Algebra, Geometry and Number Theory

David Rufino

February 25, 2024

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

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 $y \in Y$ 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**.*

Definition 2.1.17 (Dual 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 2.1.18
Let $\mathcal{F}$ be a family of subsets of a fixed set E. Then $(\mathcal{F}, \subseteq)$ is a poset ordered under inclusion.

Definition 2.1.19 (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 2.1.20 (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 2.1.21
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 2.1.22 (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 2.1.23 (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 2.1.24 (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 2.1.25 (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 2.1.26
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 2.1.27 (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 2.1.28 (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 2.1.29
Let $(X, \leq)$ be a poset. Then $\{\sup S\}^{\uparrow} = S^{\uparrow}$ and $\{\inf T\}^{\downarrow} = T^{\downarrow}$ when these exist.

Lemma 2.1.30 (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 2.1.31
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 2.1.32 (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. A subset* Y *is called a* ***sub-lattice*** *if*

$$a, b \in Y \implies a \wedge b \in Y \text{ and } a \vee b \in Y\,.$$

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 2.1.33 (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* $\bot = \emptyset$*.*

Proposition 2.1.34 (Principal down-sets are lattices)
Let $(X, \leq)$ *be a lattice and* $x, y \in X$*. Then the subsets* $\{x\}^{\uparrow}$*,* $\{x\}^{\downarrow}$ *and* $\{x\}^{\uparrow} \cap \{y\}^{\downarrow}$ *are sub-lattices.*

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

Lemma 2.1.35 (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 (2.1.25) $S^{\uparrow\downarrow\uparrow} = S^{\uparrow}$ so they are equivalent. □

Proposition 2.1.36 (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 2.1.37
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 2.1.38 (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 2.1.39 (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 2.1.40 (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. *a)* $\implies$ *b)* By (2.1.37) $S \subseteq Y \implies \bigwedge_Y S = \bigwedge_X S$. By (2.1.36) then Y is a complete lattice.

b) $\implies$ *c)* 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 (2.1.30) 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 (2.1.37) 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.

c) $\implies$ *a)* 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 (2.1.29) $\{\bigvee_X S\}^{\uparrow} = S^{\uparrow}$ 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 (2.1.40)

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

□

Remark 2.1.41
For a given complete lattice $(X, \leq)$ we have established a correspondence between

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

Corollary 2.1.42 (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 2.1.43 (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 $S \subset X$

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

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

Proof. By (2.1.40) the expression for $c(\bigvee_X S)$ yields

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

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 Distributive Lattice

Proposition 2.1.44
Let $(X, \leq)$ be a lattice then the following relations hold

a) $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

b) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

Proof. *a*) By definition $x \wedge y \leq x$ and $x \wedge y \leq y \leq y \vee z$. Therefore $x \wedge y \leq x \wedge (y \vee z)$. By symmetry in y and z we have $x \wedge z \leq x \wedge (y \vee z)$. Whence $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$ as required.

b) follows by duality □

Definition 2.1.45 (Distributive Lattice)
*We say a lattice $(X, \leq)$ is **distributive** if it satisfies the following relations for all $x, y, z \in X$*

- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
- $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Proposition 2.1.46
Let $(X, \leq)$ be a lattice then TFAE

a) $(X, \leq)$ *is a distributive lattice*

b) $x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$

c) $x \vee (y \wedge z) \geq (x \vee y) \wedge (x \vee z)$

Example 2.1.47
Any family of subsets closed under finite intersection and union is a distributive lattice.

2.1.6 Galois Connections

Definition 2.1.48 (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 2.1.49 (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 2.1.50 (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 2.1.51 (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***

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

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 (2.1.49)

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

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 (2.1.49). 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 2.1.52 (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 2.1.53 (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 2.1.54 (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. □

2.1.7 Axiom of Choice

Theorem 2.1.55 (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 2.1.56 (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 $\#S = \#T$.

Definition 2.1.57 (Finite Character)
*A family of sets $\mathcal{F}$ has **finite character** if it satisfies the following property*

$$A \in \mathcal{F} \iff (B \subseteq A \text{ and finite} \implies B \in \mathcal{F})$$

Corollary 2.1.58 (Tukey's Lemma)
Let $\mathcal{F}$ be a family of sets of finite character. Then it is chain-complete when ordered by inclusion.

In particular every set is contained in a maximal set.

2.1.8 Chain Conditions

Definition 2.1.59 (Totally ordered / chains)
*A poset $(\mathcal{F}, \leq)$ is **totally ordered** if $x \leq y$ or $y \leq x$ for all $x, y \in \mathcal{F}$.*

Definition 2.1.60 (Chain)
*A non-empty subset C of $\mathcal{F}$ is a **chain** if it is totally ordered under $\leq$.*

The length of the chain is simply $\ell(C) := |C| - 1$.

A chain C is

- ***saturated** if $x \leq z \leq y$ and $x, y \in C \implies z \in C$.*
- ***maximal** if it's not contained properly in another chain.*

Definition 2.1.61 (Chain-Complete)
*A poset $(\mathcal{F}, \leq)$ is **chain complete** if every chain C has a supremum in $\mathcal{F}$. It is **co-chain complete** if every chain C has an infimum in $\mathcal{F}$.*

Proposition 2.1.62 (Noetherian / Artinian Poset)
Let $(X, \leq)$ be a poset then the following conditions are equivalent

a) *Any ascending chain*

$$x_1 \leq x_2 \leq \ldots \leq x_n \leq \ldots$$

eventually stabilizes

b) *Any non-empty subset $Y \subseteq X$ has a maximal element*

*Such a poset is called **Noetherian**. If it satisfies the dual condition then it is called **Artinian**.*

Proof. *a)* $\implies$ *b)* If Y has no maximal elements then we may (by axiom of dependent choice) construct a strictly increasing sequence, which by definition does not stabilize.

b) $\implies$ *a)* Clear. □

2.2 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.

2.2.1 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
  - $-0 = 0$
  - $-(-x) = x$
  - $x = -x \iff x = 0$
  - $x + 0 = 0 = 0 + x$
  - $x + y = y + x$
  - $(x + y) + z = x + (y + z)$
  - $x + (-x) = 0 = (-x) + x$
  - $-(x + y) = (-x) + (-y)$
- A subset $\mathbb{N}$ such that
  - $0, 1 \in \mathbb{N}$
  - $x, y \in \mathbb{N} \implies x + y \in \mathbb{N}$
  - $x \in \mathbb{Z} \implies (x \in \mathbb{N}) \vee (-x \in \mathbb{N})$
  - $x \in \mathbb{N} \wedge -x \in \mathbb{N} \implies x = 0$

  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 2.2.1 (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 2.2.2 (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 2.2.3
*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 2.2.4 (Well-Ordering Principle)
Let $S \subset \mathbb{N}$ be a non-empty subset. Then it contains a minimal element d.

2.2.2 Arithmetic

Proposition 2.2.5 (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 2.2.6 (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 2.2.7 (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 2.2.8
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 2.2.9 (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 (2.2.6) 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 2.2.10
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 $\{mx + ny\}$. □

2.2.3 Prime Factorization

Definition 2.2.11
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 2.2.12
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 2.2.13 (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 (2.2.10) $(x', a') = 1$. 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 (2.2.12) 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.

2.3 Matroids

The theory of bases of vector spaces (Section 3.4.14) and transcendence bases of field extensions (Section 3.14.15) have some formal similarities, as noted in [vdW91]. Here we use the theory of Matroids to formalise this precisely so that the proofs need not be repeated in each case.

Definition 2.3.1 (Matroid)
Consider a set X together with a closure operator $c : \mathcal{P}(X) \to \mathcal{P}(X)$ ("span" operator) such that $c(\emptyset) = \emptyset$. 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. Moreover all singletons $\{x\}$ are independent.

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

- ***Finitary** $x \in c(\Gamma) \implies x \in c(\Gamma')$ for some finite subset Γ' of Γ.*
- ***Exchange Property** For all $x, y \in X$ and $Y \subseteq X$ we have*

$$x \in c(Y \cup \{y\}) \setminus c(Y) \implies y \in c(Y \cup \{x\})$$

*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 2.3.2
Suppose $S \subset X$ is a subset

a) $A \subseteq c(S) \implies c(S \cup A) = c(S)$

b) *S is independent if and only if no proper subset has the same span.*

Proof. We prove each in turn

a) By monotonicity

$$c(S) \subseteq c(S \cup A) \subseteq c(c(S) \cup A) = c(c(S)) = c(S)$$

b) Suppose S is independent and $S' \subsetneq S$ is a proper subset such that $c(S') = c(S)$. Choose $x \in S \setminus S'$ then by definition $x \in S \implies x \in c(S) = c(S') \subseteq c(S \setminus \{x\})$ contradicting independence.

Conversely suppose for some $x \in S$ we have $x \in c(S \setminus \{x\})$. Define $S' := S \setminus \{x\}$. Then $x \in c(S')$ implies $c(S) = c(S')$ by a). As S' is a proper subset this contradicts the hypothesis.

□

Lemma 2.3.3
Every subset of an independent set is independent. Furthermore the family of independent sets has finite character.

Proof. The first statement is straightforward. Suppose S a dependent set such that every finite subset is independent. Then there exists $x \in S$ such that $x \in c(S \setminus \{x\})$. Then by the finitary property there exists a finite subset $S' \subseteq S \setminus \{x\}$ such that $x \in c(S')$. Therefore by definition $S' \cup \{x\}$ is not independent, a contradiction. □

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

Corollary 2.3.4
Let $\{S_i\}_{i \in I}$ be a chain of independent subsets. Then $S = \bigcup_{i \in I} S_i$ is also independent.

Proof. This follows from Tukey's Lemma (2.1.58). □

Lemma 2.3.5 (Extension Property)
Suppose S is an independent set and $x \notin c(S)$, then $S \cup \{x\}$ is independent.

Proof. We require to prove that for all $y \in S$ we have $y \notin c(S \cup \{x\} \setminus \{y\})$. By independence of S we have $y \notin c(S \setminus \{y\})$, so by the Exchange Property $y \in c(S \cup \{x\} \setminus \{y\})$ would imply $x \in c(S)$, contradicting the hypothesis. □

Proposition 2.3.6
Let $\mathcal{F}$ be a family of independent sets which satisfies the following properties

- $\emptyset \in \mathcal{F}$
- ***extension property*** *$S \in \mathcal{F}$ and $x \notin c(S) \implies S \cup \{x\} \in \mathcal{F}$*
- *$\mathcal{F}$ has finite character*

then $\mathcal{F}$ consists of all independent sets.

Proof. It's enough to show that $\mathcal{F}$ contains all finite independent sets, which follows by induction on $\#S$. For given an independent set S and $x \in S$, then by definition $x \notin c(S \setminus \{x\})$. By the induction hypothesis $S \setminus \{x\} \in \mathcal{F}$ whence by the extension property $S \in \mathcal{F}$ as required. □

Proposition 2.3.7 (Basis exists)
Let (X, c) be a matroid, S independent and Γ a subset such that $S \subseteq \Gamma$. Then there exists an independent set $\mathcal{B}$ such that $S \subseteq \mathcal{B} \subseteq \Gamma$ and $c(\mathcal{B}) = c(\Gamma)$.

In particular if Γ is spanning then $\mathcal{B}$ is a basis.

Proof. Consider the collection

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

By (2.3.4) is chain-complete. Therefore it has a maximal element $\mathcal{B}$ by Zorn's Lemma. Suppose $x \in \Gamma \setminus c(\mathcal{B})$ then $\mathcal{B} \cup \{x\}$ is independent by (2.3.5), contradicting maximality. Therefore $\Gamma \subseteq c(\mathcal{B}) \implies c(\Gamma) \subseteq c(\mathcal{B})$. The reverse inequality is clear so that $c(\Gamma) = c(\mathcal{B})$. □

Corollary 2.3.8 (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* Γ*)*

Proof. $a) \implies b)$. Let $\mathcal{B}$ be a basis and $\Gamma \subseteq \mathcal{B}$ a spanning set. Then by (2.3.2).b) $\Gamma = \mathcal{B}$.

$b) \implies a)$. Let $\mathcal{B}$ be a minimal spanning set, then by (2.3.7) there exists a subset $\mathcal{B}'$ which is a basis, and in particular spanning. By minimality $\mathcal{B} = \mathcal{B}'$.

$c) \implies a)$. By (2.3.7) there exists a basis $\mathcal{B}'$ containing $\mathcal{B}$. By maximality $\mathcal{B}' = \mathcal{B}$.

$a) \implies c)$. Suppose $\mathcal{B} \subseteq S$ where S is independent. Then S is spanning too, and so by (2.3.2) $\mathcal{B} = S$. □

Lemma 2.3.9 (Mini Exchange Lemma)
Let $S \subseteq \Gamma$ *be finite sets and* $x \in X \setminus S$ *such that*

- S *is independent*
- $x \in c(\Gamma) \setminus c(S)$

Then there exists $y \in \Gamma \setminus S$ *such that* $c(\Gamma \setminus \{y\} \cup \{x\}) = c(\Gamma)$.

Proof. We may assume without loss of generality that $x \notin \Gamma$.

Consider $\widetilde{\Gamma} \subseteq \Gamma$ minimal subject to $S \subseteq \widetilde{\Gamma}$ and $x \in c(\widetilde{\Gamma})$. If $S = \widetilde{\Gamma}$ then $x \in c(S)$ a contradiction. Therefore we may choose $y \in \widetilde{\Gamma} \setminus S$. By minimality we have $x \in c(\widetilde{\Gamma}) \setminus c(\widetilde{\Gamma} \setminus \{y\})$. Therefore by the Exchange Property we have $y \in c(\widetilde{\Gamma} \setminus \{y\} \cup \{x\})$. Then by (2.3.2) applied twice

$$c(\Gamma \setminus \{y\} \cup \{x\}) = c(\Gamma \cup \{x\}) = c(\Gamma)$$

as required. □

Proposition 2.3.10 (Exchange Lemma)
Let S *be an independent set and* Γ *be a finite set such that* $S \subseteq c(\Gamma)$. *Then there exists a subset* $T \subseteq \Gamma$ *such that*

- $\#T = \#S$
- $c(\Gamma \setminus T \cup S) = c(\Gamma)$.

In particular $\#S \leq \#\Gamma$.

Proof. By considering the sub-matroid $(c(\Gamma), c)$ we may assume without loss of generality that $X = c(\Gamma)$.

Let $n = \#\Gamma$ and consider the set of pairs

$$\mathcal{F} := \big\{(A, B) \mid A \subseteq S, \quad B \subseteq \Gamma, \quad \#A = \#B, \quad c(\Gamma \setminus B \cup A) = X\big\}$$

Essentially $\mathcal{F}$ is the set of swaps we may perform from S to Γ whilst preserving the span. It is non-empty because $(\emptyset, \emptyset) \in \mathcal{F}$ and we wish to show that $(S, B) \in \mathcal{F}$ for some B.

Observe that for all $(A, B) \in \mathcal{F}$ we have $\#B \leq n$ so choose a pair such that $\#B$ is maximal. We wish to show that in this case $A = S$, so we suppose to the contrary that $A \subsetneq S$.

We claim that $B \subsetneq \Gamma$, for $B = \Gamma$ implies by construction $c(A) = X$ which would imply $c(A) = c(S)$, contradicting the criteria for independence of S given by Lemma (2.3.2).

Define $\Gamma' := \Gamma \setminus B \cup A$. Then by assumption $c(\Gamma') = X$ and $A \subseteq \Gamma'$ is independent. Choose $x \in S \setminus A$ then by definition of independence $x \notin c(A)$. By (2.3.9) there exists $y \in \Gamma' \setminus A$ such that

$$c(\Gamma' \setminus \{y\} \cup \{x\}) = c(\Gamma') = X$$

Note by construction that $y \notin B$, so we see that $(A \cup \{x\}, B \cup \{y\}) \in \mathcal{F}$ has greater length, which contradicts maximality. □

Corollary 2.3.11 (Bases have the same cardinality)
Every base of a finite rank matroid is finite and of the same size. Denote this by $r(X)$.

Proof. There is a finite basis by (2.3.7). Then apply (2.3.10). □

Corollary 2.3.12
Let (X, c) be a finite-rank matroid and $S \subseteq X$ an independent subset, then $\#S \leq r(X)$. Similarly a spanning subset Γ satisfies $\#\Gamma \geq r(X)$.

Proof. Apply (2.3.7) and (2.3.11). □

Corollary 2.3.13 (Basis Criteria)
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 (2.3.7) and (2.3.11). □

Definition 2.3.14 (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 2.3.15
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 (2.3.13) $\mathcal{B}$ is a basis for X and hence $X = c(\mathcal{B}) = Y$. □

2.4 Decomposition in Noetherian and Distributive Lattices

An analogue of irreducible factorization in rings (see Section 3.11) applies to Noetherian Lattices. Furthermore uniqueness holds when the lattice is distributive. For a canonical reference see [Bir40].

Definition 2.4.1 (Meet-Prime and Meet-Irreducible)
Let $(X, \leq)$ be a lattice and $x \in X$. Then we say that x is

- ***meet-irreducible*** *if $y \wedge z = x \implies y = x$ or $z = x$*
- ***meet-prime*** *if $y \wedge z \leq x \implies y \leq x$ or $z \leq x$*
- ***join-irreducible*** *if $y \vee z = x \implies y = x$ or $y = z$*
- ***join-prime*** *if $x \leq y \vee z \implies x \leq y$ or $x \leq z$*

The following result is proven in [Bir40, Ch. IX Lemma 4.1].

Proposition 2.4.2 (Prime = Irreducible)
Let $(X, \leq)$ be a lattice. In general meet-prime $\implies$ meet-irreducible and join-prime $\implies$ join-irreducible. If X is a distributive lattice, then the converse holds.

In the distributive case we denote by $\mathcal{M}(X)$ and $\mathcal{J}(X)$ the sub-poset of meet-prime and join-prime elements respectively.

Proof. The first statement is straightforward. Conversely suppose X is a distributive lattice and x is meet-irreducible. If $y \wedge z \leq x$ then $x = x \vee (y \wedge z) = (y \vee x) \wedge (z \vee x) \implies x = y \vee x$ or $x = z \vee x$, whence the result follows. □

Proposition 2.4.3
Let $(X, \leq)$ be a distributive lattice and Y a sub-lattice, then

$$\mathcal{M}(Y) = \mathcal{M}(X) \cap Y$$
$$\mathcal{J}(Y) = \mathcal{J}(X) \cap Y$$

In particular this holds when $Y = \{x\}^{\uparrow}, \{y\}^{\downarrow}, \{x\}^{\uparrow} \cap \{y\}^{\downarrow}$.

Proposition 2.4.4
Let $(X, \leq)$ be a distributive lattice. If it is chain-complete (resp. co-chain-complete) then so is $\mathcal{J}(X)$ (resp. $\mathcal{M}(X)$).

Every join-prime element is bounded above by a maximal join-prime element, and every meet-prime element is bounded below by a minimal meet-prime element

Proof. Let C be a chain of join-prime elements and $x := \bigvee C$. Suppose that $y \vee z \geq x$ then $y \vee z \geq w$ for all $w \in C$. Then $y \geq w$ or $z \geq w$ for all $w \in C$. Let $C_1 := \{w \in C \mid y \geq w\}$. If $C_1 = C$ then we are done as $x \leq y$. Otherwise suppose $w_0 \notin C_1$ then by prime-ness $z \geq w_0$. Clearly $w \leq w_0 \implies w \leq z$. Further $w \geq w_0 \implies w \not\leq y$ (as otherwise $w_0 \leq y$) whence $w \leq z$. Therefore $x \leq z$.

The last statement follows from Zorn's Lemma by considering the sub-lattices $\{x\}^\uparrow$ and $\{y\}^\downarrow$ which inherit the chain complete properties. □

Definition 2.4.5
Let $(X, \leq)$ be a lattice and $Y \subseteq X$ a finite subset. Then we say that Y is

- ***(meet-)irredundant** if no proper subset has the same meet*
- ***incomparable** (or an **antichain**) if no two elements are comparable*

Lemma 2.4.6 (incomparable $\iff$ irredundant)
Let $(X, \leq)$ be a lattice and $Y \subseteq X$ then Y meet-irredundant $\implies$ Y incomparable. Conversely if Y is a finite incomparable subset of meet-prime elements then Y is meet-irredundant.

Proof. The first part is straightforward, for if $y_1 \lneq y_2$ are elements of Y then $\bigwedge Y = \bigwedge Y \setminus \{y_2\}$.

Conversely suppose $Y' \subsetneq Y$ is such that $\bigwedge Y' = \bigwedge Y$. Choose $y_2 \in Y \setminus Y'$, then $\bigwedge Y' \leq y_2$, whence by definition of meet-prime (and induction) $y_1 \leq y_2$ for some $y_1 \in Y'$. □

The following is [Bir40, Chapter IX Theorem 9]

Proposition 2.4.7 (Decomposition in Noetherian Lattice)
Let $(X, \leq)$ be a Noetherian distributive lattice. Then every element $x \in X$ has a unique decomposition

$$x = x_1 \wedge \ldots \wedge x_n$$

where x_i are meet-prime and meet-irredundant (equivalently incomparable). These are precisely the meet-primes minimal over x.

Dually, if $(X, \leq)$ is an Artinian distributive lattice, then every element $x \in X$ has a unique decomposition

$$x = x_1 \vee \ldots \vee x_n$$

where x_i are join-prime and join-irredundant (equivalently incomparable). These are precisely the join-primes maximal below x.

Proof. Let Y be the subset of elements which are not finite meets of meet-prime elements, and suppose it is non-empty. Then by (2.1.62) Y has a maximal element x_0. It cannot be meet-prime, and therefore not meet-irreducible (2.4.2), so there must exist elements $y_0, z_0 \in X$ such that $x_0 = y_0 \wedge z_0$ but $x_0 \lneq y_0$ and $x_0 \lneq z_0$. By maximality y_0, z_0 are finite meets of prime elements, and therefore so is x_0 a contradiction.

Therefore we have a decomposition into distinct primes

$$x = x_1 \wedge \ldots \wedge x_n$$

Consider the family of subsets of $\{x_1, \ldots, x_n\}$ which have the same meet. Then there exists a minimal subset which by definition is meet-irredundant and by (2.4.6) incomparable. Suppose there is another such decomposition $x = x'_1 \wedge \ldots \wedge x'_m$. Then for every $i = 1 \ldots n$ we have $x'_{\sigma(i)} \leq x_i$ and for every $j = 1 \ldots m$ we have $x_{\tau(j)} \leq x'_j$ whence $x_{\tau(\sigma(i))} \leq x'_{\sigma(i)} \leq x_i$. As the decomposition is incomparable we have $\tau(\sigma(i)) = i$ and $x'_{\sigma(i)} = x_i$. Therefore σ is injective and $n \leq m$. By symmetry $m \leq n$ and σ is a bijection. In otherwords the decomposition is unique.

Note $x \leq z$ and z meet-prime implies $x_j \leq z$ for some j. Therefore if z is a minimal prime then $x_j = z$. Similarly if $z \leq x_i$ then by incomparability $x_j = z = x_i$. Therefore each x_i is also minimal. □

2.5 Krull Dimension

The purpose of this section is to abstract the notions of Krull Dimension in commutative ring theory (Section 3.21) and topology (Section 4.1.4). A more standard approach (eg EGA IV) would be to develop the topological notion first, and then link to commutative ring case using the prime spectrum (Section 5.2.2). Generally the concept is not well-behaved, so stronger conditions are defined which generally hold in geometric cases. Principle references are (EGA0 IV 14.3, Heinrich).

Definition 2.5.1 (Finite-Dimensional Poset)
*Let $(\mathcal{G}, \leq)$ be a poset, we say that it is **finite-dimensional** if*

$$\dim(\mathcal{G}) := \sup\{\ell(C) \mid C \subseteq \mathcal{G} \text{ a chain }\} < \infty$$

In this case we define

$$\begin{aligned} \dim(x) &:= \dim(\{x\}^{\downarrow}) \\ \operatorname{codim}(y) &:= \dim(\{y\}^{\uparrow}) \\ \operatorname{codim}(y, x) &:= \dim(\{x\}^{\downarrow} \cap \{y\}^{\uparrow}) \end{aligned}$$

Note $\mathcal{G}$ is both Noetherian and Artinian, but finite-dimensionality is a stronger condition. Note also that $\{x\}^{\downarrow}, \{y\}^{\uparrow}$ and $\{x\}^{\downarrow} \cap \{y\}^{\uparrow}$ are finite-dimensional posets

Definition 2.5.2 (Krull Lattice)
*Let $(\mathcal{F}, \leq)$ be an **Artinian** distributive lattice. We say it is a **Krull Lattice** if the poset of join-prime elements $\mathcal{J}(\mathcal{F})$ is finite-dimensional and define*

$$\dim(\mathcal{F}) := \dim(\mathcal{J}(\mathcal{F}))$$

By (2.4.3) we have $\mathcal{H} = \{x\}^{\downarrow}, \{y\}^{\uparrow}, \{x\}^{\downarrow} \cap \{y\}^{\uparrow}$ are Krull Lattices such that

$$\mathcal{J}(\mathcal{H}) = \mathcal{J}(\mathcal{F}) \cap \mathcal{H}$$

For $x, y \in \mathcal{F}$ we have a unique decomposition into maximal join-prime elements $x_i, y_j \in \mathcal{J}(\mathcal{F})$ (2.4.7)

$$x = x_1 \vee \ldots \vee x_n$$

$$y = y_1 \vee \ldots \vee y_m$$

Note that $y \leq x \iff$ for all j we have $y_j \leq x_i$ for some i and we may define

$$\dim(x) := \max_i \dim(x_i) = \dim(\{x\}^{\downarrow}) \tag{2.2}$$

$$\operatorname{codim}(y) := \min_j \operatorname{codim}(y_j) \tag{2.3}$$

$$\operatorname{codim}(y, x) := \min_j \max_i \{\operatorname{codim}(y_j, x_i) \mid y_j \leq x_i\} \tag{2.4}$$

$$= \min_j \operatorname{codim}(y_j, x) \tag{2.5}$$

note it's required to be careful in definition of co-dimension in order to have a sensible co-dimension formula. Note also that

$$\dim(y; \{x\}^{\downarrow}) = \dim(y) \tag{2.6}$$

Remark 2.5.3
For the topological case, we would define $\mathcal{F}$ to be the closed subsets of X and $\mathcal{J}(\mathcal{F})$ would be the collection of irreducible closed subsets, see (4.1.18).

Proposition 2.5.4 (Extending chains)
Let $(\mathcal{G}, \leq)$ be a finite-dimensional poset

- *Every chain is contained in a saturated chain*
- *Every chain is contained in a maximal chain*
- *Every maximal chain is of the form*

  $$x_0 \lneq x_1 \ldots \lneq x_n$$

  for x_0 minimal and x_n maximal in $\mathcal{G}$.

Definition 2.5.5 (Properties)
Let $\mathcal{G}$ be a finite-dimensional poset. Then we say it is

- ***Irreducible** if it has a top element*
- ***Equidimensional** if every maximal element has the same dimension*

- ***Equicodimensional*** *if every minimal element has the same codimension*
- ***Biequidimensional*** *if every maximal chain has the same length*
- ***Quasi-Biequidimensional*** *if* $\{x\}^{\downarrow}$ *is biequidimensional for all* x *(equivalently all maximal* x*)*
- ***Catenary*** *if for every pair* $y \leq x$*, every saturated chain in* $[y,x] := \{y\}^{\uparrow} \cap \{x\}^{\downarrow}$ *has the same length, namely* $\operatorname{codim}(y,x)$.

If $\mathcal{F}$ *is a Krull Lattice then we say it inherits these properties from* $\mathcal{J}(\mathcal{F})$*. Note if* $\mathcal{F}$ *is irreducible then it also has (the same) top element.*

Trivially irreducible implies equidimensional. Similarly biequidimensional implies both equidimensional and equicodimensional, but not conversely.

Finally ***quasi-biequidimensional + equidimensional*** $\iff$ ***biequidimensional***.

Proposition 2.5.6 (Simple Properties)
Let $\mathcal{G}$ *be a finite-dimensional poset then*

a) *If* x *is maximal then* $\operatorname{codim}(x) = 0$

b) *If* x *is minimal then* $\dim(x) = 0$

c) $\dim(\mathcal{G}) = \sup\{\dim(x) \mid x \text{ maximal }\} = \sup\{\operatorname{codim}(x) \mid x \text{ minimal }\}$

d) *For all* $z \leq y \leq x$ *we have* $\operatorname{codim}(z,y) + \operatorname{codim}(y,x) \leq \operatorname{codim}(z,x)$

If $\mathcal{F}$ *is a Krull Lattice then*

e) For all $y \leq x$ *we have* $\dim(y) + \operatorname{codim}(y,x) \leq \dim(x)$

f) For all $y \leq x$ *we have* $\operatorname{codim}(y,x) = 0 \iff y_j = x_i$ *some* i,j

Alternatively $\operatorname{codim}(y,x) > 0$ *if and only if* $(y_j \leq x_i \implies y_j \neq x_i)$.

Proof. *e)* The case of a finite-dimensional poset is (relatively) clear. In the general case then we have

$$\dim(y_j) + \operatorname{codim}(y,x) \leq \dim(y_j) + \operatorname{codim}(y_j,x) = \max_i(\dim(y_j) + \operatorname{codim}(y_j,x_i)) \leq \max_i \dim(x_i) = \dim(x)$$

and taking max over j yields the result.

f) The case $x,y \in \mathcal{J}(\mathcal{F})$ is clear by (2.5.4). For the general case $\operatorname{codim}(y,x) = 0 \iff \operatorname{codim}(y_j,x) = 0$ for some $j \iff (y_j \leq x_i \implies \operatorname{codim}(y_j,x_i) = 0) \iff y_j = x_i$ for some i,j. □

Corollary 2.5.7 (Codimension 1 formula)
Let $\mathcal{F}$ *be a Krull Lattice with* $y \in \mathcal{F}$*,* $x \in \mathcal{J}(\mathcal{F})$ *and* $y \leq x$*. Then*

$$\dim(y) = \dim(x) - 1 \implies \operatorname{codim}(y,x) = 1$$

Suppose further that $\mathcal{F}$ *is irreducible then*

$$\dim(y) = \dim(\mathcal{F}) - 1 \implies \operatorname{codim}(y) = 1$$

Proof. By (2.5.6).*e)* $\operatorname{codim}(y,x) \leq 1$. If $\operatorname{codim}(y,x) = 0$ then by *f)* we see that $y_j = x$ for some j, whence $y = x$ which contradicts $\dim(y) = \dim(x) - 1$. Therefore $\operatorname{codim}(y,x) = 1$ as required.

If $\mathcal{F}$ is irreducible the result follows with $x = \top$. □

Remark 2.5.8 (Duality)
We note that the concepts of ***dimension*** *(of a poset).* ***biequidimensional*** *and* ***catenary*** *are* self-dual*, in the sense that they are preserved when considering the dual poset* $(\mathcal{G}, \leq^d)$.

Similarly the concepts of ***equidimensional*** *and* ***equicodimensional*** *are dual to each other.*

Proposition 2.5.9
Let $\mathcal{G}$ *be a finite-dimensional poset. Then the following are equivalent*

- $\mathcal{G}$ *is catenary*
- *For every triplet* $z < y < x$ *in* $\mathcal{G}$ *we have*

$$\operatorname{codim}(z,x) = \operatorname{codim}(z,y) + \operatorname{codim}(y,x)$$

When $\mathcal{G}$ is irreducible this is equivalent to

$$\operatorname{codim}(z) = \operatorname{codim}(z, y) + \operatorname{codim}(y)$$

for all $z < y$.

Proof. Suppose $\mathcal{G}$ is catenary. Choose saturated chains C_1 in $[z, y]$ and C_2 in $[y, x]$. One may show that $C_1 \cap C_2 = \{y\}$ and $C_1 \cup C_2$ is a saturated chain in $[x, z]$. The result follows by definition of catenary.

Conversely, consider a saturated chain between x and y of length n

$$x = x_0 \lneq x_1 \lneq \ldots \lneq x_n = y$$

Then clearly $\operatorname{codim}(x_i, x_{i+1}) = 1$ for all $i = 0 \ldots n-1$. Therefore by repeatedly applying the relation we may show that

$$\operatorname{codim}(x, y) = n$$

and therefore every saturated chain between x and y has the same length.

When $\mathcal{G}$ is irreducible we may deduce the second formula by setting $x = \top$. Conversely we may see that

$$\operatorname{codim}(z, x) = \operatorname{codim}(z) - \operatorname{codim}(x) = \operatorname{codim}(z) - \operatorname{codim}(y) + \operatorname{codim}(y) - \operatorname{codim}(x) = \operatorname{codim}(z, y) + \operatorname{codim}(y, x)$$

□

Lemma 2.5.10
Let $\mathcal{G}$ be a biequidimensional finite-dimensional poset. Then for $x \in \mathcal{G}$ we have

a) *$\{x\}^{\downarrow}$ and $\{x\}^{\uparrow}$ are biequidimensional*

b) *$\dim(\mathcal{G}) = \dim(x) + \operatorname{codim}(x)$*

c) *If x is maximal then $\dim(x) = \dim(\mathcal{G})$ and in particular $\mathcal{G}$ is equidimensional*

d) *If x is minimal then $\operatorname{codim}(x) = \dim(\mathcal{G})$ and in particular $\mathcal{G}$ is equicodimensional*

In particular $\mathcal{G}$ is quasi-biequidimensional.

Proof. Consider a fixed maximal chain C of $\{x\}^{\uparrow}$, necessarily containing x. Any maximal chain C' of $\{x\}^{\downarrow}$ also contains x and combines with C to yield a maximal chain of $\mathcal{F}$. Whence $\ell(C') + \ell(C) = \dim(\mathcal{F})$ and $\{x\}^{\downarrow}$ is biequidimensional. By duality $\{x\}^{\uparrow}$ is biequidimensional and $\ell(C) = \operatorname{codim}(x)$ from which the formula follows.

If x is maximal then clearly $\operatorname{codim}(x) = 0$, and similarly if x is minimal then $\dim(x) = 0$, so the last two statements follow immediately.

□

Lemma 2.5.11
Let $\mathcal{G}$ be a quasi-biequidimensional finite-dimensional poset. Then for every $x \in \mathcal{G}$ we have $\{x\}^{\downarrow}$ is biequidimensional.

If in addition $\mathcal{G}$ is equidimensional then $\mathcal{G}$ is biequidimensional.

Proposition 2.5.12 (Equivalent Characterizations of Biequidimensionality)
Let $\mathcal{G}$ be a finite-dimensional poset. Then the following are equivalent

a) *$\mathcal{G}$ is quasi-biequidimensional*

b) *$\mathcal{G}$ is catenary and for every maximal x we have $\{x\}^{\downarrow}$ is equicodimensional*

c) *$\mathcal{G}$ satisfies $\dim(x) = \dim(y) + \operatorname{codim}(y, x)$ for $y \leq x$*

d) *$\mathcal{G}$ satisfies c) whenever $\operatorname{codim}(y, x) = 1$*

Furthermore the following relationship holds

$$\operatorname{codim}(y) = \operatorname{codim}(y, x) + \operatorname{codim}(x) \quad y \leq x$$

Proof. *a)* $\implies$ *c)*. By assumption $\{x\}^{\downarrow}$ is biequidimensional. Then

$$\dim(x) = \dim(\{x\}^{\downarrow}) \overset{(2.5.10)}{=} \dim(y; \{x\}^{\downarrow}) + \operatorname{codim}(y; \{x\}^{\downarrow}) = \dim(y) + \operatorname{codim}(y, x)$$

For *c)* $\implies$ *b)*. Suppose $z < y < x$ in $\mathcal{G}$ then by the codimension formula applied twice

$$\operatorname{codim}(z,x) = \dim(x) - \dim(z) = \dim(x) - \dim(y) + \dim(y) - \dim(z) = \operatorname{codim}(y,x) + \operatorname{codim}(z,y)$$

so by (2.5.9) $\mathcal{G}$ is catenary. Let x be a maximal element and z a minimal element of $\{x\}^{\downarrow}$, then by the codimension formula

$$\operatorname{codim}(z,x) = \dim(x) - \dim(z) = \dim(x)$$

whence $\{x\}^{\downarrow}$ is equicodimensional.

b) $\implies$ *a)*. Let x be a maximal element and C a maximal chain in $\{x\}^{\downarrow}$ with minimum element y then, as $\mathcal{G}$ is catenary, we have $\ell(C) = \operatorname{codim}(y,x)$. As $\{x\}^{\downarrow}$ is equicodimensional we have $\operatorname{codim}(y,x) = \dim(x)$ which shows that $\{x\}^{\downarrow}$ is biequidimensional.

Clearly *c)* $\implies$ *d)*. Conversely for *d)* $\implies$ *a)* consider a maximal chain in $\{x\}^{\downarrow}$

$$x_0 \lneq \ldots \lneq x_n = x$$

Then clearly $\operatorname{codim}(x_i, x_{i+1}) = 1$ whence by induction $\ell(C) = \dim(x)$.

The final statement follows from (2.5.9) because $\{x\}^{\downarrow}$ is irreducible and catenary. □

Remark 2.5.13
This is a corrected version of EGA IV 14.3.3, as noted by Heinrich.

Corollary 2.5.14
When $\mathcal{F}$ is a quasi-biequidimensional Krull Lattice then we have the following codimension formulas for $x, y \in \mathcal{F}$.

$$\begin{aligned} \dim(x) &= \dim(y) + \operatorname{codim}(y,x) \\ \operatorname{codim}(y) &= \operatorname{codim}(y,x) + \operatorname{codim}(x) \end{aligned}$$

Furthermore

$$\dim(\mathcal{F}) = \dim(y) + \operatorname{codim}(y)$$

Proof. The first two relations hold when $x, y \in \mathcal{J}(\mathcal{F})$ by (2.5.12). We may generalise this as follows.

For fixed $y \in \mathcal{J}(\mathcal{F})$ the first relation shows $\dim(x_i)$ is maximal precisely when $\operatorname{codim}(y, x_i)$ is maximal so it holds for any $x \in \mathcal{F}$. Similarly for fixed $x \in \mathcal{F}$ we see $\dim(y_j)$ is maximal precisely when $\operatorname{codim}(y_j, x)$ is minimal. Therefore it holds for all $y \in \mathcal{F}$.

A similar argument applies to the second relationship. The final statement follows from the first relation by taking the supremum over all maximal elements x. □

Corollary 2.5.15
Let $\mathcal{G}$ be an irreducible finite-dimensional poset. Then the following are equivalent

a) *$\mathcal{G}$ is biequidimensional*

b) *$\mathcal{G}$ is quasi-biequidimensional*

c) *$\mathcal{G}$ is catenary and equicodimensional*

d) $\dim(x) = \dim(y) + \operatorname{codim}(y,x) \quad \forall y \leq x$

e) *$\mathcal{G}$ satisfies d) when* $\operatorname{codim}(y,x) = 1$

Proof. The equivalence follows from (2.5.12) by noting that an irreducible poset has only one maximal element and is in particular equidimensional. □

2.6 Category Theory

2.6.1 Categories

Definition 2.6.1 (Category)
A (locally small) ***category*** *$\mathcal{C}$ consists of*

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

- *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 2.6.2
The category of sets is **Set** *with maps in the usual way. Note associativity is automatically satisfied.*

Example 2.6.3 (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 2.6.4 (Opposite Category)
Given a category $\mathcal{C}$ the ***opposite category*** *is denoted $\mathcal{C}^{op}$ and given by*

- *The same class of objects* $\mathrm{ob}\,\mathcal{C}^{op} = \mathrm{ob}(\mathcal{C})$
- *For every pair of objects $a, b \in \mathrm{ob}\,\mathcal{C}$ the morphisms are reversed*

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

- *The law of composition is reversed*

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

Definition 2.6.5 (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 2.6.6
The polynomial ring $A[X]$ is an initial object in the category of pointed A-algebras.

Definition 2.6.7 (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 2.6.8 (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 η_-^a and $\eta_-^{a'}$ respectively. Then by definition

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

and vice-versa.

□

Definition 2.6.9 (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** $\mathcal{C} \to \mathcal{D}$ is equivalent to a covariant functor on the opposite category $\mathcal{C}^{op} \to \mathcal{D}$, namely where arrows are reversed.*

Definition 2.6.10 (Full and faithful)
A functor F is said to be

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

Definition 2.6.11 (Concrete Category)
*A **concrete category** is a pair $(\mathcal{C}, U)$ where $\mathcal{C}$ and a "**forgetful functor**" $U : \mathcal{C} \to \mathbf{Set}$ which is faithful*

Example 2.6.12 (Forgetful Functor)
The category of groups (resp. rings, modules, ...) is a concrete category in the obvious way.

Definition 2.6.13 (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 2.6.14 (Natural Transformation)
*Let $F, G : \mathcal{C} \to \mathcal{D}$ be covariant 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 2.6.15 (Natural isomorphism)
A natural transformation $\eta : F \Rightarrow G$ is a natural isomorphism if η_c is an isomorphism for all $c \in \mathcal{C}$.

Definition 2.6.16
*We say $\mathcal{C}' \subset \mathcal{C}$ is a **subcategory** if*

- $\mathrm{ob}(\mathcal{C}') \subseteq \mathrm{ob}(\mathcal{C})$
- $\mathrm{Mor}_{\mathcal{C}'}(c, d) \subseteq \mathrm{Mor}_{\mathcal{C}}(c, d)$
- *Composition agrees when it is well-defined*

*We say $\mathcal{C}'$ is a **full subcategory** if additionally $\mathrm{Mor}_{\mathcal{C}'}(c, d) = \mathrm{Mor}_{\mathcal{C}}(c, d)$.*

2.6.2 Product Categories and Bifunctors

Definition 2.6.17 (Product Category)
Given two categories $\mathcal{C}$, $\mathcal{D}$ we may construct the product category $\mathcal{C} \times \mathcal{D}$ as follows

- *The objects are given by pairs*

$$\mathrm{ob}(\mathcal{C} \times \mathcal{D}) := \mathrm{ob}(\mathcal{C}) \times \mathrm{ob}(\mathcal{D})$$

- *The morphisms are given by pairs*

$$\mathrm{Mor}((c, c'), (d, d')) := \mathrm{Mor}(c, c') \times \mathrm{Mor}(d, d')$$

  Concretely given $f : c \to c'$ and $g : d \to d'$ write $f \times g : (c, d) \to (c', d')$

- *The law of composition is determined by*

$$(f \times g) \circ (h \times k) := (f \circ h) \times (g \circ k)$$

It's clear that the law of composition is associative and the identity morphism for (c, d) is $(1_c, 1_d)$. Furthermore we observe the following property

$$(f \times 1_d) \circ (1_c \times g) = (f \times g) = (1_c \times g) \circ (f \times 1_d) \tag{2.7}$$

Definition 2.6.18 (Bifunctor)
*A functor on a product category, $F : \mathcal{C} \times \mathcal{D} \to \mathcal{E}$ is termed a **bifunctor**. F induces a family of functors*

- *$F(c, -) : \mathcal{D} \to \mathcal{E}$ given by*

$$F(c, g) := F(1_c \times g)$$

- *$F(-, d) : \mathcal{C} \to \mathcal{E}$ given by*

$$F(f, d) := F(f \times 1_d)$$

which satisfy the compatibility conditions

$$\begin{array}{ccc} F(c,d) & \xrightarrow{F(f,d)} & F(c',d) \\ {\scriptstyle F(c,g)}\downarrow & \searrow^{F(f,g)} & \downarrow{\scriptstyle F(c',g)} \\ F(c,d') & \xrightarrow[F(f,d')]{} & F(c',d') \end{array}$$

by applying F to Eq. (2.7).

Proposition 2.6.19 (Reconstruct Bifunctor)
Consider a family of functors $\{F_L(c) : \mathcal{D} \to \mathcal{E}\}_{c \in \mathrm{ob}(C)}$ and $\{F_R(d) : \mathcal{C} \to \mathcal{E}\}_{d \in \mathrm{ob}(\mathcal{D})}$. Suppose the following conditions hold

- $F_L(c)(d) = F_R(d)(c)$
- $F_L(c')(g) \circ F_R(d)(f) = F_R(d')(f) \circ F_L(c)(g)$

then these determine a well-defined bifunctor given by

$$F(f \times g) := F_L(c')(g) \circ F_R(d)(f)$$

Proposition 2.6.20
Let $F : \mathcal{C} \times \mathcal{D} \to \mathcal{E}$ be a bifunctor. For $f : c \to c'$ then there is a natural transformation

$$F(f, -) : F(c, -) \Rightarrow F(c', -)$$

given by $F(f, -)_d := F(f, 1_d)$. Similarly for $g : d \to d'$ then there is a natural transformation

$$F(-, g) : F(-, d) \Rightarrow F(-, d')$$

Proof. The naturality condition is immediate from Equation (2.7) and the commutative diagram in (2.6.18). □

Proposition 2.6.21 (Criteria for Natural Transformation)
Let $F, G : \mathcal{C} \times \mathcal{D} \to \mathcal{E}$ be two bifunctors and suppose we have a family of natural transformations

$$\eta_c : F(c, -) \Rightarrow G(c, -)$$

for all $c \in \mathcal{C}$. Then the following are equivalent

a) *$\eta : F(-,-) \Rightarrow G(-,-)$ is a natural transformation*

b) *The following diagram commutes for all $d \in \mathcal{D}$ and $f : c \to c'$*

$$\begin{array}{ccc} F(c,d) & \xrightarrow{\eta_{c,d}} & G(c,d) \\ {\scriptstyle F(f\times 1_d)}\downarrow & & \downarrow{\scriptstyle G(f\times 1_d)} \\ F(c',d) & \xrightarrow{\eta_{c',d}} & G(c',d) \end{array}$$

Proof. *a)* $\implies$ *b)* This diagram is a special case of the naturality condition.

b) $\implies$ *a)* Suppose $f : c \to c'$ and $g : d \to d'$ then we require to show that

$$G(f \times g)(\eta_{c,d}(\phi)) = \eta_{c',d'}(F(f \times g)(\phi))$$

However

$$\begin{aligned} G(f \times g)(\eta_{c,d}(\phi)) &= G(f \times 1_{d'})(G(1_c \times g)(\eta_{c,d}(\phi))) \\ &= G(f \times 1_{d'})\eta_{c,d'}(F(1_c \times g)(\phi)) \\ &= \eta_{c',d'}(F(f \times 1_{d'})(F(1_c \times g)(\phi))) \\ &= \eta_{c',d'}(F(f \times g)(\phi)) \end{aligned}$$

where we have used that $\eta_{c,d}$ is natural in d and c individually. □

Example 2.6.22 (Mor is a bifunctor)
The canonical example is the following, given any locally small category $\mathcal{C}$, we have a bifunctor

$$\mathrm{Mor} : \mathcal{C}^{op} \times \mathcal{C} \to \mathbf{Set}$$

given by the set of morphisms. The action on morphisms is given by

$$\mathrm{Mor}(f \times g)(\phi) = g \circ \phi \circ f$$

and we verify by associativity of $\mathcal{C}$ that

$$\mathrm{Mor}((f \times g) \circ (h \times k)) = \mathrm{Mor}(f \times g) \circ \mathrm{Mor}(h \times k)$$

and it's clear that the commutativity condition in Eq. (2.7) is satisfied.

Example 2.6.23 (Concrete bifunctors)
Let $\mathcal{C}$, $\mathcal{D}$ be concrete categories and consider the following bifunctor

$$\begin{aligned} F &: \mathcal{D}^{op} \times \mathcal{C} \to \mathbf{Set} \\ F(d,c) &:= \{\phi : d \to c \mid P(\phi)\} \end{aligned}$$

where $P(-)$ is some predicate such that $P(\phi) \implies P(g \circ \phi \circ f)$.

2.6.3 Equivalence of categories

Definition 2.6.24 (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 2.6.25
*We say a functor $F : \mathcal{C} \to \mathcal{D}$ 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 2.6.26
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 η_c is an isomorphism we may cancel to find $GF(\eta_c) = \eta_{GF(c)}$. □

Proposition 2.6.27 (Equivalence is full and faithful)
Let $F : \mathcal{C} \to \mathcal{D}$ be a functor 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 η and ϵ^{-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 ϵ so F is essentially surjective. □

Proposition 2.6.28 (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. □

2.6.4 Properties of Morphisms

Definition 2.6.29 (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 2.6.30
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 2.6.31 (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 2.6.32 (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 2.6.33 (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 2.6.34 (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 2.6.35 (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 2.6.36 (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 (2.6.35).
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 2.6.37
For the category **Set** *we have*

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

Definition 2.6.38 (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 2.6.39
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 2.6.40
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 (2.6.39) and so by (2.6.37) $U(f)$ is injective.

Suppose $U(f)$ injective, then by (2.6.37) $U(f)$ is monic. By (2.6.39) U reflects monics and so f is monic.

The other statements are similar. □

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

Proposition 2.6.41
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 2.6.42 (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 (2.6.41) with (2.6.36). □

Definition 2.6.43 (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*

2.6.5 Directed Limits

Definition 2.6.44 (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 2.6.45 (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

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

*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*

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

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, ϕ_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 2.6.46 (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

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

where we consider the equivalence relation

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

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

Proposition 2.6.47 (Restricted Direct Limit)
Let I be a directed category and I' a full subcategory which is also directed. Suppose the limits

$$A := \varinjlim_{i \in I} A_i$$

$$A' := \varinjlim_{i \in I'} A_i$$

exist. Then there is a unique morphism

$$\Phi : A' \to A$$

such that

$$\Phi \circ \phi'_{i'} = \phi_{i'} \quad \forall i' \in I'$$

Suppose that

- *there exists $\pi : \mathrm{ob}(I) \to \mathrm{ob}(I')$ such that $\pi(i) \prec i$*

Then this morphism is an isomorphism with two-sided inverse $\Psi : A \to A'$ such that $\Psi \circ \phi_{i'} = \phi'_{i'}$ for all $i' \in I'$.

Proof. Given the property we may define a morphism $\Psi : A \to A'$ such that $\Psi \circ \phi_i = \phi'_{\pi(i)} \circ \rho_{i\pi(i)}$. Then considering the morphism $\Phi \circ \Psi : A \to A$ we see

$$\Phi \circ \Psi \circ \phi_i = \Phi \circ \phi'_{\pi(i)} \circ \rho_{i\pi(i)} = \phi_{\pi(i)} \circ \rho_{i\pi(i)} = \phi_i \quad \forall i \in I$$

By uniqueness $\Phi \circ \Psi = 1_A$. Similarly

$$\Psi \circ \Phi \circ \phi'_{i'} = \Psi \circ \phi_{i'} = \phi'_{\pi(i')} \circ \rho_{i'\pi(i')} = \phi'_{i'}$$

whence $\Psi \circ \Phi = 1_A$ as required. □

2.6.6 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 2.6.48 (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

$$\psi_{c',d'}(\beta \circ f \circ F(\alpha)) = G(\beta) \circ \psi_{c,d}(f) \circ \alpha \tag{2.8}$$

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

$$\beta \circ \psi^{-1}_{c,d}(g) \circ F(\alpha) = \psi^{-1}_{c',d'}(G(\beta) \circ g \circ \alpha) \tag{2.9}$$

Proposition 2.6.49 (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

$$\begin{aligned} G(F(\alpha)) \circ \eta_c &= G(F(\alpha)) \circ \psi_{c,F(c)}(1_{F(c)}) \\ &= \psi_{c,F(c')}(F(\alpha) \circ 1_{F(c)}) \quad (2.8) \\ &= \psi_{c,F(c')}(1_{F(c')} \circ F(\alpha)) \\ &= \psi_{c',F(c')}(1_{F(c')}) \circ \alpha \quad (2.8) \\ &= \eta_{c'} \circ \alpha \end{aligned}$$

so η 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 $\beta : d \to d'$

$$\begin{aligned} \beta \circ \epsilon_d &= \beta \circ \psi^{-1}_{G(d),d}(1_{G(d)}) \\ &= \psi^{-1}_{G(d),d'}(G(\beta) \circ 1_{G(d)}) \quad (2.9) \\ &= \psi^{-1}_{G(d),d'}(1_{G(d')} \circ G(\beta)) \\ &= \psi^{-1}_{G(d'),d'}(1_{G(d')}) \circ F(G(\beta)) \quad (2.9) \\ &= \epsilon_{d'} \circ F(G(\beta)) \end{aligned}$$

□

Given two natural transformations we may recover a corresponding adjoint

Proposition 2.6.50 (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 η, ϵ*

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

$$1_{G(d)} : G(d) \xrightarrow{\eta_{G(d)}} GFG(d) \xrightarrow{G(\epsilon_d)} G(d) \tag{2.10}$$

$$1_{F(c)} : F(c) \xrightarrow{F(\eta_c)} FGF(c) \xrightarrow{\epsilon_{F(c)}} F(c) \tag{2.11}$$

More precisely the adjunction is given by

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

Proof. Let ψ, ϕ denote the proposed adjunction maps. We will use the triangular identities to show that these are mutually inverse. First observe by naturality of η and ϵ that

$$\psi\phi(g) = G(\epsilon_d \circ F(g)) \circ \eta_c = G(\epsilon_d) \circ \eta_{G(d)} \circ g \tag{2.12}$$

$$\phi\psi(f) = \epsilon_d \circ F(G(f) \circ \eta_c) = f \circ \epsilon_{F(c)} \circ F(\eta_c) \tag{2.13}$$

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 ψ, ϕ 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 2.6.51 (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 η, ϵ unit and counit transformations. Then

- *G is faithful if and only if ϵ is pointwise epic*
- *G is full if and only if ϵ is pointwise split-monic*
- *G is full and faithful if and only if ϵ 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 (2.6.41) $\mathrm{Mor}(\epsilon_{d'}, d)$ 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 (2.6.36). □

The following criteria will be useful

Proposition 2.6.52 (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 η, ϵ induce an adjoint relationship between F and G as in (2.6.50).

Proof. Recall the proposed adjoint maps from (2.6.50), ψ and ϕ, 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. ϕ has a left-inverse and ψ has a right inverse.

Suppose that the given map ψ is injective, then by (2.6.37) ψ has a left-inverse too. By (2.6.36) ψ is an isomorphism with inverse $\psi^{-1} = \phi$.

The case that ϕ is surjective is similar. □

2.6.7 Yoneda Lemma

The motivation for the following result becomes more clear in the next section. Roughly speaking properties of an object, c, are encoded in the functor $\mathrm{Mor}(c, -)$.

Proposition 2.6.53 (Yoneda Lemma)
Suppose $c, c' \in \mathcal{C}$ then there is a bijection between morphisms and natural transformation of functors

$$\begin{array}{rcl} \mathrm{Mor}(c', c) & \xrightarrow{\sim} & \mathrm{Nat}(\mathrm{Mor}(c, -), \mathrm{Mor}(c', -)) \\ f & \longrightarrow & \mathrm{Mor}(f, -) : (\phi \to \phi \circ f) \\ \alpha_c(1_c) & \longleftarrow & \alpha \end{array}$$

Observe that under this correspondence

- $f = \mathrm{Mor}(f, c)(1_c)$
- $\mathrm{Mor}(f \circ g, -) = \mathrm{Mor}(g, -) \circ \mathrm{Mor}(f, -)$
- *f is an isomorphism* $\iff$ $\mathrm{Mor}(f, -)$ *is a natural isomorphism.*

In the latter case $\mathrm{Mor}(f, -)^{-1} = \mathrm{Mor}(f^{-1}, -)$

In many cases the set of morphisms $\mathrm{Mor}(c, c')$ has an additional structure (typically an abelian group or module). We encode this with the following definition

Definition 2.6.54 (Enriched Hom Functor)
Let $(\mathcal{S}, U)$ be a concrete category for which U reflects isomorphisms. We say a bifunctor

$$\mathrm{Hom} : \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{S}$$

*is an **enriched hom functor** if we have $U(\mathrm{Hom}(c, d)) = \mathrm{Mor}(c, d)$ and bijections*

$$\begin{array}{ccc} & \mathrm{Mor}(c', c) & \\ {\scriptstyle \mathrm{Hom}(f,-)}\swarrow_{\sim} & & \searrow^{\sim}{\scriptstyle \mathrm{Mor}(f,-)} \\ \mathrm{Nat}(\mathrm{Hom}(c, -), \mathrm{Hom}(c', -)) & \xrightarrow[\sim]{U} & \mathrm{Nat}(\mathrm{Mor}(c, -), \mathrm{Mor}(c', -)) \end{array}$$

Write the inverse of $f \to \mathrm{Hom}(f, -)$ as $\mathcal{Y}$. Then for $\alpha \in \mathrm{Nat}(\mathrm{Hom}(c, -), \mathrm{Hom}(c', -))$

a) *α is a natural isomorphism* $\iff$ *$U\alpha$ is a natural isomorphism* $\iff$ *$\mathcal{Y}(\alpha)$ is an isomorphism.*

b) $\mathcal{Y}(\alpha) = U(\alpha_c)(1_c)$

Note the right hand arrow is always a bijection by Yoneda's Lemma (2.6.53) and the diagram always commutes by assumption.

