nabla(\phi \circ \psi^{-1})(\psi(p))w$. Then $(V, \psi, w) \sim (U, \phi, v)$ and the map is surjective. We claim the map is injective for consider two tangent vectors $(U, \phi, v) \sim (U, \phi, v')$ then since the transition map is the identity $v = v'$.

We show that the map $T_pX \to \mathcal{D}_pX$ is well-defined. For suppose $(U, \phi, v) \sim (V, \psi, w)$ then by the chain rule

$$D_{w,p}(f_p) = \nabla(f \circ \psi^{-1})(\psi(p))w = \nabla(f \circ \phi^{-1})(\phi(p))\nabla(\phi \circ \psi^{-1})(\psi(p))w = \nabla(f \circ \phi^{-1})(\phi(p))v = D_{v,p}(f_p)$$

and so the mapping is well-defined. □

In order to devise a more intrinsic definition we may introduce the cotangent space

**Proposition 4.4.11** (Tangent and Cotangent space are dual)
*Let $X$ be a smooth manifold and $p \in X$ define the cotangent space*

$$T_p^\star X := \mathfrak{m}_p/\mathfrak{m}_p^2$$

*which is a $k$-vector space.*

- $\dim_k T_p^\star X = n$, *more precisely given a coordinate chart $(U, \phi)$ with local coordinates $x_i$ the following determines a basis*

$$(dx_i)_p := \overline{(x_i - x_i(p))_p}$$

- *There is a sequence of canonical isomorphisms*

$$\begin{array}{rcccl} T_pX & \xrightarrow{\sim} & \mathcal{D}_pX & \xrightarrow{\sim} & \mathrm{Hom}_k(T_p^\star X, k) \\ (U, \phi, v) & \longrightarrow & D_{v,p} & \longrightarrow & (\bar{f} \to D_{v,p}(f)) \end{array}$$

- *There is a corresponding perfect pairing*

$$\psi : T_pX \times T_p^\star X \to k$$

*with*

$$([(U, \phi, v)], \bar{f}_p) \to D_{v,p}(\bar{f}_p)$$

*for which $\psi_L$ is equal to the isomorphism described above. In particular there is a corresponding isomorphism*

$$\psi_R : T_p^\star X \xrightarrow{\sim} \mathrm{Hom}_k(T_pX, k)$$

*Proof.* The fact $\dim_k T_p^\star X = n$ follows essentially from the multivariate version of Taylor's Theorem and the fact the remainder term vanishes to second order.

Given a derivation $D$ define $\theta_D \in \mathrm{Hom}_k(T_p^\star X, k)$ by $\theta_D(\overline{f}) = D(f)$. Observe $D$ annihilates $\mathfrak{m}_p^2$ (since $D(fg) = f(p)D(g) + g(p)D(f)$) so this is well-defined. Further $\theta$ is clearly $k$-linear. Conversely given $\theta$ define $D_\theta(f) := \theta(\overline{f - f(p)})$. Observe that

$$(fg - f(p)g(p)) = (f - f(p))(g - g(p)) + f(p)(g - g(p)) + g(p)(f - f(p))$$

and as the first term lies in $\mathfrak{m}_p^2$ we see that $D_\theta(f)$ satisfies the product rule. It's easily seen that these are mutual inverses (as any $D$ annihilates $k$) so the second map is a bijection. Further it's clearly $k$-linear and so a vector space isomorphism.

Recall, given a chart $(U, \phi)$, that $T_pX$ has basis $\left.\frac{\partial}{\partial x_i}\right|_p$. It's clear that under the composite map stated that

$$\left.\frac{\partial}{\partial x_i}\right|_p (dx_j)_p = \delta_{ij}$$

which means by (3.4.102) that a basis of $T_pX$ is mapped to the basis $(dx_j)^\star$ of $\mathrm{Hom}_k(T_p^\star X, k)$. By (3.4.85) the composite is then an isomorphism. □

**Remark 4.4.12**
*We have exhibited natural isomorphism between the more concrete tangent space construction and the more algebraic version as dual to the cotangent space.*

**Proposition 4.4.13** (Functoriality of Cotangent Space)
*Let $f : X \to Y$ be a smooth map and $p \in X$ a point. Then there is a corresponding linear map*

$$\begin{aligned}(df)_p^\star = \overline{f_p^\sharp} : T^\star_{f(p)}Y &\longrightarrow T_p^\star X \\ \overline{g_{f(p)}} &\longrightarrow \overline{(g\circ f)_p} = \overline{f_p^\sharp}(\overline{g_{f(p)}})\end{aligned}$$

*Proof.* By Definition (4.4.8) the homomorphism $f_p^\sharp$ is local, that is $(f_p^\sharp)(\mathfrak{m}_p) \subseteq \mathfrak{m}_{f(p)}$. It's easy to show that $(f_p^\sharp)(\mathfrak{m}_p^2) \subseteq \mathfrak{m}^2_{f(p)}$. This shows that the given map is well-defined. □

A key property is that a smooth map of manifolds induces linear maps of the tangent space at every point. We demonstrate this for each construction of the tangent space.

**Proposition 4.4.14** (Functoriality of Tangent Space)
*Let $f : X \to Y$ be a smooth map and $p \in X$ a point. Then there are corresponding linear maps $df_p$, $\widetilde{df}_p$, $(df)_p^{\star\star}$ making the following diagram commute, for any pair of charts $(U,\phi)$, $(V,\psi)$ on $X$ and $Y$ respectively*

$$\begin{array}{ccccccc}
\mathbf{E} & \xrightarrow{\sim} & T_pX & \xrightarrow{\sim} & \mathcal{D}_pX & \xrightarrow{\sim} & \mathrm{Hom}_k(T_p^\star X, k) \\
{\scriptstyle v\to\nabla(\psi f\phi^{-1})(p)v}\downarrow & & \downarrow{\scriptstyle df_p} & & \downarrow{\scriptstyle \widetilde{df}_p} & & \downarrow{\scriptstyle (df)_p^{\star\star}} \\
\mathbf{F} & \xrightarrow{\sim} & T_{f(p)}Y & \xrightarrow{\sim} & \mathcal{D}_{f(p)}Y & \xrightarrow{\sim} & \mathrm{Hom}_k(T^\star_{f(p)}Y, k)
\end{array}$$

*given by*

$$\begin{aligned}df_p : (U,\phi,v) &\longrightarrow (V,\psi,\nabla(\psi f\phi^{-1})(\phi(p))v) \\ \widetilde{df}_p : D &\longrightarrow (g_{f(p)} \to D((g\circ f)_p)) \\ (df)_p^{\star\star} : \theta &\longrightarrow \theta \circ \overline{f_p^\sharp}\end{aligned}$$

*where $(df)_p^{\star\star}$ is the dual map to $(df)_p^\star$ defined in (4.4.13).*
*These maps are well-defined and independent of the local charts. Furthermore they are functorial in the sense that*

$$d(\mathbf{1}_X)_p = \mathbf{1}_{T_pX}$$

*and*

$$dg_{f(p)} \circ df_p = d(g\circ f)_p$$

*Let* $\left\{ \frac{\partial}{\partial x_i}\Big|_p \right\}_{i=1\ldots n}$ *and* $\left\{ \frac{\partial}{\partial y_j}\Big|_{f(p)} \right\}_{j=1\ldots m}$ *be the standard bases for $T_pX$ and $T_{f(p)}Y$ then*

$$df_p\left(\frac{\partial}{\partial x_i}\Big|_p\right) = \sum_{j=1}^m \frac{\partial(y_j\circ f\circ\phi^{-1})}{\partial x_i}(\phi(p))\ \frac{\partial}{\partial y_j}\Big|_{f(p)}$$

*and more succinctly has matrix representation*

$$\frac{\partial f^i}{\partial x_j}(p)$$

*with respect to the standard basis just given.*

*Proof.* Largely follows from the multivariate chain rule. □

**Definition 4.4.15** (Regular Point)
*Let $f : X \to k^d$ be a smooth map then we say $p$ is a* regular *point for $f$ if the differential map*

$$df_p : T_pX \longrightarrow T_pk^d$$

*is surjective (if and only if* $\mathrm{rank}(df_p) = d$ *by (2.2.13)). Otherwise it is a* critical *point. NB by the rank-nullity theorem we require* $\dim T_pX \leq d$ *for any regular point.*

*We say $c \in k^d$ is a* regular *value if $f^{-1}(c)$ is consists of regular points. When $f^{-1}(c)$ is empty then $c$ is automatically regular.*

It's possible to show that a regular level set $Y = f^{-1}(c)$ is an embedded (smooth) submanifold. We may identify the tangent space of $Y$ with $T_pY = \ker(df_p)$. When $X = \mathbb{R}^n$ then $\ker(df_p)$ has a geometric interpretation as lines on which $f$ is locally constant. The regular points are where $\ker(df_p)$ has the minimal possible rank.

## 4.5 Locally Ringed Spaces

It's possible to abstract the notion of space with $k$-functions, by embedding in the category of locally ringed spaces.

