Algebra, Geometry and Number Theory

David Rufino

February 19, 2025

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 - Serge 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 - Robin Hartshorne [Har13]
- Algebraic Geometry - J.S. Milne [Mil17]
- Basic Algebraic Geometry - Shafarevich [Sha94]
- Introduction to Algebraic Geometry - Serge Lang [Lan19]
- Elements of Algebraic Geometry (EGA) - Alexander Grothendieck

Analysis and Geometry

- General Topology - Kelley [Kel71]
- Foundations of Modern Analysis - Dieudonne [Die11]
- Real and Functional Analysis - Serge Lang [Lan12]
- Differential Calculus - Henri Cartan [Car67]

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*

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

*and the **range** of R*

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

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

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 $\sup X = \top$, otherwise 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 $S \subset X$

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

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

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

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

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

as required. □

2.1.5 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

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

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 $X \underset{f_\star}{\overset{f^\star}{\longleftrightarrow}} Y$. 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 3.4.15) and transcendence bases of field extensions (Section 3.18.16) 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 3.15) 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 $x_j = z$ and all the meet-primes minimal over x must occur in the decomposition. 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 3.25) and topology (Section 4.1.9). 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 6.3.2). 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

$$\begin{aligned} \dim(x) &:= \max_i \dim(x_i) = \dim(\{x\}^{\downarrow}) && (2.2)\\ \operatorname{codim}(y) &:= \min_j \operatorname{codim}(y_j) && (2.3)\\ \operatorname{codim}(y, x) &:= \min_j \max_i \{\operatorname{codim}(y_j, x_i) \mid y_j \leq x_i\} && (2.4)\\ &= \min_j \operatorname{codim}(y_j, x) && (2.5) \end{aligned}$$

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 (4.1.37).

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.

□

Proposition 2.5.11 (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 2.5.12
This is a corrected version of EGA IV 14.3.3, as noted by Heinrich.

Corollary 2.5.13
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 (2.5.11). 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 2.5.14
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 (2.5.11) by noting that an irreducible poset has only one maximal element and is in particular equidimensional. □

Proposition 2.5.15
Let $\mathcal{F}$ be a quasi-biequidimensional Krull Lattice. Then for all $x \in \mathcal{F}$ we have $\{x\}^{\downarrow}$ is a quasi-biequidimensional Krull Lattice.

Proof. Consider $y \in \mathcal{J}(\{x\}^{\downarrow}) \overset{(2.4.3)}{=} J(\mathcal{F}) \cap \{x\}^{\downarrow}$. Then by definition $\{y\}^{\downarrow}$ is biequidimensional, and so $\{x\}^{\downarrow}$ is quasi-biequidimensional. □

2.6 Category Theory

2.6.1 Categories

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

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

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

such that the following conditions hold

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

Example 2.6.2
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

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

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

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

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

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

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

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

*A **directed limit** is a cone $(\varinjlim_i A_i, \{\phi_i : A_i \to \varinjlim_i A\})$ for which given any other cone (A, 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

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

$$\psi^{-1}_{c,d}(g) = \epsilon_d \circ F(g)$$

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

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

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*

- $U(\mathrm{Hom}(c, d)) = \mathrm{Mor}(c, d)$
- $U(\mathrm{Hom}(f, d)) = \mathrm{Mor}(f, d)$
- $U(\mathrm{Hom}(c, g)) = \mathrm{Mor}(c, g)$

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.

Proof. Suppose α is a natural isomorphism then $U\alpha^{-1} \circ U\alpha = U(1_{\mathrm{Hom}(c,-)}) = 1_{\mathrm{Mor}(c,-)}$ and similarly $U\alpha \circ U\alpha^{-1} = 1_{\mathrm{Mor}(c',-)}$, so $U\alpha$ is a natural isomorphism.

□

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 Set-Valued Functor = Universal Element)
Let $F : \mathcal{C} \to \mathbf{Set}$ be a functor then there is a natural correspondence between representations and universal elements

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

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

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

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

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

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*

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

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

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

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

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

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

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

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.*

Proposition 3.2.7 ($\mathbb{N}$ is an initial object)
Let $(X, \cdot)$ be a monoid and $x \in X$. Then there is a unique monoid morphism

$$x^{(-)} : (\mathbb{N}, +) \to (X, \cdot)$$

such that

$$x^1 = x$$

Furthermore if $\phi : (X, \cdot) \to (Y, \cdot)$ is a monoid morphism then

$$\phi(x^n) = \phi(x)^n$$

for all $x \in X$ and $x \in \mathbb{N}$.

Proposition 3.2.8 ($\mathbb{Z}$ is an initial object)
Let $(X, \cdot)$ be a monoid and $x \in X$ be an invertible element. Then there is a unique monoid morphism

$$x^{(-)} : (\mathbb{Z}, +) \to (X, \cdot)$$

such that

$$x^1 = x$$

and

$$x^{-n} \text{ is the inverse of } x^n$$

Furthermore if $\phi : (X, \cdot) \to (Y, \cdot)$ is monoid morphism then

$$\phi(x^n) = \phi(x)^n$$

for all $x \in X$ invertible and $n \in \mathbb{Z}$.

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 **right coset** and we denote the set of right 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 $[g_1] = g_1H$. Then $g_2 \in [g_1] \iff g_1 \sim_H g_2 \iff g_2 \sim_H g_1 \iff g_2 g_1^{-1} \in H \iff g_2 \in g_1H$, which shows that the sets are equal.

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

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

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

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

More generally if $K \leq H$ then

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

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

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

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

Furthermore

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

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

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

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

$$G/N$$

forms a group under the binary operation

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

with identity eN.

a) *There is a canonical surjective group homomorphism*

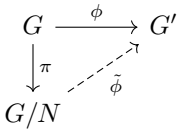
$$\pi : G \longrightarrow G/N$$
$$g \to gN$$

with kernel N.

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

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

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



such that

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

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

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

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

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

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

which preserves index, that is

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

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

3.3.1 Cyclic Groups

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

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

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

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

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

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

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

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

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

Proof. We prove each in turn

a) By (2.2.6) 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 $\{1, \ldots, n\}$.

*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*

c) *There is a well-defined group homomorphism*

$$\epsilon : S_n \to \{-1, 1\}$$

such that

$$\epsilon((i\,j)) = -1$$

and $\epsilon(1) = 1$.

d) *A cycle* σ *of length* r *satisfies* $\epsilon(\sigma) = (-1)^{r+1}$

3.3.4 Shuffle Permutations

Definition 3.3.36
Let $p + q = n$ *be positive integers. We define the subgroup of* ***shuffle permutations***

$$\mathrm{Sh}(p, q) := \{\sigma \in S_n \mid \sigma(1) < \ldots < \sigma(p) \text{ and } \sigma(p+1) < \ldots < \sigma(p+q)\}$$

Similarly if $p + q + r = n$ *are positive integers define the subgroup*

$$\mathrm{Sh}(p, q, r) := \{\sigma \in S_n \mid \sigma(1) < \ldots < \sigma(p) \text{ and } \sigma(p+1) < \ldots < \sigma(p+q) \text{ and } \sigma(p+q+1) < \ldots < \sigma(p+q+r)\}$$

Let $u : [1, p] \to [1, n]$ *and* $v : [1, q] \to [1, n]$ *be injective maps such that* $u([1, p]) \cap v([1, q]) = \emptyset$. *Define* $u \star v \in S_n$ *by*

$$(u \star v)(i) := \begin{cases} u(i) & 1 \leq i \leq p \\ v(i-p) & p < i \leq p+q \end{cases}$$

If u, v *are order preserving then* $u \star v \in \mathrm{Sh}(p, q)$. *Every shuffle permutation is of this form.*

Lemma 3.3.37
Let $X, Y \subset \mathbb{N}$ *be a finite sets of order* n. *There exists a unique order isomorphism*

$$u : X \to Y$$

Proposition 3.3.38
Let $p + q = n$ *be positive integers. There is a bijection*

$$\mathrm{Sh}(p, q) \to \{u : [1, p] \to [1, n] \text{ order preserinvg }\}$$

$$\sigma \to \sigma|_{[1,p]}$$

Proof. We provide an explicit inverse. For given u the set $Y := [1, n] \setminus u([1, p])$. As u is order preserving it is injective, whence $\#Y = n - \#u([1, p]) = n - p = q$. Therefore there is an order isomorphism $v : [1, q] \to Y$ and we may define the shuffle permutation $\sigma := u \star v$. □

Proposition 3.3.39
Let $p + q = n$ *be positive integers. There is an injective group homomorphism*

$$\begin{array}{ccc} S_p \times S_q & \to & S_n \\ (\sigma_1, \sigma_2) & \to & \sigma_1 \star (\sigma_2 + p) \end{array}$$

The image is the set $\sigma \in S_n$ *for which* $\sigma([1, p]) = [1, p]$ *(equivalently* $\sigma([p+1, q]) = \sigma([p+1, q])$.

Proposition 3.3.40
Let $p + q = n$ *be positive integers. There is a bijection*

$$\mathrm{Sh}(p, q) \to S_n / (S_p \times S_q)$$

Furthermore $\#\,\mathrm{Sh}(p, q) = \frac{(p+q)!}{p!q!}$. *By a similar argument* $\#\,\mathrm{Sh}(p, q, r) = \frac{(p+q+r)!}{p!q!r!}$.

Proof. Let $\sigma \in S_n$. Then there exists an order isomorphism $u : [1, p] \to \sigma([1, p])$ and $v : [1, q] \to \sigma([p+1, p+q])$. Define $\sigma_1(i) := u^{-1}(\sigma(i))$ and $\sigma_2(j) := v^{-1}(\sigma(j+p))$. Then we may verify that $\sigma_1 \in S_p$, $\sigma_2 \in S_q$ and

$$(u \star v) \circ (\sigma_1 \star (\sigma_2 + p)) = \sigma$$

so the map is surjective.

Suppose $\sigma, \sigma' \in \mathrm{Sh}(p,q)$ are such that

$$\sigma = \sigma' \circ (\sigma_1 \star (\sigma_2 + p))$$

for $\sigma_1 \in S_p$ and $\sigma_2 \in S_q$. If $\sigma_1 \neq e$ then there exists $1 \leq i < j \leq p$ such that $\sigma_1(j) < \sigma_1(i)$. Then by monotonicity of σ' we have $\sigma(j) = \sigma'(\sigma_1(j)) < \sigma'(\sigma_1(i)) = \sigma(i)$, which contradicts monotonicity of σ. So we conclude $\sigma_1 = e$ and similarly $\sigma_2 = e$. Therefore $\sigma = \sigma'$, and the map is injective. By the Orbit-Stabilizer theorem we have

$$\#\,\mathrm{Sh}(p,q) = \#S_n / \#(S_p \times S_q)$$

from which the result follows. □

Definition 3.3.41 (Circulant Permutation)
Let n be an integer, and write $\rho_n \in S_n$ for the permutation

$$\{1, \ldots, n\} \to \{2, 3, \ldots, n, n+1\}$$

Note that $\epsilon(\rho_n) = (-1)^{n+1}$.

Proposition 3.3.42 (Symmetry of Shuffling)
Let $p + q = n$ be positive integers. Then there is a bijection

$$\begin{aligned} \mathrm{Sh}(p,q) &\to \mathrm{Sh}(q,p) \\ \sigma &\to \sigma \circ \rho^p_{p+q} \end{aligned}$$

Note that $\epsilon(\rho^p_{p+q}) = (-1)^{pq}$ by (3.3.41).

Proposition 3.3.43 (Associativity of Shuffling)
The following map is a bijection

$$\begin{aligned} \pi : \mathrm{Sh}(p+q,r) \times \mathrm{Sh}(p,q) &\to \mathrm{Sh}(p,q,r) \\ (\sigma_1, \sigma_2) &\to \sigma_1 \circ (\sigma_2 \star (1_r + p + q)) \end{aligned}$$

Similarly so is

$$\begin{aligned} \pi' : \mathrm{Sh}(p,q+r) \times \mathrm{Sh}(q,r) &\to \mathrm{Sh}(p,q,r) \\ (\sigma_1, \sigma_2) &\to \sigma_1 \circ (1_p \star (\sigma_2 + p)) \end{aligned}$$

Proof. It is straightforward to verify that $\pi(\sigma_1, \sigma_2)$ is injective and satisfies the ordering properties. Therefore π is well-defined and we claim it is surjective.

Given $\sigma \in \mathrm{Sh}(p,q,r)$ let $u : [1, p+q] \to \sigma([1, p+q])$, $v : [1, r] \to \sigma([p+q+1, p+q+r])$ be the unique order isomorphisms. Define $\sigma_1 = u \star v$ and $\sigma_2 := u^{-1} \circ \sigma|_{[1,p+q]}$. We may verify that $\sigma_1 \in \mathrm{Sh}(p+q,r)$ and $\sigma_2 \in \mathrm{Sh}(p,q)$, and furthermore that $\pi(\sigma_1, \sigma_2) = \sigma$. By counting π is injective.