Note this trivially includes the usual case $\mathcal{S} = \mathbf{Set}$.

2.6.8 Representable Functors

Many algebraic constructions (e.g. tensor product) may be formalised in terms of "representable" functors (2.6.55). The usual definition involves the set-valued functor $\mathrm{Mor}(c, -)$ as defined in (2.6.13).

As a generalisation follows we consider an enriched hom functor $\mathrm{Hom}(-, -)$ taking values in the concrete category $(\mathcal{S}, U)$ and where U reflects isomorphisms. This clearly generalises the usual case.

Definition 2.6.55 (Representable Functor)
*Let $F : \mathcal{C} \to \mathcal{S}$ a functor. We say F is **representable** if there is a pair (x, Φ) where $x \in \mathcal{C}$ and Φ is a natural isomorphism*

$$\mathrm{Hom}(x, -) \xrightarrow[\sim]{\Phi} F(-)$$

*We say F is **represented** by the pair (x, Φ). Note this implies $U \circ F$ is represented by $U\Phi$.*

It is often useful to have another conception of representable functor in terms of universal properties as this is more intuitive for applications.

Definition 2.6.56 (Universal Element)
*Let $F : \mathcal{C} \to \mathcal{S}$ be a functor, then we say that a pair (x, i), where $x \in \mathcal{C}, i \in (U \circ F)(x)$, is a **universal element** for F if for all $c \in \mathcal{C}$ there are bijections*

$$\begin{array}{rcl} \mathrm{Mor}(x, c) & \longrightarrow & (U \circ F)(c) \\ f & \to & (U \circ F)(f)(i) \end{array} \tag{2.14}$$

*In this case we may also say F is **represented** by the universal element (x, i).*

We show the equivalence of the two notions by some abstract nonsense

Proposition 2.6.57 (Representable Functor = Universal Element)
Let $F : \mathcal{C} \to \mathcal{S}$ be a functor then there is a natural correspondence between representations and universal elements

$$\begin{array}{rcl} \left\{ \text{ representations of } F \right\} & \longleftrightarrow & \left\{ \text{ universal elements of } F \right\} \\ (x, \Phi) & \longrightarrow & (x, (U\Phi)(1_x)) \\ (x, U^{-1}\left(f \to (U \circ F)(f)(i)\right)) & \longleftarrow & (x, i) \end{array}$$

The following may in particular be used to show that representations are unique up to isomorphism.

Proposition 2.6.58 (Morphisms Between Representations)
Suppose (x, Φ) and (x', Φ') represent the functors $F, F' : \mathcal{C}^{op} \to \mathcal{S}$ respectively. Then there are bijections

$$\begin{array}{ccccccc} \mathrm{Mor}(x, x') & \xrightarrow{\sim} & \mathrm{Nat}(\mathrm{Hom}(x', -)\,\mathrm{Hom}(x, -)) & \xrightarrow{\sim} & \mathrm{Nat}(F'(-), F(-)) \\ f & \to & \mathrm{Hom}(f, -) & \to & \widehat{f} \\ U(\eta_{x'})(1_{x'}) & \leftarrow & \eta \qquad \Phi^{-1} \circ \alpha \circ \Phi' & \leftarrow & \alpha \end{array}$$

where we define the mutual inverses

$$\begin{array}{rcl} \widehat{f} & = & \Phi \circ \mathrm{Hom}(f, -) \circ (\Phi')^{-1} \\ \alpha^\star & = & U(\Phi_{x'}^{-1} \circ \alpha_{x'} \circ \Phi'_{x'})(1_{x'}) \end{array}$$

Note this has the following properties

- $\widehat{1_x} = \mathrm{id}_F$
- $\widehat{g \circ f} = \widehat{f} \circ \widehat{g}$ *where $g : x' \to x''$ is morphism and (x'', Φ'') represents F''*
- *f is an isomorphism $\iff$ $\widehat{f}$ is a natural isomorphism and in this case $\widehat{f^{-1}} = \widehat{f}^{-1}$.*

Further $\alpha^\star$ is the unique morphism such that the following diagram of natural transformations commutes

$$\begin{array}{ccc} \mathrm{Hom}(x', -) & \xRightarrow{\Phi'} & F'(-) \\ {\scriptstyle \mathrm{Hom}(\alpha^\star, -)}\downarrow & & \downarrow{\scriptstyle \alpha} \\ \mathrm{Hom}(x, -) & \xRightarrow{\Phi} & F(-) \end{array}$$

and satisfies

- $\mathrm{id}_F^\star = 1_x$
- $(\beta \circ \alpha)^\star = \alpha^\star \circ \beta^\star$
- *$\alpha^\star$ is an isomorphism $\iff$ α is a natural isomorphism*

Proof. The first bijection is simply the Yoneda Lemma and the second bijection is obvious. □

Corollary 2.6.59 (Representation is Unique)
Let $F : \mathcal{C} \to \mathcal{S}$ be a functor which is represented by pairs (x, Φ) and (x', Φ'). Then they are isomorphic with two-sided inverses

$$x \underset{U(\Phi'^{,-1})(i)}{\overset{U(\Phi^{-1})(i')}{\rightleftarrows}} x'$$

where $i := (U\Phi)(1_x)$ and $i' := (U\Phi')(1_{x'})$.

Proof. We may apply the previous result with $F = F'$ and the identity natural transformation id_F. □

In practice we typically have a family of representations, and we want to show the construction is functorial

Definition 2.6.60 (Representable Bifunctor)
*Let $F : \mathcal{D}^{op} \times \mathcal{C} \to \mathcal{S}$ be a bifunctor. We say that it is **representable** by (G, Φ) where $G : \mathcal{D} \to \mathcal{C}$ is a functor, if Φ is a natural isomorphism of bifunctors*

$$\Phi : \mathrm{Hom}(G(-), -) \xRightarrow{\sim} F(-, -)$$

The following shows we only need to construct the representation pointwise.

Proposition 2.6.61
Let $F : \mathcal{D}^{op} \times \mathcal{C} \to \mathcal{S}$ be a bifunctor such that $F(d, -)$ is representable for all $d \in \mathcal{D}$, by $(G(d), \Phi_d)$. Then G can be made into a covariant functor uniquely such that Φ constitutes a natural isomorphism of bifunctors

$$\Phi : \mathrm{Hom}(G(-), -) \xRightarrow{\sim} F(-, -)$$

Denote by $i_d := (U\Phi)_{d,G(d)}(1_{G(d)}) \in (U \circ F)(d, G(d))$ the universal element corresponding to d. Then we have

$$(U \circ F)(1_d \times G(h))(i_d) = (U\Phi)_{d,G(d')}(G(h)) = (U \circ F)(h \times 1_{G(d')})(i_{d'})$$

Proof. It is straightforward to verify that for any covariant functor G, the mapping $\mathrm{Mor}(G(-), -)$ is a bifunctor (contravariant in the first "slot").

By (2.6.20) $F(h, -) : F(d', -) \to F(d, -)$ is a natural transformation. Therefore we may define

$$G(h) := F(h, -)^\star$$

in the notation of (2.6.58). Explicitly we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(G(d'), -) & \xRightarrow{\Phi_{d'}} & F(d', -) \\ {\scriptstyle \mathrm{Hom}(G(h),-)}\downarrow & & \downarrow{\scriptstyle F(h,-)} \\ \mathrm{Hom}(G(d), -) & \xRightarrow{\Phi_d} & F(d, -) \end{array}$$

Furthermore $G(h \circ k) = F(h \circ k, -)^\star = (F(k, -) \circ F(h, -))^\star = F(h, -)^\star \circ F(k, -)^\star = G(h) \circ G(k)$. We conclude by (2.6.21) that Φ is a natural transformation of bifunctors.

The last statement follows by chasing $1_{G(d')}$ round the commutative diagram and using Equation (2.14). □

Example 2.6.62 (Concrete Interpretation)
Let $\mathcal{C}$, $\mathcal{D}$ be concrete categories and consider the following bifunctor

$$\begin{aligned} F &: \mathcal{D}^{op} \times \mathcal{C} \to \mathbf{Set} \\ F(d, c) &:= \{\phi : d \to c \mid P(\phi)\} \end{aligned}$$

where $P(-)$ is some predicate such that $P(\phi) \implies P(g \circ \phi \circ f)$. Then the universal element is simply an object $G(d) \in \mathcal{C}$ together with a mapping

$$i_d : d \to G(d)$$

satisfying P such that there is a bijection

$$\begin{array}{ccc} \mathrm{Mor}(G(d), c) & \xleftrightarrow{\sim} & F(d, c) := \{f : d \to c \mid P(f)\} \\ \phi & \longrightarrow & \phi \circ i_d \end{array}$$

The functoriality of G corresponds to a commutative diagram

$$\begin{array}{ccc} d & \xrightarrow{\quad f \quad} & d' \\ \downarrow{\scriptstyle i_d} & & \downarrow{\scriptstyle i'_d} \\ G(d) & \xrightarrow{\quad G(f) \quad} & G(d') \end{array}$$

where $G(f)$ is the unique morphism making the diagram commute.

Proposition 2.6.63 (Functorial Yoneda Lemma)
Let $G, G' : \mathcal{D} \to \mathcal{C}$ be functors. Then there is a bijection

$$\begin{array}{ccc} \mathrm{Nat}(G(-), G'(-)) & \xrightarrow{\sim} & \mathrm{Nat}(\mathrm{Hom}(G'(-), -)\,\mathrm{Hom}(G(-), -)) \\ f_d & \to & \mathrm{Hom}(f_d, 1_c) \\ U(\eta_{d,G'(d)})(1_{G'(d)}) & \leftarrow & \eta_{d,c} \end{array}$$

We have the following properties

- $\widehat{\mathrm{id}_G} = \mathrm{id}$
- $\widehat{g \circ f} = \widehat{f} \circ \widehat{g}$
- *f is a natural isomorphism iff* $\mathrm{Hom}(f, -)$ *is a natural isomorphism*

Proof. In order to demonstrate that $\mathrm{Hom}(f_d, 1_c)$ is a natural transformation of bifunctors it's enough by (2.6.20) to show the following diagram commutes for $h : d' \to d$

$$\begin{array}{ccc} \mathrm{Hom}(G'(d), c) & \xrightarrow{\circ f_d} & \mathrm{Hom}(G(d), c) \\ \downarrow{\scriptstyle \circ G'(h)} & & \downarrow{\scriptstyle \circ G(h)} \\ \mathrm{Hom}(G'(d'), c) & \xrightarrow{\circ f_{d'}} & \mathrm{Hom}(G(d'), c) \end{array}$$

However $f_d \circ G(h) = G'(h) \circ f_{d'}$ by definition of natural transformation, from which it follows immediately. The map is a pointwise bijection (for every $d \in D$) with the inverse given by the usual Yoneda Lemma.

The first two properties are straightforward. From these it follows that if f is a natural isomorphism then so is $\mathrm{Hom}(f, -)$. Conversely if $\mathrm{Hom}(f, -)$ is a natural isomorphism then it has a two-sided inverse which is of the form $\mathrm{Hom}(g, -)$. It's then straightforward to argue that g is a two-sided inverse of f.

□

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 ϕ is **unital** if*

$$\phi(e_X) = e_Y$$

*If $(X,\cdot)$ and $(Y,\cdot)$ are monoids then ϕ 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 ϕ 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*

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \downarrow{\scriptstyle \pi} & \nearrow_{\tilde{\phi}} & \\ G/N & & \end{array}$$

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 (2.2.6) 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 (2.2.5) 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) $(g^r)^s = e_G \iff g^{rs} = e_G \overset{(3.3.14)}{\iff} n \mid rs \overset{(2.2.13)}{\iff} \frac{n}{(n,r)} \mid s$. 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 π 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

$$\#G = \#Gs$$

3.3.3 Symmetric Group

Definition 3.3.33 (Symmetric Group)
Let S_n denote the set of permutations (bijections) of $J_n := \{1, \ldots, n\}$.

*Permutations $\sigma, \tau \in S_n$ are called **disjoint** if the supports are disjoint. Note disjoint permutations commute.*

Definition 3.3.34 (Cycle)
Let $i_1, \ldots, i_r \in J_n$ be an ordered r-tuple, the permutation which maps

$$i_k \to \begin{cases} i_{k+1} & k < r \\ i_1 & k = r \end{cases}$$

*is denoted by $(i_1\, i_2 \ldots\, i_r)$ and called a **cycle**.*

*A cycle with two elements $(i\, j)$ is called a **transposition**. Finally an **adjacent transposition** is one of the form $(i\, i+1)$.*

Proposition 3.3.35
Let $\sigma \in S_n$. Then σ may be represented by

a) *a product of disjoint cycles, which is unique up to permutation of cycles.*

b) *a product of transpositions, the number of which is unique modulo 2*

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.*

Example 3.4.2
The set of integers (Section 2.2.1) $\mathbb{Z}$ is the canonical example of a ring with operations of addition and multiplication.

Definition 3.4.3 (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 3.4.4 (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 3.4.5 (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 3.4.6 (Reduced)
A commutative ring A is said to be ***reduced*** *if for all $a \in A$*

$$a^n = 0 \implies a = 0$$

Definition 3.4.7 (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 3.4.8 (Field)
A ***field*** *K is a commutative non-zero ring such that every non-zero element is a unit, so that $K^\star$ is a group under multiplication and $K^\star = K \setminus \{0\}$.*

Proposition 3.4.9
Every subring of a field K is an integral domain.

Proof. Suppose $A \subset K$ is a subring. Suppose that $a, b \in A$ such that $ab = 0$. Suppose $a \neq 0$ then $a^{-1}ab = 0 \implies b = 0$. □

Note we have the implications

Corollary 3.4.10
Let A be a ring then we have the following implications

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

Definition 3.4.11 (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 ϕ is defined to be*

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

Definition 3.4.12 (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 3.4.13 (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 3.4.14
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) *ϕ is injective if and only if $\ker(\phi) = \{0\}$*

Proposition 3.4.15 (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.

Proposition 3.4.16 (Criteria to be a Field)
Let A be a ring. Then the following are equivalent

a) *A is a field*

b) *A is not the zero-ring and the only proper ideal is $\{0\}$.*

Proof. *a)* $\implies$ *b)*. By definition A is not the zero-ring. Let $\mathfrak{a}$ be a proper ideal. By (3.4.13) $\mathfrak{a} \cap A^\star = \emptyset \implies \mathfrak{a} = \{0\}$ as required.

b) $\implies$ *a)*. Suppose $0 \neq a \in A$ then the ideal $Aa = (a)$ is either $\{0\}$ or A. However $a = 1 \cdot a \in (a)$ which implies $(a) \neq \{0\}$ and therefore $(a) = A$. In particular there exists $a^{-1} \in A$ such that $a^{-1}a = 1_A$ and a is invertible. □

3.4.2 Modules I

Definition 3.4.17 (Module)
*Let A be a ring. A **left A-module** $(M, +, \cdot)$ is an abelian group $(M, +)$ together with a "multiplication" operation*

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

which satisfies the following properties

- $(a \times_A a') \cdot x = a \cdot (a' \cdot x)$
- $(a +_A a') \cdot x = a \cdot x + a' \cdot x$
- $a \cdot (x + y) = a \cdot x + a \cdot y$

*Similarly a **right A-module** $(M, +, \cdot)$ is an abelian group $(M, +)$ together with a multiplication operation*

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

- $(a \times_A a') \cdot x = (x \cdot a') \times_A a$
- $(a +_A a') \cdot x = a \cdot x + a' \cdot x$
- $a \cdot (x + y) = a \cdot x + a \cdot y$

*Considering the first property M is a left A-module iff it is a right A^{op} module in the obvious way. Therefore in the usual case that A is commutative the concepts coincide and we may speak simply of an **A-module**, though we almost always write the action on the left.*

Similarly almost all results for left A-modules carry over unchanged for right A-modules. In this case we may simply by refer to A-modules rather than state the result for both cases separately.

Definition 3.4.18 (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. Similar definition applies for a right A-module.

Definition 3.4.19 (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. In this way we have the following categories

- *A-**Mod** the category of modules over a* commutative *ring A*
- *${}_A$**Mod** the category of left A-modules*
- *$\mathbf{Mod}_A$ the category if right A-modules*

Definition 3.4.20 (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 3.4.21 (Trivial Examples)
A ring A is a left A-module over itself, denoted A_s.

Definition 3.4.22 (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 3.4.23 (Submodules constitute a lattice)
Let M be an 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 (2.1.40) 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 3.4.24
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 (2.1.43) 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 3.4.25 (Hom Sets)
*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 abelian group of A-module homomorphisms

$$\mathrm{Hom}_A(M, N)$$

and the endomorphism ring

$$\mathrm{End}_A(M) := \mathrm{Hom}_A(M, M)$$

When A is commutative then these have natural A-module and A-algebra structures respectively.

3.4.3 Operations on Ideals

For this section we assume A is a commutative ring.

Definition 3.4.26 (Product of ideal and module)
Let M be an A-module and $\mathfrak{a} \triangleleft A$ an ideal. Define

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

Proposition 3.4.27 (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 3.4.28
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 3.4.29 (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 3.4.30 (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 3.4.31 (Principal Ideal)
*A **principal ideal** is an ideal generated by a single element*

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

Lemma 3.4.32
A principal ideal (a) is proper if and only if $a \notin A^\star$

Definition 3.4.33 (Maximal Ideal)
*An ideal $\mathfrak{m} \lhd A$ is **maximal** if it is both proper and not contained in another proper ideal.*

Definition 3.4.34 (Prime Ideal)
*An ideal $\mathfrak{p} \lhd A$ 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 3.4.35 (Radical Ideal)
*An ideal $\mathfrak{a} \lhd A$ is **radical** if it satisfies the following property*

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

Proposition 3.4.36 (Maximal ideals exist)
Let A be a ring and $\mathfrak{a} \lhd A$ 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 3.4.37 (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 3.4.38 (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 (3.4.37). 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 3.4.39 (Prime ideals are meet-prime)
Let $\mathfrak{p}$ be a prime ideal. Then

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p} \implies \mathfrak{a}_i \subseteq \mathfrak{p} \text{ some } i = 1 \dots n$$

in other words $\mathfrak{p}$ is meet-prime in the lattice of ideals.

Proof. Suppose $\mathfrak{a}_i \not\subseteq \mathfrak{p}$ for all i then there exists $x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$. Then $x_1 \dots x_n \in \bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p}$ by hypothesis, so by primality $x_i \in \mathfrak{p}$ for some i, a contradiction. □

Lemma 3.4.40 (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. □

Definition 3.4.41 (Minimal prime)
*Let A be a ring and $\mathfrak{a} \triangleleft A$ a proper ideal. A prime ideal $\mathfrak{p}$ is a **minimal prime over** $\mathfrak{a}$ if it contains $\mathfrak{a}$, and every other such prime ideal contains $\mathfrak{p}$.*

*We say it is simply a **minimal prime** if it is minimal over (0).*

Proposition 3.4.42 (Prime ideals are chain complete)
*Let $\{\mathfrak{p}_i\}_{i \in I}$ be a **chain** of prime ideals, then $\bigcap_i \mathfrak{p}_i$ and $\bigcup_i \mathfrak{p}_i$ are prime ideals.*

Proof. By (3.4.36) $\bigcup_i \mathfrak{p}_i$ is an ideal, and it's easily verified to be prime. Clearly $\bigcap_i \mathfrak{p}_i$ is an ideal. Suppose $a, b \notin \bigcap_i \mathfrak{p}_i$ then $a \notin \mathfrak{p}_j$ and $b \notin \mathfrak{p}_k$ with $j \leq k$. Then $b \notin \mathfrak{p}_j$, and $ab \notin \mathfrak{p}_j$ by primality, whence $ab \notin \bigcap_i \mathfrak{p}_i$. □

Corollary 3.4.43 (Minimal primes exist)
Let A be a ring and $\mathfrak{a} \triangleleft A$ be a proper ideal contained in a prime ideal $\mathfrak{p}$. Then there exists a minimal prime over $\mathfrak{a}$ contained in $\mathfrak{p}$.

In particular there always exists a minimal prime over $\mathfrak{a}$ and every prime ideal contains a minimal prime ideal.

Proof. We may use (3.4.42) together with Zorn's Lemma. □

Proposition 3.4.44
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 (2.1.40) 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 3.4.45 (Prime Nullstellensatz)
The radical of an ideal satisfies

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

Further the intersection may be taken over all minimal *primes over* $\mathfrak{a}$.

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 (3.4.40) there is a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ which does not intersect S. Therefore $x \notin RHS$ as required. □

Proposition 3.4.46 (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 (3.4.45) and (3.4.37).

b) This follows by applying (2.1.43) 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 $d), b)$ and a)

□

Definition 3.4.47 (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 3.4.48 (Operations on ideals)
Let $\phi : A \to B$ *a ring homomorphism and* $\mathfrak{a} \lhd A$, $\mathfrak{b} \lhd B$ *ideals then*

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

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* ϕ *is surjective*

When ϕ *is surjective every ideal* $\mathfrak{b} \triangleleft B$ *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 ϕ is surjective every ideal is extended, in which case the equality follows from *e)*.

Suppose that ϕ 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 3.4.49
Let $\phi : A \to B$ *be a ring homomorphism then extension and contraction constitute a monotone Galois connection*

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

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 (2.1.49) by (3.4.48).c) and d) □

Corollary 3.4.50
Let $\phi : A \to B$ *be a ring homomorphism then there is a order-preserving bijection between "contracted" and "extended ideals"*

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

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 3.4.51 (Inverse image of maximal / prime ideals)
Let $\phi : A \to B$ *be a morphism then*

- $\mathfrak{q} \triangleleft B$ *prime* $\implies \phi^{-1}(\mathfrak{q})$ *prime*
- $\mathfrak{n} \triangleleft B$ *maximal and* ϕ *surjective* $\implies \phi^{-1}(\mathfrak{n})$ *is maximal*

Proposition 3.4.52
Consider maps $\phi : A \to B$ *and* $\psi : B \to C$ *and an ideal* $\mathfrak{a} \triangleleft A$. *Then extension of ideals is transitive, that is*

$$\psi(\phi(\mathfrak{a})B)C = (\psi \circ \phi)(\mathfrak{a})C$$

3.4.4 Quotient Rings

Proposition 3.4.53 (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 π.*

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle \pi} & \nearrow_{\tilde{\phi}} & \\ A/\mathfrak{a} & & \end{array}$$

- $\ker(\tilde{\phi}) = \ker(\phi)/\mathfrak{a}$
- *$\tilde{\phi}$ is injective if and only if $\ker(\phi) = \mathfrak{a}$*
- *$\tilde{\phi}$ is surjective if and only if ϕ 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

$$\{\mathfrak{b}' \lhd A/\mathfrak{a}\} \underset{\pi^{-1}(-)}{\overset{\pi(-)}{\rightleftarrows}} \{\mathfrak{b} \lhd A \mid \mathfrak{a} \subseteq \mathfrak{b}\}$$

under which maximal (resp. prime, radical) ideals of A containing $\mathfrak{a}$ correspond to maximal (resp. prime, radical) ideals of $A/\mathfrak{a}$.

Corollary 3.4.54 (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 3.4.55 (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 3.4.56 (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*

Proof. Suppose $\mathfrak{a}$ is maximal then it is by definition proper so $A/\mathfrak{a}$ is not the zero-ring. By (3.4.53) then $A/\mathfrak{a}$ has no proper non-zero ideals and so by (3.4.16) is a field.

Conversely if $A/\mathfrak{a}$ is a field it is by definition not the zero ring, and so by (3.4.53) $\mathfrak{a}$ is proper. Furthermore by the same result $\mathfrak{a}$ is maximal.

Suppose $\mathfrak{a}$ is prime and $\overline{x} \cdot \overline{y} = 0$. Then by definition $\overline{x \cdot y} = 0 \implies x \cdot y \in \mathfrak{a} \implies x \in \mathfrak{a}$ or $y \in \mathfrak{a} \implies \overline{x} = 0$ or $\overline{y} = 0$. This shows that $A/\mathfrak{a}$ is an integral domain. The converse is similar. □

Corollary 3.4.57
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 combining (3.4.10) and (3.4.56). □

Corollary 3.4.58 (Field Morphisms are injective)
Let $\phi : k \to B$ *be a homomorphism from a field to a non-zero ring. Then* ϕ *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 ϕ is injective. □

3.4.5 Irreducible and Reduced rings

We say an element x is nilpotent if $x^n = 0$. By (3.4.44) these form an ideal.

Definition 3.4.59 (Nilradical)
Define the ***nilradical*** *to be the set (ideal) of nilpotents*

$$N(A) := \sqrt{(0)} \overset{(3.4.45)}{=} \bigcap_{\mathfrak{p}} \mathfrak{p}$$

Clearly A *is reduced if and only if* $N(A) = \{0\}$.

We also make the following definition

Definition 3.4.60 (Irreducible)
Let A *be a ring. We say* A *is* ***irreducible*** *if* $N(A)$ *is prime.*

The notion of irreducible ring is related to the notion of minimal primes

Proposition 3.4.61
A ring A *is irreducible if and only if it has a unique minimal prime ideal. In this case it is equal to* $N(A)$.

Proof. First we note that every prime ideal contains $N(A)$. If A is irreducible then by definition $N(A)$ is prime and it is therefore the unique minimal prime ideal.

Conversely if $\mathfrak{p}_0$ is the unique minimal prime ideal then by (3.4.43) it is contained in every prime ideal. Therefore (3.4.59) $N(A) = \bigcap_{\mathfrak{p}} \mathfrak{p} = \mathfrak{p}_0$ is prime and A is irreducible. □

Proposition 3.4.62 (Integral Domain $\iff$ Reduced and Irreducible)
Let A *be a ring. Then the following are equivalent*

- A *is an integral domain*
- A *is reduced and has a unique minimal prime*
- (0) *is prime*
- A *is reduced and irreducible.*

The following may be useful

Proposition 3.4.63
Let A *be a ring then the sum of an invertible and nilpotent element is again invertible*

$$A^\star + N(A) \subseteq A^\star$$

Proof. For if

$$a = u + n = u(1 - (u^{-1})(-n))$$

with $n \in N(A)$ and $u \in A^\star$. Then way may reduce to the case $1 - n$ and observe that

$$(1-n)^{-1} = \sum_{i=0}^{\infty} n^i$$

which by assumption is a finite sum. □

3.4.6 Algebra over a Commutative Ring

For what follows let A be a commutative ring.

Definition 3.4.64 (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 3.4.65 (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 3.4.66 (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 3.4.67 (Algebra generated by a set)
Let B be an A-algebra. The collection of A-subalgebras forms a Moore family. Therefore by (2.1.40) 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 3.8. More generally we have

$$A[S] = \bigcup_{S' \subset S | S' \text{ finite}} A[S']$$

Proposition 3.4.68
Let $B = A[S]$ be an A-algebra and $\mathfrak{a}$ a sub-A-module of B. Then $\mathfrak{a}$ is an ideal if and only if

$$s \in S \implies s\mathfrak{a} \subseteq \mathfrak{a}$$

Proof. One direction is obvious. Suppose the condition given holds, and define

$$B' := \{b \in B \mid b\mathfrak{a} \subseteq \mathfrak{a}\}$$

Then clearly $S \subseteq B'$. It's easy to show that B' is a sub-A-algebra of B, so $B' = B$ and $\mathfrak{a}$ is an ideal. □

3.4.7 Bimodules

For applications it is often useful to have multiple rings acting on a single module ("bimodule"). For example an A-algebra B naturally has an action from both A and B. It may also allow us to generalise results which would otherwise only hold in the commutative case.

Definition 3.4.69 (Bimodule)
*Let A, B be rings. We say an abelian group M is a (A,B)-**bimodule** if it is both a left A-module and a right B-module for which the two actions commute*

$$a \cdot (m \cdot b) = (a \cdot m) \cdot b \quad \forall a \in A, b \in B, m \in M$$

We may denote this by ${}_AM_B$ in order to emphasise the actions. If homomorphisms are defined in the obvious way then these constitute a category ${}_A\mathbf{Mod}_B$. Recall that every abelian group is automatically both a left and right $\mathbb{Z}$-module with the following action for $N \in \mathbb{Z}$

$$N \cdot m = m \cdot N := \begin{cases} \underbrace{m + \ldots + m}_{N \text{ times}} & N \geq 0 \\ -(m \cdot (-N)) & N < 0 \end{cases}$$

Therefore we have the following generalisations

- *A right B-module is precisely a $(\mathbb{Z}, B)$-bimodule*
- *A left A-module is precisely a $(A, \mathbb{Z})$-bimodule*
- *When A is commutative an A-module has a well-defined (A,A)-bimodule structure by defining*

  $$a \cdot m \cdot a' := a'a \cdot m = aa' \cdot m$$

  *in other words A-**Mod** is (equivalent to) a full subcategory of ${}_A\mathbf{Mod}_A$.*
- *A ring A has an obvious (A,A)-bimodule structure by associativity of the multiplication operation*

We will understand by the notation N_B that N is a $(\mathbb{Z}, B)$-bimodule and by ${}_AM$ that M is a $(A, \mathbb{Z})$-bimodule.

We generalize slightly the consideration of the third bullet point

Proposition 3.4.70 ((A,A)-Bimodule $\equiv$ A-module)
Let $\phi : A \to B$ be a homomorphism of commutative rings and Z a B-module. Then Z is naturally a (B,A)-module with the following action

$$b \cdot m \cdot a := \phi(a)b \cdot m \quad \forall a \in A, b \in B, m \in Z \tag{$\star$}$$

Suppose M is another (B,A)-bimodule satisfying $\star$ then we may identify the (B,A)-bimodule homomorphisms and the left B-module homomorphisms.

$$\mathrm{Hom}(M, {}_BZ_A) \xrightarrow{\sim} \mathrm{Hom}({}_BM, {}_BZ)$$

In particular when $\phi = 1_A$ and $B = A$ we may identify (A,A)-bimodules and A-modules, as well as the corresponding homomorphisms. Explicitly for M, Z A-modules these have well-defined (A,A)-bimodule structures and there is a bijection

$$\mathrm{Hom}({}_AM_A, {}_AZ_A) \xrightarrow{\sim} \mathrm{Hom}(M, Z)$$

Proof. We may show that the right A-module structure on Z is well-defined because B is commutative and using the associativity of the B-module action. Similarly the associativity of the B-module action ensures that the actions commute and so form a (B,A)-bimodule structure.

Suppose $\theta : M \to Z$ is a (left) B-module homomorphism. Then

$$\theta(m \cdot a) = \theta(\phi(a) \cdot m) = \phi(a)\theta(m) = \theta(m) \cdot a$$

so it is (B,A)-bilinear as required. The converse is clear, so we see that the sets are equal as subsets of the set of abelian group homomorphisms.

The case $\phi = 1_A$ is immediate. □

We generalize the notion of "Hom-Set"

Definition 3.4.71 (Hom Functors)
Let A, B, C be arbitrary rings. Then we have an enriched hom functor for ${}_A\mathbf{Mod}_B$

$$\mathrm{Hom} : {}_A\mathbf{Mod}_B^{op} \times {}_A\mathbf{Mod}_B \quad \to \quad \mathbf{AbGrp}$$

In order to generalise the Tensor-Hom adjunction we consider the following functors ("right-linear" and "left-linear" respectively)

$$\begin{aligned} \mathrm{RHom} : {}_B\mathbf{Mod}_A^{op} \times {}_C\mathbf{Mod}_A &\to {}_C\mathbf{Mod}_B \\ \mathrm{LHom} : {}_A\mathbf{Mod}_B^{op} \times {}_A\mathbf{Mod}_C &\to {}_B\mathbf{Mod}_C \end{aligned}$$

For example if $\psi \in \mathrm{RHom}({}_BM_C, {}_AN_C)$ *then the* (A,B)*-bimodule action is defined to be*

$$(a\psi b)(m) := a\psi(bm)$$

and similarly if $\phi \in \mathrm{LHom}({}_AM_B, {}_AN_C)$ *then*

$$(b\phi c)(m) := \phi(mb)c$$

which we may verify satisfies the axioms of a bimodule. In order to standardize notation we may write Hom_A *in place of* RHom *and* LHom*.*

If $B = C = \mathbb{Z}$ *then we recover the simple case (3.4.25).*

If A *is a commutative ring then we've observed that* A-**Mod** *is a full subcategory of* ${}_A\mathbf{Mod}_A$ *and the functors* RHom, LHom *become equal to the simple case (3.4.25) when restricted to this subcategory.*

3.4.8 Module Direct Product and Sum

Definition 3.4.72 (External Direct Product / Sum)
Let A *be a ring and* $\{M_i\}_{i\in I}$ *a family of* A*-modules. Define the* ***external direct product*** *as the set of ordered tuples indexed over* I

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

with the obvious module operations. The ***external direct sum*** *is the subset of tuples for which all but finitely many elements are zero. We denote this as follows*

$$\bigoplus_{i\in I} M_i$$

Clearly when I *is finite then these are equal.*

Proposition 3.4.73 (Categorical Product)
Let $\{M_i\}_{i\in I}$ *be a family of left* A*-modules and consider the family of projections*

$$\pi_i : \prod_{i\in I} M_i \to M_i$$

For Z *an* (A,C)*-bimodule there is a natural isomorphism of left* C*-modules*

$$\begin{aligned} \mathrm{Hom}_A(Z, \prod_{i\in I} M_i) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A(Z, M_i) \\ \theta &\to (\pi_i \circ \theta)_{i\in I} \end{aligned}$$

This in particular includes the case $A = C$ *is commutative.*

Proposition 3.4.74 (Categorical Coproduct)
Let $\{M_i\}_{i\in I}$ *be a family of left* A*-modules and consider the family of inclusions*

$$u_i : M_i \to \bigoplus_{i\in I} M_i$$

For Z *a* (A,C)*-bimodule there is a natural isomorphism of right* C*-modules*

$$\begin{aligned} \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, Z) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A(M_i, Z) \\ \theta &\to (\theta \circ u_i)_{i\in I} \end{aligned}$$

This in particular includes the case $A = C$ *is commutative.*

Corollary 3.4.75
Let $(M_i)_{i\in I}$ and $(N_j)_{j\in J}$ be families of left A-modules. Then there is an isomorphism of abelian groups

$$\begin{aligned}\mathrm{Hom}_A\left(\bigoplus_{i\in I} M_i, \prod_{j\in J} N_j\right) &\cong \prod_{(i,j)\in I\times J} \mathrm{Hom}_A(M_i, N_j)\\ \psi &\to (\pi_j \circ \psi \circ u_i)_{(i,j)}\end{aligned}$$

where $\pi_j : \prod_{j\in J} N_j \to N_j$ and $u_i : M_i \to \bigoplus_{i\in I} M_i$ are the canonical projections and injections respectively.

These maps are A-linear if A is commutative.

Definition 3.4.76 (Free Module)
An A-module M is

- ***free*** *if it is isomorphic to*
$$\bigoplus_{i\in A} A =: A^{(I)}$$
for some indexing set I
- ***finite free*** *if it is free with respect to a* finite *indexing set I*

Under the isomorphism $M \to \bigoplus_{i\in I} A$ the set of elements $\{m_i\}_{i\in I}$ corresponding to the standard basis vectors e_i is called a ***basis*** *for M.*

Proposition 3.4.77
Let M be an (A, C)-bimodule then there is a canonical isomorphism of right C-modules

$$\begin{aligned}\mathrm{Hom}_A(A, M) &\cong M\\ \theta &\to \theta(1_A)\end{aligned}$$

This in particular includes the case $A = C$ is commutative.

Proposition 3.4.78
Let M be a free left A-module with basis $(m_i)_{i\in I}$ and N an (A, C)-bimodule then there is an isomorphism of right C-modules

$$\begin{aligned}\mathrm{Hom}_A(M, N) &\cong \prod_{i\in I} N\\ \theta &\to (\theta(m_i))_{i\in I}\end{aligned}$$

This in particular includes the case $A = C$ is commutative.

3.4.9 Free Modules

Definition 3.4.79 (Faithful Module)
We say an A-module M is ***faithful*** *if*

$$am = 0 \quad \forall m \in M \implies a = 0$$

Definition 3.4.80 (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*
$$\sum_{i=1}^{n} a_i s_i = 0 \implies a_i = 0 \quad 1 \le i \le n$$
- *a* ***basis*** *if it is both spanning and linearly independent*

Definition 3.4.81 (Finite Module)
An A-module M is ***finite*** *if there exists a finite spanning set.*

Definition 3.4.82 (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 3.4.83 (Free Module)
*Let M be an A-module. We say that M is a **free module** over A if it has a basis.*

Proposition 3.4.84 (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 3.4.85 (Internal Direct Sum Module)
*An A-module M is an **internal direct sum** of submodules $\{M_i\}_{i\in I}$ the canonical mapping of the external direct sum*

$$\bigoplus_{i\in I} M_i \to M$$

is an isomorphism.

Proposition 3.4.86
Let M be an A-module and $\{M_i\}_{i\in I}$ a family of submodules. Then the following are equivalent

a) *$\sum_{i\in I} M_i$ is the internal direct sum of the family $\{M_i\}_{i\in I}$*

b) *The relation $\sum_{i\in I} m_i = 0$ implies $m_i = 0$ for all $i \in I$*

c) *For any $i \in I$ we have $M_i \cap \left(\sum_{k\neq i} M_k\right) = \{0\}$*

Proposition 3.4.87
*We say that M_1, M_2 are **supplementary** submodules of M if M is the internal direct sum of M_1 and M_2.*

*We say that M_1 is a **direct factor** of M if it is supplementary to another submodule.*

3.4.10 Exact Sequences

Definition 3.4.88 (Vector space)
*If k is a field and V a k-module, then we say V is a **vector space** over k.*

Remark 3.4.89
We will see that every vector space is free and every k-submodule is a direct factor.

Proposition 3.4.90 (Kernel)
*Let $\phi : M \to N$ be an A-module homomorphism, then the **kernel** of ϕ*

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

is an A-submodule of M. Observe ϕ is injective iff $\ker(\phi) = 0$.

Proposition 3.4.91 (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 3.4.92 (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 3.4.93 (Quotient Module Properties)
Let $N \subseteq M$ be an A-submodule then there is a canonical surjective morphism

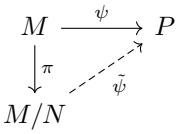
$$\pi : M \to M/N$$

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 π*



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 3.4.94
Let $\psi : M \to N$ be an A-module homomorphism, then this induces an isomorphism

$$M/\ker(\psi) \cong \mathrm{Im}(\psi)$$

Definition 3.4.95 (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 3.4.96
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 3.4.97 (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 3.4.98 (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 3.4.99 (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 3.4.100 (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

$$\bar{a} \cdot m := a \cdot m$$

3.4.11 Dual Module

Proposition 3.4.101 (Dual Module)
Let M be a left (resp. right) A-module. Then the set

$$M^\vee := \mathrm{Hom}_A(M, A)$$

is canonically a right *(resp.* left*) A-module.*

If M is a finite free left (resp. right) A-module with basis $\{v_1, \dots, v_n\}$ then $M^\vee$ is a finite free right *(resp.* left*) A-module with basis $\{v_1^\vee, \dots, v_n^\vee\}$ where these are the unique homomorphisms satisfying*

$$v_i^\vee(v_j) = \delta_{ij}$$

Moreover every basis of $M^\vee$ is of this form.

Proposition 3.4.102 (Hom-Set is free)
Let M be a finite free left A-module with basis $\{v_1, \dots, v_n\}$ and N a (A, B)-bimodule. Then there is an isomorphism of right B-modules

$$\begin{aligned} \mathrm{Hom}_A(M, N) &\cong \bigoplus_{i=1}^{n} N \\ \theta &\to (\theta(v_i))_{i \in I} \end{aligned}$$

If A is commutative and N is a finite-free A-module with basis $\{w_1, \dots, w_m\}$ then there is further an isomorphism of A-modules

$$\begin{aligned} \mathrm{Hom}_A(M, N) &\cong \bigoplus_{i,j=1}^{n,m} A \\ \theta &\to (w_j^\vee(\theta(v_i)))_{i,j} \end{aligned}$$

where $w_1^\vee, \dots, w_m^\vee$ is the dual basis for $N^\vee$. In particular $\mathrm{Hom}_A(M, N)$ is a finite-free A-module with basis

$$\{w_j v_i^\vee\}_{i,j}$$

Definition 3.4.103 (Dual Functor)
Let A be a commutative ring and $\phi : M \to N$ an A-module homomorphism. Define the dual homomorphism $\phi^\vee : N^\vee \to M^\vee$ by

$$\phi^\vee(\psi) := \psi \circ \phi$$

This determines a contravariant functor

$$(-)^\vee : A\textbf{-Mod} \to A\textbf{-Mod}$$

Corollary 3.4.104 (Double Dual Natural Isomorphism)
Let A be a commutative ring and M a finite free A-module then the canonical A-module homomorphism

$$\begin{aligned} \eta : M &\longrightarrow M^{\vee\vee} \\ x &\to (\phi \to \phi(x)) \end{aligned}$$

is an isomorphism, which is natural in M.

Corollary 3.4.105
The contravariant functor $(-)^\vee : \mathbf{FiniteFreeMod}_A \to \mathbf{FiniteFreeMod}_A$ is an equivalence of categories and therefore full and faithful.

Proof. Use the dual isomorphism η together with (2.6.28) and (2.6.27). □

3.4.12 Matrices

For this section we assume that A is a commutative ring. In this context $A^n := A \times \ldots \times A$ is a finite free module with basis $e_1, \ldots, e_n$. Matrices are concrete realisations of linear maps of finite free modules.

Proposition 3.4.106 (Matrices as linear maps)
Let M, N be free A-modules with ordered bases $\mathcal{B} := \{v_1, \ldots, v_n\}$, $\mathcal{B}' := \{w_1, \ldots, w_m\}$ respectively. Then there are mutually inverse isomorphisms of A-modules

$$\begin{array}{rcl} \mathrm{Mat}_{m\times n}(A) & \longleftrightarrow & \mathrm{Hom}_A(M,N) \\ E & \longrightarrow & \widehat{E} \\ [\phi]^{\mathcal{B}}_{\mathcal{B}'} & \longleftarrow & \phi \end{array}$$

where

$$\begin{aligned} \widehat{E}\left(\sum_{i=1}^{n} \lambda_i v_i\right) &:= \sum_{j=1}^{m}\left(\sum_{i=1}^{n} E_{ji}\lambda_i\right) w_j \\ \phi(v_i) &= \sum_{j=1}^{m} [\phi]_{ji}\, w_j \end{aligned}$$

If we further consider a free A-module P with ordered bases $\mathcal{B}'' = \{u_1, \ldots, u_p\}$ then

$$\begin{aligned} \widehat{E} \circ \widehat{F} &= \widehat{EF} \\ [\psi \circ \phi]^{\mathcal{B}}_{\mathcal{B}''} &= [\psi]^{\mathcal{B}'}_{\mathcal{B}''}\, [\phi]^{\mathcal{B}}_{\mathcal{B}'} \end{aligned}$$

Observe that

$$[1_M]^{\mathcal{B}}_{\mathcal{B}} = I_n$$

Furthermore there is an isomorphism of A-algebras

$$\begin{array}{rcl} \mathrm{End}_A(M) & \longleftrightarrow & \mathrm{Mat}_{n,n}(A) \\ \phi & \longrightarrow & (v_i^\vee(\phi(v_j)))_{ij} \\ \sum_{ij} E_{ij} v_i v_j^\vee & \longleftarrow & E \end{array}$$

Corollary 3.4.107
Matrix multiplication is associative. In particular

$$(EF)v = E(Fv)$$

Proof. We may consider the free A-modules A^n, A^m and A^p with canonical bases. The result follows because function composition is associative and $\widehat{\cdot}$ is injective. □

Corollary 3.4.108
There is an isomorphism of A-modules

$$\begin{array}{rcl} \mathrm{Mat}_{m\times n}(A) & \longleftrightarrow & \mathrm{Hom}_A(A^n, A^m) \\ E & \to & (v \to Ev) \end{array}$$

and further an isomorphism of A-algebras

$$\mathrm{Mat}_{n,n}(A) \longleftrightarrow \mathrm{End}_A(A^n)$$

Corollary 3.4.109
Let M be a finite free A-module with bases $\mathcal{B}, \mathcal{B}'$ and $\phi \in \mathrm{End}_A(M)$. Then ϕ is an isomorphism if and only if $[\phi]^{\mathcal{B}}_{\mathcal{B}'} \in \mathrm{Mat}_{n\times n}(A)$ is invertible.

Corollary 3.4.110 (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.

Definition 3.4.111 (Transpose)
*Let E be an $m \times n$ matrix in A, then define the **transpose** of E to be the $n \times m$ matrix E^t where*

$$(E^t)_{ij} := E_{ji}$$

Proposition 3.4.112
Let M, N be finite-free A-modules with bases $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{B}' = \{w_1, \ldots, w_m\}$. Let $\phi : M \to N$ be an A-module homomorphism and $\phi^\vee : N^\vee \to M^\vee$ the dual homomorphism then

$$[\phi^\vee]^{\mathcal{B}'^\vee}_{\mathcal{B}^\vee} = \left([\phi]^{\mathcal{B}}_{\mathcal{B}'}\right)^t$$

Similarly if E is an $m \times n$ matrix over A then

$$\widehat{E^\vee} = \widehat{E^t}$$

where the right hand side is understood to be with respect to the dual bases.

Corollary 3.4.113
Let E, F be matrices then

$$(EF)^t = (FE)^t$$

3.4.13 Multilinear Maps and Determinants

Definition 3.4.114 (Multilinear Map)
Let $M_1, \ldots, M_n, N$ be A-modules then a map

$$\psi : M_1 \times \ldots \times M_n \longrightarrow N$$

*is A-**multilinear** if it is A-linear in each variable, whilst fixing the other variables at any value.*

Definition 3.4.115 (Bilinear form)
*Let M, N be A-modules then $\psi : M \times N \to A$ is a **bilinear form** if it is A-multilinear.*

Denote the set of such bilinear pairings by $\mathrm{Bilin}_A(M, N)$. It is naturally an A-module.

Proposition 3.4.116
Let M, N be A-modules then there is a natural bijection

$$\begin{array}{ccccc} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, A)) & \longleftrightarrow & \mathrm{Bilin}_A(M, N) & \longleftrightarrow & \mathrm{Hom}_A(N, \mathrm{Hom}_A(M, A)) \\ \psi_L & \longleftarrow & \psi & & \\ & & \psi & \longrightarrow & \psi_R \end{array}$$

where

$$\psi_L(m)(n) = \psi(m, n) = \psi_R(n)(m)$$

Definition 3.4.117 (Alternating map)
*An A-multilinear map $f : M^n \to N$ is **alternating** if*

$$f(x_1, \ldots, x_n) = 0$$

whenever $x_i = x_{i+1}$ for some $i = 1 \ldots, n-1$.

*Denote by $L^n_a(M, N)$ the set of such alternating maps, and $L^n_a(M) := L^n_a(M, A)$ the set of **alternating forms**. These are clearly A-modules.*

Proposition 3.4.118 (Functorial Properties)
Let M be an A-module and $L_a^k(M)$ the set of k-alternating forms. Then

- *It is contravariant functor in M, that is if $g : M \to N$ then there is a well-defined map*

$$\begin{aligned} L_a^k(g) : L_a^k(N) &\to L_a^k(M) \\ \psi &\to \psi \circ g^{(k)} \end{aligned}$$

  such that $L_a^k(g \circ h) = L_a^k(h) \circ L_a^k(g)$.

- *There is a pairing*

$$\chi : M^\vee \times L_a^k(M) \to L_a^{k+1}(M)$$

  given by

$$\chi_f(\psi)(w_1, \ldots, w_{k+1}) = \sum_{i=1}^{k+1} (-1)^{i+1} f(w_i)\psi(w_1, \ldots, \widehat{w_i}, \ldots, w_{k+1})$$

Lemma 3.4.119
Let $f : M^n \to N$ be an alternating map then

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \epsilon(\sigma) f(x_1, \ldots, x_n)$$

for any permutation $\sigma \in S_n$.

Furthermore if any of the x_i are equal then $f(x_1, \ldots, x_n) = 0$

Proof. A permutation σ may be represented as a product of adjacent transpositions (...) therefore it's enough to demonstrate the case $\sigma = (i\ i+1)$. This follows directly from the definition because

$$0 = f(x+y, x+y) = f(x,x) + f(y,x) + f(x,y) + f(y,y) = f(x,y) + f(y,x)$$

Suppose $x_i = x_j$, then we may apply the first result to the transposition $\sigma = (i\ j)$ to see that $f(x_1, \ldots, x_n) = 0$. □

Definition 3.4.120 (Transpose)
Let M be a finite free A-module with basis $v_1, \ldots, v_n$. Define the transpose operation

$$\begin{aligned} (-)^t : M^n &\to M^n \\ (\sum_{j=1}^n a_{1j} v_j, \ldots, \sum_{j=1}^n a_{nj} v_j) &\to (\sum_{j=1}^n a_{j1} v_j, \ldots, \sum_{j=1}^n a_{jn} v_j) \end{aligned}$$

and for $f \in \mathrm{End}_A(M)$ define the transpose $f^t \in \mathrm{End}_A(M)$ to be the unique map such that $[f^t] = [f]^t$.

For $\Delta \in L_a^n(M)$ define $\Delta^t := \Delta \circ (-)^t$.

We claim that $(fg)^t = g^t f^t$ and in each case $(-)^{tt} = (-)$. Further $(f^n)^t = (f^t)^n$ as multilinear maps on M^n.

Lemma 3.4.121
Let $f : M^n \to N$ be an alternating map. Suppose $v_1, \ldots, v_n \in M$ and $w_1, \ldots, w_n \in M$ such that

$$w_i = \sum_{j=1}^n a_{ij} v_j$$

then

$$f(w_1, \ldots, w_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)} f(v_1, \ldots, v_n)$$

Proof. By expansion

$$f(w_1, \ldots, w_n) = \sum_{\sigma} a_{1\sigma(1)} \ldots a_{n\sigma(n)} f(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$$

where σ ranges over all maps from $\{1, \ldots, n\}$ to itself. If σ is not a permutation, then it must not be injective and by (3.4.119) the corresponding term is zero. Therefore we may restrict to the case $\sigma \in S_n$. By the first part of (3.4.119) the result follows. □

Proposition 3.4.122 (Existence and Uniqueness of Determinants)
There is a unique $D \in L_a^n(A^n)$ such that $D(e_1, \ldots, e_n) = 1$, given by the Leibniz Formula

$$D(v_1, \ldots, v_n) = \sum_\sigma \epsilon(\sigma) v_{1\sigma(1)} \ldots v_{n\sigma(n)}$$

Further $L_a^n(A^n)$ is a free module of rank 1 generated by D. Explicitly every $\Delta \in L_a^n(A^n)$ satisfies

$$\Delta = \Delta(e_1, \ldots, e_n) D$$

The form D also satisfies the "Laplace Expansion" formula

$$D(v_1, \ldots, v_n) = \sum_{i=1}^n (-1)^{i+k} v_{ik} D(v_1^{(k)}, \ldots, \widehat{v_i^{(k)}}, \ldots, v_n^{(k)})$$

and the transpose rule $D = D^t$.

Proof. We prove the existence by induction on n, where the case $n = 1$ is clear. The Laplace Expansion formula

$$\sum_{i=1}^n (-1)^{i+k} v_{ik} D(v_1^{(k)}, \ldots, \widehat{v_i^{(k)}}, \ldots, v_n^{(k)})$$

is an alternating form by (3.4.118). By induction it evaluates to 1 when $v_i = e_i$. This demonstrates the existence of D.

By (3.4.121) D satisfies Leibniz' Formula and furthermore so does any $\Delta \in L_a^n(M)$. Therefore $\Delta = \Delta(e_1, \ldots, e_n) D$, and D is unique, satisfying the Expansion Formula for any k.

Finally the transpose rule follows from Leibniz' Formula and considering the involution $\sigma \to \sigma^{-1}$.

□

Corollary 3.4.123 (Existence and Uniqueness of Determinants)
Let M be a finite free A-module of rank n. Then $L_a^n(M)$ is a free A-module of rank 1. In particular for every basis $\{v_1, \ldots, v_n\}$ there is a unique alternating map $\Delta_v \in L_a^n(M)$ such that $\Delta_v(v_1, \ldots, v_n) = 1$. Moreover every $\Delta \in L_a^n(M)$ satisfies the formula

$$\Delta = \Delta(v_1, \ldots, v_n) \Delta_v$$

Proof. For every basis $\{v_1, \ldots, v_n\}$ there is an isomorphism $\theta : M \cong A^n$, which by (3.4.118) induces an isomorphism $\widetilde{\theta} : L_a^n(A^n) \cong L_a^n(M)$ under which $\Delta \to \Delta \circ \theta^{(n)}$. Define $\Delta_v := \widetilde{\theta}(D)$ and the desired properties are easy to verify. □

Definition 3.4.124 (Determinant of a Module)
*Let M be a finite free A-module, then we say a generator for $L_a^n(M)$ is a **determinant** and Δ_v is the **determinant** corresponding to the basis $v_1, \ldots, v_n$.*

*The determinant for A^n corresponding to the standard basis $e_1, \ldots, e_n$ is called the **standard determinant** for A^n, and denoted by D.*

Corollary 3.4.125 (Determinant of an endomorphism)
Let M be a finite free A-module of rank n and $f \in \mathrm{End}_A(M)$ an endomorphism. Then the corresponding linear map

$$L_a^n(f) : L_a^n(M) \quad \to \quad L_a^n(M)$$

satisfies

$$L_a^n(f)(\psi) = D(f)\psi$$

*for a unique $D(f) \in A$, which we call the **determinant** of f. We have the following properties*

$$\begin{aligned} D(f \circ g) &= D(f)D(g) \\ D(1_M) &= 1_A \\ D(f) &= \Delta_v(f(v_1), \ldots, f(v_n)) \\ D(f^t) &= D(f) \end{aligned}$$

for Δ_v any generator for $L_a^n(M)$ corresponding to basis $v_1, \ldots, v_n$.

Proof. Let Δ be a generator then $L^n_a(f)(\Delta) = c\Delta$ for some $c \in A$ by (3.4.122). Clearly $D(f) := c$ satisfies the equation for all such $\psi = a\Delta$. It's unique because $L^n_a(M)$ is a free module, and the properties follow from uniqueness.

The last relation follows because $\Delta_v = \Delta^t_v$ and $f^n \circ (-)^t = (f^t)^n$. □

Proposition 3.4.126
*Let M be a finite free A-module and $f \in \mathrm{End}_A(M)$. Then there is an **adjugate** endomorphism $f^{ad} \in \mathrm{End}_A(M)$ such that*

$$f \circ f^{ad} = f^{ad} \circ f = D(f)\mathbf{1}_M$$

Proof. Suppose we pick an isomorphism $\theta : M \cong A^n$ corresponding to some basis $v_1, \ldots, v_n$ and define $f' := \theta \circ f \circ \theta^{-1} \in \mathrm{End}_A(A^n)$. Then

$$D(f') = D(f'(e_1), \ldots, f'(e_n)) = D(\theta(f(v_1)), \ldots, \theta(f(v_n))) = \Delta_v(f(v_1), \ldots, f(v_n)) = D(f)$$

If we show that $(f')^{ad}$ exists then it's easy to verify that $f^{ad} := \theta^{-1} \circ (f')^{ad} \circ \theta$ satisfies the required properties. Therefore we may reduce to the case $M = A^n$.