**Definition 4.5.1** (Locally ringed space)
*A locally ringed space is a pair $(X, \mathcal{O}_X)$ where $X$ is a topological space and $\mathcal{O}_X$ is a sheaf of rings over $X$, such that all the stalks $\mathcal{O}_{X,x}$ are local rings.*

*A morphism of locally ringed spaces consists of a pair*

$$(f, f^\sharp) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

*where $f : X \to Y$ is a continuous map and $f^\sharp : \mathcal{O}_Y \to f_\star \mathcal{O}_X$ is a morphism of sheaves such that for all $x \in X$ the composite map*

$$f_x^\sharp : \mathcal{O}_{Y,f(x)} \longrightarrow (f_\star \mathcal{O}_X)_{f(x)} \xrightarrow{4.2.10} \mathcal{O}_{X,x}$$

*is a local homomorphism. This constitutes a category $\mathfrak{Lrs}$.*

To complete the analogy we need to ensure that the ring $\mathcal{O}_X$ is a sheaf of $k$-algebras

**Definition 4.5.2** (Locally ringed space over a ring)
*Let $A$ be a commutative ring (e.g. a field $k$). A locally ringed space over $A$ is a locally ringed space $(X, \mathcal{O}_X)$ such that $\mathcal{O}_X$ is a sheaf of $A$-algebras.*

*This constitutes a category $\mathfrak{Lrs}/A$.*

**Proposition 4.5.3**
*There is a canonical full and faithful functor*

$$\mathfrak{Fns}/k \longrightarrow \mathfrak{Lrs}/k$$

*Proof.* This mapping is well-defined by (4.3.4) and is clearly faithful. We require to show that it is full. Suppose $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are two spaces with $k$-functions and we have a morphism of locally ringed spaces

$$(f, f^\sharp) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

Then it's enough to show $f^\sharp(\sigma) = \sigma \circ f$. Suppose $y = f(x)$ then

$$\begin{aligned} f^\sharp(\sigma)(x) - \sigma(y) &= f^\sharp(\sigma - \sigma(y))(x) \\ &= (f^\sharp(\sigma - \sigma(y)))_x(x) \\ &= f_x^\sharp(\sigma_y - \sigma(y))(x) \\ &= 0 \end{aligned}$$

because $f^\sharp$ is a $k$-algebra homomorphism, $\sigma_y - \sigma(y) \in \mathfrak{m}_y$ and $f_x^\sharp$ is a local homomorphism. □

# Chapter 5

# Algebraic Geometry

Throughout we assume that $k$ is perfect and contained in an algebraic closure $\bar{k}$. In particular we may assume any algebraic extension $K/k$ is contained in $\bar{k}$ and is separable. However we don't assume that $k$ is algebraically closed which makes the development of "classical algebraic geometry" slightly more complex than e.g. Hartshorne Chap I.

## 5.1 Affine Algebraic Sets over a Field

**Proposition 5.1.1**
*Let $A = k[X_1, \dots, X_n]$ be the polynomial ring in $n$-variables over a field $k$. For a set $S \subset k[X_1, \dots, X_n]$ and a field extension $K/k$ define the* ***zero-locus***

$$V_K(S) := \{\alpha \in K^n \mid f(\alpha) = 0 \quad \forall f \in S\}.$$

*Similarly for a subset $Y \subset K^n$ define*

$$I_K(Y) := \{f \in A \mid f(y) = 0 \quad \forall y \in Y\}$$

*Therefore we may consider the pair of maps*

$$\mathcal{P}(k[X_1, \dots, X_n]) \underset{V_K}{\overset{I_K}{\leftrightarrows}} \mathcal{P}(K^n)$$

*$V_K$ and $I_K$ constitute a Galois Connection*

a) *$V_K$ and $I_K$ are order-reversing*

b) *$S \subseteq I_K(V_K(S))$*

c) *$Y \subseteq V_K(I_K(Y))$*

*Furthermore (omitting the subscript $K$)*

4. *$VIV = V$ and $IVI = I$*
5. *$I(Y)$ is a radical ideal and $\sqrt{\langle S \rangle} \subseteq I(V(S))$*
6. *$V(S) = V(\langle S \rangle) = V(\sqrt{\langle S \rangle})$ and $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$*
7. *$\bigcap_i V(S_i) = V(\bigcup_i S_i)$ and $\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$*
8. *$\bigcap_i I_K(W_i) = I_K(\bigcup_i W_i)$*
9. *$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$*
10. *$V((0)) = K^n$ and $V(A) = \emptyset$*

*The sets of the form $V_K(\mathfrak{a})$ constitute the closed sets of a topology on $K^n$, denoted by $\mathrm{Zar}_k(K^n)$. In this case we have the following form for the topological closure*

$$V_K(I_K(Y)) = \overline{Y}$$

*Furthermore this restricts to a dual isomorphism*

$$\mathrm{Assoc}(k[X_1, \dots, X_n]; K) \underset{V_K}{\overset{I_K}{\leftrightarrows}} \mathrm{Zar}_k(K^n)$$

*where $\mathrm{Assoc}(k[X_1, \dots, X_n]; K)$ are the $K$-**associated ideals** (which are all radical), that is the ideals which are in the image of $I_K$.*

*Proof.* We make use of general results on Galois connections (Section 2.1.5), though many results may be shown more directly. The fact it's a Galois connection follows from Example 2.1.47.

1-3. These follow (2.1.43)

4. This follows from (2.1.45).

5. It's clear that $I(Y)$ is an ideal. It is radical because $K$ is reduced (...). The second statement follows from (2.1.46) by considering the closure operator $\sqrt{\langle - \rangle}$.

6. This follows from (2.1.46) by considering the closure operators $\sqrt{\langle - \rangle}$ and $\langle - \rangle$.

7. The first equality follows from (2.1.48). The second equality follows from (3.4.26).

8. This follows from (2.1.48).

9. Observe that $M_{X,x} = I(\{x\})$ is prime (because $K$ is an integral domain) and $x \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq M_{X,x}$. the result follows from (3.4.35) because $\mathfrak{a} \subseteq M_{X,x} \vee \mathfrak{b} \subseteq M_{X,x} \iff \mathfrak{ab} \subseteq M_{X,x} \iff \mathfrak{a} \cap \mathfrak{b} \subseteq M_{X,x}$

The family of sets $\mathrm{Zar}_k(K^n) := \mathrm{Im}(V_K)$ constitute the closed sets of a topology precisely because they are closed under arbitrary intersections and finite unions. Furthermore by (2.1.45) $V_K \circ I_K$ is a closure operator with image precisely the closed sets. Therefore by (2.1.38)

$$(V_K \circ I_K)(Y) = \bigcap_{Y \subseteq Z \in \mathrm{Zar}_k(K^n)} Z$$

which is the definition of the topological closure. □

For a fixed ideal $\mathfrak{a} \triangleleft k[X_1, \ldots, X_n]$ we may vary the field $K$ to obtain families of solutions in different fields.

**Definition 5.1.2** (Algebraic Set, Coordinate Ring and $K$-rational points)
*We say $X \subset k^n$ is an algebraic set if it is of the form $V(\mathfrak{a})$ for $\mathfrak{a} \triangleleft k[X_1, \ldots, X_n]$ an associated ideal.*

*Define the coordinate ring to be $k[X] := k[X_1, \ldots, X_n]/\mathfrak{a}$. Note $k[X]$ is a reduced f.g. $k$-algebra*

*For $K/k$ a field extension define the $K$-rational points to be*

$$X(K) := V_K(\mathfrak{a}) \subset K^n$$

*For a point $x \in X(K)$ define the degree of $x$ to be*

$$\deg(x) = \dim_k k(x_1, \ldots, x_n)$$

*Note if we have a tower $k \subset K_1 \ldots \subset K_n \subset \bar{k}$ then we have a tower of sets*

$$X(k) \subset X(K_1) \ldots \subset X(K_n) \subset X(\bar{k})$$

**Remark 5.1.3**
*$X = \mathbb{A}^n_k := V((0))$ is an algebraic set and $\mathbb{A}^n_k(K) = K^n$.*

**Proposition 5.1.4** (Coordinate ring as functions)
*Let $X = V(\mathfrak{a})$ be a $k$-algebraic set with coordinate ring $k[X]$. Then there is a well-defined embedding*

$$k[X] \hookrightarrow \mathrm{Fun}(X(K), K)$$
$$\bar{f} \longrightarrow \mathrm{ev}_x(f)$$

*given by function evaluation.*

For completeness we also consider sub-algebraic sets in the same way as before

**Definition 5.1.5** (Sub-algebraic sets)
*For $X$ an algebraic set with coordinate ring $k[X]$. For $\mathfrak{b} \triangleleft k[X]$ and $K/k$ algebraic define*

$$V_K(\mathfrak{b}; X) := \{x \in X(K) \mid f(x) = 0 \quad \forall f \in \mathfrak{b}\}$$

*Similarly for $Y \subset X(K)$ define*

$$I_K(Y; X) := \{f \in k[X] \mid f(y) = 0 \quad \forall y \in Y\}$$

*Note in the case $X = \mathbb{A}^n_k$ then this is exactly the same notion as before.*

We can reduce to the case $\mathbb{A}^n_k$ easily as follows

**Proposition 5.1.6** (Transitivity of algebraic sets)
*Let $X = V(\mathfrak{a})$ be an algebraic set and $\pi : k[X_1, \dots, X_n] \to k[X]$ be the canonical surjective homomorphism with kernel $\mathfrak{a}$. Then if we regard $X(K) \subset K^n$*

$$V_K(\mathfrak{b}; X) = V_K(\pi^{-1}(\mathfrak{b})) \cap X$$
$$I_K(Y \cap X; X) = \pi(I_K(Y))$$

*and in particular*

$$I_K(V_K(\mathfrak{b}; X); X) = \pi(I_K V_K(\pi^{-1}\mathfrak{b}))$$

**Proposition 5.1.7** (Galois connection on sub-algebraic set)
*Let $X = V(\mathfrak{a})$ be a $k$-algebraic set. Then for any field extension $K/k$ there is a Galois connection*

$$\mathcal{P}(k[X]) \underset{V_K(-;X)}{\overset{I_K(-;X)}{\leftrightarrows}} \mathcal{P}(X(K))$$