For the second case let $u : [1,p] \to \sigma([1,p])$, $v : [1, q+r] \to \sigma([p+1, p+q+r])$ be the unique order isomorphisms. Define $\sigma_1 = u \star v$ and $\sigma_2(j) := v^{-1}(\sigma(j+p))$. The verification follows as before. □

3.3.5 Totally Ordered Abelian Group

Definition 3.3.44 (Ordered Abelian Group)
*An abelian group $(G, +)$ together with a total order $\leq$ is an **ordered abelian group** if it satisfies*

$$x \leq y \implies x + z \leq y + z \quad \forall x, y, z \in G$$

Define $G^+ := \{g \in G \mid (0 \leq g) \wedge (g \neq 0)\}$ and $G^- := \{g \in G \mid (g \leq 0) \wedge (g \neq 0)\}$.

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*
- ***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 $\mathfrak{a} \lhd A$ 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 $\mathfrak{b} \lhd A$ such that $\mathfrak{b} \cap S = \emptyset$ then

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

has a maximal element, which is prime.

Proof. 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 $\mathfrak{a} \lhd A$ 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 $\mathfrak{a} \lhd A$ 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 (Minimal Primes consist of Zero Divisors)
Let $\mathfrak{p}$ be a proper prime ideal minimal over $\mathfrak{a}$. Then for every $x \in \mathfrak{p}$ there exists $a \in A \setminus \mathfrak{a}$ such that $xa \in \mathfrak{a}$.

In particular a minimal prime ideal consists of zero-divisors.

Proof. Observe that $\mathfrak{p}/\mathfrak{a}$ is a proper minimal prime ideal of $A/\mathfrak{a}$ by (3.4.55). Then the first statement is equivalent to showing every $x \in \mathfrak{p}/\mathfrak{a}$ is a zero divisor and we may reduce to the case $\mathfrak{a} = (0)$.

Consider the ring $A_\mathfrak{p}$, it has a unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$ which is also minimal by (3.6.32). Every other prime ideal is contained in $\mathfrak{p}A_\mathfrak{p}$ by (3.4.36), and therefore equal by minimality. Therefore $\sqrt{(0)A_\mathfrak{p}} = \mathfrak{p}A_\mathfrak{p}$ by (3.4.46). Suppose $x \in \mathfrak{p}$ then $x^n/1 = 0$ and $tx^n \in \mathfrak{a}$ for $t \notin \mathfrak{p}$. Choose n minimal subject to this condition. Then $n \geq 1$ because $t \notin \mathfrak{a}$, and so $a = tx^{n-1}$ has the required properties. □

Proposition 3.4.45
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 3.4.46 (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 3.4.47 (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 (3.4.46) 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)

□

Lemma 3.4.48 (Ideal Finitely Generated by Nilpotents is Nilpotent)
Let A be a ring with ideals $\mathfrak{a}, \mathfrak{b}$ such that $\sqrt{\mathfrak{a}} \subseteq \mathfrak{b}$ and $\mathfrak{b}$ finitely generated. Then there exists an integer $n > 0$ such that $\mathfrak{b}^n \subseteq \mathfrak{a}$.

Definition 3.4.49 (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 3.4.50 (Operations on ideals)
Let $\phi : A \to B$ a ring homomorphism and $\mathfrak{a} \lhd A$, $\mathfrak{b} \lhd B$ ideals then

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

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

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

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

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

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

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

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

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

Proof. We prove each in turn

a-c) Straightforward

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

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

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

h) By c) and g) we find $(\sqrt{\mathfrak{b}^c})^e = \left(\sqrt{\mathfrak{b}}\right)^{ce} \subseteq \sqrt{\mathfrak{b}}$. We will show that when 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 3.4.51
Let $\phi : A \to B$ be a ring homomorphism then extension and contraction constitute a monotone Galois connection

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

and therefore is order-preserving and satisfies the adjoint property

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

is satisfied.

Proof. Extension and contraction satisfy conditions of (2.1.49) by (3.4.50).c) and d) □

Corollary 3.4.52
Let $\phi : A \to B$ be a ring homomorphism then there is a order-preserving bijection between "contracted" and "extended ideals"

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

which restricts to proper ideals.

Proof. We've shown that $\mathfrak{a}$ (resp. $\mathfrak{b}$) is contracted (resp. extended) if and only if the given maps are mutually inverse. Note that $\mathfrak{b}$ is proper implies $\mathfrak{b}^c$ is proper. Furthermore $\mathfrak{b}^c$ proper implies $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ is proper. Therefore it restricts to proper ideals. □

Proposition 3.4.53 (Inverse image of maximal / prime ideals)
Let $\phi : A \to B$ be a morphism then

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

Proposition 3.4.54
Consider maps $\phi : A \to B$ and $\psi : B \to C$ and an ideal $\mathfrak{a} \lhd A$. 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 3.4.55 (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

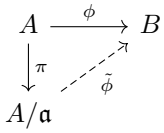
$$\cdot : A/\mathfrak{a} \times A/\mathfrak{a} \to A/\mathfrak{a}$$
$$(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) \to (a \cdot b + \mathfrak{a})$$

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.*



- $\ker(\tilde{\phi}) = \ker(\phi)/\mathfrak{a}$
- $\tilde{\phi}$ *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

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

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

Corollary 3.4.56 (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 3.4.57 (Second Isomorphism Theorem)
Let $\mathfrak{b}$,$\mathfrak{a}$ *be ideals then there is a unique morphism making the diagram commute*

$$\begin{array}{ccc} A & \xrightarrow{\quad\pi\quad} & A/\mathfrak{a} \\ \downarrow{\scriptstyle\pi} & \swarrow & \downarrow{\scriptstyle\pi} \\ A/(\mathfrak{a}+\mathfrak{b}) & \xrightarrow{\sim} & (A/\mathfrak{a})/((\mathfrak{a}+\mathfrak{b})/\mathfrak{a}) \end{array}$$

which is in fact an isomorphism. If $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$ *this restricts to an isomorphism of* $A/\mathfrak{b}$*-modules*

$$\begin{array}{ccc} \mathfrak{c} & \xrightarrow{\quad\pi\quad} & \mathfrak{c}/\mathfrak{a} \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ \mathfrak{c}/(\mathfrak{a}+\mathfrak{b}) & \xrightarrow{\sim} & (\mathfrak{c}/\mathfrak{a})/((\mathfrak{a}+\mathfrak{b})/\mathfrak{a}) \end{array}$$

Proposition 3.4.58 (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 (3.4.55) 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 (3.4.55) $\mathfrak{a}$ 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 3.4.59
Let $\mathfrak{a} \lhd A$ *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 (3.4.58). □

Corollary 3.4.60 (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 (3.4.45) these form an ideal.

Definition 3.4.61 (Nilradical)
*Define the **nilradical** to be the set (ideal) of nilpotents*

$$N(A) := \sqrt{(0)} \overset{(3.4.46)}{=} \bigcap_{\mathfrak{p}} \mathfrak{p}$$

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

We also make the following definition

Definition 3.4.62 (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 3.4.63
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 (3.4.61) $N(A) = \bigcap_{\mathfrak{p}} \mathfrak{p} = \mathfrak{p}_0$ is prime and A is irreducible. □

Proposition 3.4.64 (Integral Domain $\iff$ Reduced and Irreducible)
Let A be a ring. Then the following are equivalent

a) *A is an integral domain*

b) *A is reduced and has a unique minimal prime*

c) *(0) is prime*

d) *A is reduced and irreducible.*

The following may be useful

Proposition 3.4.65
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 3.4.66 (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 3.4.67 (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 3.4.68 (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 3.4.69 (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 3.10. More generally we have

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

Proposition 3.4.70
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 3.4.71 (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 3.4.72 ((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 3.4.73 (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)

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

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

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

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 3.4.74 (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 3.4.75 (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

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

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

Proposition 3.4.76 (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

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

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

Corollary 3.4.77
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

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

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 3.4.78 (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 3.4.79
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 3.4.80
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 3.4.81 (Faithful Module)
We say an A*-module* M *is* ***faithful*** *if*

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

Definition 3.4.82 (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 3.4.83 (Finite Module)
An A*-module* M *is* ***finite*** *if there exists a finite spanning set.*

Definition 3.4.84 (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 3.4.85 (Free Module)
Let M *be an* A*-module. We say that* M *is a* ***free module*** *over* A *if it has a basis.*

Proposition 3.4.86 (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 3.4.87 (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 3.4.88
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 3.4.89
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 3.4.90 (Vector space)
If k *is a field and* V *a* k*-module, then we say* V *is a* ***vector space*** *over* k.

Remark 3.4.91
We will see that every vector space is free and every k*-submodule is a direct factor.*

Proposition 3.4.92 (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 3.4.93 (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 3.4.94 (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 3.4.95 (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

$$\begin{array}{ccc} M & \xrightarrow{\psi} & P \\ \downarrow{\scriptstyle \pi} & \nearrow_{\tilde{\psi}} & \\ M/N & & \end{array}$$

Furthermore there is a bijection of A-submodules

$$\{P' \subseteq M/N\} \longleftrightarrow \{P \mid N \subseteq P \subseteq M\}$$

given by $P' = P/N$. *In the situation above* $\ker(\tilde{\psi}) = \ker(\psi)/N$. *In particular if* $\ker(\psi) = N$ *then* $\tilde{\psi}$ *is injective.*

Corollary 3.4.96
Let $\psi : M \to N$ *be an A-module homomorphism, then this induces an isomorphism*

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

Definition 3.4.97 (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 3.4.98
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 3.4.99 (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 3.4.100 (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 3.4.101 (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 3.4.102 (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 3.4.103 (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 $\{v_1, \ldots, v_n\}$ then $M^\vee$ is a finite free right *(resp.* left*) A-module with basis $\{v_1^\vee, \ldots, v_n^\vee\}$ 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 3.4.104 (Hom-Set is free)
Let M be a finite free left A-module with basis $\{v_1, \ldots, v_n\}$ and N a (A, B)-bimodule. Then there is an isomorphism of right B-modules

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

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

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

where $w_1^\vee, \ldots, w_m^\vee$ 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 3.4.105 (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

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

Corollary 3.4.106 (Double Dual Natural Isomorphism)
Let A be a commutative ring and M a finite free A-module then the canonical A-module homomorphism

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

is an isomorphism, which is natural in M.

Corollary 3.4.107
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 3.4.108 (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 3.4.109
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 3.4.110
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

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

Corollary 3.4.111
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 3.4.112 (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 3.4.113 (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 3.4.114
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 3.4.115
Let E, F be matrices then

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

3.4.13 Multilinear Maps and Determinants

Definition 3.4.116 (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 3.4.117 (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 3.4.118
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 3.4.119 (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 $L_a^n(M, N)$ the set of such alternating maps, and $L_a^n(M) := L_a^n(M, A)$ the set of **alternating forms**. These are clearly A-modules.*

Proposition 3.4.120 (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*

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

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

- *There is an "exterior product"*

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

  given by

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

Lemma 3.4.121
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 3.4.122 (Transpose)
Let M be a finite free A-module with basis $v_1, \dots, v_n$. Define the transpose operation

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

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 3.4.123
Let $f : M^n \to N$ be an alternating map. Suppose $v_1, \dots, v_n \in M$ and $w_1, \dots, w_n \in M$ such that

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

then

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

Proof. By expansion

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

where σ ranges over all maps from $\{1, \dots, n\}$ to itself. If σ is not a permutation, then it must not be injective and by (3.4.121) the corresponding term is zero. Therefore we may restrict to the case $\sigma \in S_n$. By the first part of (3.4.121) the result follows. □

Proposition 3.4.124 (Existence and Uniqueness of Determinants)
There is a unique $D \in L_a^n(A^n)$ such that $D(e_1, \dots, e_n) = 1$, given by the Leibniz Formula

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

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

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

The form D also satisfies the "Laplace Expansion" formula

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

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

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

is an alternating form by (3.4.120). By induction it evaluates to 1 when $v_i = e_i$. This demonstrates the existence of D.

By (3.4.123) D satisfies Leibniz' Formula and furthermore so does any $\Delta \in L_a^n(M)$. Therefore $\Delta = \Delta(e_1, \dots, e_n)D$, 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 3.4.125 (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 (3.4.120) 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 3.4.126 (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 3.4.127 (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 $L_a^n(f)(\Delta) = c\Delta$ for some $c \in A$ by (3.4.124). Clearly $D(f) := c$ satisfies the equation for all such $\psi = a\Delta$. It's unique because $L_a^n(M)$ is a free module, and the properties follow from uniqueness.

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

Proposition 3.4.128
*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 (3.4.120) it is an alternating form such that $D^{ik}(e_1, \ldots, e_n) = \delta_{ik}$. We therefore conclude from (3.4.124) 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 (3.4.122). 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 3.4.129
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 3.4.130 (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 (3.4.126) with (3.4.127) 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 3.4.131 (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 (3.4.108) and (3.4.127). 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 Exterior Product

Proposition 3.4.132
Let M be an A-module. There is a bilinear map

$$\wedge : L_a^p(M) \times L_a^q(M) \quad \to \quad L_a^{p+q}(M)$$

given by

$$(f \wedge g)(x_1, \ldots, x_{p+q}) \quad := \quad \sum_{\sigma \in \mathrm{Sh}(p,q)} \epsilon(\sigma) f(x_{\sigma(1)}, \ldots, x_{\sigma(p)}) g(x_{\sigma(p+1)}, \ldots, x_{\sigma(p+q)})$$

where the sum is taken over shuffle permutations (3.3.36).