Define $x_i = f(e_i)$ and

$$f^{ad}(e_i) := \sum_{j=1}^{n} (-1)^{i+j} D(x_1^{(i)}, \ldots, \widehat{x_j^{(i)}}, \ldots, x_n^{(i)}) e_j$$

Then

$$\begin{aligned} f(f^{ad}(e_i)) &= \sum_{j=1}^{n} (-1)^{i+j} D(x_1^{(i)}, \ldots, \widehat{x_j^{(i)}}, \ldots, x_n^{(i)}) x_j \\ &= \sum_{k=1}^{n} \sum_{j=1}^{n} (-1)^{i+j} x_{jk} D(x_1^{(i)}, \ldots, \widehat{x_j^{(i)}}, \ldots, x_n^{(i)}) e_k \end{aligned}$$

Consider the mapping $D^{ik} : A^n \to A$

$$(y_1, \ldots, y_n) \longrightarrow \sum_{j=1}^{n} (-1)^{j+k} y_{jk} D(y_1^{(i)}, \ldots, \widehat{y_j^{(i)}}, \ldots, y_n^{(i)})$$

By (3.4.118) it is an alternating form such that $D^{ik}(e_1, \ldots, e_n) = \delta_{ik}$. We therefore conclude from (3.4.122) that $D^{ik} = \delta_{ik} D$ and

$$f(f^{ad}(e_i)) = D(x_1, \ldots, x_n) e_i = D(f) e_i \,,$$

which shows $f \circ f^{ad} = D(f)\mathbf{1}_M$. We may show that $f^{ad} \circ f = D(f)\mathbf{1}_M$ by a duality argument. For define $(x_1^t, \ldots, x_n^t) := (x_1, \ldots, x_n)^t$, then $x_i^t = f^t(e_i)$ and

$$D(f^t) = D(x_1^t, \ldots, x_n^t) = D^t(x_1, \ldots, x_n) = D(x_1, \ldots, x_n) = D(f)$$

Further

$$\begin{aligned} (f^t)^{ad}(e_i) &= \sum_{j=1}^{n} (-1)^{i+j} D(x^{t(i)}_1, \ldots, \widehat{x^{t(i)}_j}, \ldots, x^{t(i)}_n) e_j \\ &= \sum_{i=1}^{n} (-1)^{i+j} D(x_1^{(j)}, \ldots, \widehat{x_i^{(j)}}, \ldots, x_n^{(j)}) e_j \end{aligned}$$

so that $(f^t)^{ad} = (f^{ad})^t$. We've already shown that $f \circ f^{ad} = D(f)\mathbf{1}$ whence $(f^t)^{ad} \circ f^t = (f^{ad})^t \circ f^t = (f \circ f^{ad})^t = D(f)\mathbf{1}$ by (3.4.120). Apply this result with $f \leftarrow f^t$ to show that $f^{ad} \circ f = D(f^t)\mathbf{1} = D(f)\mathbf{1}$ as required. □

Corollary 3.4.127
Let M be a finite free A-module. Then $f \in \mathrm{End}_A(M)$ is an isomorphism if and only if $D(f) \in A^\star$.

We may use this to define the determinant of a matrix

Definition 3.4.128 (Determinant of a Matrix)
*Let $E \in \mathrm{Mat}_{n\times n}(A)$ then we define the **determinant** of E to be simply $D(\widehat{E})$.*

Using the standard determinant (3.4.124) with (3.4.125) we derive the classical form of Leibniz' Formula

$$\det(E) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} E_{i\sigma(i)}$$

and Laplace Expansion

$$\det(E) = \sum_{j=1}^{n} E_{ij} \det(E_{(ij)})$$

where $E_{(ij)}$ is obtained by removing both the i-th row and the j-th column.

Corollary 3.4.129 (Properties of Matrix Determinant)
The determinant satisfies a number of properties

a) $\det(EF) = \det(E)\det(F)$

b) $\det(I_n) = 1$

c) $\det(PEP^{-1}) = \det(E)$

d) $\det(E^t) = \det(E)$

Proof. These follow from (3.4.106) and (3.4.125). Explicitly

$$\det(EF) = D(\widehat{EF}) = D(\widehat{E}\circ\widehat{F}) = D(\widehat{E})D(\widehat{F}) = \det(E)\det(F)$$

and

$$\det(I_n) = D(\widehat{I_n}) = D(\mathbf{1}_{A^n}) = 1_A$$

□

3.4.14 Vector Spaces

Definition 3.4.130 (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 2.3. First we need to show that the notions of independence coincide

Proposition 3.4.131 (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** $x \in S \implies x \notin \langle S \setminus \{x\}\rangle$*

Further S is independent if and only if every finite subset of S is.

Proof. *b* $\iff$ *c*) This is (2.3.2).

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

$$0 = \sum_{i=1}^{n} \lambda_i v_i \quad v_i \in S$$

By renumbering assume 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 3.4.132 (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

$$y = \lambda x + \sum_i \lambda_i s_i \quad s_i \in S$$

We may assume $x \notin S$ (otherwise the statement is vacuous). Then by assumption we must have $\lambda \neq 0$ (for otherwise $x \in \langle S\rangle$). Therefore we may rearrange to find

$$x = \lambda^{-1} y - \sum_i \lambda^{-1}\lambda_i s_i$$

whence $x \in \langle S \cup \{y\}\rangle$. □

Therefore we have the following

Proposition 3.4.133 (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 $\dim_k V$.

More generally every linearly independent set is contained in a basis (so has order at most $\dim_k V$) and every spanning set contains a basis (so has order at least $\dim_k V$)

Proof. Follows from (2.3.7) and (2.3.11). The final statement follows from (2.3.12). □

Proposition 3.4.134 (Basis Criteria)
Let V be a vector space with $n = \dim_k V$ and $\mathcal{B} \subseteq V$. Then TFAE

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

b) *$\mathcal{B}$ is linearly independent and $\#\mathcal{B} \geq \dim_k V$*

c) *$\mathcal{B}$ is spanning and $\#\mathcal{B} \leq \dim_k V$*

If $\Delta \in L^n_a(V)$ is a determinant then this is equivalent to $\Delta(v_1, \ldots, v_n) \neq 0$ and $\mathcal{B} = \{v_1, \ldots, v_n\}$.

Proof. The equivalence of $a), b)$ and $c)$ follows from (2.3.13).

Suppose $a)$ holds and $\mathcal{B}$ is a basis, then $\Delta_v(v_1, \ldots, v_n) = 1$, whence $\Delta(v_1, \ldots, v_n) \neq 0$, since $\Delta = \lambda\Delta_v$ for some $\lambda \neq 0$.

Conversely suppose $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\Delta(v_1, \ldots, v_n) \neq 0$. Firstly by (3.4.119) the v_i must be distinct. We claim that $\mathcal{B}$ is linearly independent and $b)$ holds, for otherwise we may renumber to find $v_1 = \sum_{i=2}^n \lambda_i v_i$ and $\Delta(v_1, \ldots, v_n) = 0$ by (3.4.119). □

Proposition 3.4.135
A vector space $V = \{0\}$ if and only if $\dim_k V = 0$

Proposition 3.4.136 (Image of a basis)
Let $\phi : V \to W$ be a linear map

a) *If S is linearly-independent and ϕ is injective, then $\phi(S)$ is linearly-independent*

b) *If Γ is spanning then (ϕ is surjective $\iff$ $\phi(\Gamma)$ is spanning)*

c) *If $\mathcal{B}$ is a basis then (ϕ is an isomorphism $\iff$ $\phi(\mathcal{B})$ is a basis and ϕ 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 ϕ is injective this implies $\sum_i \lambda_i s_i = 0 \implies \lambda_i = 0$.

b) If ϕ 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 ϕ is surjective as required.

c) Suppose ϕ is isomorphism, then it's surely injective on $\mathcal{B}$ and by a),b) $\phi(\mathcal{B})$ is a basis. Conversely if $\phi(\mathcal{B}) =: \mathcal{B}'$ is a basis then by b) ϕ 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 ϕ is injective and hence bijective.

□

Corollary 3.4.137 (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 3.4.138
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 (3.4.133). 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 3.4.139 (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 ϕ we have $\phi(0) = 0$. Therefore ϕ 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 3.4.140 (Rank)
Let $\phi : V \to W$ be a linear map then define

$$\text{rank}_k(\phi) := \dim_k(\text{Im}(\phi))$$

Proposition 3.4.141 (Surjective Criteria)
Let $\phi : V \to W$ be a linear map with W finite-dimensional then

$$\phi \text{ surjective} \iff \text{rank}_k(\phi) = \dim_k W$$

Proof. This follows directly from (2.3.15). □

Proposition 3.4.142 (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 3.4.143 (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 ϕ is isomorphism as required. □

Corollary 3.4.144 (Endomorphism Isomorphism Criteria)
Let V be a finite-dimensional vector space and $\phi : V \to V$ then TFAE

a) ϕ *is injective*

b) ϕ *is surjective*

c) ϕ *is an isomorphism*

d) $D(\phi) \neq 0$

Proof. For the equivalence of $a), b)$ and $c)$ we may use the previous result with $W = V$ and note $\dim_k W = \dim_k V$ is automatically satisfied.

Then $c) \iff d)$ is (3.4.127). □

Proposition 3.4.145 (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 3.4.146 (Subspaces are direct factors)
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 3.4.147 (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

$$\dim_k V = \dim_k U_1 + \dim_k U_2$$

3.4.14.1 Dual Space

Definition 3.4.148 (Dual Space)
Let V be a k-vector space and define the ***dual space*** *to be*

$$V^\vee := \operatorname{Hom}_k(V, k)$$

This is an abelian group and even a k-vector space under the obvious operations. The construction $V \to V^\vee$ determines a contravariant functor

$$(-)^\vee : \mathbf{Vect}_k \to \mathbf{Vect}_k$$

Definition 3.4.149 (Annihilator)
Let V be a vector space and $U \subseteq V$ a subspace. Define the ***annihilator*** *of U by*

$$U^\circ = \{\theta \in V^\vee \mid \theta(u) = 0 \quad \forall u \in U\}$$

This is a linear subspace of $V^\vee$.

Proposition 3.4.150 (Dimension formula for annihilators)
There is a canonical isomorphism by restriction

$$V^\vee / U^\circ \longrightarrow U^\star$$

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°. The dimension formula follows from (3.4.142) and (3.4.101). □

Corollary 3.4.151 (Dual rank = rank)
Let $\phi : V \to W$ be a linear map and $\phi^\vee : W^\vee \to V^\vee$ then

$$\begin{aligned} \ker(\phi^\vee) &= \operatorname{im}(\phi)^\circ \\ \operatorname{im}(\phi^\vee) &\subseteq \ker(\phi)^\circ \end{aligned}$$

In the finite-dimensional case $\operatorname{im}(\phi^\vee) = \ker(\phi)^\circ$ and

$$\begin{aligned} \dim_k \ker(\phi^\vee) &= \dim_k W - \operatorname{rank}_k(\phi) \\ \operatorname{rank}_k(\phi^\vee) &= \operatorname{rank}_k(\phi) \end{aligned}$$

Proof. Note $\ker(\phi^\vee) = \operatorname{im}(\phi)^\circ$ and $\operatorname{im}(\phi^\vee) \subseteq \ker(\phi)^\circ$ by the definitions.

Consider the finite-dimensional case. By (3.4.150)

$$\dim_k \ker(\phi^\vee) = \dim_k \operatorname{im}(\phi)^\circ = \dim_k W - \operatorname{rank}_k(\phi)$$

By rank-nullity applied to $\phi^\vee$ and $\dim_k W = \dim_k W^\vee$ we deduce

$$\operatorname{rank}_k(\phi^\vee) = \operatorname{rank}_k(\phi)\,.$$

By (3.4.150) and rank-nullity applied to ϕ

$$\dim_k \ker(\phi)^\circ = \dim_k V - \dim_k \ker(\phi) = \operatorname{rank}_k(\phi)\,.$$

Finally by (2.3.15) $\operatorname{im}(\phi^\vee) = \ker(\phi)^\circ$.

□

From this it follows that taking duals reflects and preserve isomorphisms

Corollary 3.4.152 ($(-)^\vee$ reflects isomorphisms)
Let $\phi : V \to W$ be a linear map of finite-dimensional spaces then

a) *ϕ is injective if and only if $\phi^\vee$ is surjective*

b) *ϕ is surjective if and only if $\phi^\vee$ is injective*

c) *ϕ is iso if and only if $\phi^\vee$ is iso*

Proof. Note by (3.4.151) we have $\operatorname{rank}_k(\phi) = \operatorname{rank}_k(\phi^\vee)$ and by (3.4.101) $\dim_k V^\vee = \dim_k V$.

ϕ is surjective $\iff \operatorname{rank}_k(\phi) = \dim_k W = \operatorname{rank}_k(\phi^\vee) \overset{(3.4.142)}{\iff} \dim_k \ker(\phi^\vee) = 0 \iff \ker(\phi^\vee) = \{0\}$

ϕ is injective $\iff \dim_k \ker(\phi) = 0 \overset{(3.4.142)}{\iff} \operatorname{rank}_k(\phi) = \dim_k V \iff \dim_k V^\vee = \operatorname{rank}_k(\phi^\vee) \iff \phi^\star$ is surjective.

The last point may be deduced from the first two, or the fact that $(-)^\vee$ is full and faithful (3.4.105) and category-theoretic result (2.6.39). □

3.4.14.2 Bilinear Pairings

Definition 3.4.153 (Bilinear maps)
Let V, W be vector spaces a bilinear map ψ is a map

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

which is k-linear in each variable. We denote the set of bilinear maps as

$$\mathrm{Bilin}_k(V, W)$$

Proposition 3.4.154 (Matrix Representation)
Let V, W be finite-dimensional vector spaces with bases $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_m\}$ then there is a canonical isomorphism

$$\begin{array}{ccc} \mathrm{Bilin}_k(V, W) & \xrightarrow{\sim} & \mathrm{Mat}_{n,m}(k) \\ \psi & \longrightarrow & (\psi(v_i, w_j))_{ij} \end{array}$$

In particular a bilinear map ψ is determined uniquely by the values $\psi(v_i, w_j)$.

Proposition 3.4.155 (Dual maps)
Let V and W be vector spaces, then there is a natural bijection

$$\begin{array}{ccccc} \mathrm{Mor}_k(V, W^\star) & \longleftrightarrow & \mathrm{Bilin}_k(V, W) & \longleftrightarrow & \mathrm{Mor}_k(W, V^\star) \\ \psi_L & \longleftarrow & \psi & & \\ & & \psi & \longrightarrow & \psi_R \end{array}$$

where

$$\psi_L(v)(w) = \psi(v, w) = \psi_R(w)(v)$$

When V, W are finite-dimensional then ψ_L is an isomorphism if and only if ψ_R is an isomorphism. In this case we say ψ is a perfect pairing. More generally

$$\mathrm{rank}_k(\psi_L) = \mathrm{rank}_k(\psi_R)$$

Proof. The bijections stated are obvious. One may show that $\psi_L = \psi_R^\star \circ \eta_V$ where η_V is the dual isomorphism. Therefore ψ_L is an isomorphism if and only if $\psi_R^\star$ is an isomorphism, and by (3.4.152) if and only if ψ_R is an isomorphism. Since η_V is surjective we have $\mathrm{rank}_k(\psi_L) = \mathrm{rank}_k(\psi_R^\star) = \mathrm{rank}_k(\psi_R)$, by (3.4.151). □

Definition 3.4.156 (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 3.4.157
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 ψ_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 ψ_R is surjective, there is $w \in W$ such that $\psi_R(w) = \theta$. By definition $w \in U^\perp$ as required.

As ψ_R is injective then $\dim_k U^\perp \overset{(3.4.137)}{=} \dim_k U^\circ \overset{(3.4.150)}{=} \dim_k V/U = \dim_k V - \dim_k U$. □

Remark 3.4.158
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 3.4.159 (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 ψ'_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 (3.4.143) ψ'_R is an isomorphism and ψ' is perfect.

□

3.4.14.3 Trace operator

Definition 3.4.160 (Rank-1 linear map)
Let V be a vector space then there is a canonical bilinear map

$$\begin{aligned} \times : V \times V^\vee &\to \mathrm{End}_k(V) \\ (v, \theta) &\to (x \to \theta(x)v) \end{aligned}$$

*This is known as a **rank-1** linear map.*

Proposition 3.4.161 (Trace operator)
Let V be a finite-dimensional vector space then there is a unique k-linear map $\mathrm{Tr} : \mathrm{End}_k(V) \to k$ making the following diagram commute

$$\begin{array}{ccc} V \times V^\vee & \xrightarrow{\times} & \mathrm{End}_k(V) \\ & \searrow & \downarrow \mathrm{Tr} \\ & & k \end{array}$$

where the diagonal arrow is given by the bilinear map $(v, \theta) \to \theta(v)$. For a given basis $\mathcal{B}$ we have

$$\mathrm{Tr}(\alpha) = \sum_i [\alpha]_{ii}$$

Proof. Let $v_1, \dots, v_n$ be a basis for V and $v_1^\vee, \dots, v_n^\vee$ the corresponding dual basis. By (3.4.102) the rank-1 linear maps $v_i \cdot v_j^\vee$ form a basis for $\mathrm{End}_k(V)$. Therefore we may define

$$\mathrm{Tr}(v_i \cdot v_j^\vee) = v_j^\vee(v_i) = \delta_{ij}$$

and extend by linearity. By (3.4.154) the diagram commutes, and in particular

$$\mathrm{Tr}(v \cdot \theta) = \theta(v)$$

for any $v \in V$ and $\theta \in V^\vee$. □

3.4.14.4 Matrix Rank

Definition 3.4.162 (Column and Row Rank)
*Let k be a field and E an $m \times n$ a matrix over k. Consider the canonical vector spaces k^n and k^m. Then define the **column rank** of E to be*

$$\mathrm{rank}_k(\widehat{E})$$

*and the **row rank** of E to be*

$$\mathrm{rank}_k(\widehat{E^t})$$

Proposition 3.4.163 (Row Rank = Column Rank)
Let E be a matrix over k, then row rank and column rank are equal, and denote this by $\mathrm{rk}(E)$.

It is also the maximal number of linearly independent rows, or columns, and furthermore $\mathrm{rk}(E) \leq \min(m,n)$.

*We say E is **full rank** if* $\mathrm{rk}(E) = \min(m,n)$.

Proof. By (3.4.151) $\mathrm{rank}_k(\widehat{E}) = \mathrm{rank}_k(\widehat{E^\vee})$ and by (3.4.112) this equals $\mathrm{rank}_k(\widehat{E^t})$ as required.

The columns (resp. rows) clearly span $\mathrm{im}(\widehat{E})$ (resp. $\mathrm{im}(\widehat{E^t})$). By (3.4.133) there are $r := \mathrm{rk}(E)$ columns (resp. rows) constituting a basis, and therefore linearly independent. For any other subset of linearly independent columns (resp. rows) we must have the order is less than r by (3.4.133). Therefore $\mathrm{rk}(E)$ is the maximal number of linearly independent rows or columns. □

Proposition 3.4.164 (Criteria for Full Rank Square Matrix)
Let E be an $n \times n$ matrix over a field k. Then the following are equivalent

a) *E is invertible*

b) $\mathrm{rk}(E) = n$ *(i.e. $\widehat{E}$ is surjective or E is full-rank)*

c) *$Ev = 0 \implies v = 0$ for all column vectors v (i.e. $\widehat{E}$ is injective).*

d) *The columns of E are linearly independent*

e) $\det(E) \neq 0$

Finally E is full rank if and only if E^t is full rank.

Proof. Consider k^n with canonical basis, then by (3.4.106) E is invertible if and only if $\widehat{E}$ is an isomorphism. By definition $\mathrm{rk}(E) = \mathrm{rank}_k(\widehat{E})$. Furthermore *c)* is equivalent to $\widehat{E}$ being injective, and is also equivalent to *d)*. Therefore the equivalence follows from (3.4.144).

Finally it's clear from either *a), b)* or *e)* that this property is self-dual. □

Definition 3.4.165 (Minor of a matrix)
*Let E be an $m \times n$ matrix, we say a k-**minor** (for $k \leq \min(m,n)$) is the determinant of a $k \times k$ submatrix obtained by deleting $m-k$ rows and $n-k$ columns.*

Proposition 3.4.166 (Criteria for rank)
Let E be an $m \times n$ matrix over k. Then the following are equivalent

a) $\mathrm{rk}(E) \geq r$

b) *There exists an $r \times r$ sub-matrix with full rank*

c) *There exists a non-zero r-minor*

Proof. We see *b)* $\iff$ *c)* by (3.4.164).e)

Suppose *b)* holds, then a-fortiori E has r linearly independent columns. Therefore by (3.4.163) $\mathrm{rk}(E) \geq r$ and *a)* holds.

Conversely suppose $\mathrm{rk}(E) \geq r$ then by (3.4.163) there are certainly r linearly independent columns. We consider the $m \times r$ sub-matrix E' consisting of these columns. By (3.4.163) $\mathrm{rk}(E') = r$ and there are r linearly independent rows. Choosing these rows yields an $r \times r$ submatrix E'' which has r linearly independent rows, and so by (3.4.164) is full rank as required. □

Corollary 3.4.167
Let E be an $m \times n$ matrix over k and r an integer. Then the following are equivalent

a) $\mathrm{rk}(E) = r$

b) *r is the maximal dimension of a full-rank square sub-matrix*

c) *r is the maximal dimension of a non-zero minor*

3.5 Tensor Products

3.5.1 Commutative Tensor Product

We consider the "Tensor Product" of modules over a single commutative ring as an important special case, and as a guide to the general bimodule case.

In order to streamline the (typically tedious) verification of standard properties we make heavy use of the notion of **representable bifunctor** (2.6.60) however all the results may be proved in an essentially identical "low-tech" way.

First we define the so-called "Internal Hom Functor"

Definition 3.5.1 (Internal Hom)
Let A be a commutative ring and M, N be A-modules. The set of A-linear homomorphisms $M \to N$ is itself an A-module. Therefore we have an enriched hom functor

$$\mathrm{Hom} : A\text{-}\mathbf{Mod}^{op} \times A\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod}$$

where

$$(a \cdot \psi)(m) := a \cdot \psi(m) = \psi(a \cdot m)$$

and in particular we have a bijection

$$\mathrm{Mor}(M, N) \xrightarrow{\sim} \mathrm{Nat}(\mathrm{Hom}(N, -), \mathrm{Hom}(M, -))$$

Definition 3.5.2 (Bilinear Map)
Let M, N, Z be A-modules. Then a map

$$\psi : M \times N \to Z$$

*is **bilinear** if it satisfies*

- ***additive*** $\psi(m + m', n) = \psi(m, n) + \psi(m', n)$ *and* $\psi(m, n + n') = \psi(m, n) + \psi(m, n')$
- ***A-linear*** $\psi(am, n) = \psi(m, an) = a\psi(m, n)$ *for all* $a \in A$

This yields a bifunctor which we denote by

$$\mathrm{Bilin}(-, -; -) : (A\text{-}\mathbf{Mod} \times A\text{-}\mathbf{Mod})^{op} \times A\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod}$$

Remark 3.5.3 (A-linearity)
The A-module structure on the image of Hom *and* Bilin *is only well-defined because A is commutative. For given $\psi : M \to N$ an A-linear map then for $(a \cdot \psi)$ to be A-linear we may verify this requires*

$$a'a\psi(m) = (a\psi)(a'm) = aa'\psi(m)$$

which in general does not hold unless A is commutative.

Proposition 3.5.4 (Existence of Tensor Product)
The bifunctor $\mathrm{Bilin}(-, -; -)$ *is representable by a functor*

$$\otimes_A : A\text{-}\mathbf{Mod} \times A\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod}$$

for which there exists an isomorphism natural in M, N, Z

$$\Phi : \mathrm{Hom}(M \otimes N, Z) \cong \mathrm{Bilin}(M, N; Z)$$

For every pair M, N there is a distinguished bilinear map

$$i : M \times N \to M \otimes N$$

*through which every bilinear map $M \times N \to Z$ factors uniquely. We denote the **elementary tensor** by*

$$m \otimes n := i(m, n)$$

Further for morphisms $f : M \to M'$ and $g : N \to N'$ there is a unique morphism

$$(f \otimes g) : M \otimes N \to M' \otimes N'$$

such that

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

Proof. In light of (2.6.61) it is sufficient to show that $\mathrm{Bilin}(M,N;-)$ is representable for fixed M,N and the rest of the properties follow, observing that $i=\Phi(1_{M\otimes N})$.

For let F be the free abelian group on $M\times N$ and let $S\subset F$ be the subgroup generated by elements of the form

- $(m+m',n)-(m,n)-(m',n)$
- $(m,n'+n)-(m,n')-(m,n)$
- $(am,n)-a(m,n)$
- $(m,n)-(m,an)$

Observe there is a canonical map $M\times N\to F$. Suppose that Z is an abelian group and $\psi:M\times N\to Z$ is a bilinear map. Then we may extend by linearity to a group homomorphism $\psi:F\to Z$. By construction $S\subseteq\ker(\psi)$ whence there is a unique group homomorphism $\widehat{\psi}:F/S\to Z$ such that $\widehat{\psi}\circ i=\psi$ where $i:M\times N\to F/S$ is the canonical inclusion. This shows that $(F/S,i)$ represents $\mathrm{Bilin}(-,-;-)$ as we required and we denote this by $M\otimes N$. □

Lemma 3.5.5 (Currying Lemma)
Let M,N,Z be A-modules then there are natural isomorphisms

$$\begin{array}{ccccccc}\mathrm{Bilin}(M,N,Z) & \cong & \mathrm{Hom}(M,\mathrm{Hom}(N,Z)) & \cong & \mathrm{Hom}(N,\mathrm{Hom}(M,Z)) & \cong & \mathrm{Bilin}(N,M,Z)\\ \psi & & m\to(n\to\psi(m,n)) & & n\to(m\to\psi(m,n)) & & (n,m)\to\psi(m,n)\end{array}$$

This gives the following important result (which may be seen as an adjoint relationship)

Proposition 3.5.6 (Tensor-Hom Adjunction)
Let M,N,Z be A-modules then we have the following natural isomorphism of functors

$$\begin{aligned}\mathrm{Hom}(M\otimes N,Z) &\cong \mathrm{Hom}(M,\mathrm{Hom}(N,Z)) &(3.1)\\ \theta &\to (m\to(n\to\theta(m\otimes n))) &(3.2)\end{aligned}$$

We may also use the Currying Lemma (3.5.5) to demonstrate symmetry of the tensor product

Proposition 3.5.7 (Symmetry of Tensor Product)
There is a natural isomorphism

$$\begin{aligned}M\otimes N &\cong N\otimes M\\ m\otimes n &\to n\otimes m\end{aligned}$$

Proof. We observe that there is a natural isomorphism of functors which the tensor products represent

$$\mathrm{Bilin}(M,N;Z)\cong\mathrm{Bilin}(N,M;Z)$$

so the result follows from (2.6.63). □

Proposition 3.5.8 (Associativity of Tensor Product)
There is a natural isomorphism of A-modules

$$\begin{aligned}(M\otimes N)\otimes P &\cong M\otimes(N\otimes P)\\ (m\otimes n)\otimes p &\to m\otimes(n\otimes p)\end{aligned}$$

Proof. We may make repeated use of the Tensor-Hom adjunction to exhibit natural isomorphisms

$$\begin{aligned}\mathrm{Hom}((M\otimes N)\otimes P,Z) &\cong \mathrm{Hom}(M\otimes N,\mathrm{Hom}(P,Z))\\ &\cong \mathrm{Hom}(M,\mathrm{Hom}(N,\mathrm{Hom}(P,Z)))\\ &\cong \mathrm{Hom}(M,\mathrm{Hom}(N\otimes P,Z))\\ &\cong \mathrm{Hom}(M\otimes(N\otimes P),Z)\end{aligned}$$

The required isomorphism is then a consequence of (2.6.63). For explicit form set $Z=M\otimes(N\otimes P)$ and consider the identity map 1_Z. We see tracing back under these natural isomorphisms this corresponds to the given map. □

3.5.2 Bimodule Tensor Product

To develop the tensor product in general it is convenient to work with bimodules. We make heavy use of the notion if bimodule hom-sets (3.4.71).

Definition 3.5.9 (Bilinear maps)
Consider the bimodules ${}_AM_B$, ${}_BN_C$. We say that a map

$$\psi : {}_AM_B \times {}_BN_C \to {}_AZ_C$$

*is (A,C)-**bilinear** if it satisfies all of the following conditions*

- ***additive*** $\psi(m+m', n+n') = \psi(m,n) + \psi(m',n) + \psi(m,n') + \psi(n,n')$
- ***balanced*** $\psi(mb, n) = \psi(m, bn)$
- ***A-linear*** $\psi(am, n) = a\psi(m,n)$
- ***C-linear*** $\psi(m, nc) = \psi(m,n)c$

Extending the notation from earlier we denote the set of additive, balanced and (A,C)-bilinear maps by $\mathrm{Bilin}(M,N;Z)$. *This determines a functor*

$$\mathrm{Bilin} : ({}_A\mathbf{Mod}_B \times {}_B\mathbf{Mod}_C)^{op} \times {}_A\mathbf{Mod}_C \to \mathbf{AbGrp}$$

where addition is defined pointwise. We may also consider the functor of only additive and balanced maps

$$\mathrm{Balan} : (\mathbf{Mod}_B \times {}_B\mathbf{Mod})^{op} \times \mathbf{AbGrp} \to \mathbf{AbGrp}$$

and the functor

$$\mathrm{RBilin} : ({}_B\mathbf{Mod}_C \times {}_C\mathbf{Mod}_D)^{op} \times {}_A\mathbf{Mod}_D \to {}_A\mathbf{Mod}_B$$

where we drop the B-linear requirement but also introduce an extra (A,B)-module structure on the maps, as follows

$$(a\psi b)(m,n) := a\psi(bm, n)$$

Proposition 3.5.10 (Existence of Bimodule Tensor Product)
Let A, B, C be arbitrary rings

- *The bifunctor* $\mathrm{Balan}(M,N;-)$ *is represented by the **balanced tensor product***

  $$\otimes_B : \mathbf{Mod}_B \times {}_B\mathbf{Mod} \to \mathbf{AbGrp}$$

  with natural isomorphism for Z an Abelian group

  $$\begin{array}{rcl} \mathrm{Hom}(M_B \otimes_B {}_BN, Z) & \cong & \mathrm{Balan}(M_B, {}_BN; Z) \\ \theta & \to & \theta \circ i \end{array}$$

  where i is a universal balanced map

  $$i : M \times N \to M_B \otimes_B {}_BN$$

  *The tensor product is generated by **elementary tensors** of the form $m \otimes n := i(m,n)$.*

- *The bifunctor* $\mathrm{Bilin}(M,N;-)$ *is represented by the balanced tensor product $M \otimes_B N$ with an additional (A,C)-bimodule structure given by*

  $$a \cdot (m \otimes n) \cdot c := (a \cdot m) \otimes (n \cdot c)$$

  This determines a bifunctor

  $$\otimes_B : {}_A\mathbf{Mod}_B \times {}_B\mathbf{Mod}_C \to {}_A\mathbf{Mod}_C$$

  and a natural isomorphism of Abelian groups

  $$\begin{array}{rcl} \mathrm{Hom}({}_AM_B \otimes_B {}_BN_C, Z) & \cong & \mathrm{Bilin}({}_AM_B, {}_BN_C; {}_AZ_C) \\ \theta & \to & \theta \circ i \end{array}$$

In either case, if $f : M \to M'$ and $g : N \to N'$ are morphisms then there is a unique morphism

$$(f \otimes g) : (M \otimes N) \to (M' \otimes N')$$

such that

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

Furthermore for maps $f' : M' \to M''$ and $g' : N' \to N''$ the following property is satisfised

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$$

Proof. In light of (2.6.61) we only need to show that the functors are representable for fixed M, N, as the functoriality will follow immediately by abstract nonsense.

We first show that $\mathrm{Balan}(-,-;-)$ is representable. For let F be the free abelian group on $M \times N$ and let $S \subset F$ be the subgroup generated by elements of the form

- $(m+m', n) - (m, n) - (m', n)$
- $(m, n'+n) - (m, n') - (m, n)$
- $(mb, n) - (m, bn)$

Observe there is a canonical map $M \times N \to F$. Suppose that Z is an abelian group and $\psi : M \times N \to Z$ is a balanced additive map. Then we may extend by linearity to a group homomorphism $\psi : F \to Z$. By construction $S \subseteq \ker(\psi)$ whence there is a unique group homomorphism $\widehat{\psi} : F/S \to Z$ such that $\widehat{\psi} \circ i = \psi$ where $i : M \times N \to F/S$ is the canonical inclusion. This shows that $(F/S, i)$ represents $\mathrm{Balan}(-,-;-)$ and we denote this by $M_B \otimes_B {}_B N$.

In order to define the (A, C)-bimodule structure in the second case let $\psi_a : M \to M$ denote multiplication by a and $\psi_c : N \to N$ multiplication by c. We note these are both B-module homomorphisms by definition so we may define the action by functoriality of the balanced tensor product case

$$\begin{aligned} a \cdot v &:= (\psi_a \otimes 1_N)(v) \quad \forall v \in M \otimes N \\ v \cdot c &:= (1_M \otimes \psi_c)(v) \quad \forall v \in M \otimes N \end{aligned}$$

These are B-linear by construction and we may demonstrate (A, C)-bimodule actions are associative and commute by using the functoriality of the tensor product

$$\begin{aligned} (\psi_{a'} \otimes 1_N) \circ (\psi_a \otimes 1_N) &= (\psi_{a'} \circ \psi_a) \otimes 1_N = (\psi_{a'a}) \otimes 1_N \\ (1_M \otimes \psi_c) \circ (1_M \otimes \psi_{c'}) &= 1_M \otimes (\psi_c \circ \psi_{c'}) = 1_M \otimes \psi_{cc'} \\ (\psi_a \otimes 1_N) \circ (1_M \otimes \psi_c) &= \psi_a \otimes \psi_c \qquad\qquad = (1_M \otimes \psi_c) \otimes (\psi_a \otimes 1_N) \end{aligned}$$

Further by construction the canonical map i is (A, C)-bilinear. Consider any (A, C)-bilinear map $\psi : M \times N \to Z$ then by the previous part there is a unique group homomorphism $\widehat{\psi} : M \otimes_B N \to Z$ such that

$$\widehat{\psi}(m \otimes n) := \psi(m, n)$$

which we see by construction (and linearity) is (A, C)-bilinear. It is clearly the unique such map so that we may conclude $\mathrm{Bilin}(-,-;-)$ is represented by $({}_A M_B \otimes_B {}_B N_C, i)$. □

Lemma 3.5.11 (Currying Lemma)
Let M, N, P, Y, Z be bimodules. Then there is an isomorphism of abelian groups and (A, D)-bimodules respectively

$$\begin{aligned} \mathrm{Bilin}({}_A M_B, {}_B N_C; {}_A Y_C) &\cong \mathrm{Hom}({}_A M_B, \mathrm{RHom}({}_B N_C, {}_A Y_C)) \\ &\cong \mathrm{Hom}({}_B N_C, \mathrm{LHom}({}_A M_B, {}_A Y_C)) \\ \mathrm{RBilin}({}_B N_C, {}_C P_D; {}_A Z_D) &\cong \mathrm{RHom}({}_B N_C, \mathrm{RHom}({}_C P_D, {}_A Z_D)) \end{aligned}$$

contravariant in M, N, P and covariant in Y and Z.

Proof. The maps on abelian groups are clear, namely given a bi-additive map ψ we have a well-defined homomorphism of abelian groups

$$m \to (n \to \psi(m, n))$$

The verification that the maps are well-defined and bijective is tedious but mechanical. □

Proposition 3.5.12 (Tensor-Hom Adjunction)
Let M, N, P, Y, Z be bimodules then

$$\begin{aligned} \mathrm{Hom}({}_A M_B \otimes {}_B N_C, {}_A Y_C) &\cong \mathrm{Hom}({}_A M_B, \mathrm{RHom}({}_B N_C, {}_A Y_C)) \\ &\cong \mathrm{Hom}({}_B N_C, \mathrm{LHom}({}_A M_B, {}_A Y_C)) \\ \mathrm{RHom}({}_B N_C \otimes {}_C P_D, {}_A Z_D) &\cong \mathrm{RHom}({}_B N_C, \mathrm{RHom}({}_C P_D, {}_A Z_D)) \end{aligned}$$

where the first is an isomorphism of Abelian Groups and the second of (A, B)-bimodules. Further the isomorphisms are contravariant in M, N, P and covariant in Y and Z.

Proof. This first two isomorphism follow directly from the Currying Lemma and universal property for bimodule tensor product.

The final isomorphism follows from the Currying Lemma if we show that there is an isomorphism

$$\begin{array}{ccc} \mathrm{RHom}({}_BN_C \otimes {}_CP_D, {}_AZ_D) & \xrightarrow{\sim} & \mathrm{RBilin}({}_BN_C, {}_CP_D; {}_AZ_D) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(N_C \otimes {}_CP, Z) & \xrightarrow{\sim} & \mathrm{Balan}(N_C, {}_CP; Z) \end{array}$$

where the bottom is simply the universal property of the balanced tensor product and the top we require to also be (A, B)-bilinear. Recall the underlying sets are the same and the horizontal maps are given by $\theta \to \theta \circ i$ in both cases. It's clear that the map is well-defined and injective. Further it's surjective because if θ is (B, D)-bilinear on elementary tensors it is (B, D)-bilinear everywhere. Finally we need to show that the isomorphism is (A, B)-bilinear as follows

$$(a(\theta \circ i)b)(n, p) = a(\theta \circ i)(bn, p) = a\theta((bn) \otimes p) = a\theta(b(n \otimes p)) = (a\theta b)(n \otimes p)$$

□

Proposition 3.5.13 (Associativity of Tensor Product)
Let ${}_AM_B$, ${}_BN_C$, ${}_CP_D$ be bimodules then there is a natural isomorphism of (A, D)-bimodules

$$\begin{array}{rcl} (M \otimes_B N) \otimes_C P & \cong & M \otimes_B (N \otimes_C P) \\ (m \otimes n) \otimes p & \to & m \otimes (n \otimes p) \end{array}$$

Proof. This follows much as in the commutative case. Let Z be an (A, D)-bimodule. Then by the Tensor-Hom adjunction there are natural isomorphisms of Abelian groups

$$\begin{array}{rcl} \mathrm{Hom}(({}_AM_B \otimes {}_BN_C) \otimes {}_CP_D, {}_AZ_D) & \cong & \mathrm{Hom}({}_AM_B \otimes {}_BN_C, \mathrm{RHom}({}_CP_D, {}_AZ_D)) \\ & \cong & \mathrm{Hom}({}_AM_B, \mathrm{RHom}({}_BN_C, \mathrm{RHom}({}_CP_D, {}_AZ_D))) \\ & \cong & \mathrm{Hom}({}_AM_B, \mathrm{RHom}({}_BN_C \otimes_C {}_CP_D, {}_AZ_D)) \\ & \cong & \mathrm{Hom}({}_AM_B \otimes_B ({}_BN_C \otimes_C {}_CP_D), {}_AZ_D) \end{array}$$

The required isomorphism is then a consequence of (2.6.63). For explicit form set $Z = M \otimes (N \otimes P)$ and consider the identity map 1_Z. We see tracing back under these natural isomorphisms this corresponds to the given map. □

3.5.3 Extensions of Scalars

We observe that for a ring homomorphism $\phi : A \to B$ we have on B a natural (A, B)-bimodule and (B, A)-bimodule structure. Using the tensor product then we may use this to extend the coefficients from A to B. We first prove some elementary lemmas

Lemma 3.5.14 (Unit Hom)
Let $\phi : B \to C$ be a ring homomorphism and Z a (A, C)-bimodule. Then there is a natural isomorphism of (A, B)-bimodules

$$\begin{array}{rcl} \mathrm{RHom}({}_BC_C, {}_AZ_C) & \cong & {}_AZ_B \\ \theta & \to & \theta(1) \\ z(-) & \leftarrow & z \end{array}$$

and similarly let $\phi : A \to B$ be a ring homomorphism and Y a (B, C)-bimodule then there is a natural isomorphism of (A, C)-bimodules

$$\begin{array}{rcl} \mathrm{LHom}({}_BB_A, {}_BY_C) & \cong & {}_AY_C \\ \theta & \to & \theta(1) \end{array}$$

Proof. Observe

$$(a\theta b)(1) = a\theta(\phi(b)) = a\theta(1)\phi(b)$$

so the left to right map is an (A, B)-bimodule homomorphism. Further $\theta(c) = \theta(1)c$ so the maps are mutual inverses. □

Lemma 3.5.15 (Unit Hom (Commutative Ring Case))
Let $\phi : A \to B$ be a homomorphism of commutative rings and Z a B-module. Then there is a natural isomorphism of B-modules

$$\begin{array}{rcl} \mathrm{Hom}(B, Z) & \cong & Z \\ \theta & \to & \theta(1) \end{array}$$

Proposition 3.5.16 (Extension of Scalars)
Let M be an (A,C)-bimodule and $\phi : A \to B$ a ring homomorphism. We may define a (B,C)-module

$$M_{(B)} := {}_BB_A \otimes_A M$$

For Z a (B,C)-bimodule there is a natural isomorphism of abelian groups

$$\begin{array}{rcl} \mathrm{Hom}(M_{(B)}, Z) & \xrightarrow{\sim} & \mathrm{Hom}(M, {}_AZ_C) \\ \psi & \to & \psi(1 \otimes -) \end{array}$$

In otherwords we have an adjunction (2.6.48)

$${}_A\mathbf{Mod}_C \leftrightarrows {}_B\mathbf{Mod}_C$$

Setting $C = \mathbb{Z}$ yields an adjunction for left modules

$${}_A\mathbf{Mod} \leftrightarrows {}_B\mathbf{Mod}$$

In particular for M a left A-module we have an isomorphism of abelian groups

$$\mathrm{Hom}(M_{(B)}, B) \xrightarrow{\sim} \mathrm{Hom}_A(M, B)$$

which is B-linear when B is commutative.

Proof. By the tensor-hom adjunction (3.5.12) and (3.5.14) there is a natural isomorphism

$$\mathrm{Hom}(B \otimes_A M, Z) \cong \mathrm{Hom}(M, \mathrm{LHom}({}_BB_A, {}_BZ_C)) \cong \mathrm{Hom}(M, {}_AZ_C)$$

□

Proposition 3.5.17 (Tensor Unit)
Let M be an (A,C)-bimodule then there is a natural isomorphism of (A,C)-bimodules

$$\begin{array}{rcl} A \otimes_A M & \cong & M \\ a \otimes m & \to & a \cdot m \\ 1 \otimes m & \leftarrow & m \end{array}$$

Similarly there is a natural isomorphism of (A,C)-bimodules

$$M \otimes_C C \cong M$$

Proof. By (3.5.16) with $\phi = 1_A$ there is a natural isomorphism

$$\mathrm{Hom}(A \otimes_A M, -) \cong \mathrm{Hom}(M, -)$$

and so natural isomorphism follows from (2.6.63).

We may deduce that there is a natural isomorphism of (C^{op}, A^{op})-bimodules

$$C^{op} \otimes_{C^{op}} M^{op} \cong M^{op}$$

which amounts to a natural isomorphism of (A,C)-bimodules

$$M \otimes_C C \cong M$$

□

Proposition 3.5.18 (Transitivity of Extension of Scalars)
Let M be a (A,D)-bimodule and $\phi : A \to B$, $\psi : B \to C$ homomorphisms of commutative rings. Then there is an isomorphism of (C,D)-bimodules

$$\begin{array}{rcl} C \otimes_B (B \otimes_A M) & \xrightarrow{\sim} & {}_CC_A \otimes_A M \\ c \otimes (b \otimes m) & \to & (c\psi(b)) \otimes m \end{array}$$

Proof. By associativity (3.5.13) and (3.5.17) there is a natural isomorphism

$$C \otimes_B (B \otimes_A M) \cong (C \otimes_B B) \otimes_A M \cong C \otimes_A M$$

□

Proposition 3.5.19 (Transitivity of Extension of Scalars (Commutative Case))
Let M be an A-module and $\phi : A \to B$ and $\psi : B \to C$ homomorphisms of commutative rings. Then there is an isomorphism of C-modules

$$C \otimes_B (B \otimes_A M) \cong {}_CC_A \otimes_A M$$

Proof. Regarding M as an (A,A)-bimodule we have an isomorphism of (C,A)-bimodules by (3.5.18) which is a-fortiori a C-module isomorphism. □

3.5.4 Tensor Product Commutes with Direct Sum

Proposition 3.5.20 (Tensor Product Commutes with Sum)
Let $(M_i)_{i\in I}$ be a family of (A,B)-bimodules and $(N_j)_{j\in J}$ a family of (B,C)-bimodules. Then there is an isomorphism of (A,C)-bimodules

$$\left(\bigoplus_{i\in I} M_i\right) \otimes_B \left(\bigoplus_{j\in J} N_j\right) \cong \bigoplus_{(i,j)\in I\times J} (M_i \otimes_B N_j)$$

Corollary 3.5.21
Suppose M is an (A,B)-bimodule and N is a (B,C)-bimodule and $M' \subseteq M$ and $N' \subseteq N$ are direct factors. Then the canonical map is injective

$$M' \otimes_B N' \quad \hookrightarrow \quad M \otimes_B N$$

Corollary 3.5.22
*Let N be **free** left A-module with basis $(n_i)_{i\in I}$ and M a (B,A)-bimodule. Then there is an isomorphism of left B-modules*

$$\begin{aligned} M \otimes_A N \quad &\cong \quad \bigoplus_{i\in I} M \\ m \otimes \sum_i a_i n_i \quad &\longrightarrow \quad (m\cdot a_i)_{i\in I} \\ \sum_i (m_i \otimes n_i) \quad &\longleftarrow \quad (m_i)_{i\in I} \end{aligned}$$

When A is commutative then this is a (B,A)-bimodule isomorphism. Further when M is an A-module then this is an isomorphism of A-modules.

Proof. By (3.5.20) and (3.5.17)

$$M \otimes_A N \cong M \otimes_A \left(\bigoplus_{i\in I} A\right) \cong \bigoplus_{i\in I} (M \otimes_A A) \cong \bigoplus_{i\in I} M$$

$$m \otimes \textstyle\sum_i a_i n_i \to \quad m \otimes (a_i)_{i\in I} \quad \to \quad (m \otimes a_i)_{i\in I} \quad \to (m\cdot a_i)_{i\in I}$$

□

Corollary 3.5.23 (Free modules are flat)
Let N be a free left A-module and $i : M' \to M$ an injective map of (B,A)-bimodules. Then the corresponding map

$$i \otimes 1_N : M' \otimes_A N \to M \otimes_A N$$

is injective.

Corollary 3.5.24 (Extension of Scalars (Free Module))
*Let M be **free** left A-module with basis $\{m_i\}_{i\in I}$ and $\phi : A \to B$ a ring homomorphism. Then there is a canonical isomorphism of left B-modules*

$$\begin{aligned} M_{(B)} \quad &\cong \quad \bigoplus_{i\in I} B \\ b \otimes \sum_i a_i m_i \quad &\to \quad (b\phi(a_i))_{i\in I} \end{aligned}$$

In particular $\{1\otimes m_i\}_{i\in I}$ is a basis for $M_{(B)}$. Further when Z is a left B-module then there is an isomorpihsm of abelian groups

$$\begin{aligned} \mathrm{Hom}_A(M,Z) \cong \mathrm{Hom}_B(M_{(B)},Z) \cong \quad & \textstyle\prod_{i\in I} Z \\ \theta \qquad\qquad \to \qquad\qquad & (\theta(m_i))_{i\in I} \end{aligned}$$

which is B-linear when B is commutative.

When M is a finite free A-module of rank n (with basis $\{v_i\}$) then $M_{(B)}$ is a finite free B-module of rank n (with basis $\{1\otimes v_i\}$). When B is commutative, $M_{(B)}^\vee$ is also a finite free B-module of rank n.

Proof. The first isomorphism follows directly from (3.5.22). Then by (3.4.75) there is an isomorphism

$$\mathrm{Hom}\left(M_{(B)}, Z\right) \cong \mathrm{Hom}\left(\bigoplus_{i\in I} B, Z\right) \cong \prod_{i\in I} \mathrm{Hom}(B, Z) \cong \prod_{i\in I} Z$$

□

We may generalize (3.4.102)

Proposition 3.5.25 (Extension of Scalars (Hom-Set))
Let $\phi : A \to B$ be a homomorphism of commutative rings, M a finite-free A-module and N a finite-free B-module. Then

$$\mathrm{Hom}_A(M, N) \cong \mathrm{Hom}_B(M_{(B)}, N)$$

is a finite-free B-module. More precisely suppose M has basis $\{v_1, \ldots, v_n\}$ and N has basis $\{w_1, \ldots, w_m\}$ then $\mathrm{Hom}_A(M, N)$ has basis

$$\{w_j v_i^\vee\}_{i,j}$$

Proof. By (3.5.24) there are isomorphisms of B-modules

$$\mathrm{Hom}_A(M, N) \cong \mathrm{Hom}_B(M_{(B)}, N) \cong \textstyle\bigoplus_{i=1}^n N \cong \bigoplus_{i=1}^n \bigoplus_{j=1}^m B$$

$$\theta \to \qquad 1 \otimes \theta \qquad \to (\theta(v_i))_i \;\to\; (w_j^\vee(\theta(v_i)))_{i,j}$$

Under this isomorphism the standard basis of the right hand side corresponds to the set $\{w_j v_i^\vee\}_{i,j}$ whence these constitute a basis. □

3.5.5 Vector Space Tensor Product

3.5.6 Algebra Tensor Product

Let A be a commutative ring and revert to the case of commutative tensor production Section 3.5.1. We show that given two A-algebras B,C the tensor product naturally forms an algebra. We first prove some preliminary results.

Lemma 3.5.26
Let B be a commutative A-algebra. Then there exists a unique homomorphism of A-modules

$$B \otimes_A B \to B$$

such that

$$b \otimes b' \to bb'$$

Proof. Multiplication is bilinear so the map exists by universal property. □

Lemma 3.5.27
Let B, C be commutative A-algebras and define the A-module $X := B \otimes_A C$. Then there is a unique homomorphism of A-modules

$$m : X \otimes_A X \to X$$

such that

$$(b \otimes c) \otimes (b' \otimes c') \to (bb') \otimes (cc')$$

Define $1_X := (1 \otimes 1)$ then it satisfies

a) $m(1_X \otimes x) = m(x \otimes 1_X) = x$

b) $m(x \otimes y) = m(y \otimes x)$

c) $m(x \otimes m(y \otimes z)) = m(m(x \otimes y) \otimes z)$

d) $m((x + y) \otimes z) = m(x \otimes z) + m(y \otimes z)$

e) $m(x \otimes (y + z)) = m(x \otimes y) + m(x \otimes z)$

for $x, y, z \in X$.

Proof. By associativity and commutativity of the tensor product there is an A-module isomorphism

$$\begin{aligned} X \otimes_A X &\cong (B \otimes_A B) \otimes_A (C \otimes_A C) \\ (b \otimes c) \otimes (b' \otimes c') &\to (b \otimes b') \otimes (c \otimes c') \end{aligned}$$

composing with $m_B \otimes m_C$ where $m_B : (B \otimes_A B) \to B$ and $m_C : (C \otimes_A C) \to C$ are the maps given in (3.5.26), yields the required map m.

The properties may be verified on tensors of the form $x_i = (b_i \otimes c_i)$ and $y_j = (b'_j \otimes c'_j)$. The results follow from linearity, since $(\sum_i x_i) \otimes \left(\sum_j y_j\right) = \sum_{i,j}(x_i \otimes y_j)$. □

Proposition 3.5.28 (Algebra Tensor Product)
Let B, C be commutative A algebras. Then the A-module $B \otimes_A C$ has a unique commutative ring structure with unit $1 \otimes 1$ and multiplication which satisfies

$$\begin{aligned} \cdot : (B \otimes_A C) \times (B \otimes_A C) &\to B \otimes_A C \\ (b \otimes c) \cdot (b' \otimes c') &:= (bb') \otimes (cc') \end{aligned}$$

and may be extended by linearity. Further there is an ring homomorphism

$$\begin{aligned} i_A : A &\to B \otimes_A C \\ a &\to (a \otimes 1) = (1 \otimes a) \end{aligned}$$

making $B \otimes_A C$ into an A-algebra.

Proof. Let $X := B \otimes_A C$ and consider the map $m : X \otimes_A X \to X$ defined in (3.5.27). Define $x \cdot y := m(x \otimes y)$ then the properties of m ensure that this satisfies the properties of a ring. □

Proposition 3.5.29 (Criteria to be an algebra homomorphism)
Let B, C, Z be commutative A-algebras and let $\phi : B \otimes_A C \to Z$ be an A-module homomorphism. Then the following are equivalent

a) *ϕ is an A-algebra homomorphism*

b) $\phi((b \otimes c) \cdot (b' \otimes c')) = \phi(b \otimes c) \cdot \phi(b' \otimes c')$

Similarly suppose $\psi : Z \to B \otimes_A C$ is an A-module homomorphism and Z is generated as an A-module by $S \subset Z$. Then the following equivalent

a) *ψ is an A-algebra homomorphism*

b) $\psi(ss') = \psi(s)\psi(s')$

Proof. In each case *a)* $\implies$ *b)* is obvious. For the converse we simply need to show that ϕ and ψ are in general multiplicative. This follows by linearity and because every element of the tensor product is a linear combination of elementary tensors. □

Proposition 3.5.30 (Tensor Product is Coproduct)
Let B, C be commutative A-algebras then there are A-algebra homomorphisms

$$\begin{aligned} i_B : B &\to B \otimes_A C \\ b &\to b \otimes 1 \\ i_C : C &\to B \otimes_A C \\ c &\to 1 \otimes c \end{aligned}$$

which are natural in B and C respectively. In particular $B \otimes_A C$ is both a C-algebra and a B-algebra.

Furthermore for Z an A-algebra there is a bijection

$$\begin{aligned} \mathrm{AlgHom}_A(B \otimes_A C, Z) &\cong \mathrm{AlgHom}_A(B, Z) \times \mathrm{AlgHom}_A(C, Z) \\ \psi &\to (\psi \circ i_B, \psi \circ i_C) \end{aligned}$$

which is natural in Z.

Proof. The existence of i_B and i_C is easily demonstrated using universal property of tensor product. Observe that in general

$$(\psi \circ i_B)(b) = \psi(b \otimes 1_C)$$
$$(\psi \circ i_C)(c) = \psi(1_B \otimes c)$$

Furthermore the map is clearly well-defined. It's injective because if ψ and ψ' have the same image then $\psi(b \otimes 1) = \psi'(b \otimes 1)$ and $\psi(1 \otimes c) = \psi'(1 \otimes c)$ whence $\psi(b \otimes c) = \psi'(b \otimes c)$. By linearity they are everywhere equal.

To show that the map is a bijection we construct a two-sided inverse. For given A-algebra homomorphisms $f : B \to Z$ and $g : C \to Z$ then $(b, c) \to (f(b)g(c))$ is A-bilinear and so corresponds to an A-module homomorphism

$$\begin{aligned} \psi_{f,g} : B \otimes_A C &\to Z \\ b \otimes c &\to f(b)g(c) \end{aligned}$$

and by (3.5.29) this is an algebra homomorphism. Clearly $\psi \circ i_1 = f$ and $\psi \circ i_2 = g$. Conversely let $\psi : B \otimes_A C \to Z$ be an algebra homomorphism and we define $f(b) := \psi(b \otimes 1_C)$ and $g(c) := \psi(1_C \otimes c)$. Then $f(b)g(c) = \psi(b \otimes c)$

which shows that $\psi_{f,g}$ agrees with ψ on elementary tensors, and therefore is identically equal. This completes the demonstration that $\psi_{f,g}$ is a two-sided inverse to the given map.

Naturality in Z is straightforward. □

Proposition 3.5.31 (Extension of Scalars)
Let B, C be commutative A-algebras. Then define the C-algebra

$$B_{(C)} := C \otimes_A B$$

There is a natural isomorphism for any C-algebra Z

$$\begin{array}{rcl} \mathrm{AlgHom}_C(B_{(C)}, Z) & \cong & \mathrm{AlgHom}_A(B, Z) \\ \psi & \to & \psi \circ i_B \end{array}$$

Proof. We consider the commutative diagram obtained from (3.5.30)

$$\begin{array}{ccc} \mathrm{AlgHom}_A(B_{(C)}, Z) & \xrightarrow{\sim} & \mathrm{AlgHom}_A(B, Z) \times \mathrm{AlgHom}_A(C, Z) \\ \cup & & \cup \\ \mathrm{AlgHom}_C(B_{(C)}, Z) & \xrightarrow{\sim} & \mathrm{AlgHom}_A(B, Z) \times \{i_{CZ}\} \end{array}$$

An A-algebra homomorphism $\phi : B_{(C)} \to Z$ is a C-algebra homomorphism precisely when $\psi \circ i_C = i_{CZ}$ so that the bottom arrow is well-defined and bijective as required. □

Proposition 3.5.32 (Transitivity of Extension of Scalars)
Let B, C be commutative A-algebras and D a commutative C-algebra. Then there is an isomorphism of D-algebras

$$\begin{array}{rcl} D \otimes_C (C \otimes_A B) & \cong & D \otimes_A B \\ d \otimes (c \otimes b) & \to & (dc) \otimes b \end{array}$$

Proof. Let Z be a D-algebra then there is a natural isomorphism of functors

$$\begin{array}{rcl} \mathrm{AlgHom}_D(D \otimes_C (C \otimes_A B), Z) & \cong & \mathrm{AlgHom}_C(C \otimes_A B, Z) \\ & \cong & \mathrm{AlgHom}_A(B, Z) \\ & \cong & \mathrm{AlgHom}_D(D \otimes_A B, Z) \end{array}$$

Consider the case $Z = D \otimes_A B$ and the identity map yields the required isomorphism (by the Yoneda Lemma). □

3.6 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 3.6.1
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 3.6.2
If $\mathfrak{p} \triangleleft A$ 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.