*which satisfies all the same properties as (5.1.1). The image of $V_K(-; X)$ constitutes a topology on $X(K)$, which we denote by $\mathrm{Zar}_k(X(K))$, whence we have a dual isomorphism*

$$\mathrm{Assoc}(k[X]; K) \underset{V_K(-;X)}{\overset{I_K(-;X)}{\leftrightarrows}} \mathrm{Zar}_k(X(K))$$

*where $\mathrm{Assoc}(k[X]; K)$ are the $K$- **associated ideals**, which are all radical. Furthermore the induced topology on $X(K)$ is precisely the subspace topology inherited from $\mathrm{Zar}_k(K^n)$.*

**Remark 5.1.8**
*When $\mathfrak{a} = (0)$ then this coincides with the previous definition.*

**Proposition 5.1.9** (Criterion for Irreducibility)
*Let $X = V_K(\mathfrak{a})$ be an algebraic set where $\mathfrak{a}$ is a $K$-associated ideal. Then $\mathfrak{a}$ is prime if and only if $X$ is an irreducible subset of $\mathrm{Zar}_k(K^n)$.*

*A similar statement applies replacing $K^n$ by an algebraic set.*

*Proof.* Suppose $X$ is not irreducible. Then we have $X \subseteq V_K(\mathfrak{b}) \cup V_K(\mathfrak{c})$ a non-trivial decomposition into closed subsets (and associated ideals). Then by the dual isomorphism we have also $\mathfrak{a} \subsetneq \mathfrak{b}$ and we may choose $f \in \mathfrak{b} \setminus \mathfrak{a}$ and similarly $g \in \mathfrak{c} \setminus \mathfrak{a}$. However $fg$ vanishes on $X$ ands so we have $fg \in \mathfrak{a}$. Therefore $\mathfrak{a}$ is not prime.

Conversely suppose $X$ is irreducible and $\mathfrak{bc} \subseteq \mathfrak{a}$. Then $X \subseteq V_K(\mathfrak{b}) \cup V_K(\mathfrak{c})$. By irreducibility we have $X \subseteq V_K(\mathfrak{b})$, whence applying $I_K(-)$ we see $\mathfrak{b} \subseteq I_K V_K(\mathfrak{b}) \subseteq \mathfrak{a}$ (since $\mathfrak{a}$ is an associated ideal). Therefore $\mathfrak{a}$ is prime. □

### 5.1.1 Nullstellensatz

For this section fix a **non-algebraically closed** base field $k$. We refine the statement of (5.1.7) when the extension field $K$ is $\bar{k}$. In this case we may establish a lattice isomorphism between maximal ideals (resp. radical ideals) and Galois orbits (resp. "closed sets"). Note that this is a more general form of the usual Nullstellensatz which requires $k = \bar{k}$. Clearly the statement of results in this section simplifies substantially in this case, because the action of $\mathrm{Aut}(\bar{k}/k)$ is then trivial.

First we establish a precise form of the so-called Weak Nullstellensatz

**Proposition 5.1.10** (Weak Nullstellensatz III)
*Let $X = V(\mathfrak{a})$ be a $k$-algebraic set with $k[X]$ the coordinate ring. There is a pair of mutually inverse maps*

$$\mathrm{Specm}(k[X]) \underset{V_{\bar{k}}(-;X)}{\overset{I_{\bar{k}}(-;X)}{\leftrightarrows}} X(\bar{k})/\mathrm{Aut}(\bar{k}/k)$$

*between maximal ideals of $k[X]$ and $\mathrm{Aut}(\bar{k}/k)$-orbits of $\bar{k}$-rational points. Explicitly we write*

$$I_{\bar{k}}([x]; X) = I_{\bar{k}}(\{x\}; X) =: M_{X,x}$$

*Proof.* First we claim that $I_{\bar{k}}([x]; X) = I_{\bar{k}}(\{x\}; X)$. For if $x = \sigma(y)$ then $f(y) = \sigma(f(x))$ and $f(y) = 0 \iff f(x) = 0$. This also holds when $X = k^n$.

Let $M_{k^n,x} = I_{\bar{k}}(\{x\})$ then by Weak Nullstellensatz II it is maximal. Further $x \in X(\bar{k}) \implies \{x\} \subseteq V_{\bar{k}}(\mathfrak{a}) \implies \mathfrak{a} \subseteq M_{k^n,x}$. Consider the canonical surjective homomorphism with kernel $\mathfrak{a}$

$$\pi : k[X_1, \dots, X_n] \to k[X]$$

then by (5.1.6)

$$M_{X,x} = \pi\left(M_{k^n,x}\right) \quad M_{k^n,x} = \pi^{-1}(M_{X,x})$$

and by (3.4.46) $M_{X,x}$ is a maximal ideal. If $M_{X,x} = M_{X,y}$ then $M_{k^n,x} = M_{k^n,y}$ which by the Weak Nullstellensatz implies $x = \sigma(y)$, and therefore the map is injective.

Similarly suppose $M_X \lhd k[X]$ is a maximal ideal then $M := \pi^{-1}(M_X)$ is a maximal ideal (3.4.46) containing $\mathfrak{a}$. By the Weak Nullstellensatz I it is of the form $M_{k^n,x}$ for $x \in \bar{k}^n$. And because $\mathfrak{a} \subseteq M_{k^n,x}$ we have $x \in X(\bar{k})$. Furthermore $M_X = \pi(M_{k^n,x}) = M_{X,x}$, and the map is surjective as required.

Note $I_{\bar{k}}V_{\bar{k}}(M_{X,x})$ is an ideal containing $M_{X,x}$. By maximality it is either $M_{X,x}$ or $k[X]$. But as $V_{\bar{k}}(M_{X,x})$ is non-empty it must be the former (since 1 does not have any zeros). Therefore the maps given are mutual inverses and $V_{\bar{k}}(M_{X,x}) = [x]$. □

**Corollary 5.1.11** (Weak Nullstellensatz IV)
*Every proper ideal $\mathfrak{b} \lhd k[X]$ has a common zero in $X(\bar{k})$, i.e. $V_{\bar{k}}(\mathfrak{b}) \neq \emptyset$.*

*In particular when $k = \bar{k}$ then $\mathfrak{b}$ proper implies $V(\mathfrak{b}) \neq \emptyset$.*

*Proof.* By (3.4.34) $\mathfrak{b}$ is contained in a maximal ideal $\mathfrak{m}$. By (5.1.10) it is of the form $M_{X,x}$ for $x \in X(\bar{k})$. By definition $x$ is a zero of $\mathfrak{b}$. □

**Proposition 5.1.12** (Characterization of closed set)
*Let $\mathfrak{b} \lhd k[X]$ and $x \in X(\bar{k})$ then*

$$x \in V_{\bar{k}}(\mathfrak{b}) \iff \mathfrak{b} \subseteq M_{X,x}$$

*In particular*

$$I_{\bar{k}}V_{\bar{k}}(\mathfrak{b}) = \bigcap_{\mathfrak{b}\subseteq\mathfrak{m}} \mathfrak{m} = \sqrt{\mathfrak{b}}^J$$

*Proof.* This follows by definition and the correspondence between maximal ideals and $\bar{k}$-rational points. □

Furthermore we have noted before that in general $\sqrt{\mathfrak{a}} \subseteq IV(\mathfrak{a})$. The more refined version is that these are equal when $K = \bar{k}$. The proof uses the Rabinowitsch Trick, which we slightly abstract here.

**Lemma 5.1.13** (Rabinowitsch Trick)
*Let $\mathfrak{a} \lhd A$ and $f \in A$. Consider the ring $B = A[Y]$. If $\mathfrak{a}B + (1 - Yf) = B$ then $f \in \sqrt{\mathfrak{a}}$.*

*Proof.* The hypothesis implies

$$1 = (1 - Yf)g(Y) + ah(Y)$$

for $a \in \mathfrak{a}$ and $h(Y) \in A[Y]$. Consider the quotient map $\bar{\cdot} : A \to A/\mathfrak{a}$ and the corresponding map $A[Y] \to (A/\mathfrak{a})[Y]$. Applying this to the above shows $1 - Y\bar{f}$ is invertible in $(A/\mathfrak{a})[Y]$. So by (3.6.3) $\bar{f}$ is nilpotent in $(A/\mathfrak{a})$ whence $f \in \sqrt{\mathfrak{a}}$. □

**Proposition 5.1.14** (Strong Nullstellensatz)
*Let $\mathfrak{b} \lhd k[X]$ then*

$$I_{\bar{k}}V_{\bar{k}}(\mathfrak{b}) = \sqrt{\mathfrak{b}} = \bigcap_{\mathfrak{b}\subseteq\mathfrak{m}} \mathfrak{m} = \sqrt{\mathfrak{b}}^J$$

*Proof.* Note the second equality has already been demonstrated in (5.1.12).

First we consider the case $X = k^n$ and $k[X] = k[X_1, \ldots, X_n]$. Let $\mathfrak{a} \lhd k[X]$ and choose $f \in I_{\bar{k}}V_{\bar{k}}(\mathfrak{a})$. Consider the ring $B := k[X_1, \ldots, X_n, Y]$ and the ideal $\widetilde{\mathfrak{a}} = \mathfrak{a}B + (1 - Yf)$. Clearly this has no zeros in $\bar{k}^{n+1}$, so by the Weak Nullstellensatz it is not proper. By the previous Lemma $f \in \sqrt{\mathfrak{a}}$ as required. The reverse inclusion is clear.