Proof. Suppose that $x_i = x_j$ then we require to prove that $(f \wedge g)(x_1, \ldots, x_{p+q}) = 0$ in order to demonstrate that it is alternating. If $1 \leq i, j \leq p$ then this follows from (3.4.121). Similarly if $p < i, j \leq p + q$. So we may consider the case $i \leq p < j$. Consider the family of right cosets $\mathrm{Sh}(p,q)/\{e, (i,j)\}$, and let Σ be some coset representatives. Then by (3.3.10)

$$\mathrm{Sh}(p,q) = \bigsqcup_{\sigma \in \Sigma} \{\sigma, (i,j)\sigma\}$$

Therefore the sum is equal to

$$\sum_{\sigma \in \Sigma} \epsilon(\sigma) \left[f(x_\sigma) g(x_\sigma) - f(x_{(i\ j)\sigma}) g(x_{((i\ j)\sigma)}) \right]$$

so when $x_i = x_j$ this sum is zero. □

Proposition 3.4.133 (Basic Properties of Exterior Product)
Let M be an A-module. Suppose $f \in L_a^p(M)$, $g \in L_a^q(M)$ and $h \in L_a^r(M)$. Then the following properties hold

a) $f \wedge g = (-1)^{pq} g \wedge f$

b) $(f \wedge g) \wedge h = f \wedge (g \wedge h)$

Proof. a) By definition and (3.3.42)

$$\begin{aligned}
(f \wedge g)(x) &= \sum_{\sigma \in \mathrm{Sh}(p;q)} \epsilon(\sigma) f(x_{\sigma(1)}, \ldots, x_{\sigma(p)}) g(x_{\sigma(p+1)}, \ldots, x_{\sigma(p+q)}) \\
&= \sum_{\sigma \in \mathrm{Sh}(q;p)} (-1)^{pq} \epsilon(\sigma) f(x_{\sigma(p+1)}, \ldots, x_{\sigma(p+q)}) g(x_{\sigma(1)}, \ldots, x_{\sigma(p)}) \\
&= (-1)^{pq} (g \wedge f)
\end{aligned}$$

b) Similarly by definition

$$\begin{aligned}((f\wedge g)\wedge h)(x_1,\dots,x_{p+q+r}) &= \sum_{\sigma\in \mathrm{Sh}(p+q,r)} \epsilon(\sigma)(f\wedge g)(x_{\sigma(1)},\dots,x_{\sigma(p+q)})h(x_{\sigma(p+q+1)},\dots,x_{\sigma(p+q+r)})\\ &= \sum_{\sigma\in \mathrm{Sh}(p+q,r)}\sum_{\tau\in \mathrm{Sh}(p,q)} \epsilon(\sigma)\epsilon(\tau) f(x_{\sigma(\tau(1))},\dots,x_{\sigma(\tau(p))})g(x_{\sigma(\tau(p+1))},\dots,x_{\sigma(\tau(p+q))})\\ &\quad h(x_{\sigma(p+q+1)},\dots,x_{\sigma(p+q+r)})\\ &\overset{(3.3.43)}{=} \sum_{\sigma\in \mathrm{Sh}(p,q,r)} \epsilon(\sigma) f(x_{\sigma(1)},\dots,x_{\sigma(p)})g(x_{\sigma(p+1)},\dots,x_{\sigma(p+q)})h(x_{\sigma(p+q+1)},\dots,x_{\sigma(p+q+r)})\end{aligned}$$

and symmetrically

$$\begin{aligned}(f\wedge(g\wedge h))(x_1,\dots,x_{p+q+r}) &= \sum_{\sigma\in \mathrm{Sh}(p,q+r)} \epsilon(\sigma) f(x_{\sigma(1)},\dots,x_{\sigma(p)})(g\wedge h)(x_{\sigma(p+1)},\dots,x_{\sigma(p+q+r)})\\ &= \sum_{\sigma\in \mathrm{Sh}(p,q+r)}\sum_{\tau\in \mathrm{Sh}(q,r)} \epsilon(\sigma)\epsilon(\tau) f(x_{\sigma(1)},\dots,x_{\sigma(p)})g(x_{\sigma(\tau(p+1))},\dots,x_{\sigma(\tau(p+q))})\\ &\quad h(x_{\sigma(\tau(p+q+1))},\dots,x_{\sigma(\tau(p+q+r))})\\ &\overset{(3.3.43)}{=} \sum_{\sigma\in \mathrm{Sh}(p,q,r)} \epsilon(\sigma) f(x_{\sigma(1)},\dots,x_{\sigma(p)})g(x_{\sigma(p+1)},\dots,x_{\sigma(p+q)})h(x_{\sigma(p+q+1)},\dots,x_{\sigma(p+q+r)})\end{aligned}$$

therefore we conclude that the expressions are equal.

□

3.4.15 Vector Spaces

Definition 3.4.134 (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 3.4.135 (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 3.4.136 (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 3.4.137 (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 3.4.138 (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 $\Delta \in L_a^n(V)$ 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 (3.4.121) 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 (3.4.121). □

Proposition 3.4.139
A vector space $V = \{0\}$ if and only if $\dim_k V = 0$

Proposition 3.4.140 (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 3.4.141 (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 3.4.142
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 (3.4.137). 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 3.4.143 (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 3.4.144 (Rank)
Let $\phi : V \to W$ be a linear map then define

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

Proposition 3.4.145 (Surjective Criteria)
Let $\phi : V \to W$ be a linear map with W finite-dimensional then

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

Proof. This follows directly from (2.3.15). □

Proposition 3.4.146 (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 3.4.147 (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 3.4.148 (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 (3.4.129). □

Proposition 3.4.149 (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 3.4.150 (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 3.4.151 (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

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

3.4.15.1 Dual Space

Definition 3.4.152 (Dual Space)
*Let V be a k-vector space and define the **dual space** to be*

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

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

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

Definition 3.4.153 (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 3.4.154 (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 (3.4.146) and (3.4.103). □

Corollary 3.4.155 (Dual rank = rank)
Let $\phi : V \to W$ be a linear map and $\phi^\vee : W^\vee \to V^\vee$ then

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

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

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

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

Consider the finite-dimensional case. By (3.4.154)

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

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

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

By (3.4.154) 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 3.4.156 ($(-)^\vee$ 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 (3.4.155) we have $\operatorname{rank}_k(\phi) = \operatorname{rank}_k(\phi^\vee)$ and by (3.4.103) $\dim_k V^\vee = \dim_k V$.

ϕ is surjective $\iff \operatorname{rank}_k(\phi) = \dim_k W = \operatorname{rank}_k(\phi^\vee) \overset{(3.4.146)}{\iff} \dim_k \ker(\phi^\vee) = 0 \iff \ker(\phi^\vee) = \{0\}$

ϕ is injective $\iff \dim_k \ker(\phi) = 0 \overset{(3.4.146)}{\iff} \operatorname{rank}_k(\phi) = \dim_k V \iff \dim_k V^\vee = \operatorname{rank}_k(\phi^\vee) \iff \phi^\star$ is surjective.

The last point may be deduced from the first two, or the fact that $(-)^\vee$ is full and faithful (3.4.107) and category-theoretic result (2.6.39). □

3.4.15.2 Bilinear Pairings

Definition 3.4.157 (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

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

Proposition 3.4.158 (Matrix Representation)
Let V, W be finite-dimensional vector spaces with bases $\{v_1, \dots, v_n\}$ and $\{w_1, \dots, w_m\}$ then there is a canonical isomorphism

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

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

Proposition 3.4.159 (Dual maps)
Let V and W be vector spaces, then there is a natural bijection

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

where

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

When V, W are finite-dimensional then 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

$$\operatorname{rank}_k(\psi_L) = \operatorname{rank}_k(\psi_R)$$

Proof. The bijections stated are obvious. One may show that $\psi_L = \psi_R^\star \circ \eta_V$ where η_V is the dual isomorphism. Therefore ψ_L is an isomorphism if and only if $\psi_R^\star$ is an isomorphism, and by (3.4.156) if and only if ψ_R is an isomorphism. Since η_V is surjective we have $\operatorname{rank}_k(\psi_L) = \operatorname{rank}_k(\psi_R^\star) = \operatorname{rank}_k(\psi_R)$, by (3.4.155). □

Definition 3.4.160 (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 3.4.161
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 $\dim_k U^\perp \overset{(3.4.141)}{=} \dim_k U^\circ \overset{(3.4.154)}{=} \dim_k V/U = \dim_k V - \dim_k U$. □

Remark 3.4.162
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 3.4.163 (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 (3.4.147) ψ'_R is an isomorphism and ψ' is perfect.

□

3.4.15.3 Trace operator

Definition 3.4.164 (Rank-1 linear map)
Let V be a vector space then there is a canonical bilinear map

$$\begin{aligned} \times : V \times V^\vee &\to \operatorname{End}_k(V) \\ (v, \theta) &\to (x \to \theta(x)v) \end{aligned}$$

*This is known as a **rank-1** linear map.*

Proposition 3.4.165 (Trace operator)
Let V be a finite-dimensional vector space then there is a unique k-linear map $\operatorname{Tr} : \operatorname{End}_k(V) \to k$ 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 (3.4.104) 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 (3.4.158) the diagram commutes, and in particular

$$\mathrm{Tr}(v \cdot \theta) = \theta(v)$$

for any $v \in V$ and $\theta \in V^\vee$. □

3.4.15.4 Matrix Rank

Definition 3.4.166 (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 3.4.167 (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 (3.4.155) $\mathrm{rank}_k(\widehat{E}) = \mathrm{rank}_k(\widehat{E}^\vee)$ and by (3.4.114) 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 (3.4.137) 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 (3.4.137). Therefore $\mathrm{rk}(E)$ is the maximal number of linearly independent rows or columns. □

Proposition 3.4.168 (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 (3.4.108) 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 (3.4.148).

Finally it's clear from either $a), b)$ or $e)$ that this property is self-dual. □

Definition 3.4.169 (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 3.4.170 (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 (3.4.168).e)

Suppose $b)$ holds, then a-fortiori E has r linearly independent columns. Therefore by (3.4.167) $\mathrm{rk}(E) \geq r$ and $a)$ holds.

Conversely suppose $\mathrm{rk}(E) \geq r$ then by (3.4.167) there are certainly r linearly independent columns. We consider the $m \times r$ sub-matrix E' consisting of these columns. By (3.4.167) $\mathrm{rk}(E') = r$ 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 (3.4.168) is full rank as required. □

Corollary 3.4.171
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

$$\mathrm{Bilin}(-,-;-) : (A\textbf{-Mod} \times A\textbf{-Mod})^{op} \times A\textbf{-Mod} \to A\textbf{-Mod}$$

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*

$$\otimes_A : A\textbf{-Mod} \times A\textbf{-Mod} \to A\textbf{-Mod}$$

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 $(F/S, i)$ is a universal element for $\mathrm{Bilin}(-,-;-)$ as we required and we denote this by $M \otimes N$. The representation exists as a functor of sets by (2.6.57), and Φ is clearly an isomorphism of A-modules because

$$\Phi(f + g) = (f + g) \circ i = f \circ i + g \circ i = \Phi(f) + \Phi(g)$$

and

$$\Phi(\lambda f) = (\lambda f) \circ i = \lambda(f \circ i) = \lambda\Phi(f)$$

□

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 (3.4.73).

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

  $$\begin{array}{rcl} \Phi : \mathrm{Hom}(M_B \otimes_B {}_BN, Z) & \cong & \mathrm{Balan}(M_B, {}_BN; Z) \\ \theta & \to & \theta \circ i \end{array}$$

  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 $(F/S, i)$ is a universal element for $\mathrm{Balan}(-, -; -)$ and we denote this by $M_B \otimes_B {}_B N$. Then (2.6.57) exhibits Φ as a natural isomorphism of sets, which may readily observed to be additive.