3.6.1 Rings

Definition 3.6.3 (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 3.6.4 (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 3.6.5
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

$$\begin{array}{rcl} i_S : A & \to & S^{-1}A \\ a & \to & \left[\frac{a}{1}\right] \end{array}$$

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 3.6.6 (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*

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

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 3.6.7 (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 3.6.8 (Field of fractions contains all localization)
Let A be an integral domain, and 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 3.6.9 (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. □

3.6.2 Modules

Definition 3.6.10 (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 3.6.11 (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 3.6.12
$S^{-1}(-)$ constitutes a functor $A - \mathbf{Mod} \to S^{-1}A - \mathbf{Mod}$. More precisely there is a unique morphism ψ making the following diagram commute as A-module morphisms

$$\begin{array}{ccc} N & \xrightarrow{\psi} & M \\ \downarrow{\scriptstyle i_S} & & \downarrow{\scriptstyle i_S} \\ S^{-1}N & \overset{S^{-1}(\psi)}{\dashrightarrow} & S^{-1}M \end{array}$$

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 3.6.13 (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 3.6.14
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 3.6.15
Let M be a finitely-generated A-module. Then

$$S^{-1}M = 0 \iff sM = 0 \text{ some } s \in S$$

3.6.3 Ideals

Recall the notion of extended and contracted ideals in Definition (3.4.47).

Definition 3.6.16 (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 3.6.17 (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 (3.4.48) 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 (3.4.48). 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 d) $\mathfrak{a}^e$ is proper if and only if $\mathfrak{a}^{ec}$ is proper. By c) we see $1 \in \mathfrak{a}^{ec}$ if and only if $S \cap \mathfrak{a} \neq \emptyset$ and the result follows.

f) By (3.4.48) 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 c) 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 d) 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 d) that $\mathfrak{q}^c \cap S = \emptyset$.

□

Corollary 3.6.18 (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 (3.6.17) every ideal of $S^{-1}A$ is extended. Therefore the bijection of proper ideals follows from (3.4.50). For prime ideals each direction is well-defined by (3.6.17).g). □

3.6.4 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 3.6.19 (Saturation)
Let A be a ring and S a multiplicatively closed set. Then the following sets are equal

a) $(i_S)^{-1}((S^{-1}A)^\star)$

b) $\{x \in A \mid ax \in S \text{ for some } a \in A\}$

c) $\bigcap_{T \supseteq S : T \text{ saturated}} T$

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. Note $x \in (i_S)^{-1}((S^{-1}A)^\star) \implies \frac{x}{1}\frac{b}{t} = 1 \implies s(xb - t) = 0 \implies (sb)x \in S$. Similarly if $ax \in S$ then $\frac{x}{1}\frac{a}{ax} = 1$.

It's clear from b) that the set thus defined is saturated and multiplicatively closed. Let T be another saturated multiplicatively closed set containing S and suppose $ax \in S \implies ax \in T \implies x \in T$, so we find that the sets are equal.

We've proved that $\bar{S}$ is saturated. Clearly $S = \bar{S}$ implies S is saturated. Conversely if S is saturated then by c) we have $\bar{S} \subseteq S$, and clearly $S \subseteq \bar{S}$. The final part follows easily. □

We also give another characterization of saturated multiplicatively closed subsets

Proposition 3.6.20
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 in Example 3.6.2 T is saturated. Therefore $\overline{S} \subseteq T$ by (3.6.19).c).

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 (3.6.19).b)). Therefore by (3.4.40) there is a prime ideal $\mathfrak{p}$ containing a which does not intersect S. Therefore $a \notin T$. Contrapositively $T \subseteq \overline{S}$ as required. □

Proposition 3.6.21 (Change of Rings)
Let $\phi : A \to B$ be a ring homomorphism, S, T corresponding multiplicative subsets. Then

- *There exists a 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 is unique and 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 ϕ injective (resp. surjective, bijective) implies $\tilde{\phi}$ is injective (resp. surjective, bijective)*
- *Further ϕ 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 (3.6.6) 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 ((3.6.19)) 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 ϕ 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 ϕ 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 3.6.22
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 Proposition 3.6.21. □

Corollary 3.6.23 (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 existence of i_{ST} follows from (3.6.21) when considering the map $\phi = 1_A$. The transitivity and reflexive relationships follow from (3.6.22). □

Corollary 3.6.24 (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 3.6.25 (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. □

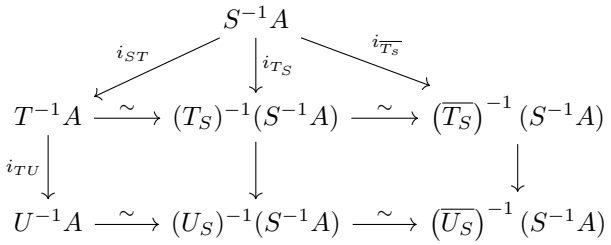
Proposition 3.6.26 (Transitivity)
Let $S \subset T$ be multiplicative subsets of A and let

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

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



3.6.5 Localization at an element

Definition 3.6.27 (Localization at an element)
Let A be a ring and $f \in A$. Then define

$$S_f = \{1, f, \dots, f^n, \dots\}$$

and

$$A_f := (S_f)^{-1} A$$

We have canonical maps

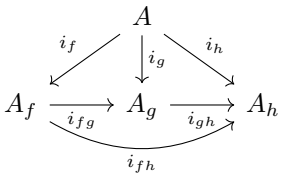
$$i_f : A \to A_f$$

given by $i_f := i_{S_f}$.

Proposition 3.6.28 (Transition maps for localization at an element)
Let A be a ring and $f, g \in A$ then

$$S_f \subseteq \overline{S_g} \iff f \mid g^N \text{ some } N > 0$$

in this case define $i_{fg} = i_{S_f S_g}$ to be the unique morphism such that $i_{fg} \circ i_f = i_g$ (3.6.23). In addition if $h \in A$ and $S_g \subseteq \overline{S_h}$ we have a commutative diagram

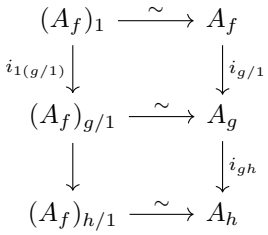


Furthermore $\overline{S_1} = A^\star$ and i_1 is an isomorphism.

Proposition 3.6.29 (Transitivity of localizing at elements)
Let A be a ring and $f, g \in A$ such that $S_f \subseteq \overline{S_g}$. There is a canonical isomorphism

$$A_g \xrightarrow{\sim} (A_f)_{g/1}$$

Furthermore $S_g \subseteq \overline{S_h} \implies S_{g/1} \subseteq \overline{S_{h/1}}$ and there is a commutative diagram



with the horizontal arrows isomorphisms and the vertical arrows are well-defined.

Proof. The existence of the isomorphism is from (3.6.26) as $i_f(S_g) = S_{g/1}$. The second statement follows because $g \mid h^N \implies g/1 \mid h^N/1$ trivially. □

3.6.6 Localization at a prime ideal

Definition 3.6.30 (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 3.6.31 (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 3.6.32
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 (3.6.18). □

Proposition 3.6.33 (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 $f \notin \mathfrak{p}$)

$$i_{S_f S_{\mathfrak{p}}} : A_f \longrightarrow A_{\mathfrak{p}}$$

Furthermore the family of multiplicatively closed sets $\{S_f\}_{f \notin \mathfrak{p}}$ (resp. rings $\{A_f\}_{f \notin \mathfrak{p}}$) form a directed system under the relation $S \prec T \iff S \subseteq \overline{T}$. Therefore we have a canonical ring homomorphism

$$\varinjlim_{f \notin \mathfrak{p}} A_f \longrightarrow A_{\mathfrak{p}}$$

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 $S_f \subseteq \overline{S_{fg}}$. To see this note $fg \in \overline{S_{fg}} \implies f \in \overline{S_{fg}} \implies S_f \subseteq \overline{S_{fg}}$.

The final isomorphism follows because we can decompose it into two maps

$$\varinjlim_{f \notin \mathfrak{p}} A_f \cong \varinjlim_{f \notin \mathfrak{p}} \overline{S_f}^{-1} A \cong A_{\mathfrak{p}}$$

The first is an isomorphism by (3.6.23) and the second by (3.6.9), in light of the first statement. □

3.7 Polynomial Rings in One Variable

Definition 3.7.1 (Polynomial Ring)
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 $\ell(f) := a_{\deg(f)}$. *By convention* $\deg(0) = -\infty$.

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

$$f(X)g(X)h(X) = \sum_{d=0}^{\infty} \left(\sum_{i+j+k=d} a_i b_j c_k \right) X^d$$

Definition 3.7.2 (Monic polynomial)
Let $f \in A[X]$. *We say* f *is* ***monic*** *if the leading coefficient,* $\ell(f)$, *is* 1.

Lemma 3.7.3
If A *is an integral domain then for elements* $f, g \in A[X]$

$$\deg(fg) = \deg(f) + \deg(g)$$

$$\ell(fg) = \ell(f)\ell(g)$$

Further $A[X]$ *is an integral domain.*

Proposition 3.7.4 (Nilpotent and Invertible Polynomials)
Let A *be a ring then*

a) $N(A[X]) = N(A)[X] \subset A[X]$

b) $A[X]^\star = A^\star + XN(A)[X]$

Proof. Suppose $a \in N(A)$ then clearly aX^i is nilpotent. Therefore $N(A)[X] \subseteq N(A[X])$ 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 $\mathfrak{p}$ was arbitrary and $N(A) = \bigcap \mathfrak{p}$ we see that $f \in N(A)[X]$ 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 $A[X]^\star \subseteq A^\star + XN(A)[X]$. Conversely by (3.4.63) and a) we have $A^\star + XN(A)[X] \subseteq A[X]^\star + N(A[X]) \subseteq A[X]^\star$ so the result follows. □

It satisfies the following universal property

Proposition 3.7.5 (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 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 3.7.6
In categorical jargon $A[X]$ *is an initial object in the category of pointed* A*-algebras.*

Proposition 3.7.7 (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 3.7.8 (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 3.7.9 (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 unique polynomials $q(X)$ and $r(X)$ such that

- $f(X) = q(X)g(X) + r(X)$
- $\deg(r) < \deg(g)$

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 $f - \ell(f)gX^{n-m}$ has degree $n-1$, so by induction

$$f - \ell(f)gX^{n-m} = q'g + r$$

with $\deg(r) < \deg(g)$. Therefore

$$f = (q' + \ell(f)X^{n-m})g + r$$

as required.

Suppose $qg + r = q' + r'$ then $(q - q')g = (r' - r)$. This implies that $\deg((q-q')g) < \deg(g)$ which implies $(q-q')g = 0 \implies q = q'$ and $r = r'$. This demonstrates uniqueness. □

3.8 Polynomial Rings in Many Variables

Definition 3.8.1
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 3.8.2
It may be useful for certain induction arguments to write

$$A[X_1, \ldots, X_n] = A$$

when $n = 0$.

Proposition 3.8.3 (Evaluation Homomorphism)
$A[X_1, \ldots, X_n]$ 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 3.8.4 (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 $\deg(f) = \deg(\psi(f); n)$.

Proposition 3.8.5 (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 ρ_{-x}. Let $F \in R$ then

$$\rho_x(F) = \sum_{n=0}^{\infty} \left(\sum_{|\alpha|_1 = n} \lambda_\alpha X_1^{\alpha_1} \ldots X_n^{\alpha_n} \right)$$

whence applying ρ_{-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 λ_α are seen to be uniquely determined by applying ρ_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. □

Definition 3.8.6 (Projection to linear terms)
Given $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$ and $x \in k^n$ define

$$\mathfrak{a}^{(i,x)} = \{F^{(i,x)} \mid F \in \mathfrak{a}\}$$

The following is useful

Lemma 3.8.7
Let A be a k-algebra and $F \in k[X_1, \dots, X_n]$ and $G_1, \dots, G_n \in k[Y_1, \dots, Y_m]$ polynomials. For $\lambda_1, \dots, \lambda_m \in A$ we have

$$F(G_1, \dots, G_n)(\lambda_1, \dots, \lambda_m) = F(G_1(\lambda_1, \dots, \lambda_m), \dots, G_n(\lambda_1, \dots \lambda_m))$$

3.9 Chain Conditions

Definition 3.9.1 (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 3.9.2 (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 3.9.3 (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 3.9.4 (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 $[M]_\phi$. □

Proposition 3.9.5
Let A be a Noetherian ring and $\mathfrak{a} \triangleleft A$ an ideal. Then $A/\mathfrak{a}$ is Noetherian.

Proof. Consider an increasing sequence of ideals $\mathfrak{a}_i \triangleleft A/\mathfrak{a}$. Then by (3.4.53) this corresponds to an increasing sequence of ideals $\mathfrak{a}_i' \triangleleft A$ containign $\mathfrak{a}$. As A is Noetherian, this sequence eventually stabilizes. Again by (3.4.53) the original sequence stabilizes. □

Proposition 3.9.6
Let A be a Noetherian ring then every finitely-generated A-algebra is Noetherian.

In particular $A[X_1, \ldots, X_n]$ is Noetherian.

Proof. By (3.9.5) it's enough to show that $A[X_1, \ldots, X_n]$ is Noetherian. By induction and (3.8.4) it's enough to consider the case $n = 1$. Let $\mathfrak{a} \lhd A[X]$ then by (3.9.3) it's enough to show that $\mathfrak{a}$ is finitely-generated.

Define

$$\widetilde{\mathfrak{a}}_i := \{\ell(f) \mid f \in \mathfrak{a} \text{ s.t. } \deg(f) = i\}$$

Then clearly $\widetilde{\mathfrak{a}}_i \lhd A$ is an ideal. This is an increasing sequence of ideals, and so it stabilizes for $i \geq d$ for some $d > 0$. Furthermore each ideal is finitely generated

$$\widetilde{\mathfrak{a}}_i := (c_{i1}, \ldots, c_{in(i)})$$

where $c_{ij} = c(f_{ij})$ for polynomials $f_{ij} \in \mathfrak{a}$ of degree i. We claim that

$$\mathfrak{a} = (f_{ij})_{i \leq d \; j \leq n(i)}$$

Denote the right hand side by $\mathfrak{b}$, then clearly $\mathfrak{b} \subseteq \mathfrak{a}$. We show by induction on $m = \deg(f)$ that $f \in \mathfrak{a} \implies f \in \mathfrak{b}$. Let $m' := \min(m, d)$. Then by assumption $\ell(f) \in \widetilde{\mathfrak{a}}_m = \widetilde{\mathfrak{a}}_{m'}$ so there exists $\lambda_j \in A$ such that

$$\ell(f) = \sum_{j=1}^{n(m')} c_{m'j}\lambda_j$$

Consider the decomposition

$$f = (f - \sum_{j=1}^{n(m')} \lambda_j f_{m'j} X^{m-m'}) + \sum_{j=1}^{n(m')} \lambda_j f_{m'j} X^{m-m'}$$

The first term has strictly smaller degree than f, so by the inductive hypothesis lies in $\mathfrak{b}$. Therefore $f \in \mathfrak{b}$ as required. □

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
A PID is Noetherian.

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. □

Proposition 3.10.3 (Integers form a PID)
$\mathbb{Z}$ is a PID.

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. □

Proposition 3.10.4
Let k be a field then the polynomial ring $k[X]$ is a PID

Proof. Let $\mathfrak{a} \lhd k[X]$ be an ideal. Choose $f \in \mathfrak{a}$ to have minimal degree, then we claim $\mathfrak{a} = (f)$. For $g \in \mathfrak{a}$ we have by (3.7.9) $g = qf + r$ for $\deg(r) < \deg(f)$. Clearly $r \in \mathfrak{a}$, so by minimality $r = 0$ and the result follows. □

Lemma 3.10.5 (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 Factorisation

For this section we assume A is a commutative integral domain.

Definition 3.11.1 (Associates)
*We say two non-zero elements x and y are **associates** if $x = uy$ for some $u \in A^\star$. We write $x \sim y$.*

Note this is an equivalence relation on $A \setminus \{0\}$.

Lemma 3.11.2
Let A be a ring and $x, y \in A$ non-zero elements then the following are equivalent

- $x \mid y$
- $(y) \subseteq (x)$
- $y \in (x)$

Lemma 3.11.3
Let A be a ring and $x, y \in A$ non-zero elements then the following are equivalent

- $x \mid y$ *and* $y \mid x$
- $(x) = (y)$

If A is an integral domain this is equivalent to $x \sim y$.

Definition 3.11.4 (Irreducible element)
*We say $0 \neq x$ is **irreducible** if it is not invertible and $x = ab \implies a$ a unit or b a unit.*

Equivalently if $y \mid x$ implies either y is a unit or $y \sim x$.

Definition 3.11.5 (Prime element)
We say $0 \neq p$ is prime if $p \mid ab \implies p \mid a$ or $p \mid b$.

Example 3.11.6
The units of $\mathbb{Z}$ are $\{-1, 1\}$ so each equivalence class is of the form $\{n, -n\}$.

Example 3.11.7
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 (2.2.13)).

The concept of associates is important to unique factorization, because we may only hope to have unique factorization upto multiplication by a unit.

Lemma 3.11.8
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 or bu a unit $\implies b$ a unit. Therefore y is irreducible as required. □

Lemma 3.11.9 (Criterion for primality)
Suppose $0 \neq p \in \mathbb{Z}$. Then 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 3.11.10 (Criterion for irreducibility)
Let A be an integral domain. Then f is irreducible if and only if (f) is maximal amongst proper 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 suppose $f = ab$, then $f \in (a) \implies (f) \subseteq (a)$. Then by hypothesis either $(a) = (f)$ or $(a) = A$. In the second case a is a unit. In the first case then $f \mid a \implies bf \mid f \implies b \mid 1$ whence b is a unit. □

Proposition 3.11.11 (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 (3.11.3) $p \sim a$ (resp. b) as required. □

Definition 3.11.12 (Unique Factorisation 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 ψ a permutation on $\{1, \ldots, n\}$.

Furthermore it may be convenient in applications to count the multiplicities

Proposition 3.11.13 (Factorisation with multiplicities)
Let A be a UFD, 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 τ and σ 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 $r_i = r'_{\sigma(i)}$. □

Definition 3.11.14
Let A be a UFD and $x \in A$ a non-zero, non-unit such that

$$x \sim \prod_{i=1}^{n} p_i^{r_i}$$

is an (almost) unique factorization into irreducibles. Then for $p \in A$ an irreducible define

$$v_p(x) := \begin{cases} r_i & p \sim p_i \\ 0 & otherwise \end{cases}$$

If $x \in A$ is a unit then simply define $v_p(x) = 0$ for all p.

Lemma 3.11.15
Let A be a UFD then the following are equivalent

a) $x \mid y$

b) $(y) \subseteq (x)$

c) $v_p(x) \leq v_p(y)$ *for all p irreducible*

In particular $x \sim y \iff (x) = (y) \iff v_p(x) = v_p(y)$ for all p irreducible.

Definition 3.11.16 (Atomic Ring)
*We say that A is **atomic** if every element has a (not necessarily unique) decomposition into irreducible elements.*

Definition 3.11.17 (Ascending Chain Condition for Principal Ideals (ACCP))
*We say a ring A satisfies **ACCP** if every ascending chain of principal ideals eventually stabilizes.*

Note every Noetherian ring satisfies this condition.

Proposition 3.11.18
An integral domain A satisfying ACCP is atomic.

In particular a Noetherian ring is atomic. .

Proof. Suppose a ring A is not atomic, then choose any non-unit $x_1 \in A$. By repeated application (3.11.10) it's possible to construct a strictly ascending sequence of proper principal ideals

$$(x_1) \subsetneq (x_2) \subsetneq \ldots \subsetneq (x_n) \subsetneq \ldots$$

therefore A does not satisfy ACCP. □

Remark 3.11.19
The converse is not in general true (...) but see (3.11.21) for a partial converse.

We show a simple criterion for a ring to be a UFD.

Definition 3.11.20
*We say an integral domain A is **AP** if p irreducible $\implies$ p prime.*

Roughly speaking, "atomic" ensures the existence of factorization and "AP" ensures the uniqueness.

Proposition 3.11.21 (Atomic + AP $\iff$ UFD)
Let A be an integral domain. The following are equivalent

a) *A is a UFD*

b) *A is atomic and AP*

c) *A satisfies ACCP and is AP*

NB a ring satisfying irreducible $\implies$ prime is referred to as an AP-domain.

Proof. $a \implies c$). Suppose A is a UFD. If p is an irreducible element and $p \mid ab$, then by uniqueness it must appear in the irreducible factorization of either a or b. Therefore p is prime. If we have an ascending chain of principal ideals $(x_1) \subseteq (x_2) \ldots$ then by (3.11.15) we have $v_p(x_i)$ is a decreasing sequence for all irreducible p occuring in the factorization of x_1. Furthermore $\max_p v_p(x_i)$ is a finite decreasing sequence. Choose $i = N$ such that $\max_p v(x_i)$ is minimal, then all these sequences must stabilise for $i \geq N$ and therefore by (3.11.15) the chain of principal ideals also stabilises.

$c \implies b$). This is (3.11.18).

$b \implies a$). We require to show that factorization into irreducibles is unique up to associates. Suppose

$$\prod_{i=1}^{n} p_i \sim \prod_{j=1}^{m} p'_j$$

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. □

Lemma 3.11.22 (PID is an AP-domain)
Let A be a PID and $a \in A$. Then the following are equivalent

a) *a is prime*

b) *a is irreducible*

c) *(a) is maximal*

Proof. *a)* $\implies$ *b)* This holds for an arbitrary integral domain (3.11.11).
b) $\iff$ *c)* as all ideals are principal this follows from (3.11.10)
c) $\implies$ *a)* By (3.4.57) (a) is prime, whence a is prime by (3.11.9) □

Proposition 3.11.23
A PID is Noetherian UFD.

Furthermore (f is irreducible $\iff$ f is prime), and every prime ideal is maximal.

Proof. A is Noetherian by (3.10.2) and atomic by (3.11.18). And by (3.11.22) an irreducible element is prime. Therefore we are done by by (3.11.21). □

If we take a suitable fixed set of irreducible elements we can obtain completely unique factorization

Definition 3.11.24
*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 (precisely) one in $\mathcal{P}$*

Example 3.11.25
For $\mathbb{Z}$ the positive *primes are a canonical set of irreducible elements.*

Proposition 3.11.26
Let A be a UFD and $K = \operatorname{Frac}(A)$ then for every irreducible $p \in A$ there is a unique map

$$v_p : K^\star \to \mathbb{Z}$$

such that

- $u \in A^\star \implies v_p(u) = 0$
- $v_p(xy) = v_p(x) + v_p(y)$
- $v_p(p) = 1$

Furthermore let $\mathcal{P}$ be a set of irreducible representatives then we have a group isomorphism

$$\begin{aligned} K^\star/A^\star &\xrightarrow{\sim} \bigoplus_{p\in\mathcal{P}} \mathbb{Z} \\ x &\longrightarrow (v_p(x))_{p\in\mathcal{P}} \\ \prod_{p\in\mathcal{P}} p^{n_p} &\longleftarrow (n_p)_{p\in\mathcal{P}} \end{aligned}$$

Finally $x \in A \iff v_p(x) \geq 0$ for all $p \in \mathcal{P}$.

Proof. By (3.11.13) there is a well-defined map $v_p : A \setminus \{0\} \to \mathbb{Z}$ satisfying the given properties. We claim that

$$\begin{aligned} v_p : K^\star &\to \mathbb{Z} \\ xy^{-1} &\to v_p(x) - v_p(y) \end{aligned}$$

is well-defined. For suppose $xy^{-1} = wz^{-1}$ then $zx = wy$ whence $v_p(z) + v_p(x) = v(w) + v(y)$ and therefore $v_p(xy^{-1}) = v_p(wz^{-1})$.

It's clear the multiplicative property also holds and so ϕ is well-defined (since by definition $A^\star$ is in the kernel of v_p). Denote by ϕ, ψ the proposed maps. By definition of unique factorization ϕ and ψ are mutual inverses when restricted as follows

$$(A \setminus \{0\})/A^\star \longleftrightarrow \bigoplus_{p \in \mathcal{P}} \mathbb{Z}_{\geq 0}$$

We also observe that $\phi(x^{-1}) = -\phi(x)$ and $\psi(-n) = \psi(n)^{-1}$, so then it's easy to demonstrate they are mutually inverse over the whole domain.

Suppose $v_p(xy^{-1}) \geq 0$ then $v_p(x) \geq v_p(y)$. If this holds for all $p \in \mathcal{P}$, then by (3.11.15) $y \mid x$ as elements of A whence by definition $xy^{-1} \in A$ as required. □

Proposition 3.11.27
Suppose A is an integral domain satisfying ACCP then so is $A[X]$.

Proof. Suppose we have an ascending chain of principal ideals

$$(f_1) \subseteq (f_2) \subseteq \dots (f_n) \dots$$

Without loss of generality the f_i are non-zero. Then $f_{i+1} \mid f_i$ and by (...) $\deg(f_{i+1}) \leq \deg(f_i)$. Choose N such that $\deg(f_i)$ is minimal, and define $a_i := \ell(f_i) \in A$. Then by (3.7.3) $a_{i+1} \mid a_i$ for $i \geq N$ as elements of A. Therefore we have an increasing sequence of principal ideals

$$(a_N) \subseteq (a_{N+1}) \subseteq \dots$$

which by hypothesis stabilizes, that is $a_i \sim a_j$ for all $i, j \geq M$ for some $M \geq N$. For $i \geq M$ we have $ua_i = a_{i+1}$, consider $uf_i - f_{i+1} \in (f_i)$. This has degree strictly smaller than N, and therefore by minimality must be 0. In particular $f_i \sim f_{i+1}$ and $(f_i) = (f_{i+1})$. □

Lemma 3.11.28
Suppose $p \in A$ is prime, then it is prime as an element of $A[X]$.

Lemma 3.11.29 (Nagata's Criterion)
Let A be a ring and S a multiplicative subset generated by prime elements and units. Let $f \in A$ be irreducible or a unit, then

a) $\frac{f}{1}$ *is irreducible or a unit in* $S^{-1}A$

b) $\frac{f}{1}$ *prime or a unit in* $S^{-1}A \implies f$ *is a prime or a unit in* A.

Furthermore if $S^{-1}A$ is AP then so is A.

Proof. Note the condition on S means every $a \in S$ satisfies $a \sim p_1 \dots p_r$ for primes $p_i \in A$.

a) Suppose $\frac{f}{1} = \frac{g}{a}\frac{h}{b}$ for $f, g, h \in A$ and $a, b \in S$, then $abf = gh$. Further $ab \sim p_1 \dots p_r$. Then $p_i \mid a$ or $p_i \mid b$, whence we can find $f \sim g'h'$ where $g = cg'$, $h = dh'$ and $c, d \in S$. As f is irreducible (or a unit), then for example g' is invertible, in which case $\frac{g}{a} = \frac{cg'}{a}$ is invertible. Therefore $\frac{f}{1}$ is either irreducible or a unit.

b) The case f a unit is clear, so assume that f is irreducible. Suppose $\frac{f}{1}$ is prime or a unit and $f \mid gh$. Then $\frac{f}{1} \mid \frac{g}{1}\frac{h}{1}$ and for example $\frac{f}{1} \mid \frac{g}{1}$. Therefore $ff' = gp_1 \dots p_r$ for some $f' \in A$ and $p_1, \dots, p_r \in A$ prime. If $p_i \mid f$ for some i then by irreducibility we have $p_i \sim f$, and we see that f is prime. Otherwise $p_i \mid f'$ for all i and we find $f \mid g$. Therefore f is prime as required.

The last statement follows immediately from the previous two results. □

3.11.0.1 Polynomial Case

We prove the following result, first by Nagata's Criterion and again by Gauss' Lemma.

Proposition 3.11.30
Suppose A is a UFD, then so is $A[X]$.

Proof. By (3.11.21) we need to show that $A[X]$ satisfies ACCP and is AP. The first follows from (3.11.27).

Let $S = A \setminus \{0\}$ the set of non-zero elements. Let $K = \mathrm{Frac}(A)$. If we regard $A[X]$ as a subring of $K[X]$ then we claim $S^{-1}(A[X]) = K[X]$; this follows by multiplying an element of $K[X]$ by the product of denominators of all the coefficients. Furthermore as A is a UFD (and by (3.11.21)) S is generated by prime elements and units. By (3.11.23) $K[X]$ is a UFD, and so in particular is AP. Therefore by (3.11.29) $A[X]$ is AP as required. □

For Gauss' Lemma we require to introduce some notation first.

Definition 3.11.31 (Primitive polynomials)
Let A be a UFD, $K := \mathrm{Frac}(A)$ and $f \in K[X]$ a polynomial given by

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

*Define the **content** of f by*

$$c(f) = \prod_{p \in \mathcal{P}} p^{\min_i v_p(a_i)} \in K^\star$$

where the product is taken over a representative set of primes for A. Changing the set of representatives only changes the value of $c(f)$ by multiplication of a unit.

*We say that f is **primitive** precisely when $c(f) = 1$*

Lemma 3.11.32 (Gauss' Lemma I)
Let A be a UFD and $f \in K[X]$ where $K = \mathrm{Frac}(A)$. Then the content $c(f)$ satisfies the following properties

a) $f \in A[X] \iff c(f) \in A$

b) f *is primitive* $\iff \min_i v_p(a_i) = 0 \quad \forall p$ *prime and in this case* $f \in A[X]$

c) $c(\lambda f) = \lambda c(f)$ *for* $\lambda \in K^\star$ *up to multiplication by a unit in* A

d) $f/c(f) \in A[X]$ *is primitive*

e) f, g *primitive* $\implies fg$ *primitive*

f) $c(fg) = c(f)c(g)$ *for all* $f, g \in K[X]$

Proof. We prove each in turn

a) $f \in A[X] \iff a_i \in A \quad \forall i \overset{(3.11.26)}{\iff} v_p(a_i) \geq 0 \, \forall i \, \forall p \in \mathcal{P} \iff \min_i v_p(a_i) \geq 0 \, \forall p \in \mathcal{P} \overset{(3.11.26)}{\iff} c(f) \in A$

b) $c(f) = 1 \iff v_p(c(f)) = 0 \quad \forall p \iff \min_i v_p(a_i) = 0 \quad \forall p$. Further $v_p(a_i) \geq 0$ whence $f \in A[X]$ by (3.11.26).

c) Note $v_p(\lambda a_i) = v_p(\lambda) + v_p(a_i) \implies v_p(c(\lambda f)) = \min_i v_p(\lambda a_i) = v_p(\lambda) + \min_i v_p(a_i) = v_p(\lambda) + v_p(c(f))$. Whence by (3.11.26) we see $c(\lambda f)$ and $\lambda c(f)$ are equal up to multiplication by a unit in A.

d) Clear by b).

e) Consider p prime and the reduction $\bar{\cdot} : A[X] \to (A/(p))[X]$. Then by assumption $\overline{f}$ and $\overline{g}$ are non-zero. Furthermore $(A/(p))[X]$ is an integral domain so that $\overline{f \cdot g} = \overline{f} \cdot \overline{g} \neq 0$. Therefore p does not divide all the coefficients of $f \cdot g$. As p was arbitrary this shows that $f \cdot g$ is primitive.

f) We may reduce to e) by dividing by the content.

□

Lemma 3.11.33 (Gauss' Lemma II)
Let A be a UFD and $f \in A[X]$. Then the following are equivalent

a) f *is irreducible in* $A[X]$

b) f *is an irreducible element of* A *or* (f *is primitive and irreducible in* $K[X]$)

where $K = \mathrm{Frac}(A)$.

In particular if $f \in K[X]$ is irreducible then $f/c(f)$ is irreducible in $A[X]$.

Proof. $b) \implies a)$. It's clear that an irreducible element of A remains irreducible in $A[X]$. Suppose $0 \neq f \in A[X]$ is primitive and irreducible in $K[X]$. Then as $f \notin K[X]^\star$ we have $\deg(f) > 0$. Suppose $f = gh$ in $A[X]$ then by irreducibility $\deg(g) = 0$ or $\deg(h) = 0$. Further $1 = c(f) = c(g)c(h)$ by Gauss' Lemma, so one of h and g must lie in $A^\star = A[X]^\star$. Therefore f is irreducible in $A[X]$ as required.

$a) \implies b)$. If $\deg(f) = 0$ then clearly f is an irreducible element of A. So assume $\deg(f) > 0$. Observe $f = c(f) \cdot (f/c(f))$ so by irreducibility we require $c(f) = 1$ and therefore f is primitive. Suppose $f = gh$ in $K[X]$ then $1 = c(g)c(h)$ and therefore

$$f = \frac{g}{c(g)} \frac{h}{c(h)}$$

is a decomposition in $A[X]$ which shows one of g, h has degree 0. Therefore f is irreducible in $K[X]$ as required. □

Proposition 3.11.34
Let A be a UFD. Then so is $A[X]$.

Proof. For $0 \neq f \in A[X]$ we may use irreducible factorisation in $K[X]$ to find

$$f = \lambda \pi_1 \dots \pi_n$$

where $\lambda \in K$ and $\pi_i \in K[X]$ are irreducible. Replace $\pi_i \to \pi_i / c(\pi_i)$ then may assume that π_i are irreducible in $A[X]$ by (3.11.33). Furthermore

$$c(f) = \lambda c(\pi_i) \dots c(\pi_n) = \lambda$$

which shows $\lambda \in A$. As A is a UFD then λ may be decomposed into irreducibles of A, which by (3.11.33) are irreducible in $A[X]$. Therefore $A[X]$ is atomic.

Suppose that $f \in A[X]$ is irreducible we require to show it is prime. The case $\deg(f) = 0$ follows from the AP property of A, so assume $\deg(f) > 0$. Suppose $f \mid gh$ then as $K[X]$ is a UFD we see that, without loss of generality, $qf = g$ for $q \in K[X]$. Then $c(qf) = c(q)c(f) = c(q) = c(g) \in A$, so $q \in A[X]$ by (3.11.32) and we see $f \mid g$ in $A[X]$. This shows that $A[X]$ is AP and therefore a UFD by (3.11.21). □

Corollary 3.11.35
Suppose A is a UFD. Then $A[X_1, \dots, X_n]$ is a UFD.

3.12 Cayley-Hamilton Theorem

Definition 3.12.1 (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 3.12.2 (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 3.12.3
Suppose $M = \langle m_1, \dots, m_n \rangle$ is a finitely generated A-module then

$$\mathfrak{a}M = \mathfrak{a}m_1 + \dots + \mathfrak{a}m_n$$

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 3.12.4 (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 $\mathfrak{a} \lhd A$, 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 $\{m_1, \ldots, m_n\}$ 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

$$\mathrm{Mat}_n(\mathrm{End}_A(M)) \times M^n \to M^n$$

$$F \cdot (x_1, \ldots, x_n)^T \to \left(\sum_j F_{ij}(x_j) \right)_i$$

such that $(EF)v = E(Fv)$ (check).
And we have shown that

$$B(\phi)\,(m_1, \ldots, m_n)^T = \mathbf{0}$$

Using (3.4.126), premultiply by the adjoint matrix to show that

$$\det(B(\phi)) I_n\,(m_1, \ldots, m_n)^T = \mathbf{0}$$

and $\det(B(\phi)) \in \mathrm{End}_A(M)$ annihilates $m_1, \ldots, m_n$ and therefore M.

Finally we claim that $P(X) := \det(B(X)) \in A[X]$ is a suitable monic polynomial. We see that

$$P(\phi) := \mathrm{ev}_\phi(\det(B(X))) \overset{??}{=} \det(B(X)^{\mathrm{ev}_\phi}) = \det(B(\phi)) = 0$$

When M is a finite free A-module then we may choose $\{m_1, \ldots, m_n\}$ to be a basis, and then the matrix E equals $[\phi]^T$ as required.

Finally when $\phi(M) \subseteq \mathfrak{a}M$ then Lemma 3.12.3 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 $\mathfrak{a}$. □

3.13 Finite-type Algebras

Definition 3.13.1 (Finite algebra)
An A-algebra B is finite *if it is finite as an A-module.*

Definition 3.13.2 (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

$$A[X_1, \ldots, X_n] \to B$$

the images of X_i are the generators.

3.14 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.

In what follows we implicitly assume all k-algebras are non-zero.

3.14.1 Prime Fields

Recall that for p prime the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field (3.10.3), (3.11.22), (3.4.56).

Definition 3.14.1 (Finite field of order p)
Denote by $\mathbb{F}_p$ the field $\mathbb{Z}/p\mathbb{Z}$ of order p.

Definition 3.14.2 (Rational Integers)
We denote by $\mathbb{Q}$ the field of ***rational numbers*** *defined to be the field of fractions of the integers,* $\mathrm{Frac}(\mathbb{Z})$ *(see Example 3.6.7).*

Definition 3.14.3 (Prime Field)
We say that a field k is a ***prime field*** *if it is isomorphic to one of $\mathbb{F}_p$ or $\mathbb{Q}$.*

Note none of these fields are mutually isomorphic by considering cardinalities.

Proposition 3.14.4 (Prime Subfield Exists)
Let A be a k-algebra. Then A contains k as a subfield. Furthermore the unique homomorphism

$$\mathbb{Z} \to A$$

has kernel equal to either (0) or (p) for p prime.

Therefore A contains a prime subfield and it is the smallest subfield contained in A.

Proof. Consider the unique homomorphism $\phi : \mathbb{Z} \to k$, then it is the same as the homomorphism into A. As A is not the zero-ring then $\phi(1) = 1 \neq 0$ and $\ker(\phi)$ is a proper ideal. Then $\mathrm{Im}(\phi)$ is an integral domain by (3.4.9). By (3.4.54) $\mathbb{Z}/\ker(\phi) \cong \mathrm{Im}(\phi)$ and therefore by (3.4.56) $\ker(\phi) =: \mathfrak{p}$ is a prime ideal.

Suppose $\mathfrak{p} = (0)$. By (3.6.6) ϕ extends to a homomorphism $\mathbb{Q} \to k$ whose kernel is zero and therefore injective (...).

Otherwise by (3.10.3) and (3.11.9) $\mathfrak{p} = (p)$ for p a prime number and we have already observed that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is isomorphic to a subfield of k. □

Definition 3.14.5 (Characteristic)
Let A be a k-algebra and (n) the kernel of the unique homomorphism $\mathbb{Z} \to A$.

Then the ***characteristic*** *of A is defined to be n. By (3.14.4) it is either 0 or p when the unique prime subfield is isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$ respectively. We denote this by* $\mathrm{char}(A)$. *We also define the* ***characteristic exponent*** *to be*

$$\begin{cases} 1 & \text{if } \mathrm{char}(A) = 0 \\ p & \text{if } \mathrm{char}(A) = p \end{cases}$$

Proposition 3.14.6 (Frobenius Homomorphism)
Let A be a k-algebra and suppose $\mathrm{char}(A) = p$. *Then the mapping*

$$a \to a^p$$

is a ring homomorphism, which we denote the ***Frobenius map****. In particular*

$$(a+b)^p = a^p + b^p \quad \forall a, b \in A$$

Proposition 3.14.7 (Perfect Field)
Let K be a field. Then the following are equivalent

a) $\mathrm{char}(K) = 0$ *or (*$\mathrm{char}(K) = p$ *and the Frobenius map is an isomorphism)*

b) $K^p = K$ *where p is the* ***characteristic exponent***

In this case we say K is ***perfect****.*

3.14.2 Field Extensions

Definition 3.14.8 (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 (3.4.58). 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*

$$\mathrm{Mor}_k(K, L) := \{\psi : K \to L \mid \psi \circ i_{kK} = i_{kL}\}$$

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 3.14.9 (Finite field extension)
A field extension K/k is finite if $[K : k] < \infty$

Definition 3.14.10 (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 3.14.11
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 3.14.12
Let $K = K_n/\ldots/K_0 = k$ be a tower of finite extensions then

$$[K : k] = \prod_{i=1}^{n} [K_i : K_{i-1}]$$

Lemma 3.14.13
Let K/k be a field extension and $f, g \in k[X]$. Then $g \mid f$ in $k[X]$ if and only if $i_{kK}(g) \mid i_{kK}(f)$.

Proof. One implication is obvious. For the converse we assume wlog that $k \subset K$ and suppose $f = gh$ for $h \in K[X]$. We may apply the division algorithm (3.14.31) in $k[X]$ to find $f = gq + r$ for $q, r \in k[X]$ and $\deg(r) < \deg(g)$. Then $r = g(h - q)$ and comparing degrees we conclude that $h = q$ and $r = 0$. This shows $f = gq$ and $g \mid f$ as elements of $k[X]$. □

Definition 3.14.14 (Evaluation homomorphism)
Let K/k be a field extension and $\alpha \in K$. There is a canonical homomorphism

$$\begin{aligned} \mathrm{ev}_\alpha : k[X] &\to K \\ \sum_{i=0}^{n} a_i X^i &\to \sum_{i=0}^{n} i_{kK}(a_i)\alpha^i \end{aligned}$$

which we write as $f(\alpha)$. We say $\alpha \in K$ is a root of $f(X)$ if $f(\alpha) = 0$.

Proposition 3.14.15 (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 α is a root of $p \iff \sigma(\alpha)$ is a root of p.

Proof. This is just a specific case of (3.7.7), The last statement is obvious, because σ is injective (3.4.58). □

Proposition 3.14.16 (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 $S = \{\alpha_1, \ldots, \alpha_n\}$ is finite then

$$k[\alpha_1, \ldots \alpha_n] = \mathrm{im}(\mathrm{ev}_\alpha) = \{p(\alpha_1, \ldots, \alpha_n) \mid p \in k[X_1, \ldots, X_n]\}$$

from the characterization from (3.8.3). In general

$$k[S] = \bigcup_{S' \subset S \text{ finite}} k[S']$$

Lemma 3.14.17 (Trivial result)
For $S, T \subset K/k$ finite

- $S \subset T \implies k[S] \subseteq k[T]$
- $k[S][T] = k[S \cup T]$

Definition 3.14.18 (Subfield generated by a set)
Let K/k be a field extension and $S \subset K$ a subset. When $S = \{\alpha_1, \ldots, \alpha_n\}$ is finite define

$$k(S) := \left\{ \frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)} \mid p, q \in k[X_1, \ldots, X_n] \right\}$$

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 3.14.19 (Trivial result)
For $S, T \subset K/k$

- $S \subset T \implies k(S) \subseteq k(T)$
- $k(S)(T) = k(S \cup T)$

Lemma 3.14.20
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 3.14.21 (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 3.14.22 (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 3.14.23 (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 α is also algebraic over k.*

Definition 3.14.24 (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. α is integral, since we can always ensure f is monic). Otherwise we say that $x \in K$ is **transcendental**.*

*We say K/k is an **algebraic extension** if every element $\alpha \in K$ is algebraic over k.*

Proposition 3.14.25 (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 (2.3.12). Therefore there is a non-zero polynomial with α as a root. □

Proposition 3.14.26 (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 (3.4.58) we only need to show that σ is surjective. Given $\alpha \in K$ let T denote the set of roots of $m_\alpha \in k[X]$ in K. Note by (3.14.36) T is finite. Further by (3.14.15) σ maps T to itself. Since σ is injective it is also surjective on T. In particular α is in the image of σ as required. □

3.14.3 Polynomials

In this section we consider the polynomial ring with coefficients in a field, $k[X]$.

Proposition 3.14.27
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 3.14.28
The units of $k[X]$ are precisely the non-zero polynomials of degree 0.

Proposition 3.14.29 (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 3.14.30
A polynomial $f \in k[X]$ is associate to precisely one monic polynomial g. If f is irreducible so is g.

Proof. **TODO** □

Proposition 3.14.31 (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 (3.7.9) to $g/\ell(g)$, and multiply by $\ell(g)$ again. □

Proposition 3.14.32 (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 3.14.33 (Unique Factorisation of Polynomials)
For the ring $k[X]$ the set of irreducible monic polynomials constitutes a representative set (Definition (3.11.24)). Therefore we have a unique factorization

$$f = \ell(f) \prod_{p \text{ irreducible monic}} p^{v_p(f)}$$

such that

$$v_p(fg) = v_p(f) + v_p(g)$$

Proof. (3.14.30) shows that the irreducible monic polynomials constitute a representative set. Therefore the result follows from (3.11.26). Let u be the unit appearing in the factorization, it must be an element of k. Compare leading coefficients to see that $u = \ell(f)$. □

Lemma 3.14.34 (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 α, and observe

$$f(X) = \ell(f)(X - a)^r g(X)$$

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 3.14.35 (Splitting Polynomial)
*Let K/k be a field extension and $f \in k[X]$. By abuse of notation we may also identify f with its image in $K[X]$. We say a polynomial f **splits completely** in K if the irreducible factorization of f in $K[X]$ is*

$$f = \ell(f) \prod_{i=1}^{n} (X - \alpha_i)^{r_i}$$

where α_i are the distinct roots of f in K and $r_i := v_{(X-\alpha_i)}(f^i)$ are the multiplicities. Equivalently f splits in K if

$$p \in K[X] \text{ irreducible } \wedge \deg(p) > 1 \implies v_p(f) = 0 \tag{3.3}$$

Observe that the number of roots counting multiplicities is $\deg(f)$

$$\deg(f) = \sum_{i=1}^{n} v_{(X-\alpha_i)}(f)$$

Corollary 3.14.36
A polynomial f has at most $\deg(f)$ *roots*

Corollary 3.14.37
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 (3.14.33) each g_i must be appear in the factorization of f, that is to say g splits completely. □

Proposition 3.14.38 (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 (3.14.34)

$$f^{(1)}(X) = (X-\alpha)^{r-1}[rg(X) + (X-\alpha)g'(X)]$$

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 α as a root of multiplicity $r-1$, so it follows by induction.
The second statement is simply the case $r = 1$. □

Definition 3.14.39 (Separable Polynomial)
*A polynomial $f \in k[X]$ is **separable** if f and f' are co-maximal, that is $(f, f') = (1)$. Otherwise it is **inseparable**.*

Proposition 3.14.40
A separable polynomial $f \in k[X]$ has no multiple roots (and f and f' have no common roots) in any extension field K/k.

Proof. Since $(f, f') = (1)$ we have $af + bf' = 1$ for some $a, b \in k[X]$. Clearly f and f' can have no common roots, and therefore f has no multiple roots by (3.14.38). □

Proposition 3.14.41
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 (3.10.5) 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 (3.10.5). □

We can provide a partial converse to (3.14.40) by working in a large enough extension field

Proposition 3.14.42 (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 and f' have no common roots in K*

d) *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 $d) \iff b)$. By (3.14.38) $b) \iff c)$

Proposition (3.14.40) shows that $a) \implies b)$. Conversely suppose f is not separable, then by (3.10.5) f and f' must have a non-trivial common divisor h. By (3.14.37) we see that h splits in K. Any root of h is a common root of f and f' in K, which by (3.14.38) is a multiple root of f in K. □

3.14.4 Algebraic Extensions

Proposition 3.14.43 (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 α over k and $(m_{\alpha,k}) = \ker(\mathrm{ev}_\alpha)$.

In particular any polynomial $f(X) \in k[X]$ which has α as a root, satisfies $m_{\alpha,k}(X) \mid f(X)$.

Proof. Let $\mathfrak{a} = \ker(\mathrm{ev}_\alpha)$. Since $k[X]$ is a PID it is of the form $(m_{\alpha,k})$. As α 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 (3.14.29) $m_{\alpha,k} = \lambda p$. In particular $\deg(m_{\alpha,k}(X)) = \deg(p(X))$ so $\deg(q(X)) = 0$ and $q(X)$ is a unit (3.14.28). 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_α 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 $m' = m_\alpha$. □

Lemma 3.14.44
Let $K/E/k$ be extensions and $\alpha \in K$ algebraic over k. Then α is algebraic over E.

Definition 3.14.45 (Conjugate elements)
*Two elements $\alpha, \beta \in K$ are said to be **conjugate elements** if they have the same minimal polynomial.*

NB it's necessary and sufficient that $m_{\alpha,k}(\beta) = 0$.

Proposition 3.14.46
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 (3.14.15). □

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 3.14.47 (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 $k(\alpha) = k[\alpha]$*
- *$m_\alpha = f/\ell(f)$ and $\deg(m_\alpha) = \deg(f) =: n$*
- *K is a finite-dimensional k-vector space with basis*

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

Example 3.14.48
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 (3.11.22) so K is a field by (3.4.56). The composition $\pi \circ i$ makes K into a k-algebra and hence a field extension. Furthermore π is then by definition a k-algebra homomorphism.

Since π is surjective every $\beta \in K$ is represented as $\pi(p(X)) \overset{(3.14.15)}{=} p(\pi(X)) = p(\alpha)$. By (3.14.16) we see $K = k[\alpha]$. Since K is a field then $K = k[\alpha] = k(\alpha)$ is simple by (3.14.20).

Similarly $f(\alpha) = f(\pi(X)) \overset{(3.14.15)}{=} \pi(f(X)) = 0$, so α is a root of f. By (3.14.29) $f/\ell(f)$ is irreducible and by uniqueness in (3.14.43) we have $m_\alpha = f/\ell(f)$.

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 3.14.49 (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

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

where $n = \deg(m_\alpha) = [k(\alpha) : k]$ and $k(\alpha) = k[\alpha]$.

Proof. By (3.14.43), Definition (3.14.16) and (3.4.54) there is a canonical isomorphism $k[X]/(m_\alpha) \to k[\alpha]$ of k-algebras induced by the evaluation homomorphism $\mathrm{ev}_\alpha : k[X] \to K$. (3.14.47) shows that the image of this isomorphism, $k[\alpha]$, is a field, whence $k[\alpha] = k(\alpha)$ by (3.14.20). Since a k-algebra isomorphism is a-fortiori a k-vector space isomorphism it maps a basis to a basis. The result follows from (3.14.47) as the basis thus defined is the image of the basis in the proposition under the specified isomorphism. □

Definition 3.14.50 (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 3.14.51 (Finitely generated by algebraic $\implies$ finite and algebraic)
Let $K = k(\alpha_1, \dots, \alpha_n)/k$ be a field extension such that α_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 (3.14.49) K_i/K_{i-1} is finite. Therefore by (3.14.12) K/k is finite. By (3.14.25) it's also algebraic. For the second statement we may proceed inductively. Note we have

$$k[\alpha_1, \dots, \alpha_{i+1}] \overset{(3.14.17)}{=} k[\alpha_1, \dots, \alpha_i][\alpha_{i+1}] = k(\alpha_1, \dots, \alpha_i)[\alpha_{i+1}] \overset{(3.14.49)}{=} k(\alpha_1, \dots, \alpha_i)(\alpha_{i+1}) \overset{(3.14.19)}{=} k(\alpha_1, \dots, \alpha_{i+1})$$

The second equality is simply the inductive hypothesis. □

Corollary 3.14.52
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 3.14.53 (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*
- *α is algebraic over E_0*
- *$m_{\alpha,E} = m_{\alpha,E_0}$*

Therefore α is algebraic over k iff it is algebraic over E 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 (3.14.51) E_0/k is finite. Clearly α is algebraic over E_0 as it is a root of $m_{\alpha,E}$. By (3.14.43) $m_{\alpha,E_0} \mid m_{\alpha,E}$ as elements of $E_0[X]$ and $m_{\alpha,E} \mid m_{\alpha,E_0}$. Therefore $m_{\alpha,E_0} = m_{\alpha,E}$.

By (3.14.49) $E_0(\alpha)/E$ is finite, therefore $E_0(\alpha)/k$ is finite. By (3.14.25) $E_0(\alpha)/k$ is algebraic, whence α is algebraic over k. The last statement follows from (3.14.43) again. □

Corollary 3.14.54
K/E and E/k are both algebraic if and only if K/k is.

Proof. One direction is (3.14.44). The converse follows from the previous result. □

We may prove the first lifting theorem

Proposition 3.14.55 (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 $\deg(m_\alpha) \overset{(3.14.49)}{=} [k(\alpha) : k]$ such extensions.

Proof. Observe $m_{\alpha,k}(\sigma(\alpha)) \overset{(3.14.15)}{=} \sigma(m_{\alpha,k}(\alpha)) = 0$. Therefore the mapping is well-defined. By (3.14.22) it is injective. We claim it is also surjective. By (3.14.49) 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 β as a root. So this follows from uniqueness of the minimal polynomial in (3.14.43). The final statement follows from (3.14.42) □

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 3.14.56 (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 σ such that $\sigma(\alpha) = \beta$.

Proof. If K/k is finite then we may proceed by induction on $[K : k]$, using (3.14.55) 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', σ'). 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 (3.14.37) $m_{\alpha,K'}(X)$ splits in L (because $m_{\alpha,k}(X)$ does). Therefore by (3.14.55) 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 $\sigma(\alpha) = \beta$. By (3.14.55) the poset is non-empty, and the same argument works. □

3.14.5 Galois Theory Summary

Definition 3.14.57 (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 (3.14.42)).*

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 $\operatorname{char}(k) = 0$ or k is finite.

d) When K/k is finite and Galois then we have an order-reversing bijection between subfields and subgroups

$$\begin{array}{rcl} \{H \leq \operatorname{Gal}(K/k)\} & \longleftrightarrow & \{F \subseteq K\} \\ H & \longrightarrow & K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \operatorname{Gal}(K/F) & \longleftarrow & F \end{array}$$

3.14.6 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 3.14.58 (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 (3.14.51) K/k is necessarily algebraic, and if S is finite then so is K/k.

Definition 3.14.59 (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 3.14.60 (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 3.14.61
Let $\sigma : K/k \to L/k$ be a morphism and $f(X) \in k[X]$ a polynomial. Then

- *σ 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 3.14.62 (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 σ satisfies

$$\sigma(K) = k(\bigcup_{f \in S} T_{f,L})$$

Proof. Clearly by (3.14.61) S splits completely in L.

By the same result σ 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 (3.14.21). □

Proposition 3.14.63 (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 σ such that $\sigma(\alpha) = \beta$.

Furthermore any two splitting fields are isomorphic.

Proof. By assumption K is generated by the roots α_{ij} of $f_i \in S$. For each α_{ij} we therefore have $m_{\alpha_{ij},k}(X) \mid f_i(X)$ and $m_{\alpha_{ij},k}(X)$ splits completely in L by (3.14.37). Therefore the morphism $\sigma : K/k \to L/k$ exists by (3.14.56).

Note by (3.14.62) 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 (3.14.60) and therefore σ is an isomorphism as required. □

Proposition 3.14.64 (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 3.14.65 (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.*

Proposition 3.14.66 (Existence of Algebraic Closure)
Given a field k there exists an algebraic closure $\bar{k}/k$

Proposition 3.14.67 (Algebraic extensions embed into Algebraic Closure)
Let K/k be an algebraic extension and M/k be field containing $\bar{k}$ then there exists a morphism $\sigma : K/k \to M/k$.

Proof. A straightforward application of (3.14.56) since every $m_{\alpha,k}(X)$ splits in M. □

Corollary 3.14.68 (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 3.14.69 (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 (3.14.47). □

Remark 3.14.70
Note if K/k is an algebraic extension then (3.14.67) 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

$$K = k_n/\ldots/k_0 = k$$

we will assume the existence of compatible embeddings $i_{k_i} : k_i \to \bar{k}$ such that $i_{k_{i+1}} \circ i_{k_i,k_{i+1}} = i_{k_i}$.

3.14.7 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 3.14.71
Let $L/K/k$ be a tower of algebraic extensions and $\alpha \in L$. If $m_{\alpha,k}(X)$ splits completely in L so does $m_{\alpha,K}(X)$. In particular

$$L/k \text{ normal} \implies L/K \text{ normal}$$

Proof. Note $m_{\alpha,K}(X) \mid m_{\alpha,k}^{i_{kK}}(X)$ as elements of $K[X]$ by (3.14.43). Apply i_{KL} and then we may use (3.14.37). □

Proposition 3.14.72 (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 (3.14.56) with $K = L$. □

Proposition 3.14.73 (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

NOR1 *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. Clearly 3 $\implies$ 2, for K is the splitting field of all the minimal polynomials of elements in K.

2 $\implies$ 1. This is (3.14.62).

1 $\implies$ 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 (3.14.72) there is $\sigma_j \in \mathrm{Aut}(L/k)$ such that $\sigma_j(\alpha_1) = \alpha_j$. By hypothesis we have $\alpha_j \in (\sigma_j \circ i_{KL})(K) = i_{KL}(K)$ whence there exists $\alpha_j' \in K$ such that $i_{KL}(\alpha_j') = \alpha_j$. By (3.14.61) $m_{\alpha,k}(X)$ splits completely in K. Therefore K/k is normal as required. □

Corollary 3.14.74 (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 (3.14.63) there is a morphism $\sigma : K/k \to L/k$ with $\sigma(\alpha) = \beta$. By (3.14.62) we have $i_{KL}(K) = \sigma(K)$ whence $\beta \in i_{KL}(K)$. As β was an arbitrary root of $m_{\alpha,k}(X)$ we see it splits completely in $i_{KL}(K)$. Finally by (3.14.61) $m_{\alpha,k}(X)$ splits completely in K. As α was arbitrary then K/k is normal. □

Proposition 3.14.75 (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

$$\begin{aligned} \mathrm{Mor}_k(i_{KL}, L) : \mathrm{Aut}(L/k) &\to \mathrm{Mor}_k(K, L) \\ \sigma &\to \sigma \circ i_{KL} \end{aligned}$$

When i_{KL} is inclusion then this is simply the restriction to K. The kernel is precisely $\mathrm{Aut}(L/K)$.