Now suppose that $X = V(\mathfrak{a})$, $k[X] = k[X_1, \ldots, X_n]/\mathfrak{a}$ and $\mathfrak{b} \lhd k[X]$ is proper. Using Propositions (5.1.6) and (3.4.42) together with the result just proven, shows

$$I_{\bar{k}}(V_{\bar{k}}(\mathfrak{b}; X); X) = \pi(I_{\bar{k}}V_{\bar{k}}(\pi^{-1}\mathfrak{b})) = \pi(\sqrt{\pi^{-1}(\mathfrak{b})}) = \sqrt{\mathfrak{b}}$$

where $\pi : k[X_1, \ldots, X_n] \to k[X]$ is canonical surjective morphism. □

**Corollary 5.1.15**
*Let $k[X]$ be any finitely generated reduced $k$-algebra, then $k[X]$ is a Jacobson ring, i.e.*

$$\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}}^J$$

**Corollary 5.1.16**
*Let $X = V(\mathfrak{a})$ be a $k$-algebraic set. Then the $\bar{k}$-associated ideals are precisely the radical ideals and there is a dual isomorphism between radical ideals and "Zariski"-closed subsets of $X(\bar{k})$.*

$$\mathrm{Rad}(k[X]) \underset{V_{\bar{k}}(-;X)}{\overset{I_{\bar{k}}(-;X)}{\leftrightarrows}} \mathrm{Zar}_k(X(\bar{k}))$$

*under which*

- *maximal ideals correspond to $\mathrm{Aut}(\bar{k}/k)$-orbits of single points $x \in X(\bar{k})$*
- *prime ideals correspond to irreducible subsets of $X(\bar{k})$*

*Proof.* The content of the Strong Nullstellensatz is precisely that $I_{\bar{k}}(-;X) \circ V_{\bar{k}}(-;X) = \mathbf{1}$. The other direction was already proven so we have a dual order isomorphism. The statement about maximal ideals was already shown in (5.1.10). □

**Remark 5.1.17**
*When $k = \bar{k}$ the $\mathrm{Aut}(\bar{k}/k)$-orbits are just the singleton sets, and we obtain the "classical" nullstellensatz results.*

### 5.1.2 Structure Sheaf for Algebraic Sets with $k = \bar{k}$

For this section assume $k = \bar{k}$ is algebraically closed.

**Definition 5.1.18** (Principal Open Set)
*For $X = V(\mathfrak{a})$ and $f \in k[X]$, define the principal open set*

$$D(f) := \{x \in X(k) \mid f(x) \neq 0\} = X \setminus V(f)$$

**Lemma 5.1.19**
*The principal open sets form a basis for the Zariski topology, closed under finite intersection.*

*Proof.* Let $U = X \setminus V(\mathfrak{b})$ be an open set. Then $f \in \mathfrak{b} \implies V(\mathfrak{b}) \subseteq V(f) \implies D(f) \subseteq U$ as required. Furthermore $V(\mathfrak{b}) = \bigcap_{f \in \mathfrak{b}} V(f)$ whence $\bigcup_{f \in \mathfrak{b}} D(f) = U$. □

**Definition 5.1.20** (Structure Sheaf)
*Let $X = V(\mathfrak{a})$ be an algebraic set. We say a function $f : U \to k$ is regular at $x \in X$ if there exists $g, h \in k[X]$ and a neighbourhood $V \ni x$ such that*

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

*We say $f$ is regular on $U$ if it is regular at all $x \in U$. Then we may define the structure sheaf*

$$\mathcal{O}_X(U) := \{f : U \to k \mid f \text{ regular }\}$$

*It's clear that by definition this is a sheaf, and furthermore that $(X, \mathcal{O}_X)$ is a space of functions.*

**Proposition 5.1.21**
*Let $X = V(\mathfrak{a})$ be an algebraic set and $f \in k[X]$. There is a canonical map*

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

*which is an isomorphism.*

*Proof.* The map is given by

$$\frac{a}{f^n} \longrightarrow (y \to a(y)f(y)^{-n})$$

Note that

$$\begin{aligned}
\frac{a}{f^n} = \frac{b}{f^m} &\iff f^r(f^m a - f^n b) \quad \text{some } r > 0 \\
&\iff f^r(y)(f^m(y)a(y) - f^n(y)b(y)) \quad \forall y \in X \\
&\iff f^r(y)(f^m(y)a(y) - f^n(y)b(y)) \quad \forall y \in D(f) \\
&\iff a(y)f(y)^{-n} = b(y)f(y)^{-m} \quad \forall y \in D(f)
\end{aligned}$$

which shows that the map is both well-defined and injective.

In order to show that the given map is surjective, consider $\sigma \in \mathcal{O}_X(D(f))$

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

If $f \in J$ then $\phi(f)\sigma = \phi(g/f^r) \implies \sigma = \phi(g/f^{r+1})$ as required.

Suppose $f \notin J$ then as $J$ is proper it's contained in a maximal ideal $\mathfrak{m}_x$. Observe $x \in D(f)$. By definition there is an open neighbourhood $x \in W \subseteq D(f)$ and elements $h_1, h_2$ such that

$$\sigma(y) = \frac{h_1(y)}{h_2(y)} \quad \forall y \in W$$

Now choose $h_3$ such that $x \in D(h_3) \subseteq W$. then $\phi(h_3 h_2)\sigma = \phi(h_1 h_3)$. Therefore $h_3 h_2 \in J$. But by construction $h_3(x)h_2(x) \neq 0$ a contradiction. □

**Proposition 5.1.22**
*Let $X = V(\mathfrak{a})$ be an algebraic set then the pair*

$$(X, \mathcal{O}_X(U))$$

*constitutes a space of k-functions.*

### 5.1.3 Morphisms of Algebraic Sets with $k = \bar{k}$

### 5.1.4 Rational points over finite fields and the Zeta Function

For this section let $k = \mathbb{F}_p$ by the finite field of order $p$ and $\phi : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ be the Frobenius automorphism. Let $k_d = \mathbb{F}_{p^d}$ be the unique subfield of $\overline{\mathbb{F}_p}$ order $p^d$ (3.15.72).

By (3.15.73) we have a tower of Galois extensions

$$k \subset k_d \subset \bar{k}$$

$\mathrm{Gal}(\bar{k}/k)$ acts on each, restricting to an action on $\mathrm{Gal}(k_d/k)$ on $k_d/k$ preserving degree.

Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n_k$ be an algebraic set (defined over $k$), then we have an inclusion

$$X(k) \subset X(k_d) \subset X(\bar{k})$$

It will also be useful to partition solutions more precisely by degree :

$$X_d := \{x \in X(\bar{k}) \mid \deg(x) = d\}.$$

The following Lemma characterizes these sets more precisely.

**Lemma 5.1.23**
*Let $x \in X(\bar{k})$ then*

$$\deg(x) = \mathrm{lcm}(\deg_k(x_i))$$

*Furthermore for $d > 0$*

$$\deg(x) \mid d \iff x \in X(k_d) \iff \phi^d(x) = x$$

*and $\mathrm{Gal}(k_d/k)$ acts freely on $X_d$.*

*Proof.* Let $k(x) := k(x_1, \ldots, x_n)$, then recall ((5.1.2)) by definition that $\deg(x) = [k(x) : k] = d$ for some $d$. Similary define $d_i := \deg(x_i) = [k(x_i) : k]$.

Note $k(x_i) \subseteq k(x)$ is a subfield therefore by (3.15.4) we have $d_i \mid d$, so $\mathrm{lcm}_i(d_i) \mid d$.

Let $d' := \mathrm{lcm}_i(d_i)$ then by (3.15.72) we have $k(x_i) \subseteq k_{d'}$ which implies $k(x) \subseteq k_{d'}$. By (3.15.4) again $d' \mid d$ and $d = d'$.

For the second statement

$$\begin{aligned}
\deg(x) \mid d &\iff \mathrm{lcm}(\deg_k(x_i)) \mid d \\
&\iff \deg_k(x_i) \mid d \quad \forall i \\
&\iff x_i \in k_d \quad \forall i \quad (3.15.75) \\
&\iff \phi^d(x_i) = x_i \quad \forall i \quad (3.15.75) \\
&\iff \phi^d(x) = x
\end{aligned}$$

By (3.15.21) $\mathrm{Gal}(k_d/k)$ preserves degree and therefore acts on $X_d$. Recall $\mathrm{Gal}(k_d/k) = \langle\phi\rangle$ is a cyclic group of order $d$. Suppose $x \in X_d$ and $\phi^r(x) = x$ for $0 < r < d$. Then we have shown $x \in X(k_r)$, which implies $d = \deg(x) \mid r$ and therefore $d \mid r$ a contradiction. Therefore $\mathrm{Gal}(k_d/k)$ acts freely on elements of degree exactly $d$. □

As $\mathrm{Gal}(k_d/k)$ acts freely on $X_d$ then by (3.3.32) the orbits have order $d$. The restriction map

$$\mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Gal}(k_d/k)$$

is surjective by (3.15.53), and the two actions on $X_d$ commute. Therefore $X_d$ also has orbits of order $d$ under the action of $\mathrm{Gal}(\bar{k}/k)$. Furthermore it's clear that

$$\#X(k_m) = \sum_{d|m} \#X_d \,.$$

Recall there is a bijection preserving degree

$$X(\bar{k})/\,\mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Specm}(k[X])$$