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 $\mathrm{Bilin}(-, -; -)$ has universal element $({}_A M_B \otimes_B {}_B N_C, i)$. The (2.6.57) exhibits Φ as a natural isomorphism of sets which may be readily exhibited to be additive. □

Lemma 3.5.11 (Currying Lemma)
Let M, N, P, Y, Z be bimodules. Then there is an isomorphism of abelian groups and (A, B)-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

$$\begin{array}{ccc} \mathrm{RHom}({}_B N_C \otimes {}_C P_D, {}_A Z_D) & \xrightarrow{\sim} & \mathrm{RBilin}({}_B N_C, {}_C P_D; {}_A Z_D) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(N_C \otimes {}_C P, Z) & \xrightarrow{\sim} & \mathrm{Balan}(N_C, {}_C P; Z) \end{array}$$

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*

$$\begin{aligned} M\otimes_A N &\cong \bigoplus_{i\in I} M \\ m\otimes\sum_i a_i n_i &\longrightarrow (m\cdot a_i)_{i\in I} \\ \sum_i (m_i\otimes n_i) &\longleftarrow (m_i)_{i\in I} \end{aligned}$$

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)

$$M\otimes_A N \cong M\otimes_A \left(\textstyle\bigoplus_{i\in I} A\right) \cong \textstyle\bigoplus_{i\in I}(M\otimes_A A) \cong \bigoplus_{i\in I} M$$

$$m\otimes\textstyle\sum_i a_i n_i \to \quad m\otimes(a_i)_{i\in I} \quad\to\quad (m\otimes a_i)_{i\in I} \quad\to (m\cdot a_i)_{i\in I}$$

□

Corollary 3.5.23
If M,N are free A-modules with bases $\{m_i\}_{i\in I}$ and $\{n_j\}_{j\in J}$ then $M\otimes_A N$ is a free A-module with basis $\{m_i\otimes n_j\}_{(i,j)\in I\times J}$.

Corollary 3.5.24 (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 3.5.25 (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*

$$\begin{aligned} M_{(B)} &\cong \bigoplus_{i\in I} B \\ b\otimes\sum_i a_i m_i &\to (b\phi(a_i))_{i\in I} \end{aligned}$$

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

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

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 (3.4.77) 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 (3.4.104)

Proposition 3.5.26 (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 (3.5.25) 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 Tensor Product Exact Sequences

Proposition 3.5.27 (Tensor Product is Right Exact)
Consider an exact sequence of A-modules (i.e. such that β is surjective and $\ker(\beta) = \mathrm{im}(\alpha)$)

$$M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

Then the corresponding sequence of A-modules

$$M \otimes_A Z \xrightarrow{\alpha\otimes 1_Z} N \otimes_A Z \xrightarrow{\beta\otimes 1_Z} P \otimes_A Z \to 0$$

is exact. Similarly the sequence

$$Z \otimes_A M \xrightarrow{1_Z\otimes\alpha} Z \otimes_A N \xrightarrow{1_Z\otimes\beta} Z \otimes_A P \to 0$$

is exact.

Proof. Trivially the submodule $\mathrm{im}(\beta \otimes 1_Z)$ contains elementary tensors and therefore equals $P \otimes_A Z$. In otherwords $\beta \otimes 1_Z$ is surjective. Furthermore by functoriality $(\beta \otimes 1_Z) \circ (\alpha \otimes 1_Z) = (\beta \circ \alpha) \otimes 1_Z$ which is zero on elementary tensors and therefore zero everywhere. In particular $\mathrm{im}(\alpha \otimes 1_Z) \subseteq \ker(\beta \otimes 1_Z)$. Consider a commutative diagram

$$\begin{array}{ccc} P \times Z & \xrightarrow{\psi} & (N \otimes_A Z)/\mathrm{im}(\alpha \otimes 1_Z) \\ & \searrow & \downarrow \overline{\beta\otimes 1_Z} \\ & & P \otimes_A Z \end{array}$$

where ψ is yet to be defined. For a given $p \in P$ and $z \in Z$ consider the subset

$$\mathcal{I}_{p,z} := \{n \otimes z \mid n \in N,\ \beta(n) = p\} \subset N \otimes_A Z$$

Observe that any ψ making the diagram commute satisfies $\psi(p, z) \in \overline{\mathcal{I}_{p,z}}$, and we aim to show this set is a singleton.

As β is surjective $\mathcal{I}_{p,z}$ is non-empty. First we show that $x, y \in \mathcal{I}_{p,z} \implies x - y \in \mathrm{im}(\alpha \otimes 1_Z)$. For if $\beta(n) = \beta(n')$ then $\beta(n - n') = 0$ by definition $n - n' = \alpha(m)$ for some $m \in M$. It follows that $n \otimes z - n' \otimes z = \alpha(m) \otimes z = (\alpha \otimes 1_Z)(m \otimes z)$. This shows that $\overline{\mathcal{I}_{p,z}}$ is a singleton, whose element we define to be $\psi(p, z)$. Then ψ is the unique map such that

$$\psi(\beta(n), z) = \overline{n \otimes z}$$

for all $n \in N$ and $z \in Z$. Clearly ψ is A-bilinear and therefore there is a map $\sigma : P \otimes_A Z \to (N \otimes_A Z)/\mathrm{im}(\alpha \otimes 1_Z)$ such that $\sigma(\beta(n) \otimes z) = \overline{n \otimes z}$. By linearity $\sigma \circ \overline{\beta \otimes 1_Z}$ is the identity which shows $\overline{\beta \otimes 1_Z}$ is injective. Therefore $\ker(\beta \otimes 1_Z) = \mathrm{im}(\alpha \otimes 1_Z)$ as required (for $x \in \ker(\beta \otimes 1_Z) \implies (\beta \otimes 1_Z)(x) = 0 \implies (\overline{\beta \otimes 1_Z})(\overline{x}) = 0 \implies \overline{x} = 0 \implies x \in \mathrm{im}(\alpha \otimes 1_Z)$). □

Proposition 3.5.28 (Quotient of a Tensor Product)
Consider exact sequences

$$0 \to M' \xrightarrow{i} M \xrightarrow{\pi_1} M/M' \to 0$$
$$0 \to N' \xrightarrow{j} N \xrightarrow{\pi_2} N/N' \to 0$$

Then there is an exact sequence

$$\begin{array}{rcccl} (M' \otimes N) \oplus (M \otimes N') & \xrightarrow{\alpha} & M \otimes N & \xrightarrow{\pi_1 \otimes \pi_2} & M/M' \otimes N/N' \to 0 \\ (m' \otimes n, m \otimes n') & \longrightarrow & i(m') \otimes n + m \otimes j(n') & \longrightarrow & \overline{m} \otimes \overline{n} \to 0 \end{array}$$

In particular there is a canonical isomorphism

$$(M \otimes N)/(M' \otimes N + M \otimes N') \cong M/M' \otimes N/N'$$

Proof. Observe $\pi_1 \otimes \pi_2 = (\pi_1 \otimes 1_{N/N'}) \circ (1_M \otimes \pi_2)$ by comparison on elementary tensors. By (3.5.27) each of these maps is surjective, and so the composite is surjective. Evidently $(\pi_1 \otimes \pi_2) \circ (i \otimes 1_N) = 0$ and $(\pi_1 \otimes \pi_2) \circ (1_M \otimes j) = 0$ by checking elementary tensors. This in particular means that $(\pi_1 \otimes \pi_2) \circ \alpha = 0$ where α is the first map. Therefore $\mathrm{im}(\alpha) \subseteq \ker(\pi_1 \otimes \pi_2)$ and it suffices to demonstrate the reverse inclusion. Suppose $z \in \ker(\pi_1 \otimes \pi_2)$. This means precisely that $(1_M \otimes \pi_2)(z) \in \ker(\pi_1 \otimes 1_{N/N'}) = \mathrm{im}(i \otimes 1_{N/N'})$ by (3.5.27). Therefore $(1_M \otimes \pi_2)(z) = (i \otimes 1_{N/N'})(y)$ for $y \in M' \otimes N/N'$. By (3.5.27) again $y = (1_{M'} \otimes \pi_2)(x)$ for $x \in M' \otimes N$ and $(1_M \otimes \pi_2)(z) = (i \otimes \pi_2)(x)$. Therefore $(1_M \otimes \pi_2)(z - (i \otimes 1_N)(x)) = 0$ and $z - (i \otimes 1_N)(x) = (1_M \otimes j)(w)$ for some $w \in M \otimes N'$. Therefore we conclude $z \in \mathrm{im}(\alpha)$ as required. □

3.5.6 Vector Space Tensor Product

Recall that vector spaces are free, every linearly independent set may be extended to a basis and every subspace is a direct factor. This simplifies the structure of tensor product.

Proposition 3.5.29
Let V, W be k-vector spaces with subspaces V' and W'. Then the canonical k-module homomorphism

$$V' \otimes_k W' \to V \otimes_k W$$

is injective.

Proof. The homomorphism exists by (3.5.35). By (3.4.150) both V' and W' are direct factors. Therefore the map is injective by (3.5.21). □

Proposition 3.5.30
Let V, W be k-modules. Suppose $\{v_i\}_{i \in I}$ and $\{w_j\}_{j \in J}$ are linearly independent (resp. bases) then $\{v_i \otimes w_j\}_{(i,j) \in I \times J}$ is a k-linearly independent subset (resp. a k-basis) of $V \otimes_k W$.

Proof. The case that they are bases is simply (3.5.23). For the general case we may use (3.4.137) to extend to bases, then a-fortiori the given set, being a subset of a basis, is linearly independent. □

3.5.7 Algebra Tensor Product

Let A be a commutative ring and revert to the case of commutative tensor product described in 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 3.5.31
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 3.5.32
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

$$\begin{array}{rcl} X \otimes_A X & \cong & (B \otimes_A B) \otimes_A (C \otimes_A C) \\ (b \otimes c) \otimes (b' \otimes c') & \to & (b \otimes b') \otimes (c \otimes c') \end{array}$$

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 (3.5.31), 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 3.5.33 (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

$$\begin{array}{rcl} \cdot : (B \otimes_A C) \times (B \otimes_A C) & \to & B \otimes_A C \\ (b \otimes c) \cdot (b' \otimes c') & := & (bb') \otimes (cc') \end{array}$$

and may be extended by linearity. Further there is an ring homomorphism

$$\begin{array}{rcl} i_A : A & \to & B \otimes_A C \\ a & \to & (a \otimes 1) = (1 \otimes a) \end{array}$$

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 (3.5.32). Define $x \cdot y := m(x \otimes y)$ then the properties of m ensure that this satisfies the properties of a ring. □

Proposition 3.5.34 (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 3.5.35 (Functoriality)
Let $\phi : B \to B'$ and $\psi : C \to C'$ be A-algebra homomorphisms. The A-module homomorphism

$$\begin{aligned} \phi \otimes \psi : B \otimes_A C &\to B' \otimes_A C' \\ b \otimes c &\to \phi(b) \otimes \phi(c) \end{aligned}$$

is an A-algebra homomorphism.

Proof. The A-module homomorphism exists by (3.5.4). It is in A-algebra homomorphism by (3.5.34). □

Proposition 3.5.36 (Tensor Product is Coproduct)
Let B, C be commutative A-algebras then there are A-algebra homomorphisms

$$\begin{aligned} u_B : B &\to B \otimes_A C \\ b &\to b \otimes 1 \\ u_C : C &\to B \otimes_A C \\ c &\to 1 \otimes c \end{aligned}$$

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

$$\begin{aligned} \mathrm{AlgHom}_A(B \otimes_A C, Z) &\cong \mathrm{AlgHom}_A(B, Z) \times \mathrm{AlgHom}_A(C, Z) \\ \psi &\to (\psi \circ u_B, \psi \circ u_C) \end{aligned}$$

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

$$(\psi \circ u_B)(b) = \psi(b \otimes 1_C)$$

$$(\psi \circ u_C)(c) = \psi(1_B \otimes c)$$

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 (3.5.34) this is an algebra homomorphism. Clearly $\psi \circ u_B = f$ and $\psi \circ u_C = g$. 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 3.5.37 (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

$$\begin{aligned} \mathrm{AlgHom}_C(B_{(C)}, Z) &\cong \mathrm{AlgHom}_A(B, Z) \\ \psi &\to \psi \circ u_B \end{aligned}$$

Proof. We consider the commutative diagram obtained from (3.5.36)

$$\begin{array}{ccc} \mathrm{AlgHom}_A(B_{(C)}, Z) & \xrightarrow{\sim} & \mathrm{AlgHom}_A(B, Z) \times \mathrm{AlgHom}_A(C, Z) \\ \cup & & \cup \\ \mathrm{AlgHom}_C(B_{(C)}, Z) & \xrightarrow{\sim} & \mathrm{AlgHom}_A(B, Z) \times \{i_{CZ}\} \end{array}$$

An A-algebra homomorphism $\phi : B_{(C)} \to Z$ is a C-algebra homomorphism precisely when $\phi \circ u_C = i_{CZ}$ so that the bottom arrow is well-defined and bijective as required. □

Proposition 3.5.38 (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). □

Proposition 3.5.39
Let B be a commutative A-algebra then there is a natural isomorphism of A-algebras

$$\begin{array}{rcl} u_B : B & \xrightarrow{\sim} & B_{(A)} \\ b & \to & 1 \otimes b \\ ab & \leftarrow & a \otimes b \end{array}$$

Furthermore for C a commutative A-algebra there is a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{u_B} & A \otimes_A B \\ & \searrow^{u_B} & \downarrow{\scriptstyle i_A \otimes 1_B} \\ & & C \otimes_A B \end{array}$$

Proof. By (3.5.37) there is an bijection natural in Z

$$\begin{array}{rcl} \mathrm{AlgHom}_A(B_{(A)}, Z) & \xrightarrow{\sim} & \mathrm{AlgHom}_A(B, Z) \\ \psi & \to & \psi(1 \otimes -) \end{array}$$

which by the Yoneda Lemma (2.6.53) yields the required isomorphism (given by the image of $1_{B_{(A)}}$). □

Proposition 3.5.40 (Structural Morphisms are Injective)
Let B, C be commutative A-algebras such that the structural morphisms are injective and A is a direct factor of B and C (e.g. if $A = k$ is a field). Then the canonical maps (3.5.36)

$$B \to B \otimes_A C$$

$$C \to B \otimes_A C$$

are injective.