Proof. Given $\widetilde{\sigma} \in \mathrm{Mor}_k(K, L)$, apply (3.14.56) to construct a morphism $\sigma : (L/K, i_{KL}) \to (L/K, \widetilde{\sigma})$. The hypotheses apply because the minimal polynomial $m_{\alpha,K}(X)$ with respect to either extension divides the minimal polynomial $m_{\alpha,k}^{i_{kK}}(X)$ which by assumption splits completely in L. By (3.14.26) it is an automorphism. Furthermore

$$\sigma \circ i_{kL} = \sigma \circ i_{KL} \circ i_{kK} = \widetilde{\sigma} \circ i_{kK} = i_{kL}$$

whence $\sigma \in \mathrm{Aut}(L/k)$ as required. □

Corollary 3.14.76 (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 (3.14.75) this composition is surjective, whence the result follows. □

Corollary 3.14.77 (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.

$$\begin{array}{ccc} \mathrm{Aut}(L/k)/\mathrm{Aut}(L/K) & \longrightarrow & \mathrm{Aut}(K/k) \\ \sigma & \to & i_{KL}^{-1} \circ \sigma \circ i_{KL} \end{array}$$

Proof. The given map is well-defined by (3.14.73) since $(\sigma \circ i_{KL})(K) = i_{KL}(K)$, and σ 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 (3.14.75) 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 3.14.78 (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 3.14.79 (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 (3.14.74) L/k is normal and by (3.14.56) 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 (3.14.60). 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 (3.14.74). By assumption $L' = L$ and therefore L/k is the splitting field for S'. Uniqueness follows from the uniqueness of splitting fields (3.14.63). □

3.14.8 Separability (Algebraic Case)

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 3.14.80 (Separable element)
*We say $\alpha \in K/k$ is **separable** over k if $m_{\alpha,k}(X)$ is a separable polynomial. Otherwise α is **inseparable**.*

*We say K/k is **separable** if every $\alpha \in K$ is **separable**.*

Lemma 3.14.81
$\alpha \in K/k$ is separable if and only if it is a root of a separable polynomial in $k[X]$.

In particular α separable over k implies it is separable over any subfield $i_{kK} \subset E \subset K$.

Proof. One direction is obvious. Conversely suppose $f(\alpha) = 0$ with f separable. Then $m_{\alpha,k} \mid f$ so the result follows from (3.14.41). □

Proposition 3.14.82 (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 3.14.83 (Separability degree of simple extension)
If $k(\alpha)/k$ is a simple extension and L/k normal overfield then

$$[k(\alpha) : k]_s = \#\{ \text{ roots of } m_\alpha \text{ in } L\} \leq \deg(m_\alpha) = [k(\alpha) : k]$$

Furthermore equality holds iff α is separable over k.

Proof. The first equality follows from (3.14.55), the final equality from (3.14.49). The inequality follows from (3.14.36). The final statement follows from (3.14.42). □

The main results of this section are the following

Proposition 3.14.84 (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 (3.14.76). 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 σ, 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 (3.14.83) we have

$$[K_i : K_{i-1}]_s \leq [K_i : K_{i-1}]$$

with equality iff α_i separable over K_{i-1}. By multiplicativity the inequality follows.

If K/k is separable then by (3.14.81) α_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 α_i is separable over K_{i-1}. Since the choice of α_1 was arbitrary we see that K/k is separable. □

Proposition 3.14.85 (Towers of separable extensions)
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 (3.14.81).

Conversely the finite case follows from (3.14.84) by multiplicativity. For the general case, consider $\alpha \in K$. Then (3.14.53) shows the existence of a finite subextension E_0/k of E such that $m_{\alpha,E} = m_{\alpha,E_0}$. Therefore α is separable over E_0. By (3.14.83) 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 (3.14.84) $[E_0 : k]_s = [E_0 : k]$. 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 α is separable over k as required.

□

Proposition 3.14.86
An algebraic extension $K = k(\alpha_1, \ldots, \alpha_n)/k$ is separable iff α_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 (3.14.81) α_i is separable over K_{i-1}. Therefore $[K_i : K_{i-1}]_s = [K_i : K_{i-1}]$ by (3.14.83) and $[K : k]_s = [K : k]$ by multiplicativity. (3.14.84) shows that K/k is separable. □

Proposition 3.14.87 (Equivalent definition of separability)
An algebraic extension K/k. TFAE

a) *K/k is separable*

b) *E/k is separable for every finite subextension*

c) *$[E : k]_s = [E : k]$ for every finite subextension*

Proof. *a)* $\implies$ *b)* is trivial and *b)* $\iff$ *c)* follows from (3.14.84). We need only show *b)* $\implies$ *a)*.

Consider $\alpha \in K$. Then by (3.14.53) there exists a finite subextension E/k such that α is algebraic over E. Therefore $E(\alpha)/k$ is finite, and by assumption $E(\alpha)/k$ separable as required. □

3.14.9 Purely Inseparable Extensions and Separable Closure

In what follows we let p be the characteristic exponent of k. In other words when $\mathrm{char}(k) = 0$ then $p = 1$ and the statements are trivial.

Definition 3.14.88
*An element $x \in K/k$ is **purely inseparable** (or p-radical) if there exists an integer $n \geq 0$ such that $x^{p^n} \in k$. The **height** of x is the least such integer.*

Lemma 3.14.89
Let $a \in k$. For every integer $e \geq 0$ the polynomial $f(X) := X^{p^e} - a$ has at most one root in any extension field K/k.

Proof. Suppose that b is a root, then by (3.14.6) we have $f(X) = (X - b)^{p^e}$. Then evidently b is the unique root. □

Lemma 3.14.90
Let $a \in k \setminus k^p$. Then for every integer $e \geq 0$ the polynomial $X^{p^e} - a$ is irreducible in $k[X]$.

Proof. Let K/k be a splitting field for $f(X) = X^{p^e} - a$, $b \in K$ a root and $g(X)$ be the minimal polynomial of b. By (3.14.6) $f(X) = (X - b)^{p^e}$ in $K[X]$. Suppose π is a monic irreducible factor of f in $k[X]$ then by unique factorisation in $K[X]$ we have $\pi(X) = (X - b)^r$ for some r. In particular π has b as a root and therefore is divisible by g. By irreducibility we conclude every irreducible factor is equal to g and the irreducible factorization of f is g^s. Furthermore $p^e = rs$. Consequently both r and s are pth powers, and we have

$$\begin{aligned} \pi &= (X - b)^{p^d} \\ f &= \pi^{p^{e-d}} \end{aligned}$$

for some $0 \leq d \leq e$. In particular $b^{p^d} \in k$ and $a = b^{p^{e-d}}$. By assumption a is not a p-th power and so we must have $d = e$, and $f = \pi$ is irreducible. □

Proposition 3.14.91
Let $x \in K/k$ be purely inseparable of height e. Then the minimal polynomial of x is $X^{p^e} - x^{p^e}$. Furthermore

$$[k(x) : k] = p^e$$

$$[k(x) : k]_s = 1$$

More precisely for every field L/k there is at most one morphism $k(x)/k \to L/k$.

Proof. By definition $x^{p^e} \in k$ is not a p-th power. Therefore the result follows from (3.14.90). The first relation follows from (3.14.49) and the second from (3.14.83). □

Proposition 3.14.92
Suppose $x \in K/k$ is both separable and purely inseparable. Then $x \in k$.

Proof. The minimal polynomial is $X^{p^e} - x^{p^e} = (X - x)^{p^e}$. Therefore by (3.14.42) $e = 0$ which means precisely $x \in k$. □

Proposition 3.14.93 (Relative Separable Closure)
Let K/k be an algebraic extension. The subset $K_s \subset K$ of separable elements form a subfield. Furthermore K/K_s is purely inseparable and the restriction map

$$\mathrm{Mor}_k(K, L) \to \mathrm{Mor}_k(K_s, L)$$

is bijective. In particular when K_s/k is finite then we have the relation

$$[K_s : k] = [K_s : k]_s = [K : k]_s$$

Proof. Suppose $\alpha, \beta \in K$ are separable then the field $k(\alpha, \beta)$ is separable by (3.14.86). As this contains $\alpha \pm \beta$ and $\alpha\beta$ then K_s is a subfield which is by definition separable. Then by (3.14.84) we have $[K_s : k] = [K_s : k]_s$ when this is finite.

For $x \in K$ let $f(X)$ be the minimal polynomial over k. There exists some integer $m \geq 0$ such that $f(X) \in k[X^{p^m}]$ but not in $k[X^{p^{m+1}}]$. In other words $f(X) = g(X^{p^m})$ and $g(X) \notin k[X^p]$. As f is irreducible so is g, and is therefore the minimal polynomial of x^{p^m}. By (3.14.95) g is separable and therefore $x^{p^m} \in K_s$. This shows that K/K_s is purely inseparable.

Let $L/K/k$ be tower such that L/k is normal. For every $x \in K$ consider the mapping

$$\mathrm{Mor}_k(K, L) \to \mathrm{Mor}_k(K_s, L)$$

obtained by restriction. By (3.14.76) it is surjective. Consider $\psi : K_s \to L$ and $\widehat{\psi} : K \to L$ an extension. For every $x \in K$ we have $\widehat{\psi}|_{K_s(x)} = i_{K_s(x)L}$ by (3.14.91). This shows that $\widehat{\psi}$ is unique and the mapping is bijective. □

This relied on the following results

Lemma 3.14.94 (Inseparable polynomials)
Let $f \in k[X]$ be a non-constant polynomial and p the characteristic exponent of k. Then $f' = 0 \iff p > 1$ and $f \in k[X^p]$.

Proposition 3.14.95 (Separable Irreducible Polynomials)
Let $f \in k[X]$ be an irreducible polynomial and p the characteristic exponent of k. Then the following are equivalent

a) *f is separable (i.e. f and f' are co-maximal)*

b) *$f' \neq 0$*

c) *$p = 1$ or $f \notin k[X^p]$*

Proof. Note by assumption f is not a unit and therefore not constant.
a) $\implies$ *b)* Suppose $f' = 0$ then $(f, f') = (f) \neq k[X]$ and therefore f is not separable.

b) $\implies$ *a)* Suppose f is not separable. By (...) (f) is maximal and so we must have $f' \in (f)$. As $\deg(f') < \deg(f)$ this implies $f' = 0$.

b) $\iff$ *c)* This is just the contrapositive of (3.14.94) □

3.14.10 Perfect Fields

Recall a perfect field k satisfies $k^p = k$ where p is the characteristic exponent. We show that in this case there are no inseparable algebraic extensions. First we show that all finite fields are perfect.

Proposition 3.14.96 (Finite fields are perfect)
Any finite field is perfect.

Proof. The Frobenius homomorphism is injective and therefore surjective by counting. □

Proposition 3.14.97 (Perfect field criteria)
Let k be a field with characteristic exponent p. Then the following are equivalent

a) *Every irreducible polynomial in $k[X]$ is separable*

b) *Every algebraic extension K/k is separable*

c) *$\bar{k}/k$ is separable*

d) *$k^p = k$*

Proof. We prove each in turn
$a) \implies b)$ Minimal polynomials are irreducible by (3.14.43) and therefore are separable by hypothesis.

$b) \iff c)$ One direction is automatic as $\bar{k}$ is algebraic. On the other hand every algebraic extension is isomorphic to a subfield of $\bar{k}$, so the implication follows from (3.14.85).

$b) \implies d)$ We need only show $k^p = k$ in the case $p > 1$. If there exists $a \in k \setminus k^p$ then by (3.14.90) the polynomial $f(X) := X^p - a$ is irreducible. Then it's clear that the field extension $K := k[X]/(X^p - a)$ is not separable. For the minimal polynomial of $\overline{X}$ is f which by (3.14.95) is not separable. This contradicts the assumption that K/k is separable.

$d) \implies a)$ Suppose that f is irreducible but not separable. Then by (3.14.95) $\mathrm{char}(k) = p > 1$ and $f \in k[X^p]$. By assumption all the coefficients are p-th powers and therefore $f = h^p$ by (3.14.6) for some $h \in k[X]$. This contradicts irreducibility of f, and so f must be separable.

□

3.14.11 Applications of Separability

Definition 3.14.98 (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 3.14.99 (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 (3.14.87) 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 (2.3.15)).

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. □

3.14.12 Normal Extensions II

We provide some more straightforward criteria based on $[K : k]_s$

Proposition 3.14.100 (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 NOR1 $\sigma(K) = i_{KL}(K)$ 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 (3.14.98) 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 3.14.101 (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 (3.14.98)

$$\#\mathrm{Aut}(K/k) \leq [K:k]_s \leq [K:k] < \infty$$

with equality if and only if K/k is both normal (3.14.100) and separable (3.14.84) □

3.14.13 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 3.14.102 (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 ((3.14.36)) 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 (3.14.36). Therefore the fact $K^\star$ is cyclic follows from (3.3.24). □

Proposition 3.14.103 (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 (3.14.26). □

Further we can show existence and uniqueness of finite fields.

Proposition 3.14.104 (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 (3.14.42) $f(X)$ 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 **??** 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 3.14.105
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 ((3.14.36)) so we must have $d \geq n$, and therefore $d = n$. Clearly ϕ generates a cyclic subgroup of order n. However by (3.14.101) 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 3.14.106 (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 ϕ^m has order n/m. Furthermore from (3.14.104) every element of $\mathbb{F}_{p^m}$ satisfies $X^{p^m} - X$. In other words ϕ^m fixes $\mathbb{F}_{p^m}$ and $\phi^m \in H$. Therefore $\langle \phi^m \rangle \leq H$ and $\#H \geq n/m$. By (3.14.101) $\#H \leq [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$, 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 3.14.107 (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 ϕ is the Frobenius automorphism.

Proof. Recall by Definition (3.14.50) 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 (3.14.105) $G = \langle \phi \rangle$ 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 α generates K we see $\phi^d = e$ (by (3.14.22)), and by (3.3.14) we have $\deg(\alpha) = m = o(\phi) \mid d$. □

3.14.14 Galois Theory

We've seen that for K/k a finite extension

$$\#\operatorname{Aut}(K/k) \leq [K:k]_s \leq [K:k]$$

with equality if and only if K/k is Galois, by (3.14.101).

Remark 3.14.108
If k is perfect then $\bar{k}/k$ is Galois.

The main result of Galois Theory is

Proposition 3.14.109
Let K/k be a finite Galois extension then there is an order-reversiing bijection between subgroups and subfields

$$\begin{aligned} \{H \leq \operatorname{Gal}(K/k)\} &\longleftrightarrow \{F \subseteq K\} \\ H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \operatorname{Gal}(K/F) &\longleftarrow F \end{aligned}$$

Proof. This is proved in a series of Propositions in the rest of this section. Firstly we show it is well-defined in (3.14.110). The maps are mutual inverses by (3.14.111) and (3.14.112). □

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 3.14.110
If K/k is Galois and $F \subset K$ then K/F is Galois.

Proof. This follows from (3.14.71) and (3.14.85). □

Proposition 3.14.111 (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 α is separable it must have another root $\beta \in K$. By (3.14.72) there is an element $\sigma \in \operatorname{Gal}(K/F)$ such that $\sigma(\alpha) = \beta$. In other words $\alpha \notin K^{\mathrm{Gal}(K/F)}$, which shows the reverse inclusion. □

Proposition 3.14.112
Let K/k be a field extension and $H \subseteq \operatorname{Aut}(K/k)$ a finite subgroup then K/K^H is finite Galois with

$$H = \operatorname{Gal}(K/K^H)$$

and order equal to $[K:K^H]$. When K/k is finite then H is automatically finite.

Proof. Firstly observe that trivially $H \subseteq \operatorname{Aut}(K/K^H)$. If we know that $[K:K^H] < \infty$, then by (3.14.101) we have

$$\#H \leq \#\operatorname{Aut}(K/K^H) \leq [K:K^H]_s \leq [K:K^H]$$

We can prove equality everywhere if we show that $[K:K^H] \leq \#H$, which is shown either by (3.14.113) or (3.14.114). Note equality also shows that K/K^H is finite Galois by the same result.

Finally when K/k is finite, then $\#\operatorname{Aut}(K/k) < \infty$. 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 3.14.113 (Bound degree of fixed field I)
Let K/k be a field extension and $H \subset \operatorname{Aut}(K/k)$ 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 (3.4.133).

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 α_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 τ to obtain

$$\sum_j \tau(v_j)(\tau \circ \sigma)(\alpha_j) = 0 \quad \forall \sigma \in H$$

and since multiplication by τ 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 λv 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 τ was arbitrary we see $0 \neq \lambda v \in S(K^H)$ as required.

□

Lemma 3.14.114 (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 α as a root and is separable by (3.14.42). Furthermore $f^\tau = f$ because τ 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 α has degree at most $\#H$ and is separable by (3.14.41).

If K/k is finite, then a-fortiori K/K^H is finite, so we may apply the Primitive Element (3.14.99) 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 α 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 (3.14.99), contradicting maximality. Finally the degree of $[K : K^H]$ is the degree of α, which we've seen is bounded above by $\#H$. □

Now we may demonstrate straightforward criteria for subfield to be normal

Proposition 3.14.115
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 (3.14.73) 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 (3.14.109) $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/F') \iff F = F'$. 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 (3.14.77). □

3.14.15 Transcendental Field Extensions

Definition 3.14.116 (Algebraic Independence)
*Let K/k be a field extension and $S \subset K$. We say S is **algebraically independent** over k if for every finite subset of distinct elements $x_1, \dots, x_n \in \mathcal{S}$ we have*

$$f(x_1, \dots, x_n) = 0 \implies f = 0$$

for all $f \in k[X_1, \dots, X_n]$.

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 Γ is **algebraically spanning** if $c(\Gamma) = K$, equivalently if $K/k(\Gamma)$ is algebraic.*

*We say that $\mathcal{B}$ is a **transcendence base** if it is both algebraically independent and spanning (i.e. $K/k(\mathcal{B})$ 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 2.3 to show that that transcendence bases exist and they satisfy certain properties.

Proposition 3.14.117
Let K/k be a field extension and $S, T \subset K$. Then the following are equivalent

a) *$S \cup T$ is algebraically independent and $S \cap T = \emptyset$*

b) *S is algebraically independent over k and T is algebraically independent over $k(S)$*

c) *T is algebraically independent over k and S is algebraically independent over $k(T)$*

Proof. By symmetry it's enough to show that $a) \iff b)$. □

Corollary 3.14.118 (Exchange Property)
Let K/k be a field extension, $\Gamma \subseteq K$. Suppose x is algebraic over $k(\Gamma \cup \{y\})$ and transcendental over $k(\Gamma)$, then y is algebraic over $k(\Gamma \cup \{x\})$.

Proof. By considering the extension $K/k(\Gamma)$ we may reduce to the case $\Gamma = \emptyset$.

It's enough to show that x transcendental over k and y transcendental over $k(x)$ implies x transcendental over $k(y)$. This follows directly from (3.14.117) by considering $S = \{x\}$ and $T = \{y\}$. □

Corollary 3.14.119 (Extension Property)
Let K/k be a field extension, $S \subseteq K$ algebraically independent and $x \in K$ transcendental over $k(S)$. Then $S \cup \{x\}$ is algebraically independent.

Proof. Follows immediately from (3.14.117). □

Corollary 3.14.120 (Equivalent form of independence)
Let K/k be a field extension and $S \subset K$. Then the following are equivalent

a) *S is algebraically independent*

b) *x is transcendental over $k(S \setminus \{x\})$ for all $x \in S$*

In other words the algebraically independent subsets are precisely the matroid independent subsets.

Proof. $a) \implies b)$ Follows from (3.14.117).

$b) \implies a)$ Let $\mathcal{F}$ be the family of algebraically independent subsets. We've shown that all such sets are also matroid independent, and by definition the family is of finite character. Furthermore by (3.14.119) it satisfies the extension property. Therefore by (2.3.6) it is precisely the family of matroid independent sets. □

Proposition 3.14.121 (Transcendence Base Exists)
Let K/k be a field extension. Suppose S is an algebraic independent subset of K and $\Gamma \supset S$ is such that $K/k(\Gamma)$ is algebraic. Then there exists a transcendence base $\mathcal{B}$ such that $S \subseteq \mathcal{B} \subseteq \Gamma$.

Proof. This is (2.3.7). □

Proposition 3.14.122 (Transcendence Base)
Let K/k be a field extension and $S \subset K$ a subset. Then the following are equivalent

a) *S is a **transcendence base***

b) *S is a maximal algebraically independent set*

c) *S is minimal under the condition $K/k(S)$ is algebraic*

*When K/k admits a finite algebraic spanning set then all bases are finite of the same size (**transcendence degree**). Write this as* $\operatorname{trdeg}(K/k)$ *or* $\operatorname{trdeg}_k(K)$.

Proof. Follows from (2.3.8) and (2.3.11). □

Proposition 3.14.123
Let K/k be a field extension of finite transcendence degree and $S \subset K$ a subset. Then

- *S algebraically independent* $\implies |S| \leq \operatorname{trdeg}(K/k)$
- *$K/k(S)$ is algebraic* $\implies |S| \geq \operatorname{trdeg}(K/k)$

Proof. Follows directly from (2.3.12). □

Proposition 3.14.124
Let K/k be a field extension of finite transcendence degree and $S \subset K$ a subset. Then the following are equivalent

- *S is a transcendence base*
- *S is algebraically independent and* $|S| \geq \operatorname{trdeg}(K/k)$
- *$K/k(S)$ is algebraic and* $|S| \leq \operatorname{trdeg}(K/k)$

In this case $|S| = \operatorname{trdeg}(K/k)$.

Proof. Follows directly from (2.3.13). □

In case K/k is finitely generated then we guarantee that $K/k(S)$ is finite.

Proposition 3.14.125
Let K/k be a finitely generated field extension. Then

- $\operatorname{trdeg}(K/k) < \infty$
- *Suppose $K/k(\Gamma)$ is algebraic then it is in fact finite.*

Proof. *a*) If K/k is finitely generated then the set of generators is algebraically spanning and so $\operatorname{trdeg}(K/k) < \infty$ by (3.14.122)

b) A-fortiori $K/k(\Gamma)$ is finitely generated and by assumption algebraic so by (...) it is finite □

3.14.16 Separating Transcendence Base

In applications the existence of a separating transcendence base is important, and is guaranteed when k is perfect.

Definition 3.14.126 (Separating Transcendence Base)
*A field extension K/k is **separably generated** if there exists a transcendence base S such that $K/k(S)$ is separable (and algebraic). We call such an S a **separating transcendence base**.*

Note when $\operatorname{char}(k) = 0$ *then every transcendence base is separating.*

Lemma 3.14.127
Let $n > 0$ and $K = k(x_1, \ldots, x_{n+1})$ then the following are equivalent

a) *$\{x_1, \ldots, \widehat{x_i}, \ldots, x_{n+1}\}$ is a transcendence base for K/k for* some *$i \in \{1, \ldots, n+1\}$*

b) $\operatorname{trdeg}(K/k) = n$

Proof. *a*) $\implies$ *b*) is clear. The converse follows from (3.14.121). □

Lemma 3.14.128
Let $n > 0$ a positive integer and $K = k(x_1, \ldots, x_{n+1})$ an extension of k such that

- *$\{x_1, \ldots, \widehat{x}_j, \ldots, x_{n+1}\}$ is a transcendence base for K/k for some $j \in \{1, \ldots, n+1\}$*
- $\operatorname{char}(k) > 0$

- $k^p = k$ *where* p *is the characteristic exponent of* k

Then there is $i \in \{1, \dots, n+1\}$ *such that* $\{x_1, \dots, \widehat{x_i}, \dots, x_{n+1}\}$ *is a* ***separating transcendence base*** *for* K/k

Proof. By assumption x_j is algebraic over $k(x_1, \dots, \widehat{x_j}, \dots, x_{n+1})$, and therefore there exists a non-zero F such that $F(x_1, \dots, x_{n+1}) = 0$. Let F be such a polynomial of minimal total degree (total degree = the maximum degree of a monomial with non-zero coefficient appearing in F). We claim it is irreducible. For suppose not, then one of the irreducible factors must vanish at $(x_1, \dots, x_{n+1})$, and this factor would have smaller total degree.

Suppose all the powers of X_i appearing in F are multiples of p, then we conclude that, since $k^p = k$, F is a p-th power which contradicts irreducibility. Choose X_i for which this is not the case and define

$$F_i(T) := F(x_1, \dots, x_{i-1}, T, x_i, \dots, x_{n+1}) \in k[S_i][T]$$

where $S_i := \{x_1, \dots, \widehat{x_i}, \dots, x_{n+1}\}$. By assumption $F_i(T)$ is non-zero and clearly $F_i(x_i) = 0$ so that x_i, and therefore by (3.14.51) K is algebraic over $k(S_i)$. By (3.14.124) S_i is a transcendence base for K and in particular algebraically independent. Therefore $k[S_i][T]$ may be identified with $k[X_1, \dots, X_{n+1}]$ and we may conclude that F_i is irreducible. Further by (3.11.33) $F_i(T)$ is irreducible as a polynomial with coefficients in $k(x_1, \dots, \widehat{x_i}, \dots, x_n)$. By assumption $F_i(T) \notin k(S_i)[T^p]$ so by (3.14.95) F_i is separable. Therefore x_i is separable over $k(S_i)$, and $K/k(S_i)$ is separable by (3.14.86) as required. □

Proposition 3.14.129
Let K/k *be a finitely-generated field extension such that* k *is perfect. Then* K/k *is separably generated.*

More precisely every generating set contains a separating transcendence base.

Proof. When $\mathrm{char}(k) = 0$ the generating set contains a transcendence base by (3.14.122). Every subfield of K also has characteristic 0, so then we are done by (3.14.97). So we may only consider the positive characteristic case, $p > 1$.

Suppose $K = k(x_1, \dots, x_n)$ and $d = \mathrm{trdeg}(K/k)$. We may immediately dispense with the case $d = 0$ as then K/k is algebraic and result follows from (3.14.97). The case $n = 1$ is also clear as K must be purely transcendental or algebraic.

We proceed by induction on the number of generators for fixed $d > 0$, the case $n = 1$ having already been demonstrated. For $n > 1$, if $n = d$ then any transcendence base will do, so consider the case $d < n$. Renumber such that x_n is algebraic over $K' := k(x_1, \dots, x_{n-1})$ (with transcendence degree d). By induction $\{x_1, \dots, x_{n-1}\}$ contains a separating transcendence base for K'. Renumber such that it is $\{x_{n-d}, \dots, x_{n-1}\}$. By assumption $\mathcal{T} := \{x_1, \dots, x_{n-d-1}\}$ (possibly empty in case K' is purely transcendental) are separable algebraic over $k(x_{n-d} \dots, x_{n-1})$. Further by (3.14.53) we may conclude x_n is algebraic over $k(x_{n-d} \dots, x_{n-1})$. By the previous Lemma (3.14.128) there is j such that $S_j := \{x_{n-d}, \dots, \widehat{x_j}, \dots, x_n\}$ is a separating transcendence base for $k(x_{n-d}, \dots, x_n) = k(S_j \cup \{x_j\})$.

It remains to show that $K/k(S_j)$ is separable algebraic. Trivially (3.14.44) (3.14.81) the elements of $\mathcal{T}$ are separable algebraic over $k(S_j \cup \{x_j\})$. Therefore by (3.14.51) (3.14.86) $K = k(S_j \cup \{x_j\})(\mathcal{T})$ is separable algebraic over $k(S_j \cup \{x_j\})$. Considering the tower $K/k(S_j \cup \{x_j\})/k(S_j)$ we may then appeal to (3.14.54) and (3.14.85). □

Remark 3.14.130
This is adapted from [Mor12, Theorem 20.18] and [Sta15, 030W].

3.15 Local Rings

Local rings arise quite naturally when localizing at a prime ideal (see (3.6.32) and Example 3.15.4) so we recall some basic properties here.

Definition 3.15.1 (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 3.15.2 (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 3.15.3 (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 (3.4.13). Conversely given $x \in A \setminus A^\star$ then (x) is a proper ideal by (3.4.32), and therefore contained in a maximal ideal (3.4.15) 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 3.15.4
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 3.15.5 (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. □

3.16 Modules over Local Rings (Nakayama's Lemma)

The main result of this section ((3.16.7)) 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 (2.3.8). 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 3.16.1 (Jacobson Radical)
*Let A be a commutative ring. Define the **Jacobson Radical** to be the intersection of all maximal ideals*

$$\sqrt{0}^J := \bigcap_{\mathfrak{m} \lhd A} \mathfrak{m}$$

Proposition 3.16.2
The Jacobson Radical $\sqrt{0}^J$ is a proper ideal

Example 3.16.3
When $(A, \mathfrak{m}_A)$ is a local ring then $\sqrt{0}^J = \mathfrak{m}_A$.

Lemma 3.16.4 (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) $\mathfrak{a} \subseteq \sqrt{0}^J \iff 1 + \mathfrak{a} \subseteq A^\star$

c) $x \in \sqrt{0}^J \iff 1 + (x) \subseteq A^\star$

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) $\mathfrak{a} \subseteq \sqrt{0}^J \implies (1 + \mathfrak{a}) \cap \mathfrak{m} = \emptyset$ for all maximal ideals $\mathfrak{m}$. By (3.4.15) 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 (3.4.13). Again by a) $\mathfrak{a} \subseteq \mathfrak{m}$ as required.

c) This follows from b) and noting $x \in \sqrt{0}^J \iff (x) \subseteq \sqrt{0}^J$.

□

Proposition 3.16.5 (Nakayama's Lemma)
Let M be a finitely generated A-module and $\mathfrak{a} \triangleleft A$ 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 $\mathfrak{a} \subseteq \sqrt{0}^J$ (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 3.12.4 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 3.12.3 (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 **??** 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 (3.16.4) $(1 - a)$ is invertible, whence $m = 0$ as required.

c) Observe $\mathfrak{a}(M/N) \overset{(3.4.99)}{=} (N + \mathfrak{a}M)/N = M/N$ whence $M/N = 0$ by b). Therefore $N = M$ as required.

We may show b) more directly. Suppose $M \neq 0$, and let $\{m_1, \ldots, m_n\}$ be a non-zero generating set for M of minimal size. Then by Lemma 3.12.3

$$m_1 = \sum_j a_j m_j \quad a_j \in \mathfrak{a}$$

whence

$$(1 - a_1)m_1 = \sum_{j \geq 2} a_j m_j$$

As $a_1 \in \sqrt{0}^J$ we have $1 - a_1 \in A^\star$ by (3.16.4). Then $\{m_2, \ldots, m_n\}$ 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 3.16.4 $S^{-1}\mathfrak{a} \subseteq J(S^{-1}A)$. 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 (3.6.15) 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 (3.4.100) 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 3.16.6
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 (3.16.5).c) as required. □

Recall from (2.1.56) 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.

Proposition 3.16.7 (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 (3.4.100) $\widetilde{M}$ is a k-module, and it's clearly finite.

b) By the (3.16.6) S spans M. Suppose $S' \subset S$ spans M, then by the same result $\widetilde{S'}$ spans $\widetilde{M}$. Recall (2.3.8) 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 (3.16.6) $\widetilde{S}$ spans $\widetilde{M}$. Suppose $\widetilde{T} \subset \widetilde{S}$ also spans $\widetilde{M}$. By (3.16.6) 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 (2.3.8) 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.

□

3.17 Lying over, Incomparability, Going Up and Going Down

Definition 3.17.1 (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 ϕ is the identity then this is equivalent to saying $\mathfrak{p} = \mathfrak{q} \cap A$.*

Definition 3.17.2 (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 $\mathfrak{q} \lhd B$ 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 $\mathfrak{q}, \mathfrak{q}' \lhd B$ then $\mathfrak{q} \subsetneq \mathfrak{q}' \implies \phi^{-1}(\mathfrak{q}) \subsetneq \phi^{-1}(\mathfrak{q}')$*

d) ***going down property** if for every pair of prime ideals $\mathfrak{p}' \subsetneq \mathfrak{p}$ in A and $\mathfrak{q} \lhd B$ lieing over $\mathfrak{p}$, there exists a prime ideal $\mathfrak{q}'$ such that $\mathfrak{q}' \subsetneq \mathfrak{q}$ and $\mathfrak{q}'$ lies over $\mathfrak{p}'$.*

Remark 3.17.3
It's possible to interpret these geometrically in terms of the map $\phi_\star : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$.

- *Lying over - $\phi_\star$ is surjective onto $V(\ker(\phi))$*
- *Going up - $\phi_\star$ is closed*
- *Incomparability - fibres have dimension 0*
- *Going down (and finite presentation) - $\phi_\star$ is open*

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 3.17.5. 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 3.17.4 (Lieing over criteria)
Let $\phi : A \to B$ be a ring map, $\mathfrak{p} \lhd A$ prime and $\mathfrak{q} \lhd B$. 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 (3.4.49) 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 3.17.5 (Lieing over correspondence)
Let $\phi : A \to B$ be a ring map and $\mathfrak{p} \triangleleft A$ a prime ideal s.t. $\ker(\phi) \subseteq \mathfrak{p}$. 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 3.17.4 $\mathfrak{q}$ 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 (3.6.18) and the second from (3.4.53).

a) $\iff$ *b)* This follows from the correspondence, since a ring without any non-zero prime ideals is simply the zero-ring.

b) $\iff$ *c)* Follows by noting $\mathfrak{p} = \mathfrak{p}^{ec} \overset{3.17.4}{\iff} \mathfrak{p}^e \cap S = \emptyset \overset{3.6.17.e)}{\iff} \mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$ □

Remark 3.17.6
Geometrically this is an explicit representation of the fiber as a prime spectrum

$$\operatorname{Spec}(\phi)^{-1}(\mathfrak{p}) \longleftrightarrow \operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p})$$

3.18 Integral Ring Extensions

Definition 3.18.1 (Integral Element)
*Let $\phi : A \to B$ be a ring map and $\alpha \in B$. Then we say α is **algebraic** over A if if $m(\alpha) = 0$ for some polynomial $m(X) \in A[X]$.*

*Furthermore we say that α is **integral** over A if $m(X)$ may be chosen to be monic.*

Note often we assume $A \subseteq B$ and ϕ is the identity.

Definition 3.18.2 (Ring Extensions)
Let $\phi : A \to B$ be a ring map (so that B is an A-algebra). Then we say ϕ 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 ϕ 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 3.18.3
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 3.12.4 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 3.18.4 (Finite $\iff$ finite-type and integral)
Let $\phi : A \to B$ be a ring map and $b_1, \ldots, b_n \in B$ integral over A. Then the ring homorphism $\phi : A \to \phi(A)[b_1, \ldots, b_n]$ is finite and integral.

In particular if ϕ 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 ϕ 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 (3.9.4)).

For any $b \in A[b_1, \ldots, b_n]$ we have $A[b] \subset A[b_1, \ldots, b_n]$ so by (3.18.3) 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 (3.18.3). □

Proposition 3.18.5 (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 ϕ integral and ψ integral (e.g. surjective) $\implies$ $\psi \circ \phi$ 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 (3.18.3) B' is a finite A-module and $B'[c]$ is a finite B'-module. Therefore $B'[c]$ is a finite A-module and by (3.18.3) we have c is integral over A. □

Definition 3.18.6 (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 3.18.7 (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 (3.18.4) the subring $A[\alpha, \beta]$ is a finite A-module containing $\alpha \pm \beta$ and $\alpha\beta$. Therefore by (3.18.3) they are also integral over A.

Clearly $\bar{A}$ is integral over A so by (3.18.5) it is integrally closed. □

Proposition 3.18.8 (Integral closure of an ideal)
Let $A \subset B$ be a subring and $\mathfrak{a} \lhd A$ an ideal. Then for $b \in B$ TFAE

a) *b integral over $\mathfrak{a}$*

b) *b^n integral over $\mathfrak{a}$ for some $n \geq 1$*

c) *$b \in \sqrt{\mathfrak{a}\bar{A}}$*

In particular $\bar{\mathfrak{a}}$ is an ideal of $\bar{A}$.

Furthermore if A is integrally closed in B then $\bar{\mathfrak{a}} = \sqrt{\mathfrak{a}}$.

Proof. It's clear that $a) \iff b)$. For $a) \implies c)$ consider the integral relation

$$b^n + a_{n-1}b^{n-1} + \dots a_0 = 0 \quad a_i \in \mathfrak{a}$$

By (3.18.7) $\bar{A}$ is a subring, and by assumption $b \in \bar{A}$. Therefore $b^k \in \bar{A}$, and the integral relation shows that $b^n \in \mathfrak{a}\bar{A}$ as required.

For $c) \implies b)$ suppose $b \in \sqrt{\mathfrak{a}\bar{A}}$ then $b^n = \sum_{i=1}^n a_i x_i$ for $a_i \in \mathfrak{a}$ and $x_i \in \bar{A}$. Let $B' := B[x_1, \dots, x_n]$, which is a finite A-submodule by (3.18.4). Let $\phi \in \mathrm{End}_A(M)$ denote multiplication by b^n then $\phi(M) \subseteq \mathfrak{a}M$ so by Theorem 3.12.4 ϕ satisfies a monic polynomial with coefficients in $\mathfrak{a}$. In particular b^n is integral over $\mathfrak{a}$. □

Proposition 3.18.9
A UFD is integrally closed.

In particular polynomial ring over a UFD is integrally closed.

Proof. □

The following criterion is also useful :

Lemma 3.18.10 (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

$$x = \phi(a_0) + \phi(a_1)x^{-1} + \dots + \phi(a_n)x^{-n}$$

Multiply by x^n to deduce an integral equation. Conversely suppose $x \in B$ is integral over A then by definition

$$x^n + \phi(a_{n-1})x^{n-1} + \dots + \phi(a_0) = 0$$

Multiply by $x^{-(n-1)}$ to deduce $x \in \phi(A)[x^{-1}]$ □

Proposition 3.18.11 (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 ϕ is injective, it induces an isomorphism between A and $\phi(A)$. So we may assume without loss of generality that $A \subseteq B$ and ϕ 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

$$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$$

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

$$-x(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1)a_0^{-1} = 1$$

and in particular x is invertible. □

Proposition 3.18.12
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 (3.4.53)) 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 3.18.13 (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 (3.4.53). By (3.18.12) 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 (3.4.56). Then we may apply (3.18.11) to show the equivalence. □

Proposition 3.18.14 (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 (3.6.6) there exists a morphism $\tilde{\phi}$, and by (3.18.12) 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 $B_{\mathfrak{p}} \neq 0$ (3.6.31). 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 (3.18.13) $\widetilde{\phi}^{-1}(\mathfrak{n})$ 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 (3.17.5) 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 (3.18.4) 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 (3.16.5) $B' = 0$, 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 (3.6.17) extending the ideals to $A_{\mathfrak{p}}$ shows $\tilde{\phi}^{-1}(\mathfrak{n}) = \mathfrak{m}$, and similarly for $\mathfrak{n}'$. By (3.18.13) both $\mathfrak{n}$, $\mathfrak{n}'$ are maximal so $\mathfrak{n} = \mathfrak{n}'$. By (3.6.18) $\mathfrak{q} = \mathfrak{q}'$.

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

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow & & \downarrow \\ A/\mathfrak{p} & \xleftarrow{\tilde{\phi}} & B/\mathfrak{q} \end{array}$$

   The induced map $\tilde{\phi}$ is integral (3.18.13). 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 (3.4.53). Then from the diagram we see $\phi^{-1}(\mathfrak{q}') = \mathfrak{p}'$ as required.

□

Proposition 3.18.15 (Coefficients of minimal polynomial)
Let $A \subseteq B$ be integral domains, A is integrally closed, and define $K = \mathrm{Frac}(A)$ and $L = \mathrm{Frac}(B)$. For $b \in B$ integral over $\mathfrak{a} \triangleleft A$ we have the non-leading coefficients of $m_b(X)$ are integral over $\mathfrak{a}$ and therefore lie in $\sqrt{\mathfrak{a}}$.

Note if b is only assumed to be integral over A then the coefficients of $m_b(X)$ lie in A.

Proof. Let M/K be a normal closure for L/K (...). By (3.18.8) the integral closure of $\mathfrak{a}$ in M is simply $\sqrt{\mathfrak{a}}$. Then the minimal polynomial $m_b(X)$ splits completely in M and by (3.14.72) all the roots b_i are conjugate by $\mathrm{Aut}(M/K)$. In particular it's clear that b_i are integral over $\mathfrak{a}$, and so lie in $\sqrt{\mathfrak{a}}$. The coefficients of $m_b(X)$ are polynomials in the b_i, and so by the observation above are also lie in $\sqrt{\mathfrak{a}}$ (and are integral over $\mathfrak{a}$).

The last statement follows by taking $\mathfrak{a} = A$. □

Proposition 3.18.16 (Going Down)
Let $A \subseteq B$ be integral ring extension such that A is an integrally closed domain and B is an integral domain. Then it has the Going Down property.

Proof. Let $\mathfrak{p} \subsetneq \mathfrak{p}'$ be prime ideals of A and $\mathfrak{q}'$ a prime ideal lieing over $\mathfrak{p}'$. We wish to find a prime ideal $\mathfrak{q} \subseteq \mathfrak{q}'$ lieing over $\mathfrak{p}$ (clearly inclusion must be strict).

Consider the inclusion of rings $A \subseteq B_{\mathfrak{q}'}$. Then by (3.17.5) $\mathfrak{p}$ lies under a prime of $B_{\mathfrak{q}'}$ if and only if $\mathfrak{p} = \mathfrak{p}^{ec} = \mathfrak{p}B_{\mathfrak{q}'} \cap A$. If this is the case then it is of the form $\mathfrak{q}B_{\mathfrak{q}'}$ for some prime ideal $\mathfrak{q} \subseteq \mathfrak{q}'$ (3.6.32) of B. It's clear that $\mathfrak{q}$ lies over $\mathfrak{p}$.

Note in general that $\mathfrak{p} \subseteq \mathfrak{p}^{ec}$, so we only need to demonstrate the reverse inclusion. Choose $x \in \mathfrak{p}B_{\mathfrak{q}'} \cap A$. By (3.6.17) $\mathfrak{p}B_{\mathfrak{q}'} = S^{-1}(\mathfrak{p}B)$ where $S = B \setminus \mathfrak{q}'$.

Then $x = \frac{y}{s}$ for $y \in \mathfrak{p}B$ and $s \in B \setminus \mathfrak{q}'$. By (3.18.8) we have y is integral over $\mathfrak{p}$ whence by (3.18.15) the minimal polynomial $m_{y,K}(X)$ is equal to

$$X^r + u_1 X^{r-1} + \ldots + u_r \quad u_i \in \mathfrak{p}$$

However $s = yx^{-1}$ and $x \in A \implies x^{-1} \in K$. So we can derive the minimal polynomial $m_{s,K}(X)$

$$X^r + v_1 X^{r-1} + \ldots + v_r \quad v_i := \frac{u_i}{x^i}$$

As s is assumed to be integral over A the coefficients must all lie in A, by (...). Consequently $v_i \in A$ and $v_i x^i \in \mathfrak{p}$ for all i. If $x \notin \mathfrak{p}$ then we have $v_i \in \mathfrak{p}$ for all i, and s is integral over $\mathfrak{p}$. By the minimal polynomial we see that $s \in B\mathfrak{p} \subseteq B\mathfrak{p}' \subseteq \mathfrak{q}'$, which contradicts the choice of s. Therefore $x \in \mathfrak{p}$ as required. □

3.19 Valuation Rings and Places

Definition 3.19.1 (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 3.19.2 (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 (3.15.3) 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 (3.18.10) $x \in A[x^{-1}] \subseteq A$ as required.

□

Definition 3.19.3 (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 3.19.4 (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 3.19.5
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 3.19.6 (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*

$$\begin{array}{ccc} A & \xrightarrow{\phi} & \Omega \\ \downarrow & \nearrow_{\tilde{\phi}} & \\ A_{\mathfrak{p}} & & \end{array}$$

Furthermore $\ker(\tilde{\phi}) = \mathfrak{p}A_{\mathfrak{p}}$ *and $\tilde{\phi}$ constitutes a* ***semi-place****.*

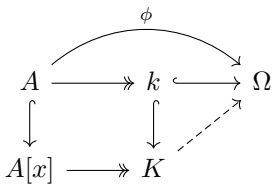
Proof. Clearly $\mathfrak{p}$ is prime because $\phi(A)$ is an integral domain. We may extend ϕ to the ring $A_{\mathfrak{p}}$ in the obvious way. The extension has kernel $\mathfrak{p}A_{\mathfrak{p}}$, the unique maximal ideal of $A_{\mathfrak{p}}$. □

Proposition 3.19.7 (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 $x \in K$, ϕ 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 (3.19.6) we may assume without loss of generality that A is a local ring with unique maximal ideal $\mathfrak{m} = \ker(\phi)$. By (3.19.5) we may also suppose 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 Ω is algebraically closed, by (3.14.67) 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 (3.19.6) may extend $\tilde{\phi}$ to $B_{\mathfrak{B}}$ and so by maximality $B = B_{\mathfrak{B}}$. Finally (3.15.5) 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 3.19.8
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 (3.19.7), such that $\mathfrak{m}_B \cap A = \ker(\phi) = \mathfrak{m}_A$. □

Corollary 3.19.9
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 (3.18.10) 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 (3.19.8) there is a valuation ring $(V, \mathfrak{m}_V)$ such that $x^{-1} \in \mathfrak{m}_V$ which implies $x \notin V$ by (3.19.2). □

3.20 Derivations

Definition 3.20.1 (Module of Derivations)
Let A be a commutative ring and M an (A, B)-bimodule, then we say a derivation is a map $D : A \to M$ satisfying the following properties

- $D(x + y) = D(x) + D(y)$ ***linearity***

- $D(xy) = xD(y) + yD(x)$ ***product rule***

We denote the family of such derivations by $\mathrm{Der}(A, M)$*, and it is an* (A, B)*-bimodule.*

We may consider case $M = B$ *and* $\phi : A \to B$ *a ring homomorphism and in this case the product rule becomes*

$$D(xy) = \phi(x)D(y) + D(x)\phi(y)$$

We observe that by induction we have $D(n \cdot 1_A) = 0$ *for all* $n \in \mathbb{Z}$*.*

Suppose that A *is a* k*-algebra then we claim the following are equivalent*

- $D(\lambda) = 0 \quad \forall \lambda \in k$
- $D(\lambda x) = \lambda D(x) \quad \forall \lambda \in k$

In this case we denote the set of k*-linear derivations by*

$$\mathrm{Der}_k(A, B)$$

Note every derivation is $\mathbb{Z}$*-linear so we may work with* $k = \mathbb{Z}$ *in these cases. Finally we write*

$$\mathrm{Der}_k(A) := \mathrm{Der}_k(A, A)$$

For our purposes the following will be the key example

Example 3.20.2 (Evaluation at a zero)
Consider the case $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ *a f.g.* k*-algebra,* L/k *a field extension and* $(x) \in L^n$ *a zero of* $\mathfrak{a}$*. Then we may define the* A*-module structure on* L *by*

$$f \cdot \lambda := f(x)\lambda$$

In this case we have the more explicit form

$$\mathrm{Der}_k(A, L; x) = \{D \in \mathrm{Hom}_k(A, L) \mid D(fg) = f(x)D(g) + g(x)D(f)\}$$

which is an (A, L)*-bimodule.*

Lemma 3.20.3 (Rigidity of Derivations)
Suppose $D, D' \in \mathrm{Der}_k(A, M)$ *agree on a set of generators for* A*, then they are identically equal. For example in the previous example when* $D(\overline{X}_i) = D'(\overline{X}_i)$*.*

The following is a useful technical tool to identify derivations as algebra homomorphisms

Definition 3.20.4 (Dual Ring)
Let M *be an* A*-module. Define the* ***dual ring*** *as follows*

$$A[M] := A \times M$$

$$(a, m) \times (a', m') = (aa', am' + a'm)$$

with addition defined in the obvious way and multiplicative unit is $(1_A, 0_M)$*. Observe that it has an ideal* $N := 0 \times M$ *such that* $N^2 = 0$ *and canonically* $A[M]/N \cong A$*.*

Proposition 3.20.5
Let M *be an* A*-module where* A *is a* k*-algebra then there is a bijection*

$$\begin{aligned} \mathrm{Der}_k(A, M) &\to \mathrm{AlgHom}_k(A, A[M]) \\ D &\to \phi_D(a) = (a, D(a)) \end{aligned}$$

Definition 3.20.6 (Partial Derivative)
Suppose $F \in A[X_1, \ldots, X_n]$ *given by*

$$F(X_1, \ldots, X_n) = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \ldots X_{i_n}^n \quad a_i \in A$$

Define the partial derivative as follows

$$\frac{\partial F}{\partial X_k} := \sum_{\substack{i\in\mathbb{N}^n \\ i_k\neq 0}} a_i i_k X_1^{i_1}\dots X_k^{i_k-1}\dots X_n^{i_n} \tag{3.4}$$

We observe that

$$\frac{\partial X_l}{\partial X_k} = \delta_{lk}$$

Note this condition uniquely determines Equation (3.4), see (3.20.8).

We show that these form a basis for $\mathrm{Der}_k(A)$.

Lemma 3.20.7 (Product Rule)
For $F, G \in A[X_1,\dots,X_n]$ we have the ***product rule***

$$\frac{\partial FG}{\partial X_k} = F\frac{\partial G}{\partial X_k} + G\frac{\partial F}{\partial X_k}$$

Proof. First we demonstrate the result in the univariate case $n = 1$. For monomials this is straightforward :

$$\frac{\partial X^r X^s}{\partial X} = (r+s)X^{r+s-1} = X^s\frac{\partial X^r}{\partial X} + X^r\frac{\partial X^s}{\partial X}$$

For general univariate polynomials the product rule follows from the linearity of $\frac{\partial}{\partial X}$. The multivariate case then follows from considering the isomorphism $A[X_1,\dots,X_n] \cong A[X_1,\dots,\widehat{X_k},\dots,X_n][X_k]$ under which $\frac{\partial}{\partial X_k}$ corresponds to $\frac{\partial}{\partial X}$. □

Lemma 3.20.8 (Multivariate Chain Rule)
Let $D \in \mathrm{Der}_k(A, M)$ be a derivation, $x_1,\dots,x_n \in A$ and $F \in A[X_1,\dots,X_n]$. Then

$$D(F(x_1,\dots,x_n)) = \sum_{k=1}^{n}\frac{\partial F}{\partial X_k}(x_1,\dots,x_n)D(x_k)$$

As a special case we find

$$\begin{aligned} D(F(x)) &= F'(x)D(x) \\ D(x^n) &= nx^{n-1}D(x) \end{aligned}$$

Proof. First we observe that by induction on n

$$D(x_1\dots x_n) = \sum_{k=1}^{n} x_1\dots\widehat{x_k}\dots x_n D(x_k)$$

and in particular

$$D(x^n) = \begin{cases} nx^{n-1}D(x) & n > 0 \\ 0 & n = 0 \end{cases}$$

Then for $F \in k[X_1,\dots,X_n]$ we have

$$\begin{aligned} D(F(x_1,\dots,x_n)) &= \sum_{i\in\mathbb{N}^n} a_i D(x_1^{i_1}\dots x_n^{i_n}) \\ &= \sum_{i\in\mathbb{N}^n} a_i \sum_{k=1}^{n} x_1^{i_1}\dots\widehat{x_k^{i_k}}\dots x_n^{i_n} D(x_k^{i_k}) \\ &= \sum_{k=1}^{n}\sum_{i\in\mathbb{N}^n} a_i x_1^{i_1}\dots\widehat{x_k^{i_k}}\dots x_n^{i_n} D(x_k^{i_k}) \\ &= \sum_{k=1}^{n}\sum_{\substack{i\in\mathbb{N}^n \\ i_k\neq 0}} i_k a_i x_1^{i_1}\dots x_k^{i_k-1}\dots x_n^{i_n} D(x_k) \end{aligned}$$

which gives the required result.

□

Proposition 3.20.9 (Extensions to Field of Fractions)
Let A be a k-algebra and M an A-module. Then we have the following isomorphisms

$$\begin{aligned} \mathrm{Der}_k(A,M) &\cong \mathrm{Der}(S^{-1}A, S^{-1}M) \\ D &\to \frac{a}{s} \to \frac{aD(s)-sD(a)}{s^2} \end{aligned}$$

In particular if $M=\Omega$ is a field containing A then we have an isomorphism

$$\mathrm{Der}_k(A,\Omega) \cong \mathrm{Der}_k(K,\Omega)$$

where $K := \mathrm{Frac}(A)$.

In light of (3.20.5) the following definition is clearly related to the existence of derivations.

Definition 3.20.10 (Formally Smooth)
*Let A be a k-algebra. We say it is **formally smooth** if for any k-algebra C with $N \triangleleft C$ such that $N^2=0$ and any homomorphism $v: A \to C/N$ there exists a lifting $\overline{v}: A \to C$.*

$$\begin{array}{ccc} k & \longrightarrow & C \\ \downarrow & \nearrow & \downarrow \pi \\ A & \xrightarrow{v} & C/N \end{array}$$

*We say that A is **formally unramified** if in addition the lifting is always unique.*

Lemma 3.20.11
Let C be a ring and $N \subseteq \sqrt{(0)}$ an ideal. Then $x \in C$ is invertible if and only if $\overline{x} \in C/N$ is invertible.

Proof. One direction is obvious. Conversely if $\overline{x}$ is invertible then $x \in C^\star + N \subseteq C^\star + \sqrt{(0)} \subseteq C^\star$ by (3.4.63) as required. □

Lemma 3.20.12
If a ring A is formally smooth (resp. unramified) then so is $S^{-1}A$.

Proof. It's enough to show that for $s \in S$ we have $\overline{v}(s)$ is invertible, which follows from (3.20.11). □

Lemma 3.20.13
The polynomial ring $k[X_1,\ldots,X_n]$ and function field $k(X_1,\ldots,X_n)$ is formally smooth.

Proof. The first follows by definition and the second by (3.20.12). □

Lemma 3.20.14
Let A be a formally smooth (resp. formally unramified) k-algebra and B is a formally smooth (resp. formally unramified) A-algebra. Then B is a formally smooth (resp. formally unramified) k-algebra.

Lemma 3.20.15 (Separable algebraic extensions are "formally unramified")
A separable algebraic extension K/k is formally uramified.

Proof. Consider the following commutative diagram

$$\begin{array}{ccc} k & \longrightarrow & C \\ \downarrow & \nearrow & \downarrow \pi \\ K & \xrightarrow{v} & C/N \end{array}$$

We suppose first that K is a finite extension. By (3.14.99) it is simple, namely $K = k(\alpha) = k[\alpha]$. Let $m(X)$ be the minimal polynomial over k and choose $x \in C$ such that $\pi(x) = v(\alpha)$. Note that $\overline{v}(\alpha) = x$ need not be well-defined because in general $m(x) \neq 0$. We show however there is an $n \in N$ such that $m(x+n)=0$. For consider any $n \in N$ and $f(X) \in k[X]$.

$$\begin{aligned} f(x+n) &= f(x) + \sum_{i=0}^{N} \lambda_i \left[(x+n)^i - x^i\right] \\ &= f(x) + f'(x)n \end{aligned}$$

as $n^2=0$. Therefore we propose $n = -m(x)/m'(x)$; to show this is well-defined, consider firstly $\pi(m(x)) = m(v(\alpha)) = v(m(\alpha)) = 0$ whence $m(x) \in N$. To show that $m'(a)$ is invertible we argue as follows. As α is separable, $m'(\alpha) \neq 0$,

hence is a unit in K and therefore $v(m'(\alpha)) = m'(v(\alpha)) = m'(\pi(x)) = \pi(m'(x))$ is a unit in C/N. By (3.20.11) $m'(x) \in C^\star$. Therefore $n \in N$ is well-defined and $m(a+n) = 0$ by construction. Therefore the map $\overline{v} : k[\alpha] \to A$ such that $\overline{v}(\alpha) = a + n$ is well-defined, and the diagram commutes because $\pi(a+n) = \pi(a) + \pi(n) = v(\alpha)$.

Suppose we had another $\overline{v}'$, then $a' := \overline{v}'(\alpha)$ again satisfies $m(a') = 0$ and $\pi(a') = v(\alpha)$ whence $a' - a \in N$. By the same argument as before

$$m(a') = m(a + (a' - a)) = m(a) + m'(a)(a' - a)$$

As $m'(a) \neq 0$ and $m(a') = m(a) = 0$ we see $a' = a$ which demonstrates uniqueness.