Then since the orbits of $X_d$ have order $d$ we have $\#X_d = d \times \#B_d$ where

$$B_d = \{\mathfrak{m} \in \mathrm{Specm}(k[X]) \mid \deg(\mathfrak{m}) = d\}$$

and

$$\#X(k_m) = \sum_{d|m} d \times \#B_d$$

**Proposition 5.1.24** (Zeta function of an algebraic set over a finite field)
*Formally as elements of the power series ring $\mathbb{Q}[[T]]$ we have*

$$Z(X,T) := \prod_{\mathfrak{m}\in\mathrm{Specm}(k[X])} (1 - T^{\deg(\mathfrak{m})})^{-1} = \exp\left(\sum_{m=1}^{\infty} \frac{\#X(k_m)}{m} T^m\right)$$

*Proof.* Let $Z(X,T)$ be the right hand side then

$$\begin{aligned}
\log(Z(X,T)) &= \sum_{m=1}^{\infty} \#X(k_m)\frac{T^m}{m} \\
&= \sum_{m=1}^{\infty}\sum_{d|m}(d \times \#B_d)\frac{T^m}{m} \\
&= \sum_{d=1}^{\infty} \#B_d \sum_{r=1}^{\infty} \frac{T^{rd}}{r} \\
&= -\sum_{d=1}^{\infty} \#B_d \log(1 - T^d)
\end{aligned}$$

□

**Example 5.1.25**
*For $X(k) = k^n$ we have $\#X(k_m) = p^{mn}$. Then*

$$Z(X,T) = \exp\left(\sum_{n=1}^{\infty} \frac{p^{mn}T^m}{m}\right) = \exp(-\log(1 - p^n T)) = \frac{1}{1 - p^n T}$$

### 5.1.5 Cotangent Space (Affine Variety)

Analogously to the case of differential manifolds we may construct the **cotangent space** in the algebraic setting. This may be motivated by showing it is dual to a more geometrically constructed **tangent space**. But the advantage of this approach is that it is clearly an algebraic invariant and is well-defined for $\bar{k}$-rational points. Furthermore it may be generalized to non-affine case by localizing (...).

**Definition 5.1.26** (Maximal Ideal at a point)
*Let $X = V(\mathfrak{a})$ be an algebraic set with coordinate ring $k[X]$. Recall for $x \in X(\bar{k})$ the ideal*

$$M_{X,x} = \{f \in k[X] \mid f(x) = 0\}$$

*is maximal by (3.22.5). There is an associated **residue field***

$$k \to k(x) := k[X]/M_{X,x}$$

*When $X = k^n$ and $x \in X(k)$ is $k$-rational we have by (3.7.5) a natural grading around $x$*

$$M_{k^n,x} = (X_1 - x_1, \ldots, X_n - x_n) = \bigoplus_{n \geq 1} k[X_1, \ldots, X_n]^{(n,x)}$$

*and*

$$(M_{k^n,x})^r = \bigoplus_{n \geq r} k[X_1, \ldots, X_n]^{(n,x)}$$

This allows us to define the cotangent space analogously to the differential manifold case

**Definition 5.1.27** (Cotangent Space)
*Let $X = V(\mathfrak{a})$ be an algebraic set with coordinate ring. Define the cotangent space at $x \in X(\bar{k})$ by*

$$T_x^\star X := M_{X,x}/M_{X,x}^2$$

*which is a $k(x)$-vector space, along with a canonical surjective homomorphism*

$$d_x : M_{X,x} \longrightarrow T_x^\star X$$

*Further in the case $X = k^n$ and $x \in X(k)$ we have the following isomorphism*

$$k[X_1, \ldots, X_n]^{(1,x)} \xrightarrow{\sim} T_x^\star k^n$$

*and $\dim_k T_k^\star k^n = n$.*

We may show that cotangent space of an algebraic set is a quotient of the cotangent space of $k^n$.

**Proposition 5.1.28** (Cotangent of algebraic subset is quotient)
*Let $X = V(\mathfrak{a})$ be an algebraic set and $x \in X(\bar{k})$. First note that $\mathfrak{a} \subset M_{k^n,x}$ by definition. There is a canonical isomorphism of $k$-modules*

$$\begin{array}{rcl} T_x^\star k^n/(d_x\mathfrak{a}) & \xrightarrow{\sim} & T_x^\star X \\ d_x F + d_x\mathfrak{a} & \longrightarrow & d_x(F + \mathfrak{a}) \end{array}$$

*where $F \in M_{X,x}$ and*

$$d_x\mathfrak{a} := \{d_x F \mid F \in \mathfrak{a}\}$$

*Note that $T_x^\star k^n \cong k[X_1, \ldots, X_n]^{(1,x)}$ and $d_x\mathfrak{a} \cong \mathfrak{a}^{(1,x)}$ so that*

$$\dim_k T_x^\star X = n - \dim_k \mathfrak{a}^{(1,x)}.$$

*Proof.* Consider the diagram

$$\begin{array}{ccc} M_{k^n,x} & \xrightarrow{\pi} & M_{X,x} \\ \downarrow{\scriptstyle d_x} & & \downarrow{\scriptstyle d_x} \\ T_x^\star k^n & \xrightarrow{i_X^\star} & T_x^\star X \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \sim} & \\ T_x^\star k^n/d_x\mathfrak{a} & & \end{array}$$

First observe that $\pi$ is surjective. Then $\ker(d_x \circ \pi) = \pi^{-1}(M_{X,x}^2) = \mathfrak{a} + M_{k^n,x}^2$ (...). Therefore by the first isomorphism theorem $i_X^\star$ exists and has $\ker(i_X^\star) = d_x(\mathfrak{a} + M_{k^n,x}^2) = d_x\mathfrak{a}$. Similarly the bottom arrow exists and is an isomorphism, by the first isomorphism theorem.

□

**Example 5.1.29**
*Consider the case $X = V(\mathfrak{a})$ with $\mathfrak{a} = (F)$ for $F \in k[X_1, \ldots, X_n]$. Then*

$$\mathfrak{a}^{(1,x)} = \left\langle \sum_{i=1}^n \frac{\partial F}{\partial X_i}(x)(X_i - x) \right\rangle$$

*and $\dim_k \mathfrak{a}^{(1,x)} = 1$ unless*

$$\frac{\partial F}{\partial X_1}(x) = \ldots = \frac{\partial F}{\partial X_n}(x) = 0$$

*in which case $\dim_k \mathfrak{a}^{(1,x)} = 0$. Therefore $\dim_k T_x^\star X = n - 1$ or $n$ accordingly.*

### 5.1.6 Tangent Space (for $k$-rational points on an Affine Variety)

For points which are $k$-rational we may motivate the construction of cotangent space, by showing it's naturally dual to the so-called "tangent" space.

**Proposition 5.1.30**
*Let $F \in k[X_1, \dots, X_n]$ and $g_i \in k[T]$. Then*

$$\frac{d}{dT}F(g_1(T), \dots, g_n(T)) = \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(g_1(T), \dots, g_n(T))g_i'(T)$$

Let $F \in k[X_1, \dots, X_n]$ and $x, v \in k^n$ Then we claim the following are equivalent

- $F(x) = 0$ and $0 = \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(x)v_i$
- $P(T) := F(x + vT)$ has zero as a root of multiplicity $\geq 2$, i.e. $v_T(P) \geq 2$.
- $P(0) = P'(0) = 0$

In this case we say the line $L_{x,v} = \{x + vt \mid t \in k\}$ is tangent to $X = V(F)$ at $x$.

**Definition 5.1.31** (Explicit Tangent Space)
*For $X = V(\mathfrak{a})$ and $x \in X(k)$ define the linear subspace of $k^n$ by*

$$T_xX = \{v \in k^n \mid \sum_{i=1}^{n} v_i \frac{\partial F}{\partial X_i}(x) = 0 \quad \forall F \in \mathfrak{a}\}$$

*In particular for $X = k^n$ define*

$$T_xk^n = k^n$$

*so that $T_xX \subset T_xk^n$ is a $k$-subspace.*

Geometrically this is an affine hyperplane at $x$ which is tangent to the algebraic set $X$. We demonstrate that it is naturally dual to the cotangent space previously defined.

**Proposition 5.1.32** (Tangent and Cotangent spaces are dual)
*Let $X = V(\mathfrak{a})$ and $x \in X(k)$. Then there is a perfect pairing*

$$\psi_{X,x} : T_x^\star X \times T_xX \to k$$

*given by*

$$(d_x(F + \mathfrak{a}), v) \longrightarrow \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(x)v_i$$

*for $F \in M_{k^n,x}$.*

*Proof.* First consider the case $X = k^n$. Then we claim there is a pairing

$$\psi_{k^n} : (d_xF, v) \longrightarrow \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(x)v_i$$

Then $(\psi_{k^n})_L$ is well-defined and injective for $d_xF = d_xG \iff d_x(F-G) = 0 \iff (F-G) \in M_{k^n,x}^2 \iff \frac{\partial F}{\partial X_i}(x) = \frac{\partial G}{\partial X_i}(x)$ for all $i$ (...). As the spaces have the same dimension, $(\psi_{k^n})_L$ is an isomorphism and $\psi_{k^n}$ is perfect.