Proof. By (3.5.21) the canonical map

$$B \otimes_A A \to B \otimes_A C$$

is injective. By (3.5.39) we have a canonical isomorphism $B \cong B \otimes_A A$ and the composite is simply the canonical map $B \to B \otimes_A C$. □

Proposition 3.5.41 (Extension of Ideals under Tensor Product)
Let B, C be commutative A-algebras and $\mathfrak{b} \lhd B$ and $\mathfrak{c} \lhd C$ ideals. Then $\mathfrak{b}^e$ (resp. $\mathfrak{c}^e$) is the image of the A-module $\mathfrak{b} \otimes_A C$ (resp. $B \otimes_A \mathfrak{c}$) in $B \otimes_A C$. Furthermore there is a canonical A-algebra isomorphism

$$(B \otimes_A C)/(\mathfrak{b}^e + \mathfrak{c}^e) \cong B/\mathfrak{b} \otimes_A C/\mathfrak{c}$$

Proof. Let $\phi : B \to B \otimes_A C$ be the structural morphism then for $b \in \mathfrak{b}$ we have $b \otimes c = (c \otimes 1)(b \otimes 1) = (1 \otimes c)\phi(b)$ whence $\phi(\mathfrak{b}) \subseteq \mathfrak{b} \otimes_A C \subseteq \mathfrak{b}^e$. Evidently $\mathfrak{b} \otimes_A C$ is an ideal and therefore we see $\mathfrak{b} \otimes_A C = \mathfrak{b}^e$ as required. The isomorphism follows from (3.5.28). □

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 composite. Then $pq \in S_n$ but $p \notin S_n$.

We denote the localization of A at S_f by A_f (or alternatively $A[1/f]$).

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. We denote the localization of A at $\mathfrak{p}$ by $A_{\mathfrak{p}}$.

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 $\mathfrak{a} \triangleleft A$ 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 $\mathrm{Frac}(A)$ *the field of fractions. Define another model for $S^{-1}A$ as follows*

$$S^{-1}A := \left\{ \frac{a}{s} \in \mathrm{Frac}(A) \mid a \in A \; s \in S \right\}$$

The canonical map $A \to S^{-1}A \subset \mathrm{Frac}(A)$ is injective, and satisfies the universal property for localization.

Proof. It's injective because A has no zero-divisors. That it satisfies the universal property is very similar as before. □

Proposition 3.6.9 (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

$$\begin{array}{ccc} N & \xrightarrow{\psi} & M \\ \downarrow{\scriptstyle i_S} & & \downarrow{\scriptstyle i_S} \\ S^{-1}N & \xrightarrow{S^{-1}(\psi)} & S^{-1}M \end{array}$$

where $S^{-1}(\psi)$ is in fact an $S^{-1}A$-module morphism.

It is an exact functor; for an exact sequence

$$N \to M \to P$$

the corresponding sequence of $S^{-1}A$-module morphisms

$$S^{-1}N \to S^{-1}M \to S^{-1}P$$

is exact. If N is a submodule of M then we may regard $S^{-1}N$ as a submodule of $S^{-1}M$.

Proposition 3.6.13 (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 (3.4.49).

Definition 3.6.16 (Localization of an ideal)
Let A be a ring, S a multiplicative set and $\mathfrak{a}$ an ideal. Then the subset

$$S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} \mid a \in \mathfrak{a},\, s \in S \right\}$$

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 (3.4.50) 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 (3.4.50). 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 (3.4.50) 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 (3.4.52). 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

$$\begin{array}{ccccc} & & S^{-1}A & & \\ & \swarrow^{i_{ST}} & \downarrow{\scriptstyle i_{T_S}} & \searrow^{i_{\overline{T_S}}} & \\ T^{-1}A & \xrightarrow{\sim} & (T_S)^{-1}(S^{-1}A) & \xrightarrow{\sim} & \left(\overline{T_S}\right)^{-1}(S^{-1}A) \\ \downarrow{\scriptstyle i_{TU}} & & \downarrow & & \downarrow \\ U^{-1}A & \xrightarrow{\sim} & (U_S)^{-1}(S^{-1}A) & \xrightarrow{\sim} & \left(\overline{U_S}\right)^{-1}(S^{-1}A) \end{array}$$

3.6.5 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

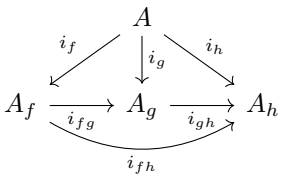
$$i_f : A \to A_f$$

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

$$\begin{array}{ccc} (A_f)_1 & \xrightarrow{\sim} & A_f \\ {\scriptstyle i_{1(g/1)}}\downarrow & & \downarrow{\scriptstyle i_{g/1}} \\ (A_f)_{g/1} & \xrightarrow{\sim} & A_g \\ \downarrow & & \downarrow{\scriptstyle i_{gh}} \\ (A_f)_{h/1} & \xrightarrow{\sim} & A_h \end{array}$$

with the horizontal arrows isomorphisms and the vertical arrows are well-defined.

Proof. 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 an order-preserving bijection between (prime) ideals contained in $\mathfrak{p}$ and (prime) ideals of $A_{\mathfrak{p}}$

$$\begin{array}{rcl} \{\mathfrak{q} \lhd A \mid \mathfrak{q} \subseteq \mathfrak{p}\} & \longleftrightarrow & \{\mathfrak{q} \lhd A_{\mathfrak{p}}\} \\ \mathfrak{q} & \longrightarrow & \mathfrak{q}A_{\mathfrak{p}} \end{array}$$

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. □

Proposition 3.6.34 (Quotient commutes with Localization at Prime ideal)
Let A be a ring, $\mathfrak{a}$ an ideal and $\mathfrak{p} \supset \mathfrak{a}$ a prime ideal. Then there is an isomorphism of non-zero rings

$$\begin{array}{rcl} A_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} & \cong & (A/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}} \\ \dfrac{a}{s} + \mathfrak{a}_{\mathfrak{p}} & \to & \dfrac{a+\mathfrak{a}}{s+\mathfrak{a}} \end{array}$$

Proof. Let $\pi : A \to A/\mathfrak{a}$ be the quotient map then we claim $\pi(A \setminus \mathfrak{p}) = \pi(A) \setminus \pi(\mathfrak{p})$. As π is surjective we only need to show that $\pi^{-1}(\pi(\mathfrak{p})) = \mathfrak{p}$. That is if $\pi(a) = \pi(b)$ and $b \in \mathfrak{p}$ then $a \in \mathfrak{p}$. However this follows by assumption because $\mathfrak{a} \subset \mathfrak{p}$. Therefore we may apply (3.6.24). □

3.7 Monoid Ring

Definition 3.7.1 (Monoid Ring)
Let A be a commutative ring and G be a commutative monoid. We define the ***monoid ring*** *to be the free abelian group*

$$A[G] := \bigoplus_{g \in G} A$$

We may write a general element as a formal sum

$$\sum_{g \in G} a_g g$$

where all but finitely many a_g are zero. Multiplication is defined extending the group operation. More precisely

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{(h,k) | h+k=g} a_h b_k g \right)$$

We may verify that the identity is simply e and the multiplication is both associative and distributive.

When G is an abelian group we say that $A[G]$ is the ***group ring****. There is a canonical map $A \to A[G]$ making $A[G]$ into an A-algebra.*

Proposition 3.7.2
Let A, B be commutative rings and G a commutative monoid. Let $\phi : A \to B$ be a ring homomorphism and $\alpha : G \to (B, \times)$ a monoid homomorphism. Then there is a unique homomorphism

$$\phi \ltimes \alpha : A[G] \to B$$

such that $(\phi \ltimes \alpha)(ae) = \phi(a)$ and $(\phi \ltimes \alpha)(1_A g) = \alpha(g)$.

Proof. Define

$$(\phi \ltimes \alpha) \left(\sum_{g \in G} a_g g \right) = \sum_{\substack{g \in G \\ a_g \neq 0}} \phi(a_g) \alpha(g)$$

□

3.8 Polynomial Rings in One Variable

Definition 3.8.1 (Polynomial Ring)
Let A be a commutative ring. Define the polynomial ring $A[X]$ to be the monoid ring $A[\mathbb{N}]$ consisting of formal

$$f(X) = \sum_{i=0}^{\infty} a_i X^i$$

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 $\deg(0) = -\infty$.

Definition 3.8.2 (Monic polynomial)
Let $f \in A[X]$. We say f is ***monic*** *if the leading coefficient, $\ell(f)$, is 1.*

Lemma 3.8.3
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 3.8.4 (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 (3.4.65) 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 3.8.5 (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 3.8.6
In categorical jargon $A[X]$ is an initial object in the category of pointed A-algebras.

Proposition 3.8.7 (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 3.8.8 (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 3.8.9 (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. □

3.9 Laurent Polynomials

Definition 3.9.1 (Laurent polynomial ring)
*Let A be a commutative ring. Define the **laurent polynomial ring** $A[X, X^{-1}]$ to be the group ring $A[\mathbb{Z}]$. Denote an element as a formal sum*

$$f(X) := \sum_{i=-\infty}^{\infty} a_i X^i$$

Proposition 3.9.2
Let B be an A-algebra and $b \in B^\star$ a unit. Then there is a unique A-algebra homomorphism $\mathrm{ev}_b : A[X, X^{-1}] \to B$ such that

$$\mathrm{ev}_b(X) \quad = \quad b$$

If the structural morphism $A \to B$ is injective, so is ev_b.

Proposition 3.9.3
Let A be a commutative ring. Then there is an isomorphism of rings

$$\begin{array}{rcll} A[X, X^{-1}] & \to & A[X]_X & \\ \displaystyle\sum_{i=-r}^{\infty} a_i X^i & \to & \dfrac{\sum_{i=0}^{\infty} a_{i-r} X^i}{X^r} & r = \min\{k \mid a_k \neq 0\} \vee 0 \\ \displaystyle\sum_{i=-r}^{\infty} a_{i+r} X^i & \leftarrow & \dfrac{\sum_{i=0}^{\infty} a_i X^i}{X^r} & \end{array}$$

Proof. Denote the maps by ψ and ϕ. Then ψ exists by (3.9.2) and ϕ exists by the universal property of localisation. □

3.10 Polynomial Rings in Many Variables

Definition 3.10.1
Let A be a ring then the polynomial ring $A[X_1, \ldots, X_n]$ is the monoid ring $A[\mathbb{N}^n]$ consisting 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.

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 3.10.2
It may be useful for certain induction arguments to write

$$A[X_1, \ldots, X_n] = A$$

when $n = 0$.

Proposition 3.10.3 (Evaluation Homomorphism)
$A[X_1, \dots, X_n]$ satisfies the following universal property. Given any A-algebra B and points $(b_1, \dots, b_n)$ there exists a ring homomorphism

$$\phi_b : A[X_1, \dots, X_n] \to B$$

such that

$$\phi_b(X_i) = \phi(b_i)$$

given by

$$\phi_b(\sum_v a_v X_1^{v_1} \dots X_n^{v_n}) = \sum_v i_B(a_v)\phi(b_1)^{v_1} \dots \phi(b_n)^{v_n}$$

In otherwords it is an initial object in the category of n-pointed A-algebras. Furthermore

$$\mathrm{Im}(\phi_b) = A[b_1, \dots, b_n]$$

Lemma 3.10.4 (Iterated polynomial ring)
Given $f \in A[X_1, \dots, X_n]$ and let $N = \deg(f, n)$ then there exist unique polynomials $g_i \in A[X_1, \dots, X_{n-1}]$ such that

$$f = \sum_{i=0}^{N} g_i X_n^i$$

in other words there is a canonical isomorphism

$$\psi : A[X_1, \dots, X_{n-1}][X_n] \to A[X_1, \dots, X_n]$$

under which $\deg(f) = \deg(\psi(f); n)$.