Suppose that K/k is algebraic than for every $\alpha \in K$ we have liftings $v_\alpha : k(\alpha) \to k$. We claim that $v_\alpha|_{k(\alpha)\cap k(\beta)} = v_\beta|_{k(\alpha)\cap k(\beta)}$. However $k(\alpha) \cap k(\beta)$ is also finite and so we are done by uniqueness. □

Proposition 3.20.16
A separably generated extension K/k is formally smooth.

Proof. This follows from (3.20.13), (3.20.15) and (3.20.14). □

3.21 Krull Dimension

Definition 3.21.1 (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** of a prime ideal $\mathfrak{p}$, denoted $\operatorname{ht}(\mathfrak{p})$, is the maximum length of chains of prime ideals contained in $\mathfrak{p}$. More generally define $\operatorname{ht}(\mathfrak{a}) = \inf\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{a} \subseteq \mathfrak{p}\}$. By (3.4.43) we may take the infimum over only minimal prime ideals.*

c) *The **dimension** of an ideal $\mathfrak{a} \triangleleft A$, denoted $\dim \mathfrak{a}$, is the maximum length of chains of prime ideals containing $\mathfrak{a}$.*

*We say A is **finite-dimensional** if $\dim A < \infty$. Observe that $\mathfrak{a} \subseteq \mathfrak{p} \iff \sqrt{\mathfrak{a}} \subseteq \mathfrak{p}$ for any prime ideal $\mathfrak{p}$ so*

$$\dim \mathfrak{a} = \dim \sqrt{\mathfrak{a}}$$
$$\operatorname{ht}(\mathfrak{a}) = \operatorname{ht}(\sqrt{\mathfrak{a}})$$

and we may, without loss of generality, consider only radical ideals.

Definition 3.21.2
Let A be a commutative ring. We say a chain of prime ideals is

- ***maximal** if it's not properly contained in any chain*
- ***saturated** if $\mathfrak{p}_i \subseteq \mathfrak{p} \subseteq \mathfrak{p}_{i+1} \implies \mathfrak{p} = \mathfrak{p}_i$ or $\mathfrak{p} = \mathfrak{p}_{i+1}$.*

*We say that A is **biequidimensional** if every maximal chain has the same length (equal to $\dim A$).*

*We say A is **quasi-biequidimensional** if $A/\mathfrak{p}$ is **biequidimensional** for every minimal prime $\mathfrak{p}$. Note that **equidimensional** + **quasi-biequidimensional** $\iff$ **biequidimensional**.*

*We say that A is **catenary** if the length of a saturated chain*

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

depends only on $\mathfrak{p}_0$ and $\mathfrak{p}_n$ and is equal to $\operatorname{ht}(\mathfrak{p}_n/\mathfrak{p}_0)$

*We say that A is **equidimensional** if every minimal prime ideal has the same dimension (equal to $\dim A$). Note an **irreducible** ring has only one minimal prime ideal so is trivially equidimensional.*

*We say that A is **equicodimensional** if every maximal ideal has the same height (equal to $\dim A$).*

In order to connect this to the lattice-theoretic notion of Krull Dimension in Section 2.5 we prove the following result (provided we consider the lattice of radical ideals ordered by *reverse* inclusion).

Proposition 3.21.3
Let A be a ring then the lattice of radical ideals $\mathrm{Rad}(A)$ is distributive, that is we have equality

$$\mathfrak{r}_1 \cap \sqrt{\mathfrak{r}_2 + \mathfrak{r}_3} = \sqrt{\mathfrak{r}_1 \cap \mathfrak{r}_2 + \mathfrak{r}_1 \cap \mathfrak{r}_3}$$

*Furthermore the meet-prime radical ideals are precisely the prime ideals. Therefore the lattice of radical ideals of a finite-dimensional Noetherian ring, ordered by **reverse inclusion**, is a Krull Lattice.*

Proof. Clearly it's enough to show that LHS $\subseteq$ RHS. Suppose $x \in LHS$ then $x \in \mathfrak{r}_1$ and $x^n = a + b$ where $a \in \mathfrak{r}_2$ and $b \in \mathfrak{r}_3$. Then $x^{n+1} = ax + bx \in \mathfrak{r}_1 \cap \mathfrak{r}_2 + \mathfrak{r}_1 \cap \mathfrak{r}_3$ whence $x \in RHS$.

We've shown that prime ideals are meet-prime (3.4.39). Suppose $\mathfrak{r}$ is a meet-prime radical ideal, and $fg \in \mathfrak{r}$. Then we claim that

$$\sqrt{\mathfrak{r} + (f)} \cap \sqrt{\mathfrak{r} + (g)} \subseteq \mathfrak{r}$$

For $x \in LHS \implies x^n \in \mathfrak{r} + (f)$ and $x^m \in \mathfrak{r} + (g) \implies x^{n+m} \in \mathfrak{r} \implies x \in \mathfrak{r}$. As $\mathfrak{r}$ is meet-prime then for example $\sqrt{\mathfrak{r} + (f)} \subseteq \mathfrak{r}$ and in particular $f \in \mathfrak{r}$. Therefore $\mathfrak{r}$ is also prime. □

Remark 3.21.4
This is easier to see in light of the dual isomorphism in (5.2.10), because the closed sets of a topological space trivially form a distributive lattice, and the irreducible closed subsets of a topological space are precisely the join-prime elements of this lattice.

Proposition 3.21.5 (Simple properties)
The following properties of Krull dimension hold

a) $\dim A = \dim A/N(A)$

b) $\mathrm{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}}$

c) $\dim \mathfrak{a} = \dim A/\mathfrak{a}$

d) $\dim \mathfrak{a} = \dim \mathfrak{a}/\mathfrak{b}$ *for any ideal* $\mathfrak{b} \subseteq \mathfrak{a}$

e) $\dim A = \sup_{\mathfrak{p}} \dim A_{\mathfrak{p}}$

f) ***codimension inequality*** $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{p}/\mathfrak{q}) + \mathrm{ht}(\mathfrak{q})$

g) $\dim k = 0$ *for any field* k

h) *A principal ideal domain A which is not a field has dimension* 1

Proof. a) By (3.4.53) there is an order-isomorphism between prime ideals of A containing $N(A)$ and prime ideals of $A/N(A)$. However by (3.4.45) 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 (3.6.32).

c) This follows similarly from (3.4.53).

d) $\dim \mathfrak{a} = \dim A/\mathfrak{a} = \dim(A/\mathfrak{a})/(\mathfrak{a}/\mathfrak{b}) = \dim \mathfrak{a}/\mathfrak{b}$

e) This follows from (2.5.6)

f) This follows from (2.5.6)

g) The only (prime) ideal is (0)

h) By (...) every prime ideal (besides (0)) is maximal so every chain has length at most 1.

□

Proposition 3.21.6 (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 ϕ integral and injective implies $\dim A = \dim B$.

Proof. Without loss of generality we can assume that ϕ is injective. The two cases follow by lifting chains of prime ideals from A (resp. B) to B (resp. A), and checking that distinct is maintained.

The final statement follows from (3.18.14). □

Corollary 3.21.7
Let $\phi : A \to B$ be integral and $\mathfrak{b} \lhd B$, then $\dim \phi^{-1}(\mathfrak{b}) = \dim(\mathfrak{b})$.

Lemma 3.21.8
Let A be a UFD and $\mathfrak{p} \lhd A$ a non-zero prime ideal. Then it contains a non-zero principal prime ideal (p).

In particular $\operatorname{ht}(\mathfrak{p}) = 1$ if and only if it is principal.

Proof. Choose $0 \neq f \in \mathfrak{p}$. Then by definition it has a factorization into primes, and at least one must be in $\mathfrak{p}$, say p. Then (p) is prime by (3.11.9). Therefore if $\operatorname{ht}(\mathfrak{p}) = 1$ then it is equal to (p).

Conversely if $\mathfrak{q} \subseteq (p)$ then $(q) \subseteq \mathfrak{q} \subseteq (p)$ for q prime, which implies $p \mid q$. As q is irreducible (...) then $(p) = (q) = \mathfrak{q}$. Therefore $\operatorname{ht}((p)) = 1$. □

Proposition 3.21.9
Let A be a Noetherian ring and $\mathfrak{a}$ a proper ideal. Then there are only finitely many minimal primes containing $\mathfrak{a}$, say $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Further we have a decomposition

$$\sqrt{\mathfrak{a}} = \bigcap_{i=1}^{n} \mathfrak{p}_i$$

which is irredundant (and the only such decomposition). Furthermore

$$\operatorname{ht}(\mathfrak{a}) = \min_i \operatorname{ht}(\mathfrak{p}_i)$$
$$\dim(\mathfrak{a}) = \max_i \dim(\mathfrak{p}_i)$$

Proof. This follows from (2.4.7) and (3.21.3) applied to the radical ideal $\sqrt{a}$. □

Remark 3.21.10
This is essentially the proof of [Kap74, Theorem 87, 88].

We've noted in general (3.21.5) that the so-called codimension formula does not hold. However it holds in the following case, for essentially trivial reasons.

Proposition 3.21.11 (Codimension 1 formula)
Let A be an irreducible Noetherian ring of finite Krull Dimension, and $\mathfrak{a}$ such that $\dim(\mathfrak{a}) = \dim(A) - 1$ then $\operatorname{ht}(\mathfrak{a}) = 1$.

Proof. Apply (2.5.7). □

In practice most rings of geometric interest are catenary or quasi-biequidimensional. We recall some properties and equivalent criteria for these cases.

Proposition 3.21.12 (Catenary Criteria)
Let A be a ring. Then the following are equivalent

a) *A is catenary*

b) *For all prime ideals $\mathfrak{r} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ the following holds*

$$\operatorname{ht}(\mathfrak{p}/\mathfrak{r}) = \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) + \operatorname{ht}(\mathfrak{q}/\mathfrak{r})$$

When A is irreducible this is equivalent to the following condition

$$\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q}) + \operatorname{ht}(\mathfrak{p}/\mathfrak{q})$$

Proof. This is restatement of (2.5.9). □

Proposition 3.21.13 (Biequidimensional Criteria)
Let A be a ring. Then the following are equivalent

a) *A is quasi-biequidimensional*

b) *A is catenary and $A/\mathfrak{p}$ is equicodimensional for every minimal prime $\mathfrak{p}$*

c) *A satisfies the formula*

$$\dim \mathfrak{q} = \dim \mathfrak{p} + \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) \quad \forall \mathfrak{q} \subseteq \mathfrak{p}$$

d) *A satisfies c) whenever $\operatorname{ht}(\mathfrak{p}/\mathfrak{q}) = 1$ (i.e. $\mathfrak{q} \subsetneq \mathfrak{p}$ is saturated)*

Furthermore

$$\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) + \operatorname{ht}(\mathfrak{q})$$

Proof. This is a restatement of (2.5.12). □

Proposition 3.21.14 (Irreducible Biequidimensional Criteria)
When A is irreducible the following are equivalent

a) *A is biequidimensional*

b) *A is quasi-biequidimensional*

c) *A is catenary and equicodimensional*

d) *A satisfies the formula*

$$\dim \mathfrak{q} = \dim \mathfrak{p} + \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) \quad \forall \mathfrak{q} \subseteq \mathfrak{p}$$

e) *A satisfies d) whenever $\operatorname{ht}(\mathfrak{p}/\mathfrak{q}) = 1$ (i.e. $\mathfrak{q} \subsetneq \mathfrak{p}$ is saturated)*

Proof. This is a restatement of (2.5.15). □

Proposition 3.21.15 (Codimension Formula)
Let A be a quasi-biequidimensional ring, $\mathfrak{a}$ an ideal and $\mathfrak{p} \subset \mathfrak{a}$ a prime ideal. Then the following properties hold

$$\begin{aligned} \dim A &= \dim \mathfrak{a} + \operatorname{ht}(\mathfrak{a}) \\ \operatorname{ht}(\mathfrak{a}) &= \operatorname{ht}(\mathfrak{a}/\mathfrak{p}) + \operatorname{ht}(\mathfrak{p}) \\ \dim \mathfrak{p} &= \dim \mathfrak{a} + \operatorname{ht}(\mathfrak{a}/\mathfrak{p}) \end{aligned}$$

Proof. This is a restatement of (2.5.14). □

3.22 Hauptidealsatz

The main result of this section is the following result due to Krull

Proposition 3.22.1 (Generalized Hauptidealsatz for Noetherian Rings)
Suppose A is a Noetherian ring then the following properties hold

a) *Every prime ideal of height n is minimal over some ideal $\mathfrak{a} := (x_1, \dots, x_n)$. Furthermore $\mathfrak{a}$ may be chosen such that $\operatorname{ht}(\mathfrak{a}) = n$ and every minimal prime of $\mathfrak{a}$ is of height n*

b) *We have the following characterization of height*

$$\operatorname{ht}(\mathfrak{p}) = \min\{n \mid \mathfrak{p} \text{ minimal over } (x_1, \dots, x_n)\}$$

In particular if $\mathfrak{p}$ is minimal over $(x_1, \dots, x_n)$ then $\operatorname{ht}(\mathfrak{p}) \leq n$.

In full generality the proof is quite subtle and in most cases of interest a simpler proof is possible. Therefore we introduce the following notions.

Definition 3.22.2 (Hauptidealsatz Ring)
*We say a ring A is a **generalized hauptidealsatz** ring if for all $x_1, \dots, x_n \in A$ and $\mathfrak{p}$ prime ideals minimal over $(x_1, \dots, x_n)$ we have $\operatorname{ht}(\mathfrak{p}) \leq n$*

*We say a ring A is simply a **hauptidealsatz** ring if this holds for $n = 1$.*

Lemma 3.22.3
Let A be a hauptidealsatz ring and $\mathfrak{p}$ a prime ideal. Then $A_{\mathfrak{p}}$ is hauptidealsatz.

Proof. Any prime ideal of $A_{\mathfrak{p}}$ has the form $\mathfrak{q}A_{\mathfrak{p}}$ by the correspondence of ideals under localization (3.6.18). If $\mathfrak{q}A_{\mathfrak{p}}$ is minimal over $(f/s) = (f/1)$, then clearly $(f) \subseteq \mathfrak{q}$. Furthermore $(f) \subseteq \mathfrak{q}' \implies (f/1) \subseteq \mathfrak{q}'A_{\mathfrak{p}}$. So $\mathfrak{q}$ is also minimal over (f) and therefore has height at most 1 by assumption. By the same result $\mathfrak{q}A_{\mathfrak{p}}$ has height at most 1. □

Proposition 3.22.4 (Hauptidealsatz $\implies$ Generalized Hauptidealsatz (Geometric))
Suppose that A is catenary, and hauptidealsatz for every quotient by a prime ideal. Then A is generalized hauptidealsatz, and so is every localization at a prime ideal.

Proof. We consider the case first that A is irreducible (which means it is hauptidealsatz by assumption because $\sqrt{(0)}$ is prime) and assume wlog that $n > 1$. Let $\mathfrak{p}$ be a minimal prime of $(x_1, \dots, x_n)$ and $\mathfrak{q}$ a minimal prime of $(x_1, \dots, x_{n-1})$. By considering the localization $A_{\mathfrak{p}}$ we may choose $\mathfrak{q} \subseteq \mathfrak{p}$. By induction $\operatorname{ht}(\mathfrak{q}) \leq n - 1$. Then $\mathfrak{p}/\mathfrak{q}$ is a minimal prime over $(x_n + \mathfrak{q})$ and therefore by assumption has height at most 1. By the codimension formula (3.21.12) we see $\operatorname{ht}(\mathfrak{p}) \leq n$ as required.

For the reducible case let $\mathfrak{r} \subseteq \mathfrak{p}$ be a minimal prime. Then the ring $A/\mathfrak{r}$ is irreducible and we see that $\mathrm{ht}(\mathfrak{p}/\mathfrak{r}) \leq n$ by the first part. Taking the supremum over all minimal primes $\mathfrak{r}$ shows that $\mathrm{ht}(\mathfrak{p}) \leq n$.

For the last statement we need only show that every localization at a prime ideal satisfies the hypotheses of the theorem. By correspondence of ideals under localisation (3.6.18) we see that every such ring is catenary. By the previous Lemma $A_{\mathfrak{p}}$ is hauptidealsatz and by (3.6.24) $A_{\mathfrak{p}}/\mathfrak{q}A_{\mathfrak{p}} \cong (A/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$ for any prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$ so every quotient by a prime ideal is hauptidealsatz. □

The catenary assumption may be relaxed by making a more complicated argument.

Proposition 3.22.5 (Hauptidealsatz $\implies$ Generalized Hauptidealsatz (Algebraic))
Suppose A is a ring such that every quotient by a prime ideal satisfies the hauptidealsatz. Then A is generalized hauptidealsatz and so is every localization at a prime ideal $\mathfrak{p}$.

Proof. We prove this by induction on n for a fixed ring A. Let $\mathfrak{p}$ be a minimal prime over $(x_1, \ldots, x_n)$. Suppose $\mathrm{ht}(\mathfrak{p}) > n$ then we may choose a saturated chain $\mathfrak{q} \subsetneq \mathfrak{p}$ such that $\mathrm{ht}(\mathfrak{q}) \geq n$. By minimality of $\mathfrak{p}$ we have $\mathfrak{q} \cap \{x_1, \ldots, x_n\} = \{x_1, \ldots, x_r\}$ with $r < n$ after a suitable reordering (possibly with $r = 0$). Furthermore we may choose $\mathfrak{q}$ such that r is maximal. Then by the induction hypothesis $\mathfrak{q}$ is not minimal over $(x_1, \ldots, x_r)$ and there is a chain

$$(x_1, \ldots, x_r) \subseteq \mathfrak{r} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$$

We claim that $\mathfrak{p}$ is minimal over $(\mathfrak{r}, x_{r+1})$ for suppose

$$(\mathfrak{r}, x_{r+1}) \subseteq \mathfrak{p}' \subseteq \mathfrak{p}$$

then by construction of $\mathfrak{q}$ (r was maximal) we see that $\mathfrak{p}' = \mathfrak{p}$. Taking quotients by $\mathfrak{r}$ the hauptidealsatz property shows that $\mathrm{ht}(\mathfrak{p}/\mathfrak{r}) \leq 1$. On the other hand we have a chain

$$(0) \subsetneq \mathfrak{q}/\mathfrak{r} \subsetneq \mathfrak{p}/\mathfrak{r}$$

which is a contradiction.

The final statement follows a similar argument as before. □

Remark 3.22.6
This argument is from [Kap74, Sec. 3.2 Ex. 6]

Before proceeding to the main result we need a some technical results related to height of ideals.

Lemma 3.22.7
Let $\mathfrak{q} \subseteq \mathfrak{p}$ be prime ideals then

$$\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{p})$$

with equality iff $\mathfrak{p} = \mathfrak{q}$.

Proof. The inequality is clear since any maximal chain below $\mathfrak{q}$ may be extended to a maximal chain below $\mathfrak{p}$. Similarly $\mathfrak{q} \subsetneq \mathfrak{p}$ implies that the inequality is strict. □

Lemma 3.22.8
Suppose $\mathfrak{a} \subseteq \mathfrak{b}$. Then

$$\mathrm{ht}(\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{b})$$

If these are equal and $\mathfrak{b}$ is prime, then it must be a minimal prime of $\mathfrak{a}$.

Proof. We consider first the case $\mathfrak{b} = \mathfrak{p}$ is prime. By (3.4.43) there is a minimal prime $\mathfrak{p}'$ such that $\mathfrak{a} \subseteq \mathfrak{p}' \subseteq \mathfrak{p}$. By definition $\mathrm{ht}(\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{p}')$. Furthermore by the previous Lemma $\mathrm{ht}(\mathfrak{p}') \leq \mathrm{ht}(\mathfrak{p})$, which yields the required result.

Suppose $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{a})$ then by definition $\mathrm{ht}(\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{p}') \leq \mathrm{ht}(\mathfrak{p})$ and therefore we conclude $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}')$. By the previous lemma we conclude that $\mathfrak{p} = \mathfrak{p}'$ is a minimal prime.

For the general case every minimal prime of $\mathfrak{b}$ also contains $\mathfrak{a}$ so the inequality follows by taking the minimum over all minimal primes. □

Lemma 3.22.9
Let $\mathfrak{a} \subseteq \mathfrak{b}$ be ideals such that there exists $x \in \mathfrak{b}$ not contained in any minimal prime of $\mathfrak{a}$. Then

$$\mathrm{ht}(\mathfrak{a}) < \mathrm{ht}(\mathfrak{b})$$

Proof. By the previous Lemma we have $\operatorname{ht}(\mathfrak{a}) \leq \operatorname{ht}(\mathfrak{b})$. Suppose they are equal then there is a minimal prime $\mathfrak{p}$ of $\mathfrak{b}$ of the same height, which by (3.22.8) is a minimal prime of $\mathfrak{a}$. This must contain x which then contradicts the assumption. □

Proposition 3.22.10 (Prime Avoidance Theorem)
Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be ideals and $\mathfrak{a}$ an ideal such that $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for all $i = 1 \ldots n$. Then there exists $x \in \mathfrak{a} \setminus (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n)$.

Proof. We proceed by induction on the number of prime ideals n, the case $n = 1$ being trivial. Consider then the case of $n+1$ prime ideals and suppose on the contrary that $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_{n+1}$. By the induction hypothesis there exists $x_i \in \mathfrak{a} \setminus \bigcup_{j \neq i} \mathfrak{p}_j$, and therefore by our assumption $x_i \in (\mathfrak{a} \cap \mathfrak{p}_i) \setminus \bigcup_{j \neq i} \mathfrak{p}_j$. Define

$$y := x_1 \ldots x_n$$

Then $y \notin \mathfrak{p}_{n+1}$ by primality and clearly $y \in \mathfrak{a} \cap \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$. Define $z := y + x_{n+1}$ then we see

a) $z \in \mathfrak{a}$

b) $z \notin \mathfrak{p}_{n+1}$

c) $z \notin \mathfrak{p}_i$ for $i = 1 \ldots n$

which contradicts our original assumption. □

Lemma 3.22.11
*Let A be a **generalized hauptidealsatz** ring and $\mathfrak{a} = (x_1, \ldots, x_n)$. Then the following are equivalent*

a) $\operatorname{ht}(\mathfrak{a}) = n$

b) *every minimal prime of $\mathfrak{a}$ has height n*

Proof. *a)* $\implies$ *b)* By definition this means every minimal prime has height at least n, and the reverse inequality follows from generalized hauptidealsatz assumption.
b) $\implies$ *a)* Recall from (3.21.1) we may take the infimum over only minimal prime ideals. □

Proposition 3.22.12 (Alternative characterization of height)
*Suppose A is a Noetherian ring satisfying **generalized hauptidealsatz**, then the following properties hold*

a) *Every prime ideal of height n is minimal over some ideal $\mathfrak{a} := (x_1, \ldots, x_n)$. Furthermore $\mathfrak{a}$ may be chosen such that $\operatorname{ht}(\mathfrak{a}) = n$ and every minimal prime is of height n*

b) *We have the following characterization of height*

$$\operatorname{ht}(\mathfrak{p}) = \min\{n \mid \mathfrak{p} \text{ minimal over } (x_1, \ldots, x_n)\}$$

In particular every prime ideal has finite height.

Proof. We first demonstrate *a)*. Suppose $\operatorname{ht}(\mathfrak{p}) = n$ then there is a saturated chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

It's clear from the above chain that $\operatorname{ht}(\mathfrak{p}_i) \geq i$. Furthermore by (3.22.7) $\operatorname{ht}(\mathfrak{p}_i) < \operatorname{ht}(\mathfrak{p}_{i+1})$ whence we see $\operatorname{ht}(\mathfrak{p}_i) = i$.

We show by induction that there are elements $x_1, \ldots, x_n \in A$ for which $\mathfrak{p}_i$ is a minimal prime over $\mathfrak{a}_i := (x_1, \ldots, x_i)$ for all $i = 0 \ldots n$ and $\operatorname{ht}(\mathfrak{a}_i) = i$.

The case $i = 0$ is clear, so suppose $i > 0$. In general by (3.21.9) there are finitely many minimal primes over $\mathfrak{a}_{i-1}$ say $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ which all have height $i - 1$ by (3.22.11). In particular $\mathfrak{p}_i \not\subseteq \mathfrak{q}_k$.

By prime avoidance (3.22.10) we may choose $x_i \in \mathfrak{p}_i \setminus (\mathfrak{q}_1 \cup \ldots \cup \mathfrak{q}_r)$. Clearly

$$\mathfrak{a}_{i-1} \subseteq \mathfrak{a}_i \subseteq \mathfrak{p}_i$$

Then by (3.22.8) and (3.22.9) we have $i - 1 = \operatorname{ht}(\mathfrak{a}_{i-1}) < \operatorname{ht}(\mathfrak{a}_i) \leq i$ whence $\operatorname{ht}(\mathfrak{a}_i) = i$. By (3.22.8) again we see $\mathfrak{p}_i$ is a minimal prime of $\mathfrak{a}_i$. This completes the inductive step.

To show *b)* let m denote the right hand side. Then by the generalized hauptidealsatz hypothesis $\operatorname{ht}(\mathfrak{p}) \leq m$. On the other hand by part *a)* we have $m \leq \operatorname{ht}(\mathfrak{p})$ whence they are equal.

Finally by the Noetherian hypothesis $\mathfrak{p}$ is finitely generated and clearly minimal over itself. □

3.23 Regular Local Rings

The results of the previous section allow a more direct characterization of the dimension of a Noetherian local ring, which naturally leads to the notion of regular local ring.

Lemma 3.23.1 ($\mathfrak{m}$-primary)
Let $(A, \mathfrak{m})$ be a local ring and $\mathfrak{a}$ a proper ideal. Then the following are equivalent

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

b) $\mathfrak{m}$ *is a minimal prime of* $\mathfrak{a}$

Furthermore $\mathfrak{a}$ is primary. A sufficient condition is that for some n

$$\mathfrak{m}^n \subset \mathfrak{a} \subset \mathfrak{m}$$

and this is necessary when $\mathfrak{m}$ is finitely generated.

Proof. *a)* $\implies$ *b)* Suppose $\mathfrak{a} \subseteq \mathfrak{p}$ then $\mathfrak{m} = \sqrt{\mathfrak{a}} \subseteq \mathfrak{p}$. In particular $\mathfrak{m}$ a minimal prime.

b) $\implies$ *a)* Every prime over $\mathfrak{a}$ is contained in, and therefore equal to, $\mathfrak{m}$ by (3.4.36). Therefore $\mathfrak{m}$ is the unique minimal prime over $\mathfrak{a}$. The result follows from (3.4.45).

Suppose $xy \in \mathfrak{a}$ and $y \notin \sqrt{\mathfrak{a}}$ then by (...) $y \in A^\star$ whence $x \in \mathfrak{a}$. This shows that $\mathfrak{a}$ is primary.

The condition is clearly sufficient. For the converse assume $\mathfrak{m} = (x_1, \dots, x_r)$ then $x_i^N \in \mathfrak{a}$. Then it's clear that sufficiently large n will ensure that $\mathfrak{m}^n \subset \mathfrak{a}$. □

An ideal satisfying one of the equivalent conditions above is called **$\mathfrak{m}$-primary**, though some authors require the stronger condition.

Proposition 3.23.2 (Criteria for Dimension of Local Ring)
Let $(A, \mathfrak{m})$ be a Noetherian local ring satisfying the generalized hauptidealsatz. Then we have the following criteria for dimension

$$\dim A = \operatorname{ht}(\mathfrak{m}) = \min\{n \mid \sqrt{(x_1, \dots, x_n)} = \mathfrak{m}\} \leq \mu(\mathfrak{m}) = \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$$

where $\mu(\mathfrak{m})$ is the least number of generators of $\mathfrak{m}$ and $k(\mathfrak{m}) = A/\mathfrak{m}$.

Proof. The first equality follows because every maximal chain must terminate at a maximal ideal by (3.4.36). The second from the characterization of height for hauptidealsatz rings (3.22.12) and the equivalent definitions of $\mathfrak{m}$-primary (3.23.1). The inequality follows because $\mathfrak{m}$ is itself $\mathfrak{m}$-primary. The final equality follows because a minimal generating set lifts to a basis of $\mathfrak{m}/\mathfrak{m}^2$ (3.16.7). □

Definition 3.23.3
Let $(A, \mathfrak{m})$ be a Noetherian local ring. We say A is ***regular*** *if*

$$\dim A = \mu(\mathfrak{m}) = \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$$

3.24 Affine Algebras

Definition 3.24.1 (Affine Domain)
We call a finitely-generated k-algebra an ***affine algebra****. If in addition it's integral we call it an* ***affine domain****.*

3.24.1 Normalisation

The following normalisation results can be seen as a refinement of results on transcendence bases (Section 3.14.15). The proof is adapted from [Bou98].

Definition 3.24.2 (Algebraically Independent)
Let A be a k-algebra and $x_1, \dots, x_n$ elements of A. Then we say they are ***algebraically independent*** *if one of the following equivalent conditions holds*

- *The unique k-algebra homomorphism $\phi : k[X_1, \dots, X_n] \to A$ such that $\phi(X_i) = x_i$ (evaluation homomorphism) is injective*
- *There are no non-zero polynomials $f(X_1, \dots, X_n)$ such that $f(x_1, \dots, x_n) = 0$.*

Note in particular it induces an isomorphism $k[X_1, \dots, X_n] \xrightarrow{\sim} k[x_1, \dots, x_n] \subset A$.

Definition 3.24.3 (Normalising Family)
*Let A be a finitely-generated k-algebra. A **normalising family** is a set $\{x_1, \dots, x_n\}$ of elements of A such that*

- *$x_1, \dots, x_n$ are **algebraically independent** over k*
- *A is a finite $k[x_1, \dots, x_n]$-module (equivalently integral over $k[x_1, \dots, x_n]$).*

NB this is completely equivalent to specifying an integral, injective map

$$k[X_1, \dots, X_n] \hookrightarrow A$$

This may be seen as a refined transcendence base. More precisely we have the following

Proposition 3.24.4 (Relationship to Transcendence Base)
Let A be an integral finitely-generated k-algebra with $K := \mathrm{Frac}(A)$. Let $S \subset A$ be a subset. Then

- *If A is integral over $k[S]$ then $K/k(S)$ is algebraic*
- *If S is a normalising family for A then S is a transcendence basis for K/k*

In particular normalising families have order $\mathrm{trdeg}(K/k)$.

Proof. By (3.14.52) the set $\{x \in K \mid x \text{ algebraic over } k(S)\}$ forms a subfield containing A, and therefore equals K.

The final statement follows from (3.14.124). □

The following is useful as it removes the necessity of showing algebraic independence in certain cases.

Corollary 3.24.5
Let A be an integral finitely-generated k-algebra with $K := \mathrm{Frac}(A)$. Let $S \subset A$ be a subset such that

- *A is integral over $k[S]$*
- *$\#S \leq \mathrm{trdeg}_k(K)$*

*then S is a **normalising family**.*

Proof. This follows from the previous result and (3.14.124). □

There are a few forms of the Normalisation Lemma which we prove, of progressively stronger form.

Lemma 3.24.6 (Hypersurface Normalisation Lemma)
Let $A = k[X_1, \dots, X_n]$ be a polynomial ring over an infinite field k and $0 \neq F \in A$. Then there exists $\lambda_1, \dots, \lambda_{n-1} \in k$ such that

- *$x_i := X_i - \lambda_i F \quad 1 \leq i \leq n-1$*
- *$x_1, \dots, x_{n-1}, F$ is a normalising family for A*
- *$FA \cap k[x_1, \dots, x_{n-1}, F] = Fk[x_1, \dots, x_{n-1}, F]$*

This may be viewed as a commutative diagram

$$\begin{array}{ccc} \phi : k[Y_1, \dots, Y_n] & \xrightarrow{\sim} & k[X_1, \dots, X_n] \\ \uparrow & & \downarrow \\ k[Y_1, \dots, Y_{n-1}] & \hookrightarrow & k[X_1, \dots, X_n]/(F) \end{array}$$

where the horizontal arrows are injective, integral (and finite) and $\phi^{-1}((F)) = (Y_n)$.

Remark 3.24.7
Reversing the arrows we get the geometric picture, where horizontal arrows are finite and surjective

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{\sim} & \mathbb{A}^n \\ \uparrow & & \downarrow \\ V(F) & \twoheadrightarrow & \mathbb{A}^{n-1} \end{array}$$

in otherwords after a linear change of variables we may express $V(F)$ as a finite covering of a standard hyperplane.

Proposition 3.24.8 (Nagata Normalisation Lemma)
Let $A = k[x_1, \dots, x_n]$ be a finitely-generated k-algebra such that k is infinite. Then there exists a ***normalising family*** *$y_1, \dots, y_d \in A$ such that each y_i is a k-linear combination of $x_1, \dots, x_n$. Further if $\mathfrak{a}_1 \triangleleft A$ is a proper ideal, then these may be chosen such that*

$$\mathfrak{a}_1 \cap k[y_1, \dots, y_d] = (y_1, \dots, y_h)k[y_1, \dots, y_d]$$

for some $0 \leq h \leq d$, where $h = 0$ denotes the zero ideal.

Proposition 3.24.9 (Bourbaki Normalisation Lemma)
Let $A = k[x_1, \dots, x_n]$ be a finitely-generated k-algebra such that k is infinite. Then there exists a ***normalising family*** *$y_1, \dots, y_d \in A$ such that each y_i is a k-linear combination of $x_1, \dots, x_n$.*

Furthermore for any finite chain of proper ideals in A

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_p \subsetneq A$$

the family may be chosen such that

$$\mathfrak{a}_j \cap k[y_1, \dots, y_d] = (y_1, \dots, y_{h(j)})k[y_1, \dots, y_d] \quad 1 \leq j \leq p\,.$$

for some non-decreasing sequence of integers $h(j)$, where $h(j) = 0$ denotes the zero ideal.

Remark 3.24.10 (Geometric Interpretation)
Note the normalisation here is equivalent to a commutative diagram

$$\begin{array}{ccc}
k[Y_1, \dots, Y_d] & \hookrightarrow & A \\
\uparrow & & \downarrow \\
k[Y_{h(1)+1}, \dots, Y_d] & \hookrightarrow & A/\mathfrak{a}_1 \\
\uparrow & & \downarrow \\
\vdots & & \vdots \\
\uparrow & & \downarrow \\
k[Y_{h(p)+1}, \dots, Y_d] & \hookrightarrow & A/\mathfrak{a}_p
\end{array}$$

where the horizontal arrows are integral and injective, and the top arrow is given by

$$\phi : Y_i \to \sum_j \lambda_{ij} x_j$$

such that $\phi^{-1}(\mathfrak{a}_i) = (Y_1, \dots, Y_{h(i)})$

As before this expresses A as a finite covering of $\mathbb{A}^d$ under which each subvariety is also a finite covering of a standard linear subspace.

We first prove the weaker form of the Normalisation Lemma

Proof of (3.24.6). First decompose F into homogenous polynomials (monomials of the same degree)

$$F = F_0 + F_1 + \ldots + F_m$$

and observe that the monomial X_n^m appears only in F_m. Define

$$F' := F(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n)$$

Furthermore in terms of homogenous polynomials

$$F'_m = F_m(X_1 + \lambda_1 T, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n)$$

and the coefficient of X_n^m in F' is simply $F'_m(0, \dots, 0, 1) = F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \in k$. There are only finitely many values of λ such that F_m is zero, whence there exists a λ such that X_n^m has non-zero coefficient in F', whence F' is monic. By the previous Lemma we have $F'(x_1, \dots, x_{n-1}, X_n) = 0$, with the leading coefficient in X_n constant.

Finally let $B := k[x_1, \dots x_{n-1}, F]$. Then clearly $B[X_n] = A$ and X_n is integral over B. Therefore by (3.18.4) A is a finite B-module. As $\operatorname{trdeg}(A/k) = n$ by (3.24.5) this is a normalising family, and B is isomorphic to a polynomial ring.

As B is a polynomial ring it is integrally closed (3.18.9). Then the final statement is a consequence of the following lemma (3.24.11) (essentially to prove that $V(F) \to \mathbb{A}^{n-1}$ is surjective). □

Lemma 3.24.11
Let A be integrally closed, $\phi : A \hookrightarrow B$ injective and integral and $a \in A$. Then

$$(a)^{ec} = \phi^{-1}(\phi(a)B) = (a)$$

Proof. Let $K = \mathrm{Frac}(A)$ and $L = \mathrm{Frac}(B)$, then ϕ extends to an injection $\phi : K \hookrightarrow L$.

Generically we have $(a) \subseteq (a)^{ec}$. Suppose $a' \in (a)^{ec}$, then $\phi(a') = \phi(a)b$. Therefore $\phi(a'a^{-1}) = b$ is integral over A, whence so is $a'a^{-1}$. As A is integrally closed we have $a' \in (a)$ as required. □

Before proving the stronger version of Normalisation Lemma, we need some preliminary technical results

Lemma 3.24.12
Let A be a k-algebra and $\mathfrak{a} \triangleleft A$ an ideal. Then $\mathfrak{a}$ is proper iff $\mathfrak{a} \cap k = \{0\}$.

Lemma 3.24.13
Let $A = k[X_1, \ldots, X_n]$ be a polynomial ring and $\mathfrak{a} \triangleleft A$ a proper ideal. Then TFAE

a) $\mathfrak{a} = (X_1, \ldots, X_h)$

b) i) $X_1, \ldots, X_h \in \mathfrak{a}$

ii) $\mathfrak{a} \cap k[X_{h+1}, \ldots, X_n] = \{0\}$

In this case $\mathfrak{a} \cap k[X_1, \ldots, X_h] = (X_1, \ldots, X_h)k[X_1, \ldots, X_h]$

Proof. We claim that there is a direct sum of k-vector spaces

$$k[X_1, \ldots, X_n] = (X_1, \ldots, X_h) \bigoplus k[X_{h+1}, \ldots, X_n]$$

from which the result largely follows. Let S be the set of monomials in which at least one of $X_1, \ldots, X_h$ appears, and let T be the set for which none appears (but including 1). Then clearly $A = \langle S \rangle \bigoplus \langle T \rangle$ and $k[X_{h+1}, \ldots, X_n] = \langle T \rangle$. We argue that $(X_1, \ldots, X_h) = \langle S \rangle$. First S is stable under multiplication by $X_1, \ldots, X_n$, and so $\langle S \rangle$ is an ideal. One inclusion is obvious, furthermore it's clear that $S \subseteq (X_1, \ldots, X_n)$ from which the claim follows. □

We may now proceed to the proof of the stronger versions of the Normalisation Lemma.

Reduction to polynomial ring case for (3.24.8), (3.24.9).

We show that for both forms it is possible to reduce to the case of a polynomial ring. For let A be a finitely-generated k-algebra then we may write $A := k[X_1, \ldots, X_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$. Then the polynomial ring case for $p = 1$ shows the existence of an integral, injective map

$$\phi : k[Y_1, \ldots, Y_m] \hookrightarrow A$$

If $\mathfrak{a}_i$ is a chain of ideals in A, then $\mathfrak{a}'_i := \phi^{-1}(\mathfrak{a}_i)$ is a chain of ideals in $k[Y_1, \ldots, Y_m]$. The general case for a polynomial ring shows the existence of an integral map

$$\psi : k[Z_1, \ldots, Z_m] \hookrightarrow k[Y_1, \ldots, Y_m]$$

such that

$$\psi^{-1}(\mathfrak{a}'_i) = (Z_1, \ldots, Z_{h(i)})$$

The composition $\phi \circ \psi$ gives the required normalisation of A. Geometrically express A as a finite covering of affine space, by considering it as a subvariety of larger affine space. □

Proof of (3.24.8) in the polynomial ring case.

Let $A = k[X_1, \ldots, X_n]$ and proceed by induction on n.

Note that as $\mathfrak{a}_1$ is proper, we must have $\mathfrak{a}_1 \cap k = \{0\}$, and we may obviously also assume that $\mathfrak{a}_1 \neq (0)$ (as otherwise we may take $h = 0$).

Choose $0 \neq x_1 \in \mathfrak{a}_1$. Then by (3.24.6) there exists $t_2, \ldots, t_n \in A$ such that $x_1, t_2, \ldots, t_n$ is a normalising family and $(x_1) \cap B = x_1 B$ where $B := k[x_1, t_2, \ldots, t_n]$. In the case that $\mathfrak{a}_1$ is principal we are done, since the choice of x_1 was arbitrary, and in this case $h(1) = 1$. In particular this covers the base case $n = 1$ because A is a PID (3.10.4).

Otherwise $B' := k[t_2, \ldots, t_n]$ is a polynomial ring and $\mathfrak{a}'_1 := \mathfrak{a}_1 \cap B'$ is proper by (3.24.12). By induction on n there is a normalising family $x_2, \ldots, x_n$ for B' such that $\mathfrak{a}'_1 \cap C' = (x_2, \ldots, x_h)C'$ where $C' := k[x_2, \ldots, x_n]$ and B' is

integral over C'.

Define $C := k[x_1, \ldots, x_n] = C'[x_1]$ then $x_1, t_2, \ldots, t_n$ are integral over C, so B is integral over C (3.18.4), and A is integral over C (3.18.5), so by (3.24.5) $x_1, \ldots, x_n$ is a normalising family for A.

We claim that $\mathfrak{a}_1'' := \mathfrak{a}_1 \cap C = (x_1, \ldots, x_h)C$. Clearly $x_1, \ldots, x_h \in \mathfrak{a}_1''$, and $\mathfrak{a}_1'' \cap k[x_{h+1}, \ldots, x_n] = \mathfrak{a}_1' \cap k[x_{h+1}, \ldots, x_n] = \{0\}$ by (3.24.13) applied to the ring C'. Then (3.24.13) applied to the ring C demonstrates the claim. □

Proof of (3.24.9) in the polynomial ring case. We can then show the case $p > 1$ by induction, for by the induction hypothesis there exists a normalising family $t_1, \ldots, t_n$ for A such that

$$\begin{aligned} \mathfrak{a}_j \cap B &= (t_1, \ldots, t_{h(j)})B \quad 1 \leq j \leq p-1 \\ B &:= k[t_1, \ldots, t_n] \end{aligned}$$

Let $r = h(p-1)$, then by the case $p = 1$ applied to the ring $B' := k[t_{r+1}, \ldots, t_n]$ and ideal $\mathfrak{a}_p \cap B'$ there exists a normalising family $x_{r+1}, \ldots, x_n$ for B' such that for some $s \leq n$ (possibly equal to r to denote the zero ideal),

$$\begin{aligned} \mathfrak{a}_p \cap C' &= (x_{r+1}, \ldots, x_s)C' \\ C' &:= k[x_{r+1}, \ldots, x_n] \end{aligned}$$

We claim that $t_1, \ldots, t_r, x_{r+1}, \ldots, x_n$ is a suitable normalising family for A, with $h(p) = s$.

For define $C := k[t_1, \ldots, t_r, x_{r+1}, \ldots, x_n] = C'[t_1, \ldots, t_r]$. Recall B' is integral over C', and $t_1, \ldots, t_r$ are obviously integral over C so $B = B'[t_1, \ldots, t_r]$ is integral over C by (3.18.7). Then A is integral over C by (3.18.5), and this is a normalising family by (3.24.5), and in particular algebraically independent.

For $j \leq p-1$ and $h := h(j) \leq r$, apply (3.24.13) to the ideal $\mathfrak{a}_j \cap B$ to see $\mathfrak{a}_j \cap k[t_{h+1}, \ldots, t_n] = \{0\}$ and therefore $\mathfrak{a}_j \cap k[t_{h+1}, \ldots, t_r, x_{r+1}, \ldots x_n] = \{0\}$. As $t_1, \ldots, t_h \in \mathfrak{a}_j$ we see by (3.24.13) that $\mathfrak{a}_j \cap C = (t_1, \ldots, t_h)C$ as required.

Similarly by (3.24.13) $\mathfrak{a}_p \cap k[x_{s+1}, \ldots, x_n] = \{0\}$ and clearly $t_1, \ldots, t_r, x_{r+1}, \ldots, x_s \in \mathfrak{a}_p$. Then by (3.24.13) again $\mathfrak{a}_p \cap C = (t_1, \ldots, t_r, x_{r+1}, \ldots, x_s)C$ as required . □

Remark 3.24.14
In Bourbaki's proof the reduction to the polynomial ring case increases p to $p+1$, so in particular the $p = 1$ case requires the more complex reduction argument at the end of the proof. With this approach the case $p = 1$ can be simplified.

3.24.2 Nullstellensatz

Definition 3.24.15 (Zeros of an ideal)
*Let $\mathfrak{a} \lhd k[X_1, \ldots, X_n]$ be an ideal and K/k a field extension. Then a point $(x) \in K^n$ is a **zero** of $\mathfrak{a}$ if*

$$f \in \mathfrak{a} \implies f(x) = 0$$

*We define the **residue field** to be*

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

and also denote

$$k[x] := k[x_1, \ldots, x_n]$$

The follow observation is useful

Proposition 3.24.16 (Zeros are homomorphisms)
Let $\mathfrak{a} \lhd k[X_1, \ldots, X_n]$ be an ideal then there is a bijection

$$\begin{aligned} \mathrm{AlgHom}_k(k[X_1, \ldots, X_n]/\mathfrak{a}, K) &\longleftrightarrow \{ \text{ zeros of } \mathfrak{a} \text{ in } K^n \} \\ \phi &\longrightarrow (\phi(\bar{X}_1), \ldots, \phi(\bar{X}_n)) \end{aligned}$$

The following notion is useful in future

Definition 3.24.17 (Generic Point)
Let $\mathfrak{a} \triangleleft k[X_1, \ldots, X_n]$ be a prime *ideal. then a point $(\xi) \in L^n$ is a* ***generic point*** *of $\mathfrak{a}$ if $\ker(\mathrm{ev}_\xi) = \mathfrak{a}$. Note one always exists, because we may take $L = \mathrm{Frac}(A)$ and $\xi_i = \overline{X}_i$.*

When (x) is another zero of $\mathfrak{a}$ this induces a k-algebra homomorphism

$$k[\xi] \to k[x]$$

which is an isomorphism precisely when (x) is a generic point.

Generally we are interested in the relationship between ideals of $k[X_1, \ldots, X_n]$ and corresponding zeros in an extension field K/k. The following proposition is fundamental

Proposition 3.24.18 (Correspondence between ideals and zeros)
Let K/k be a field extension and $(x) \in K^n$. Define $\mathfrak{m}_x$ to be the kernel of the homomorphism

$$\mathrm{ev}_x : k[X_1, \ldots, X_n] \to K$$

Then

- *$\mathfrak{m}_x$ is a prime ideal*
- *If K/k is an algebraically closed field of transcendence degree $\geq n$ then every prime ideal is of this form.*
- *If x_i are algebraic over k (e.g. if K/k is algebraic) then $\mathfrak{m}_x$ is maximal*
- *If $\bar{k} \subset K$ then every maximal ideal is of the form $\mathfrak{m}_x$ for $x \in \bar{k}^n$ an algebraic point.*

In this case we have a canonical isomorphism

$$k[X_1, \ldots, X_n]/\mathfrak{m}_x \xrightarrow{\sim} k[x] \subset K$$

and when (x) is algebraic then $k[x] = k(x)$.

Proof. The canonical isomorphism follows from (3.8.3). Any subring of a field is an integral domain, which means $\mathfrak{p}_x$ is prime by (3.4.56).

By (3.14.51) x_i are algebraic over k if and only if $k(x_1, \ldots, x_n)/k$ is algebraic. By the same result $k[x_1, \ldots, x_n] = k(x_1, \ldots, x_n)$ and therefore $\mathfrak{m}_x$ is maximal by (3.4.56).

Let $\mathfrak{p}$ be a prime ideal and define $k(x) := \mathrm{Frac}(k[x])$ and $k[x] := k[X_1, \ldots, X_n]/\mathfrak{p}$. If K has transcendence degree $\geq n$ then there is an embedding $k(x)/k \to K/k$ by (3.14.67). This restricts to an isomorphism $k[x] \xrightarrow{\sim} k[\bar{x}]$ for some $\bar{x}_i \in K$. It's clear that $\mathfrak{p} = \mathfrak{m}_x$.

The proof of the final part we defer to Section 3.24.2.1. □

The final part is what is usually known as the **Weak Nullstellensatz**. It can be rephrased in multiple forms

Proposition 3.24.19 (Weak Nullstellensatz I)
Let k be a field, then the following are trivially equivalent

a) *Every proper / prime / maximal ideal in $k[X_1, \ldots, X_n]$ has a zero in $\bar{k}^n$*

b) *Every maximal ideal $\mathfrak{m} \triangleleft k[X_1, \ldots, X_n]$ is of the form $\mathfrak{m}_x$ for $x \in \bar{k}^n$*

c) *For every maximal ideal $\mathfrak{m}$, the field extension $K := k[X_1, \ldots, X_n]/\mathfrak{m}$ 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 $\mathfrak{m} \subseteq \mathfrak{m}_x$ by assumption, and by maximality $\mathfrak{m} = \mathfrak{m}_x$.

b) $\implies$ *c)* Observe $\mathfrak{m} = \mathfrak{m}_x$ for $x \in \bar{k}^n$ so K is isomorphic to $k[x_1, \ldots, x_n]$ which is an algebraic field extension by (3.14.51).

c) $\implies$ *a)* By (3.14.67) there is an embedding $K \to \bar{k}$. Therefore by (3.24.16) every maximal ideal has a root.

c) $\implies$ d) Every finitely generated k-algebra A is of the form $k[X_1,\dots,X_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$. If A is a field then $\mathfrak{a}$ is maximal by (3.4.56) and so by assumption A/k is a finitely-generated algebraic field extension and therefore finite by (3.14.51).

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 $\mathfrak{a}\bar{k}[X_1,\dots,X_n]$ in a). □

When $K=\bar{k}$ is an algebraic closure we may use these results to make the connection more precise

Proposition 3.24.20 (Weak Nullstellensatz II)
There is a bijective map

$$\begin{array}{ccc} \bar{k}^n/\operatorname{Aut}(\bar{k}/k) & \longrightarrow & \{\mathfrak{m} \lhd k[X_1,\dots,X_n] \text{ maximal }\} \\ x & \longrightarrow & \mathfrak{m}_x \end{array}$$

When $x \in k^n$ then

$$\mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n)$$

Proof. The map is surjective by (3.24.19). It's well-defined because $\mathfrak{m}_{\sigma(x)} = \mathfrak{m}_x$.

By (3.24.18) we have an isomorphism $k[X_1,\dots,X_n]/\mathfrak{m}_x \xrightarrow{\sim} k[x_1,\dots,x_n] \subset \bar{k}$. If $\mathfrak{m}_x = \mathfrak{m}_y$ then these compose to yield an isomorphism $\sigma : k[x_1,\dots,x_n] \xrightarrow{\sim} k[y_1,\dots,y_n] \subset \bar{k}$ such that $\sigma(x_i) = y_i$. By (3.14.75) this extends to $\sigma \in \operatorname{Aut}(\bar{k}/k)$. Therefore the given mapping is injective. □

3.24.2.1 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 $A := k[X_1,\dots,X_n]/\mathfrak{a}$ is integral over $B := k[z_1,\dots,z_d]$ where $z_1,\dots,z_d$ are algebraically independent.

If $\mathfrak{a}$ is maximal then A is a field and by (3.18.11) B 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 $\mathfrak{m}_z$ for any $\bar{z} \in \bar{k}^d$ (except maybe when $d=0$). By (3.18.14) there is a maximal ideal $\mathfrak{m} \lhd A$ lieing above. Then we have a diagram

$$\begin{array}{ccccc} A & \longrightarrow & A/\mathfrak{m} & \dashrightarrow & \bar{k} \\ \uparrow & & \uparrow & \nearrow & \\ B & \longrightarrow & B/\mathfrak{m}_z & & \end{array}$$

which may be completed because $A/\mathfrak{m}$ is algebraic over $B/\mathfrak{m}_z$. By (3.24.16) this yields a zero of $\mathfrak{a}$. □

Proof of Nullstellensatz avoiding normalisation. Consider only the case $\mathfrak{a}=\mathfrak{p}$ is prime.

Define $A := k[X_1,\dots,X_n]/\mathfrak{p}$ an integral domain and $k(x) = k(x_1,\dots,x_n) := \operatorname{Frac}(A)$.

Let $z_1,\dots,z_d$ be a transcendence basis for $k(x)$. Then $k(x)/k(z_1,\dots,z_d)$ is algebraic and therefore there exist polynomials $g_{ij} \in k[Z_1,\dots,Z_d]$ such that

$$g_{im}(z)x_i^m + \dots g_{i0} \quad = \quad 0 \tag{3.5}$$

(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 $i = 1 \dots n$. Then evaluation gives a homomorphism

$$\phi : k[z_1,\dots,z_d] \to k[\bar{z}_1,\dots,\bar{z}_d] \subset \bar{k}$$

This extends to a place $\tilde{\phi}$ of $k(x)$ by (3.19.7). 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

$$\tilde{\phi} : k[x_1,\dots,x_n] \to \bar{k}$$

which yields a zero of $\mathfrak{p}$ by (3.24.16) as required. □

3.24.3 Krull Dimension of Affine Algebra

The Krull Dimension of affine domains is particularly well-behaved. Specifically they are biequidimensional and therefore satisfy a co-dimension formula (3.24.27). Further there's a geometric proof of the "Hauptidealsatz" (3.24.24). We first show that it is equal to transcendence degree in the integral case.

Proposition 3.24.21
Let A be an affine algebra with normalising family $x_1, \dots, x_n$, then $\dim A = n$.

In particular every affine domain A satisfies $\dim A = \operatorname{trdeg}_k(A)$, and the polynomial ring $k[X_1, \dots, X_n]$ has dimension n.

Proof. By definition A is integral over $k[x_1, \dots, x_n]$, which is isomorphic to a polynomial ring so we may reduce to the case of polynomial ring by (3.21.6).

$\dim A \geq n$). This is clear by considering the chain of prime ideals

$$(X_1) \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, \dots, X_n)$$

$\dim A \leq n$). We may argue by the Strong Normalisation Lemma (3.24.9) and the subsequent remark that any chain of prime ideals must have length at most n, as any normalising family has order n.

Alternatively we may proceed by induction on n to show $\dim k[X_1, \dots, X_n] = n$. Consider a maximal chain

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_m$$

Clearly $\mathfrak{q}_0 = 0$, and $\mathfrak{q}_1 = (f)$ principal by (3.21.8). By (3.24.6) there is an integral, injective map

$$k[Y_1, \dots, Y_{n-1}] \hookrightarrow k[X_1, \dots, X_n]/(f)$$

whence $\dim(\mathfrak{q}_1) = \dim(k[X_1, \dots, X_n]/(f)) = \dim(k[Y_1, \dots, Y_{n-1}]) = n - 1$, and by definition $m - 1 \leq n - 1$. As the maximal chain was arbitrarily chosen, we have $\dim k[X_1, \dots, X_n] \leq n$. The reverse inequality was already shown so we are done.

The final statement follows from the existence of a normalising family (3.24.8) and (3.24.4)

□

Corollary 3.24.22
The ideal $(X_1, \dots, X_r) \triangleleft k[X_1, \dots, X_n]$ has dimension $n - r$.

Corollary 3.24.23
Let A be an integral finitely-generated k-algebra and $0 \neq f$ then $\dim A = \dim A_f$

The following proof is due to Tate, and presented in the Red Book [Mum99, I.7 Theorem 2].

Proposition 3.24.24 (Hypersurface has pure codimension 1)
Let A be an affine domain of dimension n and $0 \neq f \in A$. Then

$$\dim((f)) = n - 1$$
$$\operatorname{ht}((f)) = 1$$

More precisely if $\mathfrak{p}$ is minimal over (f) then it has dimension $n - 1$ and height 1.

Proof. Consider the case $A = k[X_1, \dots, X_n]$. Suppose first that f is prime, then $\mathfrak{p} = (f)$ and by (3.24.6) there is an integral injective map

$$k[Y_1, \dots, Y_{n-1}] \hookrightarrow A/(f)$$

Therefore

$$\dim((f)) = \dim(A/(f)) \overset{(3.21.6)}{=} \dim(k[Y_1, \dots, Y_{n-1}]) \overset{(3.24.21)}{=} n - 1$$

When f is not prime then, as $k[X_1, \dots, X_n]$ is a UFD, we have a prime factorisation

$$f = \prod_{i=1}^{n} f_i^{m_i}$$

and the minimal prime decomposition is

$$\sqrt{(f)} = (f_1) \cap \ldots \cap (f_n)$$

In particular any prime minimal over (f) has the form $\mathfrak{p} = (f_i)$ for some i, and we may reduce to the case of f prime.