Define the subspace $d_x\mathfrak{a} := \{d_xF \mid F \in \mathfrak{a}\}$ of $T_x^\star k^n$. Then by definition $T_xX = (d_x\mathfrak{a})^\perp$ is an orthogonal complement with respect to $\psi_{k^n}$. By (3.4.112) there is then a canonical perfect pairing

$$T_x^\star k^n/(d_x\mathfrak{a}) \times T_xX \to k$$

$$(d_xF + d_x\mathfrak{a}, v) \to \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(x)v_i$$

Finally by (5.1.28) there is an isomorphism

$$\begin{array}{ccc} T_x^\star k^n/(d_x\mathfrak{a}) & \xrightarrow{\sim} & T_x^\star X \\ (d_xF + d_x\mathfrak{a}) & \longrightarrow & d_x(F + \mathfrak{a}) \end{array}$$

which may be combined with the perfect pairing just constructed, to yield $\psi_{X,x}$. □

## 5.2 Abstract Affine Varieties and Schemes

We observed that for $X$ an (affine) algebraic set that the coordinate ring $k[X]$ is an algebraic invariant which quite rigidly determines the regular functions. The idea behind the abstract approach is to reverse the direction, and construct a geometric object from an algebraic one in an "essentially inverse" way. First this will be just reduced $k$-algebras, and secondly for schemes this will be for arbitrary commutative rings.

### 5.2.1 Maximal Spectrum

We observed that for $X$ an algebraic set that $k[X]$ is a finitely generated reduced $k$-algebra. It's possible to reverse the construction in some sense

**Definition 5.2.1** (Maximal Spectrum)
*Let $A$ be a ring. Define*

$$\operatorname{Specm}(A) := \{[\mathfrak{m}] \mid \mathfrak{m} \lhd A\}$$

*For $S \subseteq A$ define*

$$V(S) := \{[\mathfrak{m}] \mid S \subseteq \mathfrak{m}\}$$

*and for $Y \subseteq \operatorname{Specm}(A)$ define*

$$I(Y) = \bigcap_{[\mathfrak{m}] \in Y} \mathfrak{m}$$

**Proposition 5.2.2** (Properties of Maximal Spectrum)
*Consider $(\operatorname{Specm}(A), A)$ for $A$ a finitely-generated reduced $k$-algebra (or more generally a Jacobson Ring) then we have a Galois connection*

$$\mathcal{P}(A) \underset{V}{\overset{I}{\leftrightarrows}} \mathcal{P}(\operatorname{Specm}(A))$$

*That is*

- *$V$ and $I$ are order-reversing*
- *$S \subseteq I(V(S))$*
- *$Y \subseteq V(I(Y))$*

*and furthermore*

- *$I(Y)$ is a radical ideal*
- *$V(S) = V(\langle S \rangle) = V(\sqrt{\langle S \rangle})$*
- *$IV(\mathfrak{a}) = \sqrt{\mathfrak{a}}$*
- *$\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$*
- *$\bigcap_i I(W_i) = I(\bigcup_i W_i)$*
- *$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$*

*In particular the closed sets $V(\mathfrak{a})$ induce a topology (Zariski) on $\operatorname{Specm}(A)$. All these properties hold for a general ring $A$, except we may have a proper inclusion*

$$\sqrt{\mathfrak{a}} \subsetneq IV(\mathfrak{a})$$

*Proof.* This follows exactly the same lines as (5.1.1). The relation $IV(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ results from the Strong Nullstellensatz, or from the definition of a Jacobson ring. □

**Proposition 5.2.3** (Maximal ideals are closed)
*All the points of $\operatorname{Specm}(A)$ are closed.*

*Proof.* $V(\mathfrak{m}) = \{[\mathfrak{m}]\}$ by maximality. □

We see that this construction is equivalent

**Proposition 5.2.4**
*Let $X = V(\mathfrak{a})$ be an algebraic set with coordinate ring $k[X]$. If $k = \bar{k}$ then there is a commutative diagram*

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

*where the left arrow is the bijection described in (3.22.5) and is in fact a homeomorphism. For general $k$ we still have a commutative diagram*

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

### 5.2.2 Prime Spectrum

The maximal spectrum construction is only useful when $A$ is a Jacobson ring, considering the prime spectrum allows the construction to work for general rings.

**Definition 5.2.5** (Prime Spectrum)
*Let $A$ be a ring, then define the prime spectrum of $A$ to be the set*

$$\mathrm{Spec}(A) = \{[\mathfrak{p}] \mid \mathfrak{p} \lhd A\}$$

*For $\mathfrak{a} \lhd A$ define*

$$V(\mathfrak{a}) := \{[\mathfrak{p}] \mid \mathfrak{a} \subseteq \mathfrak{p}\}$$

*and for $Y \subseteq \mathrm{Spec}(A)$ define*

$$I(Y) = \bigcap_{[\mathfrak{p}] \in Y} \mathfrak{p}$$

**Proposition 5.2.6** (Properties of Prime Spectrum)
*Consider $(\mathrm{Spec}(A), A)$ for a ring $A$ then we have a Galois connection*

$$\mathcal{P}(A) \underset{V}{\overset{I}{\leftrightarrows}} \mathcal{P}(\mathrm{Spec}(A))$$

*That is*

- *$V$ and $I$ are order-reversing*
- *$S \subseteq I(V(S))$*
- *$Y \subseteq V(I(Y))$*

*and furthermore*

- *$I(Y)$ is a radical ideal*
- *$V(S) = V(\langle S \rangle) = V(\sqrt{\langle S \rangle})$*
- *$IV(\mathfrak{a}) = \sqrt{\mathfrak{a}}$*
- *$\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$*
- *$\bigcap_i I(W_i) = I(\bigcup_i W_i)$*
- *$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$*

*In particular the closed sets $V(\mathfrak{a})$ induce a topology (Zariski) on $\mathrm{Spec}(A)$. Furthermore*

- *$VI(Y) = \overline{Y}$*

*Proof.* The proof is the same as (5.2.2), except for the relation $IV(\mathfrak{a}) = \mathfrak{a}$ which is precisely (3.4.39).

Last bit TODO □

The Zariski topology differs to the maximal case because not all points are closed. More precisely

**Proposition 5.2.7** (Closed points are maximal ideals)
$[\mathfrak{p}] \in \operatorname{Spec}(A)$ *is a closed point if and only if* $\mathfrak{p}$ *is a maximal ideal. In other words*

$$\operatorname{Specm}(A) = \operatorname{Spec}(A)^{\circ}$$

*More precisely*

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}) = \{\mathfrak{q} \mid \mathfrak{q} \supseteq \mathfrak{p}\} \tag{5.1}$$

*Proof.* Equation (5.1) follows from the definitions and the fact $V(\mathfrak{p}) = VI(\{\mathfrak{p}\}) = \overline{\{\mathfrak{p}\}}$ from the final result in (5.2.6). Then by (4.1.10) $\{\mathfrak{p}\}$ is closed if and only $\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}}$ if and only if $\mathfrak{p}$ is contained in no proper prime ideals, i.e. if and only if it is maximal (see **??**). □

Similarly to (5.1.9) we may characterize irreducible subsets of $\operatorname{Spec}(A)$ as the zero-locus of prime ideals

**Proposition 5.2.8** (Irreducible subsets)
*Let* $A$ *be a ring (resp. Jacobson ring) and* $X = \operatorname{Spec}(A)$ *(resp.* $\operatorname{Specm}(A)$*).*

*A closed subset* $Y = V(\mathfrak{b})$ *is irreducible if and only if* $\sqrt{\mathfrak{b}}$ *is prime.*

*Proof.* The proof is formally the same as (5.1.9). □

**Corollary 5.2.9**
$\operatorname{Spec}(A)$ *(resp.* $\operatorname{Specm}(A)$*) is irreducible if and only if* $A$ *is irreducible as a ring (i.e.* $\mathfrak{N}(A)$ *is prime).*

*Proof.* Note $X = V((0))$ and $\mathfrak{N}(A) = \sqrt{(0)}$ so the result follows from (5.2.8) □

We may summarize in a correspondence much as in the classical case

**Corollary 5.2.10** (Closed set and ideal correspondence)
*Let* $A$ *be a ring (resp. Jacobson ring) and* $X = \operatorname{Spec}(A)$ *(resp.* $\operatorname{Specm}(A)$*) then there is a bijective correspondence*

$$\{Y \subset X \text{ closed }\} \underset{I}{\overset{V}{\rightleftarrows}} \{\mathfrak{a} \lhd A \text{ radical }\}$$

*under which*

- *Prime ideals correspond to irreducible closed subsets*
- *Minimal prime ideals correspond to irreducible components*
- *Maximal ideals correspond to closed points*

*Proof.* The correspondence follows directly from (5.2.6). The first statement follows from (5.2.8) □

There is another way of viewing the non-closed points :

**Proposition 5.2.11** (Prime Spectrum is Sober)
*The prime spectrum* $\operatorname{Spec}(A)$ *is sober, i.e. there is a bijection*

$$\mathfrak{p} \to \overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$$

*between points and irreducible closed subsets. Minimal primes correspond to irreducible components and maximal ideals correspond to closed singleton sets.*

*Proof.* It's well-defined and surjective by Proposition (5.2.8). And $\overline{\{\mathfrak{p}\}} = \overline{\{\mathfrak{q}\}}$ implies $\mathfrak{p} \subseteq \mathfrak{q}$ and $\mathfrak{q} \subseteq \mathfrak{p}$ so the map is injective.