Proposition 3.10.5 (Homogenous grading)
Consider $R = k[X_1, \dots, X_n]$ and $x \in k^n$. Then there is a direct sum of k-submodules

$$R = \bigoplus_{n \geq 0} R^{n,x}$$

where

$$R^{n,x} = \Big\{ \sum_{|\alpha|_1 = n} \lambda_\alpha (X_1 - x_1)^{\alpha_1} \dots (X_n - x_n)^{\alpha_n} \mid \lambda_\alpha \in k \quad \alpha \in \mathbb{N}^n \Big\}$$

and every $F \in R$ may be written uniquely as

$$F(X) = F(x) + F^{(1,x)}(X) + \dots + F^{(n,x)}(X) + \dots$$

with $F^{(n,x)} \in R^{n,x}$. Note that

$$\ker(\mathrm{ev}_x) =: M_x = \bigoplus_{n \geq 1} R^{n,x} = (X_1 - x_1, \dots, X_n - x_n)$$

and

$$M_x^k = \bigoplus_{n \geq k} R^{n,x}$$

Finally there is a canonical isomorphism

$$k[X_1, \dots, X_n]^{(1,x)} \cong M_x / M_x^2$$

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

$$\rho_x(F) = \sum_{n=0}^{\infty} \left(\sum_{|\alpha|_1 = n} \lambda_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n} \right)$$

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 3.10.6 (Projection to linear terms)
Given $\mathfrak{a} \lhd k[X_1, \dots, X_n]$ and $x \in k^n$ define

$$\mathfrak{a}^{(i,x)} = \{F^{(i,x)} \mid F \in \mathfrak{a}\}$$

The following is useful

Lemma 3.10.7
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

$$F(G_1, \dots, G_n)(\lambda_1, \dots, \lambda_m) = F(G_1(\lambda_1, \dots, \lambda_m), \dots, G_n(\lambda_1, \dots \lambda_m))$$

3.11 Δ-Graded Rings

References :

- [Bou98b, Chap. II §11]

Let Δ be a commutative monoid. By convention we write the monoid operation additively and 0 for the identity. Further we assume it is **cancellable**: $\lambda + \mu = \lambda + \mu' \implies \mu = \mu'$. Typically $\Delta = \mathbb{Z}$, but for example we may also consider $\mathbb{N}^k$ for some positive integer k.

Definition 3.11.1 (Graded Abelian Groups)
*Let Δ be a cancellable commutative monoid. An abelian group G is Δ-**graded** if it may be written as internal direct sum (3.4.87) of $\mathbb{Z}$-modules*

$$G = \bigoplus_{\lambda \in \Delta} G_\lambda$$

for subgroups $G_\lambda \leq G$. In particular the subgroups G_λ are disjoint. This means for every $g \in G$ there is a unique decomposition into a finite sum

$$g = \sum_{\lambda \in \Lambda} g_\lambda$$

*If $g \in G_\lambda$ then we say g is **homogenous**. In this case we write $\delta(g) := \lambda$ for the **degree** of g.*

We may write $\pi_\lambda : G \to G_\lambda$ and $i_\lambda : G_\lambda \to G$ for projection and inclusion respectively. For $g \in G$ we may abbreviate $\pi_\lambda(g)$ by g_λ.

Definition 3.11.2 (Graded Ring)
*Let Δ be a cancellable commutative monoid. A commutative ring A is **graded** of type Δ if the additive group $(A, +)$ is Δ-graded, and the multiplication is compatible in the sense that*

$$a \in A_\lambda, b \in A_\mu \implies a \cdot b \in A_{\lambda+\mu}$$

Lemma 3.11.3
Let A be a Δ-ring. Then A_0 is a subring.

In the case $\Delta = \mathbb{N}$ the additive subgroups

$$A_{\geq k} := \sum_{l \geq k} A_l$$

*are homogenous ideals. We write $A_+ := A_{\geq 1}$ which we call the **irrelevant ideal**.*

Proof. We need only show $1 \in A_0$. By hypothesis there is a unique decomposition

$$1 = \sum_{\lambda \in \Delta} e_\lambda \quad e_\lambda \in A_\lambda$$

For every $x \in A_\mu$ we have

$$x = x \cdot 1 = \sum_{\lambda \in \Delta} x \cdot e_\lambda$$

By the cancellable assumption we have $\lambda \neq 0 \implies \lambda + \mu \neq \mu$. Therefore $x \cdot e_0 = x$. By distributivity this then holds for all $x \in A$ and in particular $1 = 1 \cdot e_0 = e_0$ □

Definition 3.11.4 (Graded Module)
*Let A be a Δ-graded ring and M a left (resp. right) A-module which is a Δ-graded as an abelian group. Then M is a **graded module** if the A-module structure is compatible with the grading, namely*

$$a \in A_\lambda, m \in M_\mu \implies a \cdot m \in M_{\lambda+\mu}$$

Elements of M_λ are known as homogenous.

Definition 3.11.5 (Graded Homomorphisms)
*Let A, B be Δ-graded rings and $\phi : A \to B$ a ring homomorphism. It is a **graded ring homomorphism** if*

$$\phi(A_\lambda) \subseteq B_\lambda \quad \forall \lambda \in \Delta$$

*Let M, M' be graded A-modules and $\phi : M \to M'$ an A-module homomorphisms. Then ϕ is a **graded module homomorphism** if*

$$\phi(M_\lambda) \subseteq M'_\lambda \quad \forall \lambda \in \Delta$$

Definition 3.11.6 (Graded Submodules)
Let M be a graded A-module, and $N \leq M$ an A-submodule. Then the following are equivalent

a) $n \in N$, $\lambda \in \Delta \implies \pi_\lambda(n) \in N$

b) *N is generated by homogenous elements*

c) *N is equal to the internal direct sum*

$$\bigoplus_{\lambda \in \Lambda} N \cap M_\lambda$$

*We say such a submodule is **graded** or **homogenous** and we write $N_\lambda := N \cap M_\lambda$.*

Proposition 3.11.7
Let M be a graded A-module and $\{N_\alpha\}_{\alpha \in I}$ be a family of submodules. Then both

$$\sum_{\alpha \in I} N_\alpha$$

and

$$\bigcap_{\alpha \in I} N_\alpha$$

are graded submodules.

Proposition 3.11.8
Let M be a finitely-generated graded A-module. Then M has a finite generating set of homogenous elements.

Definition 3.11.9 (Homogenous Ideal)
*Let A be a commutative graded ring. An ideal $\mathfrak{a} \triangleleft A$ which is homogenous as an A-submodule of A is a **homogenous ideal**. We write $\mathfrak{a}_\lambda := \mathfrak{a} \cap A$, then by definition*

$$\mathfrak{a} = \bigoplus_{\lambda \in \Delta} \mathfrak{a}_\lambda$$

Note if A is Noetherian then every homogenous ideal has a finite generating set of homogenous elements.

Example 3.11.10 (Polynomial Ring)
The polynomial ring $k[X_0, \ldots, X_n]$ is a graded ring over $\mathbb{N}$ with

$$k[X_0, \ldots, X_n]_d = k\langle \{X_1^{\alpha_1} \cdot \ldots \cdot X^{\alpha_n} \mid \alpha_1 + \ldots + \alpha_n = d\} \rangle$$

Furthermore

$$\bigoplus_{i \geq d} k[X_0, \ldots, x_N]_i = (X_0, \ldots, X_n)^d$$

Proposition 3.11.11 (Quotient by a Homogenous Ideal)
Suppose Δ is a commutative cancellable monoid. Let A be a Δ-graded ring and $\mathfrak{a} \triangleleft A$ a homogenous ideal. Then $A/\mathfrak{a}$ is a Δ-graded ring by considering the internal direct sum of abelian groups

$$\begin{aligned} A/\mathfrak{a} &= \bigoplus_{\lambda \in \Delta} (A/\mathfrak{a})_\lambda \\ (A/\mathfrak{a})_\lambda &:= \left\{ \overline{a} \mid a \in A_\lambda \right\} \end{aligned}$$

Furthermore there is an isomorphism of A-modules

$$(A/\mathfrak{a})_\lambda \xrightarrow{\sim} A_\lambda/(\mathfrak{a} \cap A_\lambda)$$

For every homogenous ideal $\mathfrak{b} \supset \mathfrak{a}$ the quotient ideal $\mathfrak{b}/\mathfrak{a}$ is homogenous with

$$\mathfrak{b}/\mathfrak{a} = \bigoplus_{\lambda \in \Delta} (\mathfrak{b}/\mathfrak{a})_\lambda$$

Proof. Evidently the $(A/\mathfrak{a})_\lambda$ are abelian subgroups and span $A/\mathfrak{a}$. Observe that

$$0 = \sum_{\lambda \in \Delta} \overline{a_\lambda} \implies \sum_{\lambda \in \Delta} a_\lambda \in \mathfrak{a}$$

Then as $\mathfrak{a}$ is homogenous we conclude $a_\lambda \in \mathfrak{a}$ and therefore $\overline{a_\lambda} = 0$. Therefore the family $(A/\mathfrak{a})_\lambda$ satisfy the criteria of (3.4.88) and the direct sum is well-defined. Evidently the ring multiplication on $A/\mathfrak{a}$ is compatible with the given Δ-grading.

The isomorphism is induced by π_λ.

Suppose that $\overline{b} \in \mathfrak{b}/\mathfrak{a}$ then we require to prove that $(\overline{b})_\lambda \in (\mathfrak{b}/\mathfrak{a})$. By assumption $b_\lambda \in \mathfrak{b}$ so $\overline{b_\lambda} \in \mathfrak{b}/\mathfrak{a}$. However by the first part $\overline{b_\lambda} = (\overline{b})_\lambda$. □

Proposition 3.11.12 (Localization at Homogenous Elements)
*Let Δ be an abelian group, A a Δ-graded ring and $S \subset A$ a multiplicative set of **homogenous** elements. Then we may define a Δ-gradation on $S^{-1}A$ by*

$$\left(S^{-1}A\right)_\lambda := \left\{ \frac{a}{s} \mid \delta(a) - \delta(s) = \lambda \right\}$$

For a homogenous ideal $\mathfrak{a} \triangleleft A$ then the ideal $S^{-1}\mathfrak{a}$ is homogenous.

Proof. We first show that $(S^{-1}A)_\lambda$ is an additive subgroup, for given homogenous $a, a' \in A$ and $s, s' \in s$ by definition

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

Suppose $\delta(a) - \delta(s) = \lambda = \delta(a') - \delta(s')$ then $\delta(as') = \delta(a's)$. Therefore $as' + a's$ is homogenous and $\delta(as' + a's) = \delta(as') = \lambda + \delta(s) + \delta(s') = \lambda + \delta(ss')$ whence $\left(S^{-1}A\right)_\lambda$ is an additive subgroup. Similarly for the multiplicative structure suppose $\delta(a) = \delta(s) + \lambda$ and $\delta(a') = \delta(s') + \lambda'$ then

$$\delta(aa') = \delta(a) + \delta(a') = \delta(\lambda) + \delta(\lambda') + (\lambda + \lambda') = \delta(\lambda\lambda') + (\lambda + \lambda')$$

so that $\frac{a}{s} \cdot \frac{a'}{s'} \in \left(S^{-1}A\right)_{\lambda + \lambda'}$ as required. Evidentally $S^{-1}A$ is the internal sum of $\left(S^{-1}A\right)_\lambda$. To show it is direct suppose that

$$0 = \sum_{i=1}^n \frac{a_i}{s_i} \quad \delta(a_i) = \delta(s_i) + \lambda_i$$

for distinct $\lambda_1, \ldots, \lambda_n$. Then

$$0 = \sum_{i=1}^n a_i t \prod_{j \neq i} s_j$$

for some $t \in S$. Furthermore

$$\delta\left(a_i t \prod_{j\neq i} s_j\right) = \delta(a_i) + \sum_{j\neq i}\delta(s_j) + \delta(t) = \lambda_i + \sum_{j=1}^{n}\delta(s_j) + \delta(t)$$

As Δ is cancellable the elements $\widehat{\lambda}_i := \lambda_i + \sum_{j=1}^n \delta(s_j) + \delta(t)$ are distinct. By assumption we conclude that $a_i t \prod_{j\neq i} s_j = 0$ and so $\frac{a_i}{s_i} = 0$. Therefore $S^{-1}A$ is the direct sum of $(S^{-1}A)_\lambda$ by (3.4.88).

For $\frac{a}{s} \in S^{-1}\mathfrak{a}$ we wish to show that $\left(\frac{a}{s}\right)_\lambda \in S^{-1}\mathfrak{a}$ for all $\lambda \in \Delta$. Here $a \in \mathfrak{a}$ so by assumption $a_\lambda \in \mathfrak{a}$ for all $\lambda \in \Delta$ and $a = \sum_{\lambda\in\Delta} a_\lambda$ so

$$\frac{a}{s} = \sum_{\lambda\in\Delta}\frac{a_\lambda}{s} = \sum_{\lambda\in\Delta}\frac{a_{\lambda+\delta(s)}}{s}$$

and so $\left(\frac{a}{s}\right)_\lambda = \frac{a_{\lambda+\delta(s)}}{s} \in S^{-1}\mathfrak{a}$ as required. □

Recall for any Δ-graded ring A the additive subgroup A_0 is also a subring.