For an arbitrary k-algebra A we have a decomposition into minimal primes of (f)

$$\sqrt{(f)} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$$

and without loss of generality $\mathfrak{p} = \mathfrak{p}_1$. We may localize to the case of a single prime, for choose $g \notin \mathfrak{p}$ and $g \in \mathfrak{p}_i$ for $i = 2 \ldots n$. Consider the localization $A \to A_g$, then we claim that

$$\sqrt{(f/1)} = \mathfrak{p}A_g$$

For by (3.6.18) there is a correspondence between primes of A_g containing $(f/1)$ and primes of A containing f and not g, which are precisely the primes containing $\mathfrak{p}$ by (3.4.39) or (3.4.43). Therefore $\mathfrak{p}A_g$ is the only minimal prime of A_g containing $(f/1)$ and the claim follows from (3.4.45).

Note that $\dim A = \dim A_g$ as they have the same field of fractions and therefore transcendence degree. Similarly $\dim(A/\mathfrak{p}) = \dim((A/\mathfrak{p})_{\bar{g}}) = \dim(A_g/\mathfrak{p}_g) = \dim(\mathfrak{p}A_g)$. So we may assume without loss of generality that $n = 1$ and $\mathfrak{p} = \sqrt{(f)}$.

By (3.24.8) there is an integral, injective map

$$\phi : B \hookrightarrow A$$

where $B = k[X_1, \ldots, X_n]$, which induces an algebraic field extension

$$K := \mathrm{Frac}(B) \hookrightarrow \mathrm{Frac}(A) =: L$$

We claim that there exists $f_0 \in B$ such that

$$\phi^{-1}(\sqrt{f}) = \sqrt{(f_0)}$$

Observe that in this case $\sqrt{(f_0)}$ is prime and therefore the unique minimal prime over (f_0). Therefore the result would follow from the first part and (3.21.7). Firstly for any $g \in A$ we have (...)

$$\mathrm{Norm}_{L/K}(g) \in B \cap \phi^{-1}((g))$$

Define $f_0 := \mathrm{Norm}_{L/K}(f)$ then we see that $f_0 \in \phi^{-1}((f)) \implies \sqrt{(f_0)} \subseteq \phi^{-1}(\sqrt{(f)})$. Conversely if $\phi(g)^n = hf$ then $g^{n[L:K]} = \mathrm{Norm}(\phi(g)^n) = \mathrm{Norm}(h)f_0 \in (f_0) \implies g \in \sqrt{(f_0)}$. Therefore the reverse inclusion holds.

Finally by the codimension 1 formula (3.21.11) we have $\mathrm{ht}((f)) = 1$. □

Remark 3.24.25
The argument is slightly less awkward in geometric language. Decompose into irreducibles

$$V(f) = Z_1 \cup \ldots \cup Z_n$$

choose a principal open affine $D(g)$ which meets only Z_1 then $Z_1 \cap D(g) = V(f) \cap D(g) = V(f/1)$ is an irreducible component of $D(g)$. We argue that $\dim(X) = \dim(D(g))$ and $\dim(Z_1) = \dim(D(g) \cap Z_1)$. Further construct finite coverings

$$V(f/1) \to V(f_0) \to H$$

onto a hyperplane in $\mathbb{A}^n$.

This allows is to prove a converse to (3.21.11)

Corollary 3.24.26 (Height 1 formula)
Let A be an affine domain. Then for a prime ideal $\mathfrak{p}$

$$\mathrm{ht}(\mathfrak{p}) = 1 \implies \dim(\mathfrak{p}) = \dim(A) - 1$$

More generally if A is an affine algebra and $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ is a saturated chain of prime ideals then

$$\dim(\mathfrak{p}_2) = \dim(\mathfrak{p}_1) - 1$$

Proof. Choose $0 \neq f \in \mathfrak{p}$ then it follows from the previous result (3.24.24). Alternatively by (3.24.8) there is an integral injective map

$$\phi : k[X_1, \ldots, X_n] \hookrightarrow A$$

with $\mathfrak{q} := \phi^{-1}(\mathfrak{p})$ and $n = \dim A$. Then by Going Down we have $\operatorname{ht}(\mathfrak{q}) = 1$. By (3.21.8) $\mathfrak{q}$ is principal and by (3.24.6) there is an integral injective map

$$k[Y_1, \ldots, Y_{n-1}] \hookrightarrow k[X_1, \ldots, X_n]/\mathfrak{q}$$

therefore $\dim(\mathfrak{q}) = n - 1$. By (3.21.7) this equals $\dim(\mathfrak{p})$ and we are done.

For the second statement we may consider the affine domain $A/\mathfrak{p}_1$ and observe that $\operatorname{ht}(\mathfrak{p}_2/\mathfrak{p}_1) = 1$. Therefore

$$\dim(\mathfrak{p}_2) = \dim(\mathfrak{p}_2/\mathfrak{p}_1) = \dim(A/\mathfrak{p}_1) - 1 = \dim(\mathfrak{p}_1) - 1$$

□

Corollary 3.24.27 (Biequidimensionality)
*Let A be an affine algebra. Then it is **quasi-biequidimensional** and satisfies the **codimension formulae** for $\mathfrak{p} \subset \mathfrak{a}$*

$$\begin{aligned} \dim A &= \dim \mathfrak{a} + \operatorname{ht}(\mathfrak{a}) \\ \dim \mathfrak{a} &= \dim \mathfrak{p} + \operatorname{ht}(\mathfrak{a}/\mathfrak{p}) \\ \operatorname{ht}(\mathfrak{a}) &= \operatorname{ht}(\mathfrak{a}/\mathfrak{p}) + \operatorname{ht}(\mathfrak{p}) \end{aligned}$$

In particular for every prime ideal $\mathfrak{p}$ we have

$$\dim A = \dim A_{\mathfrak{p}} + \dim A/\mathfrak{p}$$

and for every maximal ideal

$$\dim A = \dim A_{\mathfrak{m}}$$

Proof. By (3.24.26) A satisfies the criteria in (3.21.13).e) and so is quasi-biequidimensional. The codimension formulas follow from (3.21.15). □

We may also consider the following result

Proposition 3.24.28 (Generalized Hauptidealsatz for Affine Algebras)
Let A be an affine algebra and $\mathfrak{p}$ a prime ideal. Then

a) *If $\operatorname{ht}(\mathfrak{p}) = n$ then it is minimal over some ideal $\mathfrak{a} := (x_1, \ldots, x_n)$. Furthermore $\mathfrak{a}$ may be chosen such that $\operatorname{ht}(\mathfrak{a}) = n$ and every minimal prime is of height n*

b) *We have the following characterization of height of a prime ideal*

$$\operatorname{ht}(\mathfrak{p}) = \min\{n \mid \mathfrak{p} \text{ minimal over } (x_1, \ldots, x_n)\}$$

In particular if $\mathfrak{p}$ is minimal over $(x_1, \ldots, x_n)$ then $\operatorname{ht}(\mathfrak{p}) \leq n$.

Furthermore the same result holds for localization of A at any prime ideal.

Proof. This is largely restatement of results in Section 3.22. By (3.24.24) we have $A/\mathfrak{p}$ is hauptidealsatz for every prime ideal $\mathfrak{p}$. Furthermore by (3.24.27) A is quasi-biequidimensional and so catenary (3.21.13). Then by (3.22.4) this means A is a generalized hauptidealsatz ring (and so is every localization $A_{\mathfrak{p}}$).

Then *a*) and *b*) follows from (3.22.12). □

Corollary 3.24.29
Let A be an affine algebra and $\mathfrak{p}$ a prime ideal. Denote the unique maximal ideal of $A_{\mathfrak{p}}$ by $\mathfrak{m} := \mathfrak{p}A_{\mathfrak{p}}$. Then

$$\dim A_{\mathfrak{p}} = \min\{n \mid \sqrt{(x_1, \ldots, x_n)} = \mathfrak{m}\} \leq \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$$

with equality iff $A_{\mathfrak{p}}$ is a regular local ring.

Proof. By (3.24.28) $A_{\mathfrak{p}}$ is a Noetherian local ring satisfying the generalized hauptidealsatz. Therefore the result follows by (3.23.2). □

3.24.3.1 ** Biequidimensionality by Strong Normalisation **

We may prove more directly the biequidimensionality property by using the strong form of the Normalisation Lemma (3.24.9) and Going Down (3.18.16). First we prove a technical result

Lemma 3.24.30 (Saturated pairs)
Let $\phi : B \to A$ be an integral map and $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ prime ideals lieing over $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$. Then

a) $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ *saturated* $\implies$ $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ *saturated.*

b) $B/\mathfrak{q}_0$ *integrally closed and* $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ *saturated* $\implies$ $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ *saturated*

We may relax the condition in b) to the existence of another integral map $\psi : C \to B$ such that $C/\psi^{-1}(\mathfrak{q}_0)$ is integrally closed.

Proof. The first follows by incomparability (3.18.14). The second follows by applying Going Down (3.18.16) to the integral map $B/\mathfrak{q}_0 \hookrightarrow A/\mathfrak{p}_0$. More precisely if $\mathfrak{q}_0 \subsetneq \mathfrak{q} \subsetneq \mathfrak{q}_1$ then $(0) \subsetneq \mathfrak{q}/\mathfrak{q}_0 \subsetneq \mathfrak{q}_1/\mathfrak{q}_0$ whence there exists $\mathfrak{p}$ such that $(0) \subsetneq \mathfrak{p}/\mathfrak{p}_0 \subsetneq \mathfrak{p}_1/\mathfrak{p}_0$. This means $\mathfrak{p}_0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_1$, a contradiction.

The final statement can be demonstrated by applying b) to $C \to A$ and then a) to $B \to A$. □

Proposition 3.24.31
*Let A be an affine domain, then every maximal chain has order $n = \dim A$, i.e. A is **irreducible** and **biequidimensional**.*

Proof of (3.24.31). Consider a maximal chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_m$. Clearly $\mathfrak{p}_m$ is maximal by (3.4.36), and as A is integral $\mathfrak{p}_0 = 0$. Apply (3.24.9) to find an integral, injective map

$$\phi : k[X_1, \ldots, X_n] \hookrightarrow A$$

such that

$$\mathfrak{q}_i := \phi^{-1}(\mathfrak{p}_i) = (X_1, \ldots, X_{h(i)}) \quad 0 \leq i \leq m$$

Note $n = \dim A$ by (3.24.21). Clearly $h(0) = 0$ and by (3.18.13) $\mathfrak{q}_m$ is maximal so $h(m) = n$. Observe that

$$k[X_1, \ldots, X_n]/\mathfrak{q}_i \xrightarrow{\sim} k[X_{h(i)+1}, \ldots, X_n]$$

is integrally closed for all i (3.18.9). Therefore we may apply (3.24.30) to ϕ and each pair $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$, to see that each chain $\mathfrak{q}_i \subsetneq \mathfrak{q}_{i+1}$ is saturated. This can only happen if $h(j) = j$ and therefore $m = n$. □

3.24.4 Derivations of Affine Algebras

The notion of derivations is a useful as a coordinate-free construction of the "tangent space" for both differentiable manifolds and algebraic varieties. We review the theory of derivations here primarily focusing on fields and f.g. k-algebras.

Proposition 3.24.32 (Derivations of Polynomial Algebra)
Let $A = k[X_1, \ldots, X_n]$ be a polynomial algebra and M an (A, B)-bimodule. Then we have an (A, B)-bimodule isomorphism

$$\begin{aligned} \mathrm{Der}_k(A, M) &\cong M^n \\ D &\to (D(X_1), \ldots, D(X_n)) \\ \sum_{i=1}^{n} \frac{\partial}{\partial X_i} \cdot v_i &\leftarrow v \end{aligned}$$

When M has a B-basis $\{m_1, \ldots, m_r\}$ then $\mathrm{Der}_k(A, M)$ also has a B-basis

$$\left\{ \frac{\partial}{\partial X_i} \cdot m_j \right\}_{i=1\ldots n, j=1\ldots r}$$

In particular $\dim_K \mathrm{Der}_k(A, K) = n$.

Proof. The first map is clearly well-defined and by (...) injective. The inverse map is well-defined because we have shown $\frac{\partial}{\partial X_i} \in \mathrm{Der}_k(A, A)$. The chain rule (3.20.8) shows that the maps are mutually inverse (the other direction following simply from orthogonality of the partial derivatives).

The final statement is straightforward. □

We may generalise this as follows, so that we may interpret derivations as tangent vectors

Proposition 3.24.33 (Derivations = Tangent Vectors)
Let $A = k[X_1, \dots, X_n]/\mathfrak{a}$ be a f.g. k-algebra and M an A-module. Then we have an A-module isomorphism

$$\begin{array}{rcl} \mathrm{Der}_k(A, M) & \cong & \left\{ v \in M^n \mid \sum_{i=1}^n \overline{\frac{\partial F}{\partial X_i}} v_i = 0 \quad \forall F \in \mathfrak{a} \right\} \subset M^n \\ D & \longrightarrow & (D(\overline{X}_1), \dots, D(\overline{X}_n)) \\ \sum_{i=1}^n \overline{\frac{\partial}{\partial X_i}} \cdot v_i & \longleftarrow & v \end{array}$$

If $\mathfrak{a} = \langle F_1, \dots, F_m \rangle$ then this is equal to the kernel of the A-module homomorphism

$$\begin{pmatrix} \overline{\frac{\partial F_1}{\partial X_1}} & \cdots & \overline{\frac{\partial F_1}{\partial X_n}} \\ \vdots & \ddots & \vdots \\ \overline{\frac{\partial F_m}{\partial X_1}} & \cdots & \overline{\frac{\partial F_m}{\partial X_n}} \end{pmatrix} : M^n \to M^m$$

When M is an (A, B)-bimodule then this is also an (A, B)-bimodule isomorphism.

Proof. According to (3.20.8) we have the following relationship for all $F \in k[X_1, \dots, X_n]$

$$D(\overline{F}) = D(F(\overline{X}_1, \dots, \overline{X}_n)) = \sum_{i=1}^n \frac{\partial F}{\partial X_i}(\overline{X}_i) D(\overline{X}_i) = \sum_{i=1}^n \overline{\frac{\partial F}{\partial X_i}} D(\overline{X}_i)$$

When $F \in \mathfrak{a}$ we have $\overline{F} = 0 \implies D(\overline{F}) = 0$, whence the first map is well-defined. Similarly for $v \in RHS$ we see by definition that

$$\sum_{i=1}^n \overline{\frac{\partial}{\partial X_i}} \cdot v_i$$

is zero on $\mathfrak{a}$, so determines a well-defined derivation on A. In the same way we see that the maps are mutually inverse.

Suppose v is in the kernel of the given matrix. For any $G \in \mathfrak{a}$ we have by hypothesis $G = \sum_{j=1}^m F_j H_j$ for some $H_j \in k[X_1, \dots, X_n]$. Then

$$\begin{array}{rcl} \sum_{i=1}^n \overline{\frac{\partial G}{\partial X_i}} v_i & = & \sum_{i=1}^n \sum_{j=1}^m \left(\overline{F_j} \overline{\frac{\partial H_j}{\partial X_j}} + \overline{H_j} \overline{\frac{\partial F_j}{\partial X_j}} \right) v_i \\ & = & \sum_{j=1}^m \sum_{i=1}^n \overline{\frac{\partial F_j}{\partial X_i}} v_i \\ & = & 0 \end{array}$$

where we have used the fact that $\overline{F_j} = 0$. As G was arbitrary this shows v is in the right-hand side of the isomorphism, and the reverse inclusion is immediate as $F_j \in \mathfrak{a}$. □

Proposition 3.24.34 (Lifting for separable algebraic extensions)
Let L/K be a separable algebraic extension (over k) and V an L-module. Then there is an isomorphism of L-modules

$$\begin{array}{rcl} \mathrm{Der}_k(L, V) & \xrightarrow{\sim} & \mathrm{Der}_k(K, V) \\ D & \to & D|_K \end{array}$$

Namely there is a unique extension from K to L.

Proof. Consider $L[V]$ the k-algebra with ideal $N := 0 \times V$ such that $N^2 = 0$ and $L[V]/N \cong L$. Furthermore a derivation $D : K \to V$ corresponds to a unique k-algebra homomorphism $\phi_D : K \to K[V] \hookrightarrow L[V]$ by (3.20.5) so we have the following commutative diagram

$$\begin{array}{ccc} K & \xrightarrow{\phi_D} & L[V] \\ \downarrow & \nearrow & \downarrow \pi_1 \\ L & = & L \end{array}$$

By (3.20.15) there is a unique homomorphism $\phi_{\hat{D}} : L \to L[V]$ completing the diagram, and in particular by (3.20.5) there is a derivation $\widetilde{D} : L \to V$ extending D. Uniqueness follows from that of $\phi_{\hat{D}}$. □

Corollary 3.24.35
Let K/k be a separable algebraic extension, A a K-algebra and M an A-module then

$$\mathrm{Der}_k(A, M) = \mathrm{Der}_K(A, M)$$

Proof. Recall that a derivation D is K-linear iff it vanishes on K. So we may reduce to the case $A = K$ by considering the restriction $D|_K$.

Therefore it's sufficient to show that $\mathrm{Der}_k(K, M) = \mathrm{Der}_K(K, M) = 0 = \mathrm{Der}_k(k, M)$, but this follows immediately from (3.24.34). □

Proposition 3.24.36
*Let A be an f.g. integral k-algebra and $K = \mathrm{Frac}(A)$. Suppose K/k is **separably generated** (e.g. if k is perfect) then we have equality*

$$\mathrm{trdeg}_k(K) = \dim_K \mathrm{Der}_k(K)$$

Proof. By hypothesis we have a transcendence basis $\eta_1, \ldots, \eta_n$ such that $n = \mathrm{trdeg}_k(K)$ and $K/k(\eta_1, \ldots, \eta_n)$ is algebraic and separable.

Therefore we have

$$\mathrm{Der}_k(K) \overset{(3.24.34)}{\cong} \mathrm{Der}_k(k(\eta_1, \ldots, \eta_n), K) \overset{(3.20.9)}{\cong} \mathrm{Der}_k(k[\eta_1, \ldots, \eta_n], K)$$

which then has dimension n by (3.24.32). □

Proposition 3.24.37 (Tangent space is dual to Cotangent space)
Let A be a k-algebra and $\mathfrak{m} \lhd A$ a maximal ideal with residue field $k(\mathfrak{m}) := A/\mathfrak{m}$. There is a homomorphism of $k(\mathfrak{m})$-modules

$$\begin{array}{rcl} \mathrm{Der}_k(A, k(\mathfrak{m})) & \longrightarrow & \mathrm{Hom}_{k(\mathfrak{m})}\left(\mathfrak{m}/\mathfrak{m}^2, k(\mathfrak{m})\right) \\ D & \longrightarrow & \theta_D : \bar{x} \to D(x) \end{array}$$

When $k(\mathfrak{m})/k$ is separable algebraic *then this is an isomorphism. In particular this holds when k is perfect and $k(\mathfrak{m})/k$ is finite (or even finitely-generated by Zariski's Lemma (3.24.19)).*

Proof. The map θ_D is well-defined because D annihilates $\mathfrak{m}^2$ by the product rule.

We claim we can reduce to the case $\mathfrak{m}^2 = 0$. For consider $A' := A/\mathfrak{m}^2$ and $\mathfrak{m}' = \mathfrak{m}/\mathfrak{m}^2$ and the commutative diagram

$$\begin{array}{ccc} \mathrm{Der}_k(A', k(\mathfrak{m}')) & \longrightarrow & \mathrm{Hom}_{k(\mathfrak{m}')}(\mathfrak{m}', k(\mathfrak{m}')) \\ \downarrow \sim & & \downarrow \sim \\ \mathrm{Der}_k(A, k(\mathfrak{m})) & \longrightarrow & \mathrm{Hom}_{k(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2, k(\mathfrak{m})) \end{array}$$

The horizontal maps have already been defined, and we claim that the vertical maps are canonical isomorphisms. The right hand isomorphism is induced by the isomorphism $k(\mathfrak{m}) \cong k(\mathfrak{m}')$ (3.4.55) and the corresponding module isomorphism $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{m}'/(\mathfrak{m}')^2$. The left hand isomorphism is simply composition with the projection $A \to A'$. It is surjective because every derivation D on A annihilates $\mathfrak{m}^2$ and therefore may be lifted to a derivation on A'.

We revert to the original notation, but with the additional assumption that $\mathfrak{m}^2 = 0$. By (3.20.16) there is a map $j : k(\mathfrak{m}) \to A$ such that $\pi \circ j$ is the identity, where $\pi : A \to A/\mathfrak{m} = k(\mathfrak{m})$ is the canonical projection. In other words there is a subfield $k \subseteq \hat{k} \subseteq A$ such that $\hat{k} \cong k(\mathfrak{m})$ under π. In particular $\hat{k}/k$ is finite and separable so by (3.24.35) we see that a derivation is k-linear if and only if it is $\hat{k}$-linear. Therefore we may without loss of generality consider only derivations which are $\hat{k}$-linear. As j is a section of π we have a direct sum of k-vector spaces

$$A = \mathrm{Im}(j) \oplus \ker(\pi) = \hat{k} \oplus \mathfrak{m}$$

Given $\theta \in \mathrm{Hom}_{k(\mathfrak{m})}(\mathfrak{m}, k(\mathfrak{m}))$ define

$$D_\theta(\lambda + x) := \theta(x) \quad \lambda \in \hat{k},\ x \in \mathfrak{m}$$

It satisfies the product rule for

$$\begin{aligned} D_\theta((\lambda + x)(\lambda' + x')) &= \theta(\lambda' x + \lambda x') \\ &= \pi(\lambda')\theta(x) + \pi(\lambda)\theta(x') \end{aligned}$$

Note that $\pi(x')\theta(x) = \theta(x'x) = \theta(0) = 0$. So we find that D_θ satisfies the product rule and the map is surjective.

As $k(\mathfrak{m})/k$ is separable then by (3.24.35) any derivation D is $\hat{k}$-linear. Therefore

$$D(\lambda + x) = D|_{\mathfrak{m}}(x) \quad \lambda \in \hat{k}\,, x \in \mathfrak{m}$$

which shows that the given map is injective. □

Remark 3.24.38
The proof is substantially simpler when $k(\mathfrak{m}) = k$, for example when k is algebraically closed.

The argument follows the suggestion of [Har13, Ex 8.1], but using the simpler result [Mat70, Prop 28.I] to argue more directly.

3.24.5 Linearly Disjoint Algebras

Definition 3.24.39
*Let A/k, B/k be (integral) subalgebras of a field extension Ω/k. Then we say that they are **linearly disjoint in** Ω/k if the canonical map*

$$A \otimes_k B \to \Omega$$

is injective. Observe this implies that $A \otimes_k B$ is an integral domain.

Recall that every k-module is free (3.4.133), moreover by (3.5.22) a basis of $A \otimes_k B$ may be formed by tensor product of bases for A and B.

Example 3.24.40
Let K/k be a non-trivial field extension then K is not linearly disjoint with itself. For $1, x$ a linearly independent subset of K and may be extended to a basis. Given the remark on the basis of the tensor product we see $1 \otimes x \neq x \otimes 1$. On the other hand the image of $1 \otimes x - x \otimes 1$ in Ω is clearly 0. The same consideration shows that $A \cap B = k$.

Remark 3.24.41
The notion of linear disjointness in general depends on the embeddings in Ω/k. For example $k(t)$ and $k(s)$ are linearly disjoint in $k(s,t)$, but not when both are identified with $k(x)$.

Proposition 3.24.42
Let A/k, B/k be algebras of Ω/k. Then the following are equivalent

a) A/k and B/k are linearly disjoint in Ω/k

b) Every $S \subset A$ which is linearly independent over k is linearly independent over B

b') Every $T \subset B$ which is linearly independent over k is linearly independent over A

c) There is a k-basis $\{a_\lambda\}_{\lambda \in \Lambda}$ which is linearly independent over B

c') There is a k-basis $\{b_\lambda\}_{\lambda \in \Lambda}$ which is linearly independent over A

Proof. *a)* $\implies$ *b)* By (3.5.21) and (3.5.22) there is an injective map

$$\begin{aligned} B^{(S)} &\hookrightarrow A \otimes_k B \\ (b_s)_{s \in S} &\to \sum_{s \in S} s \otimes b_s \end{aligned}$$

By hypothesis the composite with $A \otimes_k B \hookrightarrow \Omega$ is injective which is precisely the required conclusion.

b) $\implies$ *c)* By (3.4.133) there exists a basis which by hypothesis is linearly independent over B

c) $\implies$ *a)* By (3.5.22) there is an isomorphism

$$B^{(\Lambda)} \cong A \otimes_k B$$

and the canonical map into Ω is identified with $(b_\lambda)_{\lambda \in \Lambda} \to \sum a_\lambda b_\lambda$. The hypothesis means precisely that this map is injective.

We immediately have the symmetric result *a)* $\iff$ *b')* $\iff$ *c')*. □

3.25 Affine Algebras under Base Change

This section covers what happens to a k-algebra A under base change, that is $A_{(L)}$ for L/k a field extension. Principally given an integral k-algebra A we would like to ensure that $A_{(L)}$ is reduced (which is related to separability), irreducible and therefore integral. We follow terminology of [Sta15], but exposition of [Bou89]. For some cases we introduce assumptions which whilst not strictly required substantially simplify the exposition. Further these assumptions will be satisfied in subsequent applications.

Definition 3.25.1 (Geometrically Reduced / Integral Algebra)
A k-algebra A is

- ***geometrically integral*** *(resp.* ***irreducible***, ***reduced****) if the ring $A_{(L)}$ is* ***integral*** *(resp.* ***irreducible***, ***reduced****) for every field extension L/k.*
- ***algebraically integral*** *(resp.* ***irreducible***, ***reduced****) if the ring $A_{(k')}$ is* ***integral*** *(resp.* ***irreducible***, ***reduced****) for every* algebraic *field extension k'/k.*

As in (3.4.61) we see that ***integral*** $\iff$ ***irreducible*** *and* ***reduced****.*

An algebraically integral field extension K/k is sometimes referred to as ***regular*** *[Bou89] [Lan11].*

In [Bou89] a geometrically reduced algebra is referred to as a separable algebra, and [LE06] calls "geometrically" what we refer to as "algebraically".

3.25.1 Etale Algebras

Etale is equivalent to geometrically reduced in the finite-dimensional case. When k is perfect then we show this is equivalent to simply being reduced.

Definition 3.25.2 (Separable Degree)
Let A be a finite-dimensional k-algebra. Then define the ***separable degree*** *as follows*

$$[A : k]_s := \#\operatorname{AlgHom}_k(A, \bar{k})$$

We say that A is ***etale*** *if this equals the dimension of A as a k-vector space*

$$[A : k]_s = [A : k]$$

Recall a finite field extension K/k is ***etale*** *if and only if it is separable (3.14.84).*

This is different to the usual definition but makes the exposition simpler.

Definition 3.25.3 (Diagonalizable)
A k-algebra A is ***diagonalized*** *by K/k if there is an isomorphism of K-algebras*

$$A_{(K)} \cong K^n$$

for some $n \geq 1$

We prove some elementary properties of finite algebras, namely that the set of algebra homomorphisms is always finite and bounded above by the separable degree. Furthermore we may replace $\bar{k}$ by some finite subextension.

Lemma 3.25.4
Let A be a finite-dimensional k-algebra and K/k a field extension. Then

$$[\operatorname{Hom}_k(A, K) : K] = [A^\vee : k] = [A : k]$$

More precisely if $\{a_1, \ldots, a_n\}$ is a k-basis for A then $\{a_1^\vee, \ldots, a_n^\vee\}$ is a K-basis for $\operatorname{Hom}_k(A, K)$.

Proof. This is simply a special case of (3.5.25). □

Lemma 3.25.5 (Dedekind's Lemma)
Let K/k be a field extension and A a k-algebra. The set of k-algebra homomorphisms

$$\operatorname{AlgHom}_k(A, K)$$

is K-linearly independent as a subset of $\operatorname{Hom}_k(A, K)$.

Proof. Suppose that the k-algebra homomorphisms are not linearly independent. Then choose a minimal subset of distinct k-algebra homomorphisms $\phi_1, \ldots, \phi_n$ with a non-trival relationship over K

$$\sum_{i=1}^{n} \lambda_i \phi_i = 0 \quad \lambda_i \in K^\star$$

If $n = 1$ then $\phi_1 = 0$ which is a contradiction. Suppose without loss of generality that $n > 1$. For a given $x \in K$ we may define

$$\widehat{\phi_i} := (\phi_i(x) - \phi_n(x))\, \phi_i \quad i = 1 \ldots n-1$$

We may choose x such that at least one is non-zero. Then for all $y \in A$ we have

$$\sum_{i=1}^{n-1} \lambda_i \widehat{\phi_i}(y) = \sum_{i=1}^{n} \lambda_i \left(\phi_i(x) - \phi_n(x)\right) \phi_i(y) = \sum_{i=1}^{n} \lambda_i \phi_i(xy) - \phi_n(x) \sum_{i=1}^{n} \lambda_i \phi_i(y) = 0$$

This contradicts minimality of the subset. □

Corollary 3.25.6 (Separable degree is finite)
Let A be a finite-dimensional k-algebra then $\#\operatorname{AlgHom}_k(A, K) \leq [A : k]$ for every field extension K/k.

Proposition 3.25.7 (Image of A is finite-dimensional)
Let A be a finite-dimensional k-algebra and Ω/k a field extension. Then there exists a finite subextension K/k such that

$$\operatorname{AlgHom}_k(A, K) = \operatorname{AlgHom}_k(A, \Omega)$$

If Ω contains $\bar{k}$ then these are both equal to $\operatorname{AlgHom}_k(A, \bar{k})$.

Proof. By (...) $\phi(A)$ has finite degree over k and therefore finitely-generated and algebraic as a k-algebra. Therefore $\phi(A) = k[a_1, \ldots, a_n] = k(a_1, \ldots, a_n)$ is a finite-dimensional field by (3.14.51).

We may take the compositum of all these images (since there are only finitely many) to obtain the finite extension K/k.

If Ω contains $\bar{k}$ then trivially

$$\operatorname{AlgHom}_k(A, K) \subseteq \operatorname{AlgHom}_k(A, \bar{k}) \subseteq \operatorname{AlgHom}_k(A, \Omega)$$

whence they are all equal. □

Proposition 3.25.8 (Etale-ness is preserved under base extension)
Let A be a finite-dimensional k-algebra and K/k a field extension then

$$\begin{aligned} [A_{(K)} : K] &= [A : k] \\ [A_{(K)} : K]_s &= [A : k]_s \end{aligned}$$

In particular A is etale if and only if $A_{(K)}$ is.

Proof. The first equality follows from (3.5.24) and (3.4.101).

For the second equality we see that by (3.25.7) and (3.5.31)

$$\operatorname{AlgHom}_k(A, \bar{k}) = \operatorname{AlgHom}_k(A, \bar{K}) \cong \operatorname{AlgHom}_K(A_{(K)}, \bar{K})$$

□

Lemma 3.25.9
Let A be a k-algebra of finite degree. Then the following are equivalent

a) $A \cong k^n$

b) $\operatorname{AlgHom}_k(A, k)$ *spans* $A^\vee$

c) $\operatorname{AlgHom}_k(A, k)$ *is a basis for* $A^\vee$

d) $\#\operatorname{AlgHom}_k(A, k) = [A^\vee : k] = [A : k]$

Proof. Clearly $c) \implies b), d)$. By (3.25.5) $b) \implies c)$ and by (3.4.134) $d) \implies c)$. Suppose $a)$ then considering the projection maps, $\#\operatorname{AlgHom}_k(A, k) \geq n = [A : k]$ whence combining with (3.25.6) yields $d)$.

It remains to show that $c) \implies a)$. Let $e_1^\vee, \ldots e_n^\vee$ be a basis for $A^\vee$ which are k-algebra homomorphisms. Then it corresponds by (3.4.101) to a basis $e_1, \ldots, e_n$ of A, and therefore induces an isomorphism of vector spaces

$$\begin{aligned} A &\cong k^n \\ v &\to (e_i^\vee(v))_{i=1\ldots n} \end{aligned}$$

which is also a k-algebra isomorphism by assumption. □

Proposition 3.25.10 (Diagonalization Criteria)
Let A be a finite-dimensional k-algebra and K/k an extension. Then we have

$$\#\operatorname{AlgHom}_k(A,K) \leq [A:k]$$

with equality if and only if A is diagonalised by K/k.

Proof. The inequality was shown in (3.25.6). By (3.5.16) and (3.5.31) there is a commutative diagram

$$\begin{array}{ccc} \operatorname{Hom}_k(A,K) & \xrightarrow{\sim} & \operatorname{Hom}_K(A_{(K)},K) = A_{(K)}^\vee \\ \cup & & \cup \\ \operatorname{AlgHom}_k(A,K) & \xrightarrow{\sim} & \operatorname{AlgHom}_K(A_{(K)},K) \end{array}$$

The top row is a K-vector space isomorphism and so the hom-sets have the same dimension over K, namely $[A^\vee : k]$ by (3.25.4). The lower map is bijective and so $\#\operatorname{AlgHom}_k(A,K) = \#\operatorname{AlgHom}_K(A_{(K)},K)$. By (3.25.9) K/k diagonalizes $A \iff \#\operatorname{AlgHom}_K(A_{(K)},K) = [A_{(K)}^\vee : K] \iff \#\operatorname{AlgHom}_k(A,K) = [A^\vee : k] = [A:k]$. This is the final statement of the proposition. □

Lemma 3.25.11
Let $A = A_1 \times \ldots \times A_d$ be a finite product of finite-dimensional k-algebras. Then A is etale if and only if each A_i is.

Proof. This follows because

$$\operatorname{AlgHom}_k(A_1 \times \ldots \times A_d, \bar{k}) \cong \operatorname{AlgHom}_k(A_1,\bar{k}) \times \ldots \times \operatorname{AlgHom}_k(A_d,\bar{k})$$

and a similar consideration for the dimension over k. □

Proposition 3.25.12 (Etale Criteria)
Let A be a finite-dimensional k-algebra. The following are equivalent

a) *A is diagonalized by some extension K/k*

b) *A is etale*

c) *A is geometrically reduced*

d) *A is algebraically reduced*

e) *$A_{(K)}$ is reduced for some perfect field extension K/k*

f) *$A \cong L_1 \times \ldots \times L_n$ for L_i/k finite separable extensions*

Proof. Recall from (3.25.10) that A is diagonalized by $K/k \iff \#\operatorname{AlgHom}_k(A,K) = [A:k] \iff \#\operatorname{AlgHom}_k(A,K) \geq [A:k]$

a) $\implies$ *b)* By (3.25.7) A is diagonalized by some finite extension k'/k, which implies it is diagonalized by $\bar{k}/k$ as $\#\operatorname{AlgHom}(k,\bar{k}) \geq \#\operatorname{AlgHom}_k(k,k')$.

b) $\implies$ *a)* is immediate as by the first observation A is diagonalized by $\bar{k}/k$.

b) $\implies$ *c)* Suppose L/k is a field extension and consider $\overline{L}/k$. Then by (...)

$$A \otimes_k \overline{L} \cong (A \otimes_k \bar{k}) \otimes_{\bar{k}} \overline{L} \cong \bar{k}^n \otimes_{\bar{k}} \overline{L} \cong \overline{L}^n$$

which is clearly reduced. By (....) $A \otimes_k L$ is a subring and therefore also reduced.

c) $\implies$ *d)* Immediate

d) $\implies$ *e)* Immediate as $\bar{k}$ is perfect.

e) $\implies$ *b)* By (3.25.14) we see $A_{(K)}$ is etale, and so by (3.25.8) A is etale.

b) $\implies$ *f)* By (3.25.14) as we know A is reduced.

f) $\implies$ *b)* Follows from (3.25.11). □

Corollary 3.25.13
Let A be a k-algebra and k perfect. Then the following are equivalent

a) *A is etale*

b) *A is finite-dimensional and geometrically reduced*

c) *A is finite-dimensional and reduced*

Note a) $\iff$ *b)* $\implies$ *c) holds in general and c)* $\implies$ *b) requires that k is perfect.*

This is a generalisation of the fact every finite extension of a perfect field is separable as proven in (3.14.97)) (and on which the proof of this statement relies).

We used the following technical result.

Lemma 3.25.14
Let A be a finite-dimensional k-algebra. The following are equivalent

a) *A is reduced*

b) $A \cong L_1 \times \ldots \times L_n$ *for some finite extensions* L_i/k

Further A is etale if and only if each L_i/k *is separable. If k is perfect then A is automatically etale.*

Proof. One direction is obvious. Suppose conversely that A is reduced. It is sufficient to show (by induction) that if A is not a field then $A \cong A_1 \times A_2$ for two (non-zero) k-algebras A_1, A_2.

Suppose A is not a field and let $\mathfrak{a}$ be a non-zero proper ideal of A which has minimal dimension over k as a vector space. As A is reduced, and by minimality, we have $\mathfrak{a}^2 = \mathfrak{a}$. By Nakayama's Lemma (3.16.5) there is $e \in \mathfrak{a}$ such that $ex = x$ for all $x \in \mathfrak{a}$ and in particular $e^2 = e$ and $\mathfrak{a} = Ae$. By assumption $e \neq 0, 1$. Define $f := 1 - e \neq 0, 1$ then evidently $f^2 = f$ and $ef = 0$. The homomorphism of A-modules

$$\begin{aligned} A &\to Ae \times Af \\ a &\to (ae, af) \end{aligned}$$

is injective because $ae + af = a$ and surjective because the image of $a_1e + a_2f$ is (a_1e, a_2f). The sub-modules Ae and Af are actually sub-rings by the idempotence property and the given map is an isomorphism of rings.

The last statement follows from (3.25.11) and (3.14.97). □

For completeness we summarize the relationship between the different notions of separability

Corollary 3.25.15 (Equivalent definitions of separability)
Let K/k be a finite extension. Then the following are equivalent

a) *K/k is separable algebraic (3.14.57)*

b) *K/k is etale*

c) *K/k is geometrically reduced*

Proof. We have already shown *b)* $\iff$ *c)*. Furthermore *a)* $\iff$ *b)* is (3.14.84). □

Corollary 3.25.16 (Equivalent definitions of separability)
Let K/k be an algebraic extension. Then the following are equivalent

a) *K/k is separable algebraic (3.14.57)*

b) *Every finite subextension of K/k is etale*

c) *K/k is geometrically reduced*

In particular an algebraic extension of a perfect field k is geometrically reduced.

Proof. We have shown *a)* $\iff$ *b)* in (3.14.87). For *c)* $\implies$ *b)* we recall that by (3.5.23) every subextension E may be embedded

$$E \otimes_k L \hookrightarrow K \otimes_k L$$

for all L and so every subextension is also separable. We may then use the equivalence already shown.

For *b)* $\implies$ *c)* observe that $K \otimes_k L$ is union of sub-rings of the form $E \otimes_k L$ for E/k finite (since K is). By the equivalence already shown $E \otimes_k L$ is reduced whence $K \otimes_k L$ is reduced as required.

The last statement follows from (3.14.97). □

3.25.2 Geometrically Reduced Algebras

The main results of this section are (3.25.18) and (3.25.20). First we require a technical result, which allows to reduce from an algebra to field by localizing at each prime ideal.

Lemma 3.25.17
Let A be a reduced k-algebra. Then the canonical map

$$i : A \hookrightarrow \prod_{\mathfrak{p}} k(\mathfrak{p})$$

is injective where $k(\mathfrak{p}) := \mathrm{Frac}(A/\mathfrak{p})$. Furthermore for any k-algebra B we have a canonical embedding

$$A \otimes_k B \hookrightarrow \prod_{\mathfrak{p}} (k(\mathfrak{p}) \otimes_k B)$$

Proof. Evidently $\ker(i) = \bigcap \mathfrak{p}$ which by (3.4.45) is (0). The final statement follows from considering the maps

$$A \otimes_k B \xrightarrow{i \otimes 1_B} \left(\prod_{\mathfrak{p}} k(\mathfrak{p}) \right) \otimes_k B \hookrightarrow \prod_{\mathfrak{p}} (k(\mathfrak{p}) \otimes_k B)$$

The first map is injective by (3.5.23) and the second by (...). □

Proposition 3.25.18
Let A be reduced k-algebra and B an geometrically reduced k-algebra, then $A \otimes_k B$ is reduced.

Proof. By the previous Lemma we have an embedding

$$A \hookrightarrow \prod (k(\mathfrak{p}) \otimes_k B)$$

As B is geometrically reduced this shows that $A \otimes_k B$ is reduced. □

Lemma 3.25.19
Let $K = k(\mathcal{B})$ be purely transcendental. Then K/k is geometrically reduced.

Proof. For L/k we have $k[\mathcal{B}] \otimes L \cong L[\mathcal{B}]$ is evidently reduced. We may then demonstrate directly that $k(\mathcal{B}) \otimes_k L$ is reduced. □

Proposition 3.25.20 (Reduced $\iff$ Geometrically Reduced)
Let A be a finitely-generated k-algebra and assume k is perfect. Then the following are equivalent

a) *A is reduced*

b) *A is algebraically reduced*

c) *A is geometrically reduced*

In particular every finitely-generated field extension K/k is geometrically reduced (c.f. (3.14.129)).

Proof. Clearly $b), c) \implies a)$ so we need only consider the converse. We first consider the case $A = K/k$ is a finitely generated extension, which is automatically reduced.

$b)$ An algebraic extension L/k over a perfect field is geometrically reduced (3.25.16) and therefore $K \otimes_k L$ is reduced.

$c)$ By (3.14.129) $K/k(\mathcal{B})$ is algebraic and separable for some transcendence base $\mathcal{B} = \{x_i\}_{i \in I}$. Then

$$K \otimes_k L \cong K \otimes_{k(\mathcal{B})} (k(\mathcal{B}) \otimes_k L)$$

By (3.25.19) $k(\mathcal{B}) \otimes_k L$ is reduced. As before $K/k(\mathcal{B})$ is geometrically reduced whence $K \otimes_k L$ is reduced by (3.25.18).

In the general case by (3.25.17) there is a canonical embedding

$$A \otimes_k L \hookrightarrow \prod_{\mathfrak{p}} (k(\mathfrak{p}) \otimes_k L)$$

By assumption $k(\mathfrak{p})$ is finitely generated and so by the first part is geometrically reduced. Therefore $A \otimes_k L$ is reduced and A is geometrically reduced as required. □

3.25.3 Geometrically Integral Algebras

Clearly a geometrically (resp. algebraically) integral algebra is integral, we are interested in providing sufficient conditions for the reverse implication.

Proposition 3.25.21
Let A be a geometrically integral k-algebra and B an integral k-algebra. Then $A \otimes_k B$ is an integral domain.

Proof. Let $L = \mathrm{Frac}(B)$ then $A \otimes_k B$ is a subring of $A \otimes_k L$ and we are done. □

Proposition 3.25.22 (Criteria for Geometrically Integral in terms of Fraction Field)
Let A be an integral k-algebra and $K := \mathrm{Frac}(A)$. Then $A \otimes_k L$ is integral if and only if $K \otimes_k L$ is integral.

In particular A is geometrically (resp. algebraically) integral if and only if K is geometrically (resp. algebraically) integral.

Proof. We observe that for any extension L/k we have an injective map $A \otimes_k L \hookrightarrow K \otimes_k L$. Therefore if $K \otimes_k L$ is integral so is $A \otimes_k L$.

Conversely suppose $A \otimes_k L$ is integral and define $\Omega := \mathrm{Frac}(A \otimes_k L)$. By the universal property there is a well-defined map $u : K \to \Omega$ and $v : L \to \Omega$, and therefore by (...) a well-defined ring homomorphism

$$\begin{aligned} K \otimes_k L &\to \Omega \\ ab^{-1} \otimes \lambda &\to (a \otimes \lambda) \cdot (b \otimes 1)^{-1} \end{aligned}$$

If we show that K, L are linearly disjoint in Ω then we are clearly done as by definition the map is injective and therefore $K \otimes_k L$ is integral. Clearly A, L are linearly disjoint in Ω. We may use (3.24.42), for suppose $\lambda_1, \dots \lambda_n \in K$ are linearly independent over k. Then for some $0 \neq a \in A$ we have $a_i := a\lambda_i \in A$ are still linearly independent over k and therefore linearly independent over L. Therefore $\lambda_1, \dots, \lambda_n$ are linearly independent over L as required. □

Lemma 3.25.23
Let K/k be a field extension such that k is algebraically closed in K. Then every irreducible polynomial $f \in k[X]$ remains irreducible in $K[X]$.

Proof. Consider the extension $\overline{K}$ which contains $\bar{k}$. And suppose $g \mid f$ in $K[X]$. As f splits completely in $\bar{k}$ then by unique factorisation in $\bar{k}[X]$ the coefficients of g lie in $K \cap \bar{k} = k$. Therefore by irreducibility $g = f$ or is constant. In particular f is irreducible in $K[X]$. □

Proposition 3.25.24 (Criteria for Primary Extension)
Let K/k be an extension for k perfect. Then the following are equivalent

a) $K \cap \bar{k} = k$

b) *K/k is algebraically integral*

c) *$K \otimes_k k'$ is a field for every algebraic extension k'/k*

d) *K and k' are linearly disjoint in $\overline{K}$ for every algebraic subextension k'/k (and in particular $\bar{k}$)*

*In this case we say that K is **primary** (when k is not perfect we would require that K/k is also geometrically reduced).*

Proof. *a)* $\implies$ *c)* It's enough to demonstrate the claim for k'/k finite, as every finite set of elements is contained in a finite subextension. Further as k is assumed perfect then k'/k is separable (3.14.97) and therefore simple (3.14.99). $k' = k(\theta)$. Then $k' = k[\theta] \cong k[X]/(f)$ and by (3.25.23) $k[X]/(f) \otimes_k K \cong K[X]/(f)$ is a field.

b) $\iff$ *c)* One direction is obvious, conversely suppose $K \otimes_k k'$ is an integral domain. We may reduce to the case k'/k finite. By (3.5.22) $K \otimes_k k' \cong K^n$ where $n = [k' : k]$. A finite-dimensional integral domain must be a field by (3.4.144) as multiplication is injective and therefore bijective.

c) $\implies$ *a)* Let k'/k be a non-trivial algebraic subextension of K/k then the multiplication map $K \otimes_k k' \to K$ is injective being a homomorphism from a field. Choose $x \in k' \setminus k$ then $0 \neq 1 \otimes x - x \otimes 1$ maps to 0 a contradiction.

c) $\implies$ *d)* Immediate as every homomorphism from a field is injective.

d) $\implies$ *a)* is the final comment in Example 3.24.40. □

Proposition 3.25.25
Let A be an integral k-algebra with k perfect and $K := \mathrm{Frac}(A)$. Then the following are equivalent

a) *A is algebraically integral*

b) *K is algebraically integral*

c) $K \cap \bar{k} = k$

Proof. *b)* $\iff$ *c)* was proven in (3.25.24) and *b)* $\implies$ *a)* is immediate.

Conversely for *a)* $\implies$ *b)*. Let $\{x_\lambda\}_{\lambda\in\Lambda}$ be a basis for an extension L/k then there is a commutative diagram

$$\begin{array}{ccc} A^{(\Lambda)} & \cong & A \otimes_k L \\ \cap & & \cap \\ K^{(\Lambda)} & \cong & K \otimes_k L \end{array}$$

of A-modules. Suppose $xx' = 0$ then by clearing denominators we find $(ax)(a'x') = 0$ in $A \otimes_k L$. By assumption $ax = 0$ or $a'x' = 0$. Examining componentwise shows that $x = 0$ or $x' = 0$ as required. □

3.26 Jacobson Rings

Definition 3.26.1 (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 (3.4.45) and (3.4.57)

$$\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}}^J$$

Proposition 3.26.2 (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 (3.4.45)

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

as required □

We prove later that the Weak Nullstellensatz implies the following result

Proposition 3.26.3 (Strong Nullstellensatz)
$k[X_1, \ldots, X_n]$ is a Jacobson ring.

Chapter 4

Topology and Sheaves

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.

Proposition 4.1.2
Let X be a topological space. Both the open sets and closed sets form a distributive lattice under inclusion.

Definition 4.1.3 (Continuous)
A map $f : X \to Y$ is continuous if the inverse image of an open (closed) set is open (closed).

Remark 4.1.4
In the case of $\mathbb{R}^n$ this can be shown to be equivalent to the usual $\delta - \epsilon$ definition.

Definition 4.1.5 (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 4.1.6 (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 4.1.7 (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 4.1.8 (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 4.1.9 (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 4.1.10
In the case of $\mathbb{R}^n$ this is equivalent to x being the limit of a convergent sequence $x_n \in Y$.

Proposition 4.1.11 (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 $x \notin Z \implies x \in X \backslash Z \implies (X \backslash Z) \cap Y \neq \emptyset$ 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 4.1.12
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 4.1.13 (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 (4.1.11) 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 4.1.14 (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 4.1.15
For a topological space X let X° denote the subset of closed points.

4.1.1 Continuous Maps

4.1.2 Irreducible Topological Spaces

Proposition 4.1.16 (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 (4.1.13) □

Proposition 4.1.17 (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) $Y \subseteq Z_1 \cup Z_2 \implies Y \subseteq Z_1$ *or* $Y \subseteq Z_2$ *where* Z_1, Z_2 *are closed subsets of* X

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. *a)* $\implies$ *b)*. Suppose that Y is irreducible in the subspace topology and $Y \subseteq Z_1 \cup Z_2$. This implies $Y = (Z_1 \cap Y) \cup (Z_2 \cap Y)$ is a decomposition of closed sets. So either $Z_1 \cap Y = Y$ or $Z_2 \cap Y = Y \implies Y \subseteq Z_1$ or $Y \subseteq Z_2$ as required.

b) $\implies$ *a)*. Suppose that $Y = (Z_1 \cap Y) \cup (Z_2 \cap Y)$. Then $Y \subseteq Z_1 \cup Z_2$, and for example $Y \subseteq Z_1$, which implies $Z_1 \cap Y = Y$. □

Proposition 4.1.18
Let $Y \subset X$ be a ***closed*** *subset then the following are equivalent*

a) Y *is an irreducible subset*

b) $Y = Z_1 \cup Z_2 \implies Y = Z_1$ *or* $Y = Z_2$ *where* Z_1, Z_2 *are closed subsets of* X

c) $Y \subseteq Z_1 \cup Z_2 \implies Y \subseteq Z_1$ *or* $Y \subseteq Z_2$ *where* Z_1, Z_2 *are closed subsets of* X

In other words in the lattice of closed subsets, the irreducible subsets are precisely the join-prime subsets.

Proof. *a)* $\implies$ *b)*. Clearly Z_1, Z_2 are also closed subsets of Y, so the result follows by definition.

b) $\iff$ *c)*. This is (2.4.2).

c) $\implies$ *a)*. This was already proven in (4.1.17). □

Remark 4.1.19
Singletons $\{x\}$ are always irreducible.

Definition 4.1.20 (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 4.1.21 (Decomposition into Irreducible Components)
A topological space X may be decomposed into irreducible components. More precisely

a) Y *irreducible* $\implies \overline{Y}$ *irreducible*

b) Y *irreducible component* $\implies Y$ *is closed*

c) *Every irreducible subset is contained in an irreducible component*

d) X *is the union of irreducible components*

Proof. We prove each in turn

a) Suppose $\overline{Y} \subseteq Z_1 \cup Z_2$ then by (4.1.17) $Y \subseteq Z_1$ say. By (4.1.11) then $\overline{Y} \subseteq Z_1$ as required.

b) Since an irreducible component is maximal and $\overline{Y}$ is irreducible we see that for Y irreducible and maximal we must have $Y = \overline{Y}$. (4.1.11) implies that such a Y is closed.

c) Clearly the lattice of closed subsets is chain complete so we may use (2.4.4).

d) As $\{x\}$ is irreducible every element is contained in an irreducible component by the previous step.

□

Corollary 4.1.22
Let $x \in X$ be a point then the closure $\overline{\{x\}}$ is an irreducible closed subset.

Corollary 4.1.23
X is irreducible if and only if it has a single irreducible component.

Definition 4.1.24 (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 4.1.25 (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.

4.1.3 Noetherian Topological Spaces

Definition 4.1.26 (Noetherian)
*A topological space X is **Noetherian** if the lattice of closed subsets is Artinian (i.e. satisfies the descending chain condition).*

Proposition 4.1.27 (Decomposition into Irreducibles)
Let X be a Noetherian topological space. Then every closed subset Y may be expressed uniquely as a finite, incomparable union of irreducible closed subsets. These are precisely the irreducible components of Y.

In particular X has only finitely many irreducible components.

Proof. The lattice of closed subsets is distributive and Artinian by definition. Therefore the result follows from (4.1.18) and (2.4.7). □

4.1.4 Krull Dimension

For a Noetherian topological space X the closed subsets form an Artinian, distributive lattice. Furthermore the irreducible subsets are precisely the join-prime elements by (4.1.18). Therefore we may use the notions of Krull Lattice developed in Section 2.5.

Definition 4.1.28 (Chain of irreducibles)
*Let X be a Noetherian topological space. A **chain** of irreducible subsets*

$$Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_n$$

*is said to have **length** n. A chain is **saturated** if there is no proper refinement, that is if Y is irreducible then*

$$Z_i \subseteq Y \subseteq Z_{i+1} \implies Y = Z_i \text{ or } Y = Z_{i+1}\,.$$

*If in addition Z_n (resp. Z_0) is maximal (resp. minimal) then the chain is **maximal**.*

Definition 4.1.29 (Krull Lattice of Closed Subsets)
Let X be a topological space.

- *The **Krull dimension** $\dim X$ of X is the maximal length of all chains of irreducible subsets. Note this may be ∞.*
- *The **height** or **codimension** of an irreducible subset $Y \subseteq X$, denoted $\operatorname{codim}(Y, X)$, is the maximal length of chains of irreducible subsets containing Y.*

- *When Y is not irreducible we write*

$$\operatorname{codim}(Y, X) = \inf_{\alpha} \operatorname{codim}(Y_\alpha, X)$$

  where Y_α varies among the irreducible components of Y.

*If $\dim X < \infty$ then we say X is **finite-dimensional**. In this case it's clear the closed subsets of a topological space form a Krull Lattice where the irreducible subsets are precisely the join-prime elements of the lattice.*

Note any saturated chain for $Y \subset X$ must start at Y and terminate at an irreducible component of X. In particular if X is irreducible then a saturated chain must terminate at X.

Proposition 4.1.30 (Extending Chains)
Let X be a finite-dimensional topological space. Then

a) *Every chain is contained in a saturated chain with the same endpoints*

b) *Every chain is contained in a maximal chain*

Proposition 4.1.31 (Simple properties of (co-)dimension)
Let X be a topological space and Y an irreducible subset. Then the following properties hold

a) $\dim(X) = \sup_\alpha \dim(X_\alpha)$ *where X_α are the irreducible components of X*

b) $\operatorname{codim}(Y, X) = \sup_\alpha \operatorname{codim}(Y, X_\alpha)$ *where X_α are the irreducible components of X containing Y*

c) $\dim X = \sup_Y \operatorname{codim}(Y, X)$

d) $\dim Y + \operatorname{codim}(Y, X) \leq \dim X$

e) $\operatorname{codim}(Y, Z) + \operatorname{codim}(Z, T) \leq \operatorname{codim}(Y, T)$ *for $Y \subset Z \subset T$ irreducible subsets*

f) *$Y \subsetneq Z$ is a saturated chain if and only if* $\operatorname{codim}(Y, Z) = 1$.

g) *Y is an irreducible component of X if and only if* $\operatorname{codim}(Y, X) = 0$. *In particular if X is irreducible then* $\operatorname{codim}(Y, X) = 0 \iff Y = X$.

In particular if X is finite-dimensional then all codimensions are also finite.

Definition 4.1.32 (Properties)
Let X be a topological space of finite dimension. Then we say X is

- ***Equidimensional** if all irreducible components of X have the same dimension*
- ***Equicodimensional** if* $\operatorname{codim}(Y, X)$ *is constant as Y varies over minimal irreducible subsets of X*
- ***Biequidimensional** if all maximal chains of irreducible subsets have the same length.*
- ***Quasi-Biequidimensional** if every irreducible component is biequidimensional*
- ***Catenary** if any two saturated chains with the same endpoints, say Y and Z, have the same length, namely* $\operatorname{codim}(Y, Z)$

Proposition 4.1.33 (Equivalent characterisations of biequidimensional)
Suppose X is a topological space of finite dimension. Then the following are equivalent

a) *X is quasi-biequidimensional*

b) *X is catenary and every irreducible component is equicodimensional*

c) *X satisfies the codimension formula for $Z \subset Y$ irreducible*

$$\dim Y = \dim Z + \operatorname{codim}(Z, Y)$$

d) *X satisfies b) in the case* $\operatorname{codim}(Z, Y) = 1$

Furthermore for irreducible subsets $Z \subset Y$

$$\operatorname{codim} Z = \operatorname{codim}(Z, Y) + \operatorname{codim} Y$$

Proof. This is a translation of (2.5.12) to the topological case. □

Proposition 4.1.34 (Codimension Formula)
Suppose X is a quasi-biequidimensional topological space. Then for $Z \subset Y$ closed subsets

$$\begin{aligned} \dim Y &= \dim Z + \operatorname{codim}(Z, Y) \\ \operatorname{codim} Z &= \operatorname{codim}(Z, Y) + \operatorname{codim} Y \end{aligned}$$

Proof. This follows from (2.5.14). □

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 σ is unique.