Clearly the relation is order-reversing and as irreducible components are simply maximal irreducible sets they correspond to minimal primes. □

**Definition 5.2.12** (Principal Open Sets of Prime Spectrum)
*Let* $A$ *be a ring (resp. Jacobson ring) and* $X = \operatorname{Spec}(A)$ *(resp.* $\operatorname{Specm}(A)$*) and define the* ***principal open set***

$$D(f) = \{[\mathfrak{p}] \mid f \notin \mathfrak{p}\}$$

*this is open being the complement of* $V((f))$*. Note that* $D(f) = X \iff f \in A^{\star}$*.*

**Proposition 5.2.13** (Principal Open Sets from a Base)
*Let $A$ be a ring (resp. Jacobson ring) and $X = \operatorname{Spec}(A)$ (resp. $\operatorname{Specm}(A)$). The open sets $D(f)$ form a base for the Zariski Topology on $X$, which we denote $\mathcal{B}$, and they are closed under intersection, because*

$$D(fg) = D(f) \cap D(g)$$

*Furthermore for any integer $N > 0$ we have*

$$D(f) = D(f^N)$$

*and*

$$D(g) \subseteq D(f) \iff f \mid g^N \text{ for some } N \iff \overline{S_f} \subseteq \overline{S_g}$$

*Proof.* We use (4.1.7) to show that the open sets $D(f)$ form a base. Given an open set $U$ we have $U = X \setminus V(\mathfrak{a})$. Further $\mathfrak{a} = \sum_{f \in \mathfrak{a}}(f) \implies V(\mathfrak{a}) = \bigcap V(f) \implies U = \bigcup D(f)$.

Note $\mathfrak{p} \in D(fg) \iff fg \notin \mathfrak{p} \iff f \notin \mathfrak{p} \wedge g \notin \mathfrak{p} \iff \mathfrak{p} \in D(f) \cap D(g)$.

Similarly $f \in \mathfrak{p} \iff f^N \in \mathfrak{p}$ therefore $D(f) = D(f^N)$.

Finally we have (by using the correspondence (5.2.10)) $D(g) \subseteq D(f) \iff V((f)) \subseteq V((g)) \iff \sqrt{(g)} \subseteq \sqrt{(f)} \iff g \in \sqrt{(f)} \iff f \mid g^N$.

If $f \mid g^N$ then clearly $S_f \subseteq \overline{S_g}$ which implies $\overline{S_f} \subseteq \overline{S_g}$ by (3.5.19). Conversely we see $f \in \overline{S_g} \implies af \in S_g$ by (3.5.19) which implies $f \mid g^N$ as required. □

**Proposition 5.2.14** (Functoriality)
*Let $\phi : A \to B$ be homomorphism then there is a natural map*

$$\operatorname{Spec}(\phi) : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$$
$$\mathfrak{p} \to \phi^{-1}(\mathfrak{p})$$

*and satisfies*

$$\operatorname{Spec}(\phi)^{-1}(D(f)) = D(\phi(f))$$

*It is continuous with respect to the Zariski topology. If any one of the following conditions holds*

- *$\phi$ is surjective.*
- *$\phi$ is integral*
- *$A$ and $B$ are finitely-generated $k$-algebras and $\phi$ is a $k$-algebra homomorphism*

*then this maps maximal ideals to maximal ideals and therefore restricts to a map*

$$\operatorname{Specm}(B) \to \operatorname{Specm}(A)$$

*Proof.* That the map is well-defined follows from (3.4.45). Note that

$$\mathfrak{p} \in \operatorname{Spec}(\phi)^{-1}(D(f)) \iff \operatorname{Spec}(\phi)(\mathfrak{p}) \in D(f) \iff \phi^{-1}(\mathfrak{p}) \in D(f) \iff f \notin \phi^{-1}(\mathfrak{p}) \iff \phi(f) \notin \mathfrak{p} \iff \mathfrak{p} \in D(\phi(f))$$

as required. As the principal open sets $D(f)$ form a base for the Zariskis topology, we see that $\operatorname{Spec}(\phi)$ is continuous.

If $\phi$ is surjective, then $\operatorname{Spec}(\phi)$ maps maximal ideals to maximal ideals by (3.4.45).

Suppose alternatively that $\phi$ is integral and $\mathfrak{m} \lhd B$ is maximal, then we have an injective ring homomorphism

$$\bar{A} := A/\phi^{-1}(\mathfrak{m}) \to B/\mathfrak{m} =: \bar{B}$$

which is integral and for which $\bar{B}$ is a field. Therefore by (3.19.9) $\bar{A}$ is a field and $\phi^{-1}(\mathfrak{m})$ is maximal by (3.4.49) as required.

In the final case $\bar{B}$ is finitely-generated over $k$ and is therefore finite and integral over $k$ by Zariski's Lemma. In particular $\bar{B}$ is integral over $\bar{A}$. The result then follows in the same way from (3.19.9). □

**Proposition 5.2.15**
*The canonical morphism $i_f : A \to A_f$ induces a homeomorphism*

$$\operatorname{Spec}(i_f) : \operatorname{Spec}(A_f) \longrightarrow D(f) \subset \operatorname{Spec}(A)$$

*Proof.* We claim that

$$D(f) = \{\mathfrak{p} \mid \overline{S_f} \cap \mathfrak{p} = \emptyset\}$$

then the bijection would follow from (3.5.18). Clearly

$$\mathfrak{p} \in D(f) \iff f \notin \mathfrak{p} \iff S_f \cap \mathfrak{p} = \emptyset$$

where last equivalence follows from primality. Clearly $\overline{S_f} \cap \mathfrak{p} = \emptyset \implies S_f \cap \mathfrak{p} = \emptyset$. Conversely suppose $\overline{S_f} \cap \mathfrak{p} \neq \emptyset$ then $g \in \overline{S_f} \cap \mathfrak{p} \implies ag \in S_f \cap \mathfrak{p} \implies S_f \cap \mathfrak{p} \neq \emptyset$.

By the previous Proposition it is continuous. We need only show that its inverse is continuous, i.e. it is an open map. TODO. □

### 5.2.3 Abstract Structure Sheaf (Integral Case)

Note in the case of an algebraic set $X$ with coordinate ring $k[X]$ we associated to it a natural structure sheaf $\mathcal{O}_X$ (5.1.20) such that $\mathcal{O}_X(D(f)) = k[X]_f$. We may mimic this for an arbitrary ring $A$ replacing the coordinate ring $k[X]$. First we illustrate the results for an integral domain $A$, as this is a bit easier and demonstrates the essential argument.

**Proposition 5.2.16**
*Let $A$ be an integral domain and $K$ its field of fractions, then define the $\mathcal{B}$-presheaf*

$$\mathcal{O}'_X(D(f)) = A_f \subset K$$

*with restriction maps equal to inclusion. Then this constitutes a $\mathcal{B}$-sheaf.*

*Proof.* Recall from (5.2.13) that $D(f) = D(g) \iff \overline{S_f} = \overline{S_g}$ so that the assignment is well-defined.

It's separated because the restriction morphisms are all injective.

Suppose that $D(f) = \bigcup_{i\in I} D(f_i)$ and $\sigma_i \in \mathcal{O}'_X(D(f_i))$. As restrictions are just inclusion, the compatibility conditions imply $\sigma_i = \sigma_j = \sigma$. We simply need to show that $f^N\sigma \in A$ for some $N$. Let $I = \{a \in A \mid a\sigma \in A\}$. We have $f_i^{r_i} \in I$ for some $r_i$, and we need to show $f^r \in I$ for some $r$, that is $f \in \sqrt{I}$. By (3.4.39) it's enough to show that $I \subseteq \mathfrak{p} \implies f \in \mathfrak{p}$. But $I \subseteq \mathfrak{p} \implies f_i \in \mathfrak{p} \implies \mathfrak{p} \notin D(f_i)$ for all $i \in I$ and therefore $\mathfrak{p} \notin D(f)$ by hypothesis. Therefore $\mathcal{O}'_X$ is a $\mathcal{B}$-sheaf as required. □

### 5.2.4 Abstract Structure Sheaf (General Case)

For this section we generalize the structure sheaf construction to a general ring $A$, and let $X = \mathrm{Spec}(A)$. We will also consider the case $A$ a Jacobson ring and $X = \mathrm{Specm}(A)$. The main result is the following

**Proposition 5.2.17** (Structure Sheaf)
*Let $A$ be a ring and $X = \mathrm{Spec}(A)$. Recall from (5.2.13) that*

$$D(f) \subseteq D(g) \iff \overline{S_f} \subseteq \overline{S_g}$$

*There is a $\mathcal{B}$-presheaf $\mathcal{O}'_X$, defined over the principal open sets by*

$$\mathcal{O}'_X(D(f)) := A_f$$

*with the canonical restriction maps defined in (3.5.28). It is in fact a $\mathcal{B}$-sheaf, and it has an associated sheaf $\mathcal{O}_X$ with an isomorphism*

$$\eta_A : \mathcal{O}'_X \longrightarrow \mathcal{O}_X|_{\mathcal{B}}$$

*and a natural bijection*

$$\mathrm{Mor}(\mathcal{O}_X, \mathcal{G}) \to \mathrm{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}})$$
$$\phi \longrightarrow \phi|_{\mathcal{B}} \circ \eta_A$$

*for all sheaves $\mathcal{G}$. Further there is an isomorphism of stalks (at $x = [\mathfrak{p}]$) yielding a commutative diagram for $f \notin \mathfrak{p}$*

$$\begin{array}{ccccc} A_f & = & \mathcal{O}'_X(D(f)) & \xrightarrow{\sim} & \mathcal{O}_X(D(f)) \\ \downarrow & & \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\sim} & \mathcal{O}'_{X,x} & \xrightarrow{\sim} & \mathcal{O}_{X,x} \end{array}$$