Definition 3.11.13
Let Δ be a commutative abelian group, A a Δ-graded ring and S be a multiplicative subset of homogenous elements. Define the subring of $S^{-1}A$

$$A_{(S)} := \left(S^{-1}A\right)_0 = \left\{\frac{a}{s} \mid \delta(s) = \delta(a)\right\}$$

Similarly for $\mathfrak{a}$ a homogenous ideal define the homogenous ideal of $S^{-1}A$

$$\mathfrak{a}_{(S)} := \left\{\frac{a}{s} \mid a \in \mathfrak{a},\ s \in S,\ \delta(s) = \delta(a)\right\}$$

In the case $\mathfrak{p}$ is a homogenous prime ideal define the local ring

$$A_{(\mathfrak{p})} := A_{(\{x\notin\mathfrak{p}\})}$$

and for $f \in A$ homogenous define

$$A_{(f)} := A_{(\{1,f,f^2,\ldots\})}$$

Lemma 3.11.14
Let Δ be an abelian group, A a Δ-graded ring and $\mathfrak{a} \lhd A$ a homogenous ideal. Then

$$\mathfrak{a}_{(S)} = A_{(S)} \cap S^{-1}\mathfrak{a}$$

as subsets of $S^{-1}A$.

Lemma 3.11.15
Let Δ be an abelian group, A a Δ-graded ring, $a \in A_\mu$ homogenous and $x \in A$. Then

$$(ax)_\lambda = a \cdot x_{\lambda-\mu}$$

In particular ax is homogenous iff x is homogenous.

Proposition 3.11.16 (Homogenous localisation comutes with quotients)
Let Δ be an abelian group, A a Δ-graded ring, $\mathfrak{a}$ a homogenous ideal and $S \subset A$ a multiplicatively closed set of homogenous elements such that $S \cap \mathfrak{a} = \emptyset$. Then there is a canonical isomorphism of Δ-graded rings

$$\begin{array}{ccc}(S^{-1}A)/(S^{-1}\mathfrak{a}) & \xrightarrow{\sim} & \pi(S)^{-1}(A/\mathfrak{a}) \\ \frac{a}{s} + S^{-1}A & \to & \frac{a+\mathfrak{a}}{s+\mathfrak{a}}\end{array}$$

where $\pi : A \to A/\mathfrak{a}$ is the canonical surjection. In particular there is an isomorphism of rings

$$A_{(S)}/\mathfrak{a}_{(S)} \xrightarrow{\sim} (S^{-1}A/S^{-1}\mathfrak{a})_0 \xrightarrow{\sim} (A/\mathfrak{a})_{(\pi(S))}$$

Proof. The first isomorphism of rings is from (3.6.24), and it is obviously compatible with the Δ-grading. For suppose $x \in (S^{-1}A)/(S^{-1}A)$ with $\delta(x) = \lambda$. Then $x = \frac{a}{s}$ with $\delta(a) - \delta(s) = \lambda$. By definition $\delta(a+\mathfrak{a}) - \delta(s+\mathfrak{a}) = \lambda$ as required.

The third isomorphism follows immediately. For the second consider the ring homomorphism

$$\phi : A_{(S)} \hookrightarrow S^{-1}A \to S^{-1}A/S^{-1}\mathfrak{a}$$

Then evidentally the image is $(S^{-1}A/S^{-1}\mathfrak{a})_0$ as the quotient map is graded. The kernel is $A_{(S)} \cap S^{-1}\mathfrak{a}$ which equals $\mathfrak{a}_{(S)}$ by (3.11.14). □

Proposition 3.11.17
Let Δ be an abelian group, A a Δ-graded ring, $\mathfrak{a}$ a homogenous ideal and $\mathfrak{p} \supset \mathfrak{a}$ a homogenous prime ideal. Then there is a canonical isomorphism of Δ-graded rings

$$\begin{array}{ccc} A_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} & \xrightarrow{\sim} & (A/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}} \\ \frac{a}{s} + \mathfrak{a}_{\mathfrak{p}} & \to & \frac{a+\mathfrak{a}}{s+\mathfrak{a}} \end{array}$$

In particular there is an isomorphism of rings

$$\begin{array}{ccccc} A_{(\mathfrak{p})}/\mathfrak{a}_{(\mathfrak{p})} & \xrightarrow{\sim} & (A_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}})_0 & \xrightarrow{\sim} & (A/\mathfrak{a})_{(\mathfrak{p}/\mathfrak{a})} \\ \frac{a}{s} + \mathfrak{a}_{(\mathfrak{p})} & & \to & & \frac{a+\mathfrak{a}}{s+\mathfrak{a}} \end{array}$$

Proof. Follows from (3.11.16) and the observation that $A/\mathfrak{a} \setminus \mathfrak{p}/\mathfrak{a} = \pi(A \setminus \mathfrak{p})$. □

3.12 Graded Rings

Definition 3.12.1 (Graded Ring over $\mathbb{Z}$)
*A ring A (resp. A-module M) is said to be $\mathbb{Z}$-**graded** (or simply **graded**) if it is graded in the sense of Definition (3.11.2) with gradation group $\Delta = \mathbb{Z}$.*

*If $i < 0 \implies A_i = 0$ (resp. $M_i = 0$) then we say A (resp. M) is **positively graded**.*

Note in this case that we have the multiplication formula

$$(a \cdot b)_i = \sum_{j+k=i} a_j \cdot b_k$$

Definition 3.12.2
*For an element $a \in A$ we define the **degree** to be*

$$\deg(a) := \max\{i \mid a_i \neq 0\}$$

Definition 3.12.3 (Essential and Irrelevant Ideals)
*Let A be a positively graded ring. Then we say a homogenous ideal $\mathfrak{a}$ is **irrelevant** if the following condition holds*

$$\exists n_0 \text{ s.t. } n \geq n_0 \implies \mathfrak{a}_n = A_n$$

*In particular A_+ is irrelevant. Otherwise we say that it is **essential**.*

Proposition 3.12.4 (Radical of Homogenous Ideal is Homogenous)
Let A be a graded ring and $\mathfrak{a}$ a homogenous ideal. Then $\sqrt{\mathfrak{a}}$ is also a homogenous ideal.

Proof. Define $\mathfrak{r} := \sqrt{\mathfrak{a}}$ and fix $x \in \mathfrak{r}$. Suppose

$$x = \sum_{i=-\infty}^{\infty} x_i$$

where $\delta(x_i) = i$ and $x^k \in \mathfrak{r}$. Then

$$x^k = \sum_{i=-\infty}^{\infty} x_i^k$$

where $\delta(x_i^k) = ki$. Without loss of generality we may assume $k > 0$ so by assumption $x_i^k \in \mathfrak{r}$ for all i and therefore $x_i \in \sqrt{\mathfrak{r}}$. □

Proposition 3.12.5
Let A be a graded ring and $\mathfrak{p}$ a homogenous ideal satisfying the following property

$$a \in A_n, b \in A_m, ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}$$

Then $\mathfrak{p}$ is a prime ideal.

Proof. Suppose $\mathfrak{p}$ is not prime. Then there exists $a, b \in A$ such that $ab \in \mathfrak{p}$ and $a, b \notin \mathfrak{p}$. Write $a = \sum_j a_j$ and $b = \sum_k b_j$. Then

$$ab = \sum_{i=-\infty}^{\infty} \left(\sum_{(j,k)|j+k=i} a_j b_k \right)$$

As $\mathfrak{p}$ is assumed homogenous then for each i we have

$$(ab)_i := \sum_{(j,k)|j+k=i} a_j b_k \in \mathfrak{p}_i$$

Let j' (resp. k') be the largest integer such that $a_{j'} \notin \mathfrak{p}$ (resp. $a_{k'} \notin \mathfrak{p}$). For all other pairs j'', k'' such that $j' + k' = j'' + k''$ we have by maximality $a_{j''} b_{k''} \in \mathfrak{p}_i$. Therefore we conclude $a_{j'} b_{k'} \in \mathfrak{p}$, which contradicts the original assumption. □

Proposition 3.12.6
Let A be a positively graded ring. Then the following are equivalent

a) *A_+ is a finitely-generated A-module*

b) *A is a finitely-generated A_0-algebra*

More precisely for homogenous elements $x_0, \ldots, x_n \in A_+$ we have

$$A_+ = \sum_{i=0}^{n} A x_i \iff A = A_0[x_0, \ldots, x_n]$$

*In this case we say that A is **finitely generated**. Further*

$$A_+^m = (x_0, \ldots, x_n)^m$$

for all integers $m > 0$.

Proposition 3.12.7 (Criteria for Irrelevant ideals)
Let A be a positively graded ring which is finitely generated and $\mathfrak{a}$ a homogenous ideal. Then the following are equivalent

a) *$\mathfrak{a}$ is irrelevant (i.e. $n \geq n_0 \implies \mathfrak{a}_n = A_n$)*

b) *$A_+ \subset \sqrt{\mathfrak{a}}$*

Proof. *a)* $\implies$ *b)* It is sufficient to show that $i > 0 \implies A_i \subset \sqrt{\mathfrak{a}}$. Given $x \in A_i$ then by the Archimedean property there exists $k > 0$ such that $ik > n_0$. Therefore by assumption $x^k \in \mathfrak{a}$ and $x \in \sqrt{\mathfrak{a}}$.

b) $\implies$ *a)* TODO. □

Proposition 3.12.8
Let A be a graded ring and $f \in A_1$. Then there is an isomorphism

$$\begin{array}{rcll} A_{(f)}[X, X^{-1}] & \xrightarrow{\sim} & A_f & \\ \sum_{i \in \mathbb{Z}} \frac{a_{n_i}}{f^{n_i}} X^i & \longrightarrow & \sum_{i \in \mathbb{Z}} \frac{a_{n_i}}{f^{n_i - i}} & a_{n_i} \in A \text{ homogenous of degree } n_i \\ \sum_{i \in \mathbb{Z}} \frac{a_i}{f^i} X^{i-r} & \longleftarrow & \frac{\sum_{i \in \mathbb{Z}} a_i}{f^r} & \end{array}$$

Proof. Denote the maps by ψ, ϕ, then ψ exists and is a ring homomorphism by (3.9.2) satisfying $\psi(X) = f$ and whence $\psi(X^i) = f^i$. To show ψ is well-defined first consider the map

$$\begin{array}{rcl} \psi' : A & \to & A_{(f)}[X, X^{-1}] \\ \sum_{i \in \mathbb{Z}} a_i & \to & \sum_{i \in \mathbb{Z}} \frac{a_i}{f^i} X^i \end{array}$$

which is evidentally a well-defined homomorphism of abelian groups. Furthermore

$$\left(\sum_{i \in \mathbb{Z}} \frac{a_i}{f^i} X^i \right) \left(\sum_{i \in \mathbb{Z}} \frac{b_i}{f^i} X^i \right) = \sum_{i \in \mathbb{Z}} \left(\sum_{j+k=i} \frac{a_j b_k}{f^{j+k}} \right) X^i = \sum_{i \in \mathbb{Z}} \left(\frac{1}{f^i} \sum_{j+k=i} a_j b_k \right) X^i$$

and so the map is a ring-homomorphism by the multiplication formula in A. By the universal property of localisation the ring homomorphism ϕ exists with $\phi(f) = X$ and hence $\phi(f^i) = X^i$. We have

$$\phi(\psi(X)) = \phi(f) = X$$

$$\phi\left(\psi\left(\frac{a_j}{f^j}\right)\right) = \phi\left(\frac{a_j}{f^j}\right) = \frac{a_j}{f^j}$$

so by linearity $\phi \circ \psi = \mathbf{1}$. Similarly

$$\psi\left(\phi\left(\frac{a_i}{f^r}\right)\right) = \psi\left(\frac{a_i}{f^i}X^{i-r}\right) = \frac{a_i}{f^i}f^{i-r} = \frac{a_i}{f^r}$$

so by linearity $\psi \circ \phi = \mathbf{1}$. □

3.13 Chain Conditions

Definition 3.13.1 (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*

$$M_0 \subseteq M_1 \subseteq \ldots \subseteq M$$

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*

$$M \supseteq M_0 \supseteq M_1 \supseteq \ldots$$

eventually stabilizes.

Definition 3.13.2 (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 3.13.3 (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 3.13.4 (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 $m_1, \ldots, m_n$, and B is generated by $b_1, \ldots, b_m$. Then we claim that the elements $b_i m_j$ generate $[M]_\phi$. □

Proposition 3.13.5
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 (3.4.55) 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 (3.4.55) the original sequence stabilizes. □

Proposition 3.13.6
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 (3.13.5) it's enough to show that $A[X_1, \ldots, X_n]$ is Noetherian. By induction and (3.10.4) it's enough to consider the case $n = 1$. Let $\mathfrak{a} \triangleleft A[X]$ then by (3.13.3) 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 $\widetilde{\mathfrak{a}}_i \triangleleft A$ 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. □

3.14 Principal Ideal Domains

Definition 3.14.1 (Principal Ideal Domain)
*An integral domain A is a **principal ideal domain** (or **PID**) if every ideal $\mathfrak{a}$ is principal.*

Proposition 3.14.2
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 3.14.3 (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 3.14.4
Let k be a field then the polynomial ring $k[X]$ is a PID

Proof. Let $\mathfrak{a} \triangleleft k[X]$ 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 (3.8.9) $g = qf + r$ for $\deg(r) < \deg(f)$. Clearly $r \in \mathfrak{a}$, so by minimality $r = 0$ and the result follows. □

Lemma 3.14.5 (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. □

3.15 Factorisation

For this section we assume A is a commutative integral domain.