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

The following will be useful later

Definition 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

- *ϕ is injective if ϕ_U is injective for all U*
- *ϕ is an isomorphism if ϕ_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 (4.1.8) 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 ρ_x is injective.

Similarly consider $[(U, \sigma)] \in \mathcal{F}_x$ with $U \in \mathcal{B}_1$. By (4.1.8) 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, σ_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, σ_i) then $\alpha^+((s_x))$ is determined by the sections $(U_i, \alpha_{U_i}(\sigma_i))$.

In order to define η and ϵ 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 Φ 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, σ_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 ρ_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 σ 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

$$\begin{aligned} \epsilon_{\mathcal{G},U} &:= \left(\Phi^{\mathcal{B}}_{\mathcal{G},U}\right)^{-1} & U \in \mathcal{T}_X \\ \eta_{\mathcal{F},U} &:= \Phi^{\mathcal{B}}_{\mathcal{F},U} & U \in \mathcal{B} \end{aligned}$$

By abstract nonsense (2.6.52) we may show an adjoint relationship arising from η, ϵ if

- $\epsilon_{\mathcal{G}}|_{\mathcal{B}} \circ \eta_{\mathcal{G}|_{\mathcal{B}}} = 1_{\mathcal{G}|_{\mathcal{B}}}$
- The following map is injective

$$\begin{aligned} \mathrm{Mor}(\mathcal{F}^+, \mathcal{G}) &\longrightarrow \mathrm{Mor}(\mathcal{F}, \mathcal{G}|_{\mathcal{B}}) \\ \alpha &\longrightarrow \alpha|_{\mathcal{B}} \circ \eta_{\mathcal{F}} \end{aligned}$$

The first follows by definition of η and ϵ. The second is essentially because $\mathcal{G}$ is separated. For suppose α_1 and α_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 (σ_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 α_1, α_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 η_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 (2.6.51). □

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 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 4.3.1 (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

$$f_x^\sharp : \mathcal{O}_{Y,f(x)} \longrightarrow (f_\star \mathcal{O}_X)_{f(x)} \overset{4.2.10}{\longrightarrow} \mathcal{O}_{X,x}$$

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 4.3.2 (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 $\mathfrak{Lrs}/A$.

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 separable and any transcendental extension K/k is separably generated. 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

In order to generalise the usual notions to non-algebraically closed field, and develop a "coordinate-free" approach, we introduce the following concept

Definition 5.1.1 (K-Rational Maximal Ideal)
*Let A be a f.g. k-algebra and $\mathfrak{m}$ a maximal ideal. Recall (3.24.18) that $k(\mathfrak{m})/k$ is an algebraic (indeed finite) field extension, and we call it the **residue field** for $\mathfrak{m}$.*

*Let K/k be an algebraic field extension, then we say that a maximal ideal $\mathfrak{m} \lhd A$ is K-**rational** if there exists a field morphism*

$$k(\mathfrak{m})/k \to K/k$$

If $\mathfrak{a} \subseteq \mathfrak{m}$ then $k(\mathfrak{m}) \cong k(\mathfrak{m}/\mathfrak{a})$ by (3.4.54). Therefore $\mathfrak{m}$ is K-rational iff $\mathfrak{m}/\mathfrak{a}$ is.

This has a very concrete interpretation, for recall every f.g. k-algebra is a quotient of a polynomial ring

Proposition 5.1.2 (K-rational points)
Let $A = k[X_1, \dots, X_n]/\mathfrak{a}$ and K/k algebraic. Then a maximal ideal $\mathfrak{m} \lhd A$ is K-rational if and only if $\mathfrak{m} = \mathfrak{m}_x/\mathfrak{a}$ for $(x) \in K^n$ a zero of $\mathfrak{a}$.

In this case there is a canonical isomorphism $k(\mathfrak{m}) \cong k(x)$.

Further every maximal ideal is $\bar{k}$-rational and, indeed K-rational for some finite extension K/k.

Proof. Observe $\mathfrak{m} = \mathfrak{m}'/\mathfrak{a}$ for $\mathfrak{m}'$ a maximal ideal containing $\mathfrak{a}$. Furthermore $\mathfrak{m}$ is K-rational iff $\mathfrak{m}'$ is. Then the first two statements follow from (3.24.18).

The final statement follows from the Weak Nullstellensatz (3.24.19). We may consider $K = k(x_1, \dots, x_n)$ which is finite by (3.14.51). □

Definition 5.1.3 (K-Radical)
Let A be a f.g. k-algebra, K/k an algebraic extension and $\mathfrak{a} \lhd A$ an ideal. Define the K-radical by

$$\sqrt{\mathfrak{a}}^K := \bigcap_{\substack{\mathfrak{a} \subseteq \mathfrak{m} \\ \mathrm{K-rational}}} \mathfrak{m}$$

Then $\sqrt{-}^K$ is a closure operator. We say that an ideal $\mathfrak{a}$ is K-radical if $\mathfrak{a} = \sqrt{\mathfrak{a}}^K$, and the K-radical ideals are precisely the image of $\sqrt{-}^K$.

When $K = \bar{k}$ then this corresponds to the usual Jacobson radical because every maximal ideal is $\bar{k}$-rational.

Now we may introduce the Zero-Loci and study relationships to ideals

Proposition 5.1.4 (Correspondence between Zero-Loci and Ideals)
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 an algebraic 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

$$I_k(Y) := \{f \in A \mid f(y) = 0 \quad \forall y \in Y\}$$

The pair of maps V_K, I_k constitute a Galois Connection

$$\mathcal{I}(k[X_1, \dots, X_n]) \underset{V_K}{\overset{I_k}{\leftrightarrows}} \mathcal{P}(K^n)$$

namely they satisfy

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 subscripts)

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. *$\bigcap_i I(W_i) = I(\bigcup_i W_i)$*
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

$$V_K(I_k(Y)) = \overline{Y}$$

Proof. We make use of general results on Galois connections (Section 2.1.6), though many results may be shown more directly. The fact it's a Galois connection follows from Example 2.1.53.

1-3. These follow (2.1.49)

4. This follows from (2.1.51).
5. It's clear that $I(Y)$ is an ideal. It is radical because K is reduced (...). The second statement follows from (2.1.52) by considering the closure operator $\sqrt{\langle - \rangle}$.
6. This follows from (2.1.52) by considering the closure operators $\sqrt{\langle - \rangle}$ and $\langle - \rangle$.
7. The first equality follows from (2.1.54). The second equality follows from (3.4.28).
8. This follows from (2.1.54).
9. Observe that $\mathfrak{m}_x$ is prime (because K is an integral domain) and $x \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{m}_x$. the result follows from (3.4.37) because $\mathfrak{a} \subseteq \mathfrak{m}_x \vee \mathfrak{b} \subseteq \mathfrak{m}_x \iff \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{m}_x \iff \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{m}_x$

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 (2.1.51) $V_K \circ I_k$ is a closure operator with image precisely the closed sets. Therefore by (2.1.40)

$$(V_K \circ I_k)(Y) = \bigcap_{Y \subseteq Z \in \mathrm{Zar}_k(K^n)} Z$$

which is the definition of the topological closure. □

For a fixed ideal $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$ we may vary the field K to obtain families of solutions in different fields.

Definition 5.1.5 (Algebraic Set and L-valued points)
*Let $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$ be a **radical** ideal. For every (not-necessarily algebraic) field extension L/k define the L-valued points to be*

$$V(\mathfrak{a})(L) := V_L(\mathfrak{a})$$

*This family is called an **affine algebraic set**, which we denote $X := V(\mathfrak{a})$ and to which we associate the **coordinate ring** $k[X] := k[X_1, \dots, X_n]/\mathfrak{a}$, which is a reduced f.g. k-algebra. Note the elements of $k[X]$ may be regarded as L-valued functions on the L-valued points $X(L)$.*

*For a point $(x) \in X(L)$ define the **residue field** to be $k(x) = k(x_1, \dots, x_n)$ and the degree of x to be*

$$\deg(x) = [k(x) : k]$$

Note we may regard this as a functor, suppose we have compatible maps $i_{jk} : K_j/k \to K_k/k$ then these induce compatible injective maps

$$X(i_{jk}) : X(K_j) \to X(X_k)$$

Furthermore we make the definition $\mathfrak{m}_{X,x} := I_k(\{(x)\})$ for $(x) \in X(L)$. Note by definition $\mathfrak{a} \subseteq \mathfrak{m}_x$ and $\mathfrak{m}_{X,x} = \mathfrak{m}_x/\mathfrak{a}$. By (5.1.2) $\mathfrak{m}_{X,x}$ is K-rational.

Remark 5.1.6
$\mathbb{A}^n_k := V((0))$ is an algebraic set and $\mathbb{A}^n_k(L) = L^n$.

For completeness we also consider sub-algebraic sets in the same way as before

Definition 5.1.7 (Sub-algebraic sets)
Let X be an affine algebraic set with coordinate ring $k[X]$. For $\mathfrak{b} \triangleleft k[X]$ and K/k a field extension define

$$V(\mathfrak{b})(K) := \{x \in X(K) \mid f(x) = 0 \quad \forall f \in \mathfrak{b}\}$$

Similarly for $Y \subset X(K)$ define

$$I_k(Y) := \{f \in k[X] \mid f(y) = 0 \quad \forall y \in Y\}$$

*When $\mathfrak{b}$ is radical the family $Y = V(\mathfrak{b})$ is also referred to as an **affine algebraic set** with **coordinate ring** $k[Y] := k[X]/\mathfrak{b}$. Note the elements of $k[Y]$ may be regarded as K-valued functions on $Y(K)$.*

Note in the case $X = \mathbb{A}^n_k$ then this is precisely the same notion as before.

We can reduce to the case $\mathbb{A}^n_k$ easily as follows

Proposition 5.1.8 (Transitivity of algebraic sets)
Let X be an affine algebraic set and $\pi : k[X_1, \dots, X_n] \to k[X]$ the canonical surjective homomorphism. Then if we regard $X(K) \subset K^n$

$$V_K(\mathfrak{b}) = V_K(\pi^{-1}(\mathfrak{b})) \cap X(K)$$
$$I_k(Y \cap X(K)) = \pi(I_k(Y)) \quad Y \subset K^n$$

and in particular

$$I_k(V_K(\mathfrak{b})) = \pi(I_k V_K(\pi^{-1}\mathfrak{b}))$$

We may now generalize the Weak Nullstellensatz to arbitrary affine algebraic sets and non-algebraically closed fields K/k.

Proposition 5.1.9 (Generalized Weak Nullstellensatz)
Let X be an algebraic set and K/k a normal algebraic field extension. Then the correspondence (...) induces a bijection between K-rational maximal ideals and Galois orbits of points

$$\begin{array}{rcl} \{\mathfrak{m} \triangleleft k[X] \mid K\text{−rational}\} & \longleftrightarrow & X(K)/\operatorname{Aut}(K/k) \\ \mathfrak{m} & \longrightarrow & V_K(\mathfrak{m}) \\ \mathfrak{m}_{X,x} & \longleftarrow & [(x)] \end{array}$$

In particular there is a bijection

$$\operatorname{Specm}(k[X]) \quad \longleftrightarrow \quad X(\bar{k})/\operatorname{Aut}(\bar{k}/k)$$

Proof. Observe that (x) and (y) are conjugate in K if and only if $\mathfrak{m}_{X,x} = \mathfrak{m}_{X,y}$ (as there is an isomorphism $k(x) \cong k(y)$, and using (3.14.75)).

Further from (5.1.5) we know $\mathfrak{m}_{X,x} = \mathfrak{m}_x/\mathfrak{a}$ is K-rational. Therefore the right-to-left map is well-defined. By (5.1.2) it is also surjective.

Using this observation we simply need to show that $[V_K(\mathfrak{m}_{X,x})] = [(x)]$. One inclusion is obvious, suppose $(y) \in LHS$ then $\sigma(y)$ is a zero of $\mathfrak{m}_{X,x}$, whence $\mathfrak{m}_{X,x} \subseteq \mathfrak{m}_{X,\sigma(y)} = \mathfrak{m}_{X,y}$, which are equal by maximality. This shows that (x) and (y) are conjugate by the first observation.

The final statement follows because every maximal ideal is $\bar{k}$-rational. □

Corollary 5.1.10 (Correspondence between Zero-Loci and K-Radical Ideals)
Let X be a k-algebraic set and K/k algebraic then we have the following formula

$$I_k(V_K(\mathfrak{a})) = \sqrt{\mathfrak{a}}^K$$

Therefore there is a a dual isomorphism

$$\mathrm{Rad}(k[X]; K) \underset{V_K}{\overset{I_k}{\rightleftarrows}} \mathrm{Zar}_k(X(K))$$

between K-radical ideals of $k[X]$ and closed subsets $\mathrm{Zar}_k(X(K))$. Furthermore $V_K(\mathfrak{a}) = V_K(\sqrt{\mathfrak{a}}^K)$ so we may always take $\mathfrak{a}$ to be K-radical.

When $K = \bar{k}$ this reduces to the standard result.

Proof. Observe that $(x) \in V_K(\mathfrak{a})$ if and only if $\mathfrak{a} \subseteq \mathfrak{m}_x$. Therefore

$$I_k(V_K(\mathfrak{a})) = \bigcap_{x \in V_K(\mathfrak{a})} I_k(x) = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m}_x} \mathfrak{m}_x$$

Therefore by the correspondence in (5.1.9) this is equal to precisely $\sqrt{\mathfrak{a}}^K$ and the image of I_k is precisely the K-radical ideals. □

Finally we may refine this in the case $K = \bar{k}$. First we require a technical result

Lemma 5.1.11 (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 (3.7.4) $\bar{f}$ is nilpotent in $(A/\mathfrak{a})$ whence $f \in \sqrt{\mathfrak{a}}$. □

Proposition 5.1.12 (Strong Nullstellensatz)
Let X be an affine algebraic set and $\mathfrak{a} \lhd k[X]$. Then

$$I_k V_{\bar{k}}(\mathfrak{a}) = \sqrt{\mathfrak{a}}^J = \sqrt{\mathfrak{a}}$$

In particular the $\bar{k}$-radical ideals are precisely the radical ideals.

Proof. Note we've already shown the first equality.

First we consider the case $X = \mathbb{A}^n_k$ and $k[X] = k[X_1, \ldots, X_n]$. Let $\mathfrak{a} \lhd k[X]$ and choose $f \in I_k V_{\bar{k}}(\mathfrak{a})$. 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 (3.24.20) 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 (5.1.8) and (3.4.48) together with the result just proven, shows

$$I_k(V_{\bar{k}}(\mathfrak{b})) = \pi(I_{\bar{k}} V_{\bar{k}}(\pi^{-1}\mathfrak{b})) = \pi(\sqrt{\pi^{-1}(\mathfrak{b})}) = \sqrt{\mathfrak{b}}$$

where $\pi : k[X_1, \ldots, X_n] \to k[X]$ is canonical surjective morphism. □

Corollary 5.1.13
Let $k[X]$ be any finitely generated reduced k-algebra, then $k[X]$ is a Jacobson ring, i.e.

$$\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}}^J$$

In particular the intersection of all maximal ideals is zero

$$\bigcap_{\mathfrak{m}} \mathfrak{m} = 0$$

5.1.1 Topological Properties

The topological notion of irreducibility is important, and may be reduced to a purely algebraic statement on the coordinate ring.

Proposition 5.1.14 (Criterion for Irreducibility)
Let X be an affine algebraic set (e.g. $\mathbb{A}^n_k$), K/k an algebraic field extension and $Y = V(\mathfrak{b})$ an algebraic subset corresponding to a K-radical ideal $\mathfrak{b} \triangleleft k[X]$. Then the following are equivalent

a) *$Y(K)$ is an irreducible subset of $\mathrm{Zar}_k(X(K))$*

b) *$\mathfrak{b}$ is prime*

c) *$k[Y]$ is an integral domain.*

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 K-radical). Therefore $\mathfrak{a}$ is prime. □

Proposition 5.1.15 (Closed sets $\longleftrightarrow$ radical ideals)
Let $X = V(\mathfrak{a})$ be an algebraic set. Recall $\bar{k}$-radical ideals are precisely the radical ideals and there is a dual lattice isomorphism between radical ideals and "Zariski"-closed subsets of $X(\bar{k})$.

$$\mathrm{Rad}(k[X]) \underset{V_{\bar{k}}(-)}{\overset{I_k(-)}{\longleftrightarrow}} \mathrm{Zar}_k(X(\bar{k}))$$

Under this isomorphism we have

- *maximal ideals correspond to $\mathrm{Aut}(\bar{k}/k)$-orbits of single points $x \in X(\bar{k})$*
- *prime ideals of $k[X]$ correspond to irreducible subsets of $X(\bar{k})$*
- *minimal prime ideals of $k[X]$ correspond to irreducible components of $X(\bar{k})$.*

Recall that prime ideals are precisely the meet-prime radical ideals and irreducible subsets are precisely the join-prime closed subsets (see (4.1.18)). Therefore we have a dual isomorphism between the Krull Lattice of radical ideals of $k[X]$ and the Krull Latice of closed subsets of $X(\bar{k})$.

Proof. The content of the Strong Nullstellensatz is precisely that $I_k(-) \circ V_{\bar{k}}(-) = \mathbf{1}$. The other direction was already proven so we have a dual order isomorphism. The statement about maximal ideals was already shown in (5.1.9) and prime ideals in (5.1.14). Then as irreducible components are precisely maximal irreducible subsets the final statement follows from the dual order isomorphism. □

Definition 5.1.16 (Irreducible Algebraic Set)
*We say an affine algebraic set $X = V(\mathfrak{a})$ is **irreducible** if the topological space $X(\bar{k})$ is irreducible.*

This is the case precisely when $\mathfrak{a}$ is prime, or when $k[X]$ is an integral domain by (5.1.15).

Proposition 5.1.17 (Decomposition into Irreducible Components)
Let $X = V(\mathfrak{a})$ be an algebraic set then the topological space $X(\bar{k})$ is Noetherian. Furthermore it has finitely many irreducible components X_i and the decomposition

$$X(\bar{k}) = X_1 \cup \ldots \cup X_n$$

is the unique incomparable decomposition into irreducible closed subsets.

Proof. By Hilbert's Basis Theorem (3.9.6) $k[X]$ is a Noetherian ring, so by (5.1.15) $X(\bar{k})$ is Noetherian. The result then follows from (4.1.27) □

Proposition 5.1.18 (Subspace Topology)
Let $X = V(\mathfrak{a})$ an algebraic set and $Y = V(\mathfrak{b})$ an algebraic subset. Then there is a commutative diagram

$$\begin{array}{ccc} \left\{\mathfrak{c} \in \operatorname{Rad}(k[X]) \mid \mathfrak{b} \subseteq \mathfrak{c}\right\} & \underset{I}{\overset{V}{\rightleftarrows}} & \left\{Z \in \operatorname{Zar}_k(X(\bar{k})) \mid Z \subseteq Y\right\} \\ {\scriptstyle \pi^{-1}}\uparrow\downarrow{\scriptstyle \pi} & & \| \\ \operatorname{Rad}(k[X]/\mathfrak{b}) & \underset{I}{\overset{V}{\rightleftarrows}} & \operatorname{Zar}_k(Y(\bar{k})) \end{array}$$

under which prime ideals correspond to irreducible subsets and the horizontal arrows induce dual isomorphisms.

In particular the subspace topology for $Y(\bar{k})$ coincides with the Zariski topology.

Proof. The left hand arrows are mutual inverses by (3.4.53). The horizontal maps are dual isomorphisms by (5.1.15). The equality then follows from (5.1.8). □

5.1.2 Dimension

Definition 5.1.19 (Dimension)
Let $X = V(\mathfrak{a})$ be an algebraic set. Then we define the dimension to be

$$\dim X := \dim X(\bar{k})$$

where this is the Krull Dimension (4.1.29) of the $\bar{k}$-rational points with the k-Zariski topology. This is the supremum of dimension over all irreducible components by (4.1.31).

Proposition 5.1.20 (Dimension of subspace)
Let $X = V(\mathfrak{a})$ be an algebraic set and $Y = V(\mathfrak{b})$ an algebraic subset. Then

a) $\dim Y = \dim(\mathfrak{b}) = \dim k[X]/\mathfrak{b} = \dim k[Y]$

b) $\operatorname{codim}(Y, X) = \operatorname{ht}(\mathfrak{b})$

Further when $Y = V(\mathfrak{p})$ is irreducible then $\operatorname{codim}(Y, X) = \dim k[X]_{\mathfrak{p}}$.

Proof. *a)* follows from (5.1.18).

b) follows similarly by observing that the definition of ideal height (3.21.1) is dual to the topological definition of codimension (4.1.29). The last statement follows from (3.21.5). □

Corollary 5.1.21
Let $X = V(\mathfrak{a})$ is an algebraic set then $\dim X = \dim k[X]$.

Proof. Follows from previous proposition with $\mathfrak{b} = (0)$. □

As we showed in Section 3.24.3 the lattice of irreducible subsets is particularly well behaved.

Proposition 5.1.22 (Biequidimensional Algebraic Sets)
Let $X = V(\mathfrak{a})$ be an algebraic set. Then $X(\bar{k})$ is quasi-biequidimensional. Furthermore for every closed subset $Y = V(\mathfrak{b})$ the codimension formula is satisfied

$$\dim X = \dim Y + \operatorname{codim}(Y, X)$$

or in algebraic terms

$$\dim k[X] = \dim k[Y] + \operatorname{ht}(\mathfrak{b})$$

Finally X is biequidimensional iff it is equidimensional.

Proof. We've observed that the lattice of radical (resp. prime) ideals of $k[X]$ is isomorphic to the lattice of closed (resp. irreducible) subsets of $X(\bar{k})$. Therefore the result follows from (3.24.27).

The codimension formula follows from (4.1.34) and the algebraic version from (5.1.20). □

In the irreducible case we recover the "classical" field-theoretic version of dimension

Proposition 5.1.23 (Dimension of Function Field)
Let $X = V(\mathfrak{p})$ be an irreducible algebraic set. Then

$$\dim X = \dim k[X] = \operatorname{trdeg}(k(X)/k)$$

where we define the "field of rational functions"

$$k(X) := \operatorname{Frac}(k[X])$$

Proof. We have already shown that $\dim X = \dim k[X]$. The second equality follows from Noether Normalisation (3.24.21). □

Proposition 5.1.24 (Criteria for dimension 0)
Let $X = V(\mathfrak{a})$ an algebraic set and $Y := V(\mathfrak{b})$ a non-empty closed subset. Then the following are equivalent

a) *Y is finite*

b) $\dim Y = 0$

c) *$\mathfrak{b}$ is the intersection of finitely many maximal ideals in $k[X]$*

Furthermore

$$\mathfrak{b} = \bigcap_{y \in Y} \mathfrak{m}_y$$

and

$$\mathrm{ht}(\mathfrak{b}) = \mathrm{codim}(Y, X) = \dim X$$

Proof. Suppose $Y = \{y_1, \dots, y_n\}$ is finite then $\mathfrak{b} = I(Y) = \bigcap_{i=1}^n I(y_i) = \bigcap_{i=1}^n \mathfrak{m}_{y_i}$. So $a) \implies c)$. Conversely if $\mathfrak{b} = \bigcap_{i=1}^n \mathfrak{m}_i$ then $V(\mathfrak{b}) = \bigcup_{i=1}^n V(\mathfrak{m}_i)$ so $c) \implies a)$.

$a) \implies b)$ The irreducible components are the singletons which clearly have dimension 0. Conversely let $\{Y_\alpha\}_\alpha$ be the finitely many irreducible components. These must have dimension 0, which by definition means they must be singletons (since every singleton is an irreducible closed subset). Therefore Y is finite as required.

The last part follows from the codimensional formula □

Proposition 5.1.25
Let $X = V(F) \subset \mathbb{A}_k^n$ be a hypersurface with $F \in k[X_1, \dots, X_n]$ an irreducible polynomial. Then

$$\dim X = n - 1$$

5.1.3 Regular Maps and Morphisms of Affine Algebraic Sets

Proposition 5.1.26 (Regular Map)
*Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ be an algebraic set and $f : X(\bar{k}) \to \bar{k}$ a function. Then we say f is **regular** if there is a polynomial $F \in k[X_1, \dots, X_n]$ such that*

$$f(x) = F(x) \quad \forall x \in X(\bar{k})$$

Furthermore there is an isomorphism of k-algebras (which we frequently identify)

$$k[X] \xrightarrow{\sim} \{f : X(\bar{k}) \to \bar{k} \mid \text{ regular } \}$$

*Let x_i be the image of $X_i + \mathfrak{a}$ under this map. Then the regular functions $x_1, \dots, x_n$ are known as the **coordinate functions**, and they generate $k[X]$ as a k-algebra.*

Proof. There is by definition a well-defined homomorphism from $k[X_1, \dots, X_n]$ to the set of regular functions. Suppose that $F(x) = 0$ for all $x \in X(\bar{k})$ then by definition $F \in I_{\bar{k}}(V_{\bar{k}}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. As $\mathfrak{a}$ is radical we see $F \in \mathfrak{a}$ by (5.1.12). □

Proposition 5.1.27 (Regular Morphism)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n$ and $Y = V(\mathfrak{b}) \subset \mathbb{A}^m$ be algebraic sets and $f : X(\bar{k}) \to Y(\bar{k})$ a map. Then the following are equivalent

a) *$y_i \circ f$ is **regular** for each coordinate function $y_i \quad i = 1 \dots m$*

b) *$u \in k[Y]$ regular $\implies u \circ f =: f^\star(u) \in k[X]$ is regular*

c) *$f(x)$ is of the form $(f_1(x), \dots, f_m(x))$ where $f_i \in k[X]$.*

*Such maps are called **regular maps**. Furthermore there is a canonical bijection*

$$\begin{array}{rcl} \mathrm{AlgHom_k(k[Y], k[X])} & \longleftrightarrow & \{f : X \to Y \mid \text{ regular } \} \\ \phi & \longrightarrow & \phi_\star : x \to (\phi(y_1)(x), \dots, \phi(y_m)(x)) \\ f^\star & \longleftarrow & f \end{array}$$

Proof. $a) \iff c)$ is clear by definition. Further $b) \implies a)$ is clear since y_i is a regular function. For $c) \implies b)$ suppose that $f(x) = (f_1(x), \dots, f_m(x))$, $f_i = \pi_X(F_i)$ and $u = \pi_Y(U)$. Then

$$\begin{aligned}(u \circ f)(x) &= U(F_1(x), \dots, F_m(x)) \\ &= U(F_1, \dots, F_m)(x) \\ &= U(f_1, \dots, f_m)(x)\end{aligned}$$

where $U(f_1, \dots, f_m) \in k[X]$, so $u \circ f$ is regular. Further

$$(f^\star)_\star(x) = (f^\star(y_1)(x), \dots, f^\star(y_m)(x)) = (f_1(x), \dots, f_m(x)) = f(x)$$

and

$$(\phi_\star)^\star(y_i) = y_i \circ \phi_\star = y_i$$

which shows that the maps are mutually inverse. □

Definition 5.1.28
Let $f : X \to Y$ be a regular morphism of affine algebraic sets. Then we say it is

- ***finite*** *if $f_\star : k[Y] \to k[X]$ is module-finite (equivalently integral)*
- ***dominant*** *if $f(X)$ is dense in Y*

Proposition 5.1.29 (Criteria for dominant morphisms)
A regular morphism $f : X \to Y$ is dominant if and only if $f_\star : k[Y] \to k[X]$ is injective. In particular when both X and Y are irreducible then this induces a field extension

$$k(Y) \hookrightarrow k(X)$$

Proof. Recall $f(X)$ is dense precisely when the closure $\overline{f(X)} = Y$. Then

$$\begin{aligned}\ker(f_\star) = I_k(f(X)) &\implies V_{\bar{k}}(\ker(f_\star)) = V_{\bar{k}}(I_k(f(X))) = \overline{f(X)} \\ &\implies \sqrt{\ker(f_\star)} = I_k(\overline{f(X)})\end{aligned}$$

by (...). If $\ker(f_\star) = 0$ then clearly $\overline{f(X)} = Y$. Conversely if this holds then

$$\sqrt{\ker(f_\star)} = I_k(Y) = I_k(V_{\bar{k}}(0)) = \sqrt{(0)} = (0)$$

as $k[Y]$ is reduced, whence $\ker(f_\star) = 0$. □

5.1.4 Sheaf of Regular Functions

In order to generalise the notion of regular map it is useful to introduce the notion of "sheaf of regular" functions, similar to differential (resp. complex) geometry where we may consider the sheaf of smooth (resp. analytic) functions.

Definition 5.1.30 (Sheaf of Regular Functions)
Let $X = V(\mathfrak{a})$ be an algebraic set and $U \subset X(\bar{k})$ an open set. We say a function $f : U \to \bar{k}$ is ***regular*** *at $x \in X$ if there exists $g, h \in k[X]$ and an open neighbourhood V of 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***

$$\mathcal{O}_X(U) := \{f : U \to \bar{k} \mid f \text{ regular } \}$$

The elements are referred to as ***sections*** *over U.*

We will see that in the case of affine algebraic sets the sheaf of regular functions can be characterized purely the coordinate ring, over particular open sets.

Definition 5.1.31 (Principal Open Set)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^k_n$ be an algebraic set and $f \in k[X]$. Define the ***principal open set***

$$D(f) := \{x \in X(\bar{k}) \mid f(x) \neq 0\} = X(\bar{k}) \setminus V_{\bar{k}}(f)$$

Proposition 5.1.32 (Coordinate ring is reduced)
Let $X = V(\mathfrak{a})$ be an algebraic set. For $f \in k[X]$ we have $D(f) = \emptyset \iff f = 0$.

Proof. If $f = 0$ then it's clear that $D(f) = \emptyset$. Conversely if $f(x) = 0$ for all $x \in X(\bar{k})$ then $f \in I_k(V_{\bar{k}}(0)) = \sqrt{0} = (0)$ as by definition $k[X]$ is reduced. □

The principal open sets constitute a basis for the topology so in some sense the sheaf of regular functions is completely characterized by behaviour on these open sets.

Lemma 5.1.33
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 $\bigcup_{f \in \mathfrak{b}} D(f) = U$. □

We show that this is equivalent to the earlier definition (5.1.26), namely that the sections which are regular everywhere are precisely the regular functions.

Proposition 5.1.34 (Sections are localisation of coordinate ring)
Let $X = V(\mathfrak{a})$ be an algebraic set and $f \in k[X]$. There is a canonical isomorphism

$$\begin{aligned} i_f : k[X]_f &\xrightarrow{\sim} \mathcal{O}_X(D(f)) \\ \frac{g}{f^n} &\longrightarrow y \to \frac{g(y)}{f(y)^n} \end{aligned}$$

Furthermore $D(g) \subseteq D(f) \iff S_f \subseteq \overline{S_g}$ and we have the following commutative diagram

$$\begin{array}{ccc} k[X]_f & \xrightarrow{\sim} & \mathcal{O}_X(D(f)) \\ {\scriptstyle i_{S_f S_g}}\downarrow & & \downarrow{\scriptstyle (-)|_{D(g)}} \\ k[X]_g & \xrightarrow{\sim} & \mathcal{O}_X(D(g)) \end{array}$$

In particular the everywhere regular maps consists of precisely the coordinate ring $k[X]$.

Proof. The map is trivially well-defined and injective. Consider a regular map $\sigma \in \mathcal{O}_X(D(f))$. Consider the ideal

$$\mathfrak{a} := \{g \in k[X] \mid g\sigma \in \mathrm{Im}(i_f)\}$$

It is enough to show $f \in \mathfrak{a}$. Suppose $f \notin \mathfrak{a}$ then it's contained in a maximal ideal which is of the form $\mathfrak{m}_x$ for some $x \in X(\bar{k})$ by (...). By definition $x \in D(f)$ and there is an open neighbourhood $W \subseteq D(f)$ and elements $h_1, h_2 \in k[X]$ such that

$$\sigma(y) = \frac{h_1(y)}{h_2(y)} \quad \forall y \in W$$

Choose $h_3 \in k[X]$ such that $x \in D(h_3) \subseteq W$ then clearly

$$\sigma(y) = \frac{(h_1 h_3)(y)}{(h_2 h_3)(y)} \quad \forall y \in D(h_3)$$

and in particular $(h_2 h_3 \sigma)(y) = (h_1 h_3)(y)$ for all $y \in D(f)$. Therefore $h_2 h_3 \in \mathfrak{a} \subseteq \mathfrak{m}_x$ which implies $h_2(x) = 0$ or $h_3(x) = 0$ a contradiction.

Therefore $f \in \mathfrak{a}$ and clearly $\sigma \in \mathrm{Im}(i_f)$ as required. □

Using the sheaf framework we may define the "stalks" at a point $x \in X$, similar to the notion of "germ" in differential geometry. We may also define "rational function" which is analogous to the notion of "meromorphic function" in the theory of Riemann surfaces.

5.1.5 Local Rings

Definition 5.1.35 (Local Ring at a point)
*Let $X = V(\mathfrak{a})$ be an algebraic set and $W \subset X(\bar{k})$ be an irreducible subset. Then we define the **local ring** at W to be*

$$\mathcal{O}_{X,W} := \varinjlim_{U \cap W \neq \emptyset} \mathcal{O}_X(U)$$

*with unique maximal ideal $\mathfrak{m}_{X,W}$. Define the **field of rational functions** to be*

$$k(W) := \mathcal{O}_{X,W}/\mathfrak{m}_{X,W}$$

In the case $W = \{(x)\}$ then we write it as $(\mathcal{O}_{X,x}, \mathfrak{m}_{X,x})$.

Proposition 5.1.36
Let $X = V(\mathfrak{a})$ be an algebraic set and $W \subset X(\bar{k})$ an irreducible subset with $\mathfrak{p} := I(W)$. Then we have isomorphisms

$$\begin{aligned} \mathcal{O}_{X,W} &\xrightarrow{\sim} k[X]_{\mathfrak{p}} \\ \mathfrak{m}_{X,W} &\xrightarrow{\sim} \mathfrak{p}k[X]_{\mathfrak{p}} \\ k(\mathfrak{m}_{X,W}) &\xrightarrow{\sim} k[X]_{\mathfrak{p}}/\mathfrak{p}k[X]_{\mathfrak{p}} \xrightarrow{\sim} \mathrm{Frac}(k[X]/\mathfrak{p}) \end{aligned}$$

Explicitly the inverse map is given by $f/g \to [(D(g), f/g)]$. We have the following dimension formula

$$\dim \mathcal{O}_{X,W} = \mathrm{codim}(W, X) = \mathrm{ht}(\mathfrak{p})$$

In particular $k(\mathfrak{m}_{X,x})$ is finitely generated as a field and when $W = \{x\}$ we have isomorphisms

$$k(\mathfrak{m}_{X,x}) \xrightarrow{\sim} k[X]_{\mathfrak{m}_x}/\mathfrak{m}_x k[X]_{\mathfrak{m}_x} \xrightarrow{\sim} k[X]/\mathfrak{m}_x \xrightarrow{\sim} k(x)$$

and the dimension formula

$$\dim \mathcal{O}_{X,x} = \mathrm{codim}(\{x\}, X) = \sup_{\alpha : x \in X_\alpha} \dim(X_\alpha)$$

Proof. This is a formal consequence of generic facts regarding localization and direct limits

$$k[X]_{\mathfrak{p}} \overset{(3.6.33)}{\cong} \varinjlim_{f \notin \mathfrak{p}} k[X]_f \cong \varinjlim_{D(f) \cap W \neq \emptyset} \mathcal{O}_X(D(f)) \overset{(2.6.47)}{\cong} \varinjlim_{U \cap W \neq \emptyset} \mathcal{O}_X(U)$$

We may demonstrate this more directly. For it is surjective because the principal open sets form a basis and by (5.1.34), observing that $f \notin \mathfrak{p} \iff D(f) \cap V(\mathfrak{p}) \neq \emptyset$. Suppose $\frac{g}{f}$ and $\frac{g'}{f'}$ have the same image then there is some h such that $D(h) \subseteq D(ff') = D(f) \cap D(f')$ and $h \notin \mathfrak{p}$ such that $\frac{g}{f} = \frac{g'}{f'}$ are equal in $k[X]_h$ and a-fortiori in $k[X]_{\mathfrak{p}}$. Therefore the map is injective as required.

The dimension formula follows from (5.1.20). □

Proposition 5.1.37 (Dimension of Local Ring)
Let $X = V(\mathfrak{a})$ be an equidimensional algebraic set and $W \subset X(\bar{k})$ an irreducible subset. Then

$$\dim \mathcal{O}_{X,W} = \dim X - \dim W$$

In particular

$$\dim \mathcal{O}_{X,x} = \dim X$$

Proof. The first statement follows from (5.1.36) and (5.1.22), the second from (5.1.24). □

Proposition 5.1.38
Let $x \in X(\bar{k})$ be a point. The minimal primes of $\mathcal{O}_{X,x}$ are in bijection with irreducible components of X containing x.

$\mathcal{O}_{X,x}$ is an integral domain if and only if x lies on a unique irreducible component.

Proof. By (5.1.36) and (3.6.32) the minimal primes of $\mathcal{O}_{X,x}$ correspond to minimal primes of $k[X]$ contained in $\mathfrak{m}_x$. These correspond to irreducible components of X containing x by (5.1.15).

As $\mathcal{O}_{X,x}$ is reduced, it is an integral domain iff it has a unique minimal prime ideal (3.4.62). □

5.1.6 Generic Points

When considering irreducible subsets $W \subset X$ there is another way of looking at these in terms of "generic points".

Definition 5.1.39 (Generic Point)
Let $X = V(\mathfrak{a})$ be an algebraic set and $(\xi) \in X(\Omega)$ for some extension field Ω/k. Then we may define the irreducible subset of $X(\bar{k})$

$$W_\xi := V_{\bar{k}}(\mathfrak{p}_\xi) = \left\{ (x) \in X(\bar{k}) \mid \forall f \in k[X]\, (f(\xi) = 0 \implies f(x) = 0) \right\}$$

There are canonical isomorphisms

$$k(\mathfrak{m}_{X,W}) \xrightarrow{\sim} k[X]_{\mathfrak{p}}/\mathfrak{p}k[X]_{\mathfrak{p}} \xrightarrow{\sim} \mathrm{Frac}(k[X]/\mathfrak{p}) \xrightarrow{\sim} k(\xi)$$

*We say that (ξ) is a **generic point** corresponding to the irreducible closed subset W_ξ. Moreover every irreducible subset is of this form for we may simply consider $\Omega := \mathrm{Frac}(k[X]/\mathfrak{p})$ and $\xi = (\overline{X}_1, \ldots, \overline{X}_n)$.*

*If $(x) \in W_\xi$ then we say that (x) is a **specialization** of (ξ) and this induces the specialization homomorphism*

$$\begin{array}{ccc} k[X]/\mathfrak{p}_\xi & \longrightarrow & k[X]/\mathfrak{m}_x \\ \wr\| & & \wr\| \\ k[\xi] & \dashrightarrow & k[x] \end{array}$$

If $W_\xi = X$ then we say simply (ξ) is a generic point.

The approach taken in "Weil Foundations" is then to consider the "generalised points" $X(\Omega)$, and on the other hand in scheme theory one considers a topological space consisting of all irreducible subsets of $X(\bar{k})$ (i.e. the individual points plus "generic" points corresponding to irreducible closed subsets). The former has the conceptual advantage of being in some sense more concrete and field theoretic, the latter of not requiring a large ambient space Ω and ambiguity over the choice of generic point.

5.1.7 Tangent Space

We propose two definitions for the tangent space and show that under mild technical conditions they are naturally isomorphic. The latter definition may be identified geometrically.

Definition 5.1.40
*Let $X = V(\mathfrak{a})$ be an algebraic set and $(x) \in X(\bar{k})$. We define the **cotangent space** to be the $k(\mathfrak{m}_{X,x})$-vector space*

$$T_x^\star X := \mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2$$

*and the **tangent space** to be the $k(x)$-vector space*

$$T_x X := \mathrm{Der}_k(\mathcal{O}_{X,x}, k(\mathfrak{m}_{X,x}))$$

This definition extends in the obvious way to an irreducible subset $W \subset X(\bar{k})$.

The tangent space has a very concrete interpretation which allows us to characterize the dimension.

Proposition 5.1.41 (Concrete interpretation of Tangent Space)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ be an algebraic set and $(x) \in X(\bar{k})$. Then there are natural $k(x)$-module isomorphisms

$$T_x X \xrightarrow{\sim} \mathrm{Der}_k\left(k[X], k(x)\right) \xrightarrow{\sim} \left\{ v \in k(x)^n \mid \sum_{i=1}^n v_i \frac{\partial F}{\partial X_i}(x) = 0 \quad \forall F \in \mathfrak{a} \right\}$$

where we have used the identification $k(\mathfrak{m}_{X,x}) \cong k(x)$ and the k-algebra homomorphism $k[X] \to k(\mathfrak{m}_{X,x})$. Suppose $\mathfrak{a} = \langle F_1, \ldots, F_m \rangle$ then the right hand side is the kernel of the following $k(x)$-module homomorphism

$$\begin{pmatrix} \frac{\partial F_1}{\partial X_1}(x) & \cdots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_m}{\partial X_1}(x) & \cdots & \frac{\partial F_m}{\partial X_n}(x) \end{pmatrix} : k(x)^n \to k(x)^m$$

In particular

$$\dim_{k(x)} T_x X = n - \mathrm{rk}\left(\frac{\partial F_i}{\partial X_j}(x)\right)$$

Proof. Recall by (5.1.35) that $\mathcal{O}_{X,x} \cong k[X]_{\mathfrak{m}_x}$ and $k(\mathfrak{m}_{X,x}) \cong k(x)$ so we have isomorphisms

$$\mathrm{Der}_k(\mathcal{O}_{X,x}, k(\mathfrak{m}_{X,x})) \cong \mathrm{Der}_k(k[X]_{\mathfrak{m}_x}, k(x)) \overset{(3.20.9)}{\cong} \mathrm{Der}_k(k[X], k(x))$$

and the final isomorphism is from (3.24.33) □

Proposition 5.1.42
Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ be an algebraic set and $(x) \in X(\bar{k})$. There is a canonical $k(\mathfrak{m}_{X,x})$-module homomorphism

$$T_x X \quad \longrightarrow \quad (T_x^\star X)^\vee$$

Under the condition that $k(\mathfrak{m}_{X,x})/k$ is separably generated (e.g. k is perfect) then this map is an isomorphism.

Proof. This follows directly from (3.24.37) by considering the local ring $A := \mathcal{O}_{X,x}$ with maximal ideal $\mathfrak{m}_{X,x}$. □

We may now show the following important result

Proposition 5.1.43 (Non-Singular Point)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n_k$ be an algebraic set, X_α an irreducible component and $(x) \in X_\alpha$. Then we have the following inequality

$$\dim_{k(x)} T_x X \geq \dim \mathrm{Der}(k(X_\alpha))) \tag{5.1}$$

*We say that (x) is a **non-singular point** when (5.1) is an equality and the irreducible component X_α containing (x) is unique.*

Furthermore the non-singular points form a non-empty dense open subset of each irreducible component.

When $k(X_\alpha)/k$ is separably generated (e.g. k perfect) then $\dim \mathrm{Der}(k(X_\alpha)) = \mathrm{trdeg}(k(X_\alpha)) = \dim X_\alpha$.

Proof. Let $\Omega := k(X_\alpha) = \mathrm{Frac}(k[X_\alpha])$, $(\xi) := (\overline{X}_1, \dots, \overline{X}_n) \in \Omega^n$ and $\mathfrak{p}_\alpha = \langle F_1, \dots, F_m \rangle \lhd k[X_1, \dots, X_n]$ is the ideal defining X_α. Then

$$\mathrm{Der}(\Omega) \overset{(3.20.9)}{=} \mathrm{Der}(k[X], \Omega) \overset{(3.24.33)}{\cong} \ker\left(\frac{\partial F_i}{\partial X_j}(\xi)\right)$$

There is a k-algebra homomorphism $k[\xi] \to k[x]$ and so by the determinant criteria of rank (3.4.166) we see

$$\mathrm{rk}\left(\frac{\partial F_i}{\partial X_j}(x)\right) \leq \mathrm{rk}\left(\frac{\partial F_i}{\partial X_j}(\xi)\right)$$

and therefore the inequality follows from (5.1.41). Suppose the rank of the right hand side is r and consider the r-minors $g_1, \dots, g_m \in k[X_\alpha]$. Then by the same result at least one is non-zero and the set of non-singular points is given by

$$\bigcup_p D(g_p)$$

which is non-empty by (5.1.32).

When $k(X_\alpha)/k$ is separably generated then $\dim \mathrm{Der}(\Omega) = \mathrm{trdeg}(\Omega/k) = \dim X_\alpha$ by (3.24.36). □

Definition 5.1.44
*Let $X = V(\mathfrak{a})$ be an algebraic set and $(x) \in X(\bar{k})$. Then we say that (x) is **regular** if $\mathcal{O}_{X,x}$ is a regular local ring, that is if*

$$\dim T^\star_x X = \dim \mathcal{O}_{X,x}$$

Proposition 5.1.45 (Regular Point)
Let $X = V(\mathfrak{a})$ an irreducible algebraic set, $(x) \in X(\bar{k})$ and k perfect. Then

$$\dim T^\star_x X = \dim T_x X$$

and the following are equivalent

a) *(x) is regular*

b) *(x) is non-singular*

c) *$\dim T_x X = \dim X$*

Proof. Recall by (5.1.37) that $\dim \mathcal{O}_{X,x} = \dim X$ and by definition $T^\star_x X = \mathfrak{m}_{X,x}/\mathfrak{m}^2_{X,x}$. Further by definition (x) is regular iff $\dim T^\star_x X = \dim \mathcal{O}_{X,x}$. Finally by (...) $\dim T^\star_x X = \dim T_x X$ so we see $a) \iff c)$.

Similarly $b) \iff c)$ is essentially by definition. □

Example 5.1.46 (Simple Points of a Plane Curve)
The canonical example is a plane curve $k[X] = k[X,Y]/(F(X,Y))$ which has dimension 1 (...). Given $(x) \in X(K)$ we see that

$$T_x X = \{(\alpha, \beta) \in k(x)^2 \mid 0 = \alpha \frac{\partial F}{\partial X}(x) + \beta \frac{\partial F}{\partial Y}(x)\}$$

*Clearly this has dimension 1 (in which case (x) is a **simple point**) unless both the partial derivatives vanish at (x) in which case it has dimension 2.*

Clearly $F(X,Y) = Y^2 - X^3$ has a non-simple point at $(0,0)$ but $F(X,Y) = Y - X^2$ has simple points everywhere.

5.1.8 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 (3.14.104).

By (3.14.105) 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 5.1.47
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 (5.1.5) 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 (3.14.11) we have $d_i \mid d$, so $\mathrm{lcm}_i(d_i) \mid d$.

Let $d' := \mathrm{lcm}_i(d_i)$ then by (3.14.104) we have $k(x_i) \subseteq k_{d'}$ which implies $k(x) \subseteq k_{d'}$. By (3.14.11) again $d' \mid d$ and $d = d'$.

For the second statement

$$\begin{aligned}
\deg(x) \mid d &\iff \mathrm{lcm}(\deg_k(x_i)) \mid d \\
&\iff \deg_k(x_i) \mid d \quad \forall i \\
&\iff x_i \in k_d \quad \forall i \quad \text{(3.14.107)} \\
&\iff \phi^d(x_i) = x_i \quad \forall i \quad \text{(3.14.107)} \\
&\iff \phi^d(x) = x
\end{aligned}$$

By (3.14.46) $\mathrm{Gal}(k_d/k)$ 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 (3.14.77), 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 5.1.48 (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 5.1.49
For $X(k) = k^n$ we have $\#X(k_m) = p^{mn}$. Then

$$Z(X,T) = \exp\left(\sum_{n=1}^{\infty}\frac{p^{mn}T^m}{m}\right) = \exp(-\log(1 - p^n T)) = \frac{1}{1 - p^n T}$$

5.2 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

$$\mathrm{Specm}(A) := \{[\mathfrak{m}] \mid \mathfrak{m} \lhd A\}$$

For $S \subseteq A$ define

$$V(S) := \{[\mathfrak{m}] \mid S \subseteq \mathfrak{m}\}$$

and for $Y \subseteq \mathrm{Specm}(A)$ define

$$I(Y) = \bigcap_{[\mathfrak{m}]\in Y} \mathfrak{m}$$

Proposition 5.2.2 (Properties of Maximal Spectrum)
Consider $(\text{Specm}(A), A)$ *for* A *a finitely-generated reduced* k*-algebra (or more generally a Jacobson Ring) then we have a Galois connection*

$$\mathcal{P}(A) \underset{V}{\overset{I}{\leftrightarrows}} \mathcal{P}(\text{Specm}(A))$$

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* $\text{Specm}(A)$*. 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 (5.1.4). 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 $\text{Specm}(A)$ *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*

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

where the left arrow is the bijection described in (3.24.20) and is in fact a homeomorphism. For general k *we still have a commutative diagram*

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

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

$$\operatorname{Spec}(A) = \{[\mathfrak{p}] \mid \mathfrak{p} \triangleleft A\}$$

For $\mathfrak{a} \triangleleft A$ define

$$V(\mathfrak{a}) := \{[\mathfrak{p}] \mid \mathfrak{a} \subseteq \mathfrak{p}\}$$

and for $Y \subseteq \operatorname{Spec}(A)$ define

$$I(Y) = \bigcap_{[\mathfrak{p}] \in Y} \mathfrak{p}$$

Proposition 5.2.6 (Properties of Prime Spectrum)
Consider $(\operatorname{Spec}(A), A)$ for a ring A then we have a Galois connection

$$\mathcal{P}(A) \underset{V}{\overset{I}{\leftrightarrows}} \mathcal{P}(\operatorname{Spec}(A))$$

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 $\operatorname{Spec}(A)$. 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 (3.4.45).

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

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}) = \{\mathfrak{q} \mid \mathfrak{q} \supseteq \mathfrak{p}\} \tag{5.2}$$

Proof. Equation (5.2) 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 (4.1.11) $\{\mathfrak{p}\}$ is closed if and only $\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}}$ if and only if $\mathfrak{p}$ is maximal (see (3.4.57), (3.4.36)). □

Similarly to (5.1.14) 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 $X = \mathrm{Spec}(A)$ (resp. $\mathrm{Specm}(A)$).

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 (5.1.14). □

Corollary 5.2.9
$\mathrm{Spec}(A)$ *(resp.* $\mathrm{Specm}(A)$*) 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 $X = \mathrm{Spec}(A)$ (resp. $\mathrm{Specm}(A)$*) then there is a bijective correspondence*

$$\{Y \subset X \text{ closed }\} \underset{I}{\overset{V}{\leftrightarrows}} \{\mathfrak{a} \lhd A \text{ radical }\}$$

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 $\mathrm{Spec}(A)$ *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 $X = \mathrm{Spec}(A)$ (resp. $\mathrm{Specm}(A)$*) 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 $X = \mathrm{Spec}(A)$ (resp. $\mathrm{Specm}(A)$*). 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 (4.1.8) 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 (3.6.19). Conversely we see $f \in \overline{S_g} \implies af \in S_g$ by (3.6.19) 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

$$\begin{aligned}\operatorname{Spec}(\phi) : \operatorname{Spec}(B) &\to \operatorname{Spec}(A)\\ \mathfrak{p} &\to \phi^{-1}(\mathfrak{p})\end{aligned}$$

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

- *ϕ is surjective.*
- *ϕ is integral*
- *A and B are finitely-generated k-algebras and ϕ 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 (3.4.51). 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 ϕ is surjective, then $\operatorname{Spec}(\phi)$ maps maximal ideals to maximal ideals by (3.4.51).

Suppose alternatively that ϕ 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 (3.18.11) $\bar{A}$ is a field and $\phi^{-1}(\mathfrak{m})$ is maximal by (3.4.56) 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 (3.18.11). □

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 (3.6.18). 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 $\mathcal{O}_X$ (5.1.30) 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 (3.4.45) 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 $X = \operatorname{Spec}(A)$. We will also consider the case A a Jacobson ring and $X = \operatorname{Specm}(A)$. The main result is the following

Proposition 5.2.17 (Structure Sheaf)
Let A be a ring and $X = \operatorname{Spec}(A)$. Recall from (5.2.13) that

$$D(f) \subseteq D(g) \iff S_f \subseteq \overline{S_g}$$

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 (3.6.28). 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

$$\operatorname{Mor}(\mathcal{O}_X, \mathcal{G}) \to \operatorname{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}})$$

$$\phi \longrightarrow \phi|_{\mathcal{B}} \circ \eta_A$$

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 (3.6.33). Finally the canonical map $i_f : A \to A_f$ induces a homeomorphism

$$\widetilde{i_f} : \operatorname{Spec}(A_f) \to D(f)$$

and an isomorphism of sheaves

$$\widetilde{i_f}_\star(\mathcal{O}_{\operatorname{Spec}(A_f)}) \longrightarrow \mathcal{O}_X|_{D(f)}$$

Explicitly for $D(h) \subseteq D(g) \subseteq D(f)$ we have a commutative diagram

$$\begin{array}{ccccccc}
\mathcal{O}_{\mathrm{Spec}(A_f)}(\mathrm{Spec}(A_f)) & \xleftarrow{\eta_{A_f,1}} & (A_f)_1 & \xleftarrow{\sim} & A_f & \xleftarrow{\eta_{A,f}} & \mathcal{O}_X(D(f)) \\
\downarrow & & \downarrow{\scriptstyle i_{1(g/1)}} & & \downarrow{\scriptstyle i_{fg}} & & \downarrow \\
\mathcal{O}_{\mathrm{Spec}(A_f)}(D(g/1)) & \xleftarrow{\eta_{A_f,g/1}} & (A_f)_{g/1} & \xleftarrow{\sim} & A_g & \xleftarrow{\eta_{A,g}} & \mathcal{O}_X(D(g)) \\
\downarrow & & \downarrow{\scriptstyle i_{(g/1)(h/1)}} & & \downarrow{\scriptstyle i_{gh}} & & \downarrow \\
\mathcal{O}_{\mathrm{Spec}(A_f)}(D(h/1)) & \xleftarrow{\eta_{A_f,h/1}} & (A_f)_{h/1} & \xleftarrow{\sim} & A_h & \xleftarrow{\eta_{A,h}} & \mathcal{O}_X(D(h))
\end{array}$$

where the inner diagram is from (3.6.29), and the outer arrows are the isomorphisms η 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 $D(f) = D(g) \iff S_f = \overline{S_g}$, so we may construct a well-defined $\mathcal{B}$-presheaf

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

with restriction maps the canonical maps from (3.6.28). 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 $\mathcal{G}$)

$$\mathrm{Mor}(\mathcal{O}_X, \mathcal{G}) \longrightarrow \mathrm{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}})$$
$$\alpha \to \alpha|_{\mathcal{B}} \circ \eta_A$$

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 (3.6.33).

We claim there is an isomorphism of $\mathcal{B}$-presheaves

$$\tilde{i_f}_\star(\mathcal{O}'_{\mathrm{Spec}(A_f)}) \longrightarrow \mathcal{O}'_X|_{D(f)} \tag{5.3}$$

This is precisely the inner part of the commutative diagram stated and is demonstrated in (3.6.29). 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

$$(f_i f_j)^M (f_j^N a_i - f_i^N a_j) = 0 \tag{5.4}$$

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 (5.4)

$$f_i^{N+M} a = f_i^{N+M} \sum_j g_j f_j^M a_j = a_i f_i^M \sum_j g_j f_j^{N+M} = a_i f_i^M$$

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 (2.6.39) 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 (5.3)) 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.

[Bou89] N. Bourbaki. *Algebra: Chapters 4-7*. Algebra. Springer-Verlag, 1989.

[Bou98] N. Bourbaki. *Commutative Algebra: Chapters 1-7*. Number vol. 1 in Elements de mathematique. English. Springer, 1998.

[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.

[Kap74] I. Kaplansky. *Commutative Rings*. The University of Chicago Press, 1974.

[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.

[LE06] Q. Liu and R. Erne. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics (0-19-961947-6). Oxford University Press, 2006.

[Mat70] H. Matsumura. *Commutative Algebra*. Mathematics lecture note series. Benjamin, 1970.

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

[Mor12] Patrick Morandi. *Field and Galois theory*, volume 167. Springer Science & Business Media, 2012.

[Mum99] 1937 Mumford, David. *The red book of varieties and schemes : includes the Michigan Lectures (1974) on Curves and their Jacobians*. Lecture notes in mathematics (Springer-Verlag). Springer, New York, 1999.

[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.

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

[vdW91] B. L. van der Waerden. *Algebra: Volume I*. Springer New York, 1991.

[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.