*where the left hand diagram is given in (3.5.33). Finally the canonical map $i_f : A \to A_f$ induces a homeomorphism*

$$\widetilde{i_f} : \mathrm{Spec}(A_f) \to D(f)$$

*and an isomorphism of sheaves*

$$\widetilde{i_f}_\star(\mathcal{O}_{\mathrm{Spec}(A_f)}) \longrightarrow \mathcal{O}_X|_{D(f)}$$

*Explicitly for $D(h) \subseteq D(g) \subseteq D(f)$ we have a commutative diagram*

$$\begin{array}{ccccccc}
\mathcal{O}_{\mathrm{Spec}(A_f)}(\mathrm{Spec}(A_f)) & \xleftrightarrow{\eta_{A_f,1}} & (A_f)_1 & \xleftrightarrow{\sim} & A_f & \xleftrightarrow{\eta_{A,f}} & \mathcal{O}_X(D(f)) \\
\downarrow & & \downarrow{\scriptstyle i_{1(g/1)}} & & \downarrow{\scriptstyle i_{fg}} & & \downarrow \\
\mathcal{O}_{\mathrm{Spec}(A_f)}(D(g/1)) & \xleftrightarrow{\eta_{A_f,g/1}} & (A_f)_{g/1} & \xleftrightarrow{\sim} & A_g & \xleftrightarrow{\eta_{A,g}} & \mathcal{O}_X(D(g)) \\
\downarrow & & \downarrow{\scriptstyle i_{(g/1)(h/1)}} & & \downarrow{\scriptstyle i_{gh}} & & \downarrow \\
\mathcal{O}_{\mathrm{Spec}(A_f)}(D(h/1)) & \xleftrightarrow{\eta_{A_f,h/1}} & (A_f)_{h/1} & \xleftrightarrow{\sim} & A_h & \xleftrightarrow{\eta_{A,h}} & \mathcal{O}_X(D(h))
\end{array}$$

*where the inner diagram is from (3.5.29), and the outer arrows are the isomorphisms $\eta$ and the sheaf restriction morphisms.*

*When $A$ is a Jacobson ring the same result follows when considering just the maximal spectrum.*

*Proof.* Let $\mathcal{B}$ be the base of principal open sets for the Zariski topology. Recall that $D(f) = D(g) \iff \overline{S_f} = \overline{S_g}$, so we may construct a well-defined $\mathcal{B}$-presheaf

$$\mathcal{O}'_X(D(f)) = A_f = \overline{S_f}^{-1}A$$

with restriction maps the canonical maps from (3.5.28). The same result shows that the restriction maps satisfy the commutativity relationships. We will show that this is in fact a $\mathcal{B}$-sheaf. Therefore by (4.2.11) there is a sheaf $\mathcal{O}_X$ together with a canonical isomorphism of sheaves

$$\eta_A : \mathcal{O}'_X \to \mathcal{O}_X|_{\mathcal{B}}$$

such that there is a bijection (natural in $\mathcal{G}$)

$$\begin{aligned}
\mathrm{Mor}(\mathcal{O}_X, \mathcal{G}) &\longrightarrow \mathrm{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}}) \\
\alpha &\to \alpha|_{\mathcal{B}} \circ \eta_A
\end{aligned}$$

This shows the existence of the required isomorphism and its universal property. Furthermore the isomorphism of stalks is also the content of Propositions (4.2.11) and (3.5.33).

We claim there is an isomorphism of $\mathcal{B}$-presheaves

$$\widetilde{i_f}_\star(\mathcal{O}'_{\mathrm{Spec}(A_f)}) \longrightarrow \mathcal{O}'_X|_{D(f)} \tag{5.2}$$

This is precisely the inner part of the commutative diagram stated and is demonstrated in (3.5.29). Using this observation we see that it's only necessary to show the sheaf conditions for $\mathcal{O}'_X$ when $U = X$, as we may reduce to the ring $A_f$.

Therefore suppose $X = \bigcup_i D(f_i)$ for $f_i \in A$. Suppose $\sigma, \tau \in \mathcal{O}'_X(X)$ such that $\sigma|_{D(f_i)} = \tau|_{D(f_i)}$. Then $\sigma = a/1$ and $\tau = b/1$ and there is an integer $N$ such that

$$f_i^N a = f_i^N b$$

for all $i$. By (5.2.18)

$$1 = \sum_i g_i f_i^N$$

for some $g_i$, which shows that $a = b$ and $\sigma = \tau$ as required. Similarly suppose $\sigma_i \in \mathcal{O}_X(D(f_i))$ such that $\sigma_i|_{D(f_i f_j)} = \sigma_j|_{D(f_i f_j)}$. Clearly $\sigma_i = a_i/f_i^N$ for sufficently large $N$. Observe the canonical map

$$A_{f_i} \to A_{f_i f_j}$$

is given by

$$a/f_i^r \to a f_j^r/(f_i f_j)^r$$

Therefore by the compatibility assumption we have

$$(f_i f_j)^M (f_j^N a_i - f_i^N a_j) = 0 \tag{5.3}$$

for sufficiently large $M$. By (5.2.18) there is a partition of unity

$$1 = \sum_j g_j f_j^{N+M}$$

Define

$$a := \sum_j g_j f_j^M a_j$$

Then using Equation (5.3)

$$f_i^{N+M} a = f_i^{N+M} \sum_j g_j f_j^M a_j = a_i f_i^M \sum_j g_j f_j^{N+M} = a_i f_i^M$$

and therefore $f_i^M (f_i^N a - a_i) = 0$, which means precisely $\sigma|_{D(f_i)} = \sigma_i$ as required. Therefore $\mathcal{O}'_X$ is a $\mathcal{B}$-sheaf.

The statement about $A_f$ is a somewhat tedious and formal consequence of the results already shown.

Let $\mathcal{B}|_f$ be the principal open sets contained in $D(f)$, which is therefore a base for $D(f)$ in the subspace topology. Note that as functors of sheaves

$$(-)|_{\mathcal{B}|_f} \circ (-)|_{D(f)} = (-)|_{D(f)} \circ (-)|_{\mathcal{B}}$$

Similarly let $\mathcal{B}_f$ be the base for $\operatorname{Spec}(A_f)$ then as functors we have

$$(-)|_{\mathcal{B}|_f} \circ \widetilde{i_{f\star}} = \widetilde{i_{f\star}} \circ (-)|_{\mathcal{B}_f}$$

By (4.2.13) $(-)|_{\mathcal{B}|_f}$ is full and faithful when acting on sheaves so there is a bijection

$$\operatorname{Mor}(\widetilde{i_{f\star}}(\mathcal{O}_{\operatorname{Spec}(A_f)}), \mathcal{O}_X|_{D(f)}) \xrightarrow{(-)|_{\mathcal{B}|_f}} \operatorname{Mor}\left(\widetilde{i_{f\star}}(\mathcal{O}_{\operatorname{Spec}(A_f)}|_{\mathcal{B}_f}), \mathcal{O}_X|_{\mathcal{B}}|_{D(f)}\right)$$

and by (2.4.30) it reflects isomorphisms. We may compose isomorphisms as follows

$$\widetilde{i_{f\star}}(\mathcal{O}_{\operatorname{Spec}(A_f)}|_{\mathcal{B}_f}) \xrightarrow{\widetilde{i_{f\star}}(\eta_{A_f})^{-1}} \widetilde{i_{f\star}}(\mathcal{O}'_{\operatorname{Spec}(A_f)}) \xrightarrow{\sim} \mathcal{O}'_X|_{D(f)} \xrightarrow{\eta_A|_{D(f)}} \mathcal{O}_X|_{\mathcal{B}}|_{D(f)}$$

(where the middle was shown in (5.2)) and reflect it back to get the stated isomorphism. □

We used the following Lemma

**Lemma 5.2.18** (Partition of Unity)
*Suppose*

$$X = \bigcup_i D(f_i)$$

*for some $f_i \in A$, then for any integers $n_i > 0$ we have a partition of unity*

$$1 = \sum_i f_i^{n_i} g_i$$

*for some $g_i \in A$, depending on $n_i$, only finitely many non-zero.*

*Proof.* Firstly trivially $D(f_i) = D(f_i^{n_i})$, because $f_i^{n_i} \in \mathfrak{p} \iff f_i \in \mathfrak{p}$. Formally we see

$$\emptyset = \bigcap_i V(f_i^{n_i}) = V\left(\sum_i (f_i^{n_i})\right)$$

and apply $I$ to see

$$A = \sqrt{\sum_i (f_i^{n_i})}$$

and the result follows easily. □

# Bibliography


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

[Bir40] G. Birkhoff. *Lattice Theory*. Number v. 25, pt. 2 in American Mathematical Society colloquium publications. American Mathematical Society, 1940.

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

[Hal17] P.R. Halmos. *Naive Set Theory*. Dover Books on Mathematics. Dover Publications, 2017.

[Har13] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2013.

[Lan11] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2011.

[Lan19] S. Lang. *Introduction to Algebraic Geometry*. Dover Books on Mathematics. Dover Publications, 2019.

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

[Nag75] M. Nagata. *Local Rings*. R.E. Krieger Publishing Company, 1975.

[Rom05] S. Roman. *Field Theory*. Graduate Texts in Mathematics. Springer New York, 2005.

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

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

[ZS76] O. Zariski and P. Samuel. *Commutative Algebra II*. Graduate Texts in Mathematics. Springer New York, 1976.