Definition 3.15.1 (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 3.15.2
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 3.15.3
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 3.15.4 (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 3.15.5 (Prime element)
We say $0 \neq p$ is prime if $p \mid ab \implies p \mid a$ or $p \mid b$.

Example 3.15.6
The units of $\mathbb{Z}$ are $\{-1, 1\}$ so each equivalence class is of the form $\{n, -n\}$.

Example 3.15.7
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 3.15.8
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 3.15.9 (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 3.15.10 (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 3.15.11 (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 (3.15.3) $p \sim a$ (resp. b) as required. □

Definition 3.15.12 (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 3.15.13 (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 3.15.14
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 3.15.15
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 3.15.16 (Atomic Ring)
*We say that A is **atomic** if every element has a (not necessarily unique) decomposition into irreducible elements.*

Definition 3.15.17 (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 3.15.18
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 (3.15.10) 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 3.15.19
The converse is not in general true (...) but see (3.15.21) for a partial converse.

We show a simple criterion for a ring to be a UFD.

Definition 3.15.20
*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 3.15.21 (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*

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 (3.15.15) 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 (3.15.15) the chain of principal ideals also stabilises.

$c \implies b$). This is (3.15.18).

$b \implies a$). 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 3.15.22 (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 (3.15.11).

b) $\iff$ *c*) as all ideals are principal this follows from (3.15.10)

c) $\implies$ *a*) By (3.4.59) (a) is prime, whence a is prime by (3.15.9) □

Proposition 3.15.23
A PID is Noetherian UFD.

Furthermore (f is irreducible $\iff$ f is prime), and every prime ideal is maximal.

Proof. A is Noetherian by (3.14.2) and atomic by (3.15.18). And by (3.15.22) an irreducible element is prime. Therefore we are done by by (3.15.21). □

If we take a suitable fixed set of irreducible elements we can obtain completely unique factorization

Definition 3.15.24
*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 3.15.25
For $\mathbb{Z}$ the positive *primes are a canonical set of irreducible elements.*

Proposition 3.15.26
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 (3.15.13) 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 (3.15.15) $y \mid x$ as elements of A whence by definition $xy^{-1} \in A$ as required. □

Proposition 3.15.27
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 (3.8.3) $a_{i+1} \mid a_i$ 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 3.15.28
Suppose $p \in A$ is prime, then it is prime as an element of $A[X]$.

Lemma 3.15.29 (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. □

3.15.1 Polynomial Ring is a UFD

We prove the following result, first by Nagata's Criterion and again by Gauss' Lemma.

Proposition 3.15.30
Suppose A is a UFD, then so is $A[X]$.

Proof. By (3.15.21) we need to show that $A[X]$ satisfies ACCP and is AP. The first follows from (3.15.27).

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 (3.15.21)) S is generated by prime elements and units. By (3.15.23) $K[X]$ is a UFD, and so in particular is AP. Therefore by (3.15.29) $A[X]$ is AP as required. □

For Gauss' Lemma we require to introduce some notation first.

Definition 3.15.31 (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 3.15.32 (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) $f \in A[X] \iff a_i \in A \quad \forall i \overset{(3.15.26)}{\iff} v_p(a_i) \geq 0 \, \forall i \, \forall p \in \mathcal{P} \iff \min_i v_p(a_i) \geq 0 \, \forall p \in \mathcal{P} \overset{(3.15.26)}{\iff} c(f) \in A$

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 (3.15.26).

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 (3.15.26) 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 3.15.33 (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 3.15.34
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 (3.15.33). 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 (3.15.33) 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 (3.15.32) and we see $f \mid g$ in $A[X]$. This shows that $A[X]$ is AP and therefore a UFD by (3.15.21). □

Corollary 3.15.35
Suppose A is a UFD. Then $A[X_1, \dots, X_n]$ is a UFD.

3.16 Cayley-Hamilton Theorem

Definition 3.16.1 (Characteristic Polynomial of a Matrix)
For a matrix $E \in \mathrm{Mat}_n(A)$ define the characteristic polynomial by

$$P_E(X) := \det(X \cdot I_n - E)$$

working in $\mathrm{Mat}_n(A[X])$. This is a monic polynomial in $A[X]$.

Definition 3.16.2 (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

$$P_\phi(X) := P_{[\phi]^{\mathcal{T}}}(X)$$

This is independent of the basis $\mathcal{B}$.

Lemma 3.16.3
Suppose $M = \langle m_1, \ldots, m_n \rangle$ is a finitely generated A-module then

$$\mathfrak{a}M = \mathfrak{a}m_1 + \ldots + \mathfrak{a}m_n$$

That is every $m \in \mathfrak{a}M$ may be written as

$$m = \sum_i a_i m_i \quad a_i \in \mathfrak{a}$$

Proof. By hypothesis

$$m = \sum_i a_i m_i' \quad m_i' \in M \, a_i \in \mathfrak{a}$$

Furthermore by finite-generation hypothesis

$$m_i' = \sum_j b_{ij} m_j \quad b_{ij} \in A \, .$$

Therefore

$$m = \sum_j (\sum_i a_i b_{ij}) m_j$$

as required. □

Theorem 3.16.4 (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

$$\phi(m_i) = \sum_{j=1}^{n} E_{ij} m_j \quad i = 1 \ldots n$$

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

$$B(\phi)_{ij} = \delta_{ij}\phi - E_{ij}1_M \quad i, j = 1 \ldots n$$

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

$$\begin{array}{rcl} \mathrm{Mat}_n(\mathrm{End}_A(M)) \times M^n & \to & M^n \\ F \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \to & \begin{pmatrix} \sum_{j=1}^n F_{1j}(x_j) \\ \vdots \\ \sum_{j=1}^n F_{nj}(x_j) \end{pmatrix} \end{array}$$

such that $(EF)v = E(Fv)$ (check). And we have shown that

$$B(\phi) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Using (3.4.128), premultiply by the adjugate matrix to show that

$$\det(B(\phi)) I_n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

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 3.16.3 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 $\mathfrak{a}$. □

3.17 Finite-type Algebras

Definition 3.17.1 (Finite algebra)
An A-algebra B is finite *if it is finite as an A-module.*

Definition 3.17.2 (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.

3.18 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.

3.18.1 Prime Fields

Recall that for p prime the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field (3.14.3), (3.15.22), (3.4.58).

Definition 3.18.1 (Finite field of order p)
Denote by $\mathbb{F}_p$ the field $\mathbb{Z}/p\mathbb{Z}$ of order p.

Definition 3.18.2 (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 3.18.3 (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 3.18.4 (Prime Subfield Exists)
*Let k be a field. Then k contains a **prime subfield**. It is the smallest subfield contained in k.*

Proof. By (...) there is a unique ring homomorphism

$$\phi : \mathbb{Z} \to k$$

As k 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 (3.4.56) $\mathbb{Z}/\ker(\phi) \cong \mathrm{Im}(\phi)$ and therefore by (3.4.58) $\ker(\phi) =: \mathfrak{p}$ is a prime ideal.

By (3.14.3) the ideal $\mathfrak{p}$ is principal. Suppose $\mathfrak{p} = (0)$. By (3.6.6) ϕ extends to a homomorphism $\phi' : \mathbb{Q} \to k$ whose kernel is zero and therefore injective (...). In particular $\mathrm{Im}(\phi')$ is a prime subfield being isomorphic to $\mathbb{Q}$.

Otherwise by (3.15.9) $\mathfrak{p} = (p)$ for p a prime number and we have already observed that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathrm{Im}(\phi)$ is a prime subfield.

Let k' be any subfield of k, then by induction we may show that $\mathrm{Im}(\phi) \subset k'$. In the case $\ker(\phi) = \{0\}$ then we may also show $\mathrm{Im}(\phi') \subset k'$. Therefore k' contains the prime subfield, whence it is the smallest subfield. □

Definition 3.18.5 (Characteristic)
*Let k be a field. Then we define the **characteristic** of k to be p if the prime subfield is isomorphic to $\mathbb{F}_p$ or 0 if the prime subfield is isomorphic to $\mathbb{Q}$. This is denoted* $\mathrm{char}(k)$.

*If A is a k-algebra then we define the characteristic of A to be that of k. We also define the **characteristic exponent** of A to be*

$$\begin{cases} 1 & \text{if } \mathrm{char}(A) = 0 \\ p & \text{if } \mathrm{char}(A) = p \end{cases}$$

Proposition 3.18.6 (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 call the **Frobenius map**. In particular*

$$(a+b)^p = a^p + b^p \quad \forall a, b \in A$$

Definition 3.18.7
*Let A be a k-algebra with characteristic exponent p. We say that A is **perfect** if A is reduced and $A^p = A$. When $p > 1$ this is equivalent to the Frobenius homomorphism being an isomorphism.*

3.18.2 Field Extensions

Definition 3.18.8 (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 (or, over $\mathbb{Q}$ or $\mathbb{F}_p$).

We typical denote the structural morphism by $i_{kK} : k \to K$, and it is automatically injective (3.4.60). 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 3.18.9 (Finite field extension)
A field extension K/k is finite if $[K:k] < \infty$

Definition 3.18.10 (Tower of Field Extensions)
We may also consider a "tower" of extensions

$$K_n/\dots/K_0 = k$$

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 $\sigma_i|_{K_j} = \sigma_i \circ i_{K_{i-1}K_i} \circ \dots \circ i_{K_jK_{j+1}}$.

Proposition 3.18.11
Let L/K and K/k be two finite extensions with basis $\{l_1,\dots,l_n\}$ and $\{k_1,\dots,k_m\}$. Then L/k has basis $\{l_ik_j\}_{i,j}$. In particular

$$[L:k] = [L:K][K:k]$$

Corollary 3.18.12
Let $K = K_n/\dots/K_0 = k$ be a tower of finite extensions then

$$[K:k] = \prod_{i=1}^{n}[K_i:K_{i-1}]$$

Lemma 3.18.13
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 (3.18.35) 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 3.18.14 (Evaluation homomorphism)
Let K/k be a field extension and $\alpha \in K$. There is a canonical homomorphism

$$\begin{aligned} \mathrm{ev}_\alpha : k[X] &\to K \\ \sum_{i=0}^{n} a_iX^i &\to \sum_{i=0}^{n} i_{kK}(a_i)\alpha^i \end{aligned}$$

which we write as $f(\alpha)$. We say $\alpha \in K$ is a root of $f(X)$ if $f(\alpha) = 0$.

Proposition 3.18.15 (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 (3.8.7), The last statement is obvious, because σ is injective (3.4.60). □

Definition 3.18.16 (Subalgebra generated by a set)
Let K/k be a field extension and $S \subset K$. Define

$$k[S] := \bigcap_{\substack{A \subset K/k \\ S \subset A}} A$$

where the intersection is taken over all k-subalgebras. It is the smallest k-subalgebra of K/k.

Proposition 3.18.17 (Subalgebra generated by directed family)
Let K/k be a field extension and $\{S_i\}_{i\in I}$ a family of directed subsets of K. Then

$$k\left[\bigcup_{i\in I} S_i\right] = \bigcup_{i\in I} k[S_i]$$

In particular for any set S we have

$$k\left[S\right] = \bigcup_{\substack{S'\subset S \\ S' \text{ finite}}} k[S']$$

Proposition 3.18.18 (Subalgebra generated by a set)
Let K/k be a field extension and $S \subset K$ a finite subset. Write $S = \{\alpha_1, \ldots, \alpha_n\}$ then

$$k[S] = \{p(\alpha_1, \ldots, \alpha_n) \mid p \in k[X_1, \ldots, X_n]\} = \operatorname{Im}\left(\mathrm{ev}_\alpha\right)$$

Lemma 3.18.19 (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 3.18.20
Let K/k be a field extension and $S \subset K$. Define

$$k(S) := \bigcap_{\substack{K'\subset K/k \\ S\subset K'}} K'$$

It is the smallest subfield of K/k containing S.

Proposition 3.18.21
Let K/k be a field extension and $\{S_i\}_{i\in I}$ be a family of directed subsets of K. Then

$$k\left(\bigcup_{i\in I} S_i\right) = \bigcup_{i\in I} k\left(S_i\right)$$

In particular for any set S we have

$$k\left(S\right) = \bigcup_{\substack{S'\subset S \\ \text{finite}}} k\left(S'\right)$$

Proposition 3.18.22
Let K/k be a field extension and $S \subset K$ be a finite subset. Write $S = \{\alpha_1, \ldots, \alpha_n\}$ then

$$k(S) := \left\{\frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)} \mid p, q \in k[X_1, \ldots, X_n]\right\}$$

Lemma 3.18.23 (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 3.18.24
If $S \subset K$ and $k[S]$ is a field then $k[S] = k(S)$

Proof. Generically $k[S] \subset k(S)$ from the definition. As $k[S]$ is a field then $k(S) \subset k[S]$. □

Lemma 3.18.25 (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 3.18.26 (Uniqueness of morphisms on a generating set)
Let K/k be a field extension and $S \subset K$. If $\sigma, \sigma' : k(S)/k \to L/k$ are morphisms of field extensions such that $\sigma|_S = \sigma'|_S$. Then $\sigma = \sigma'$.

Definition 3.18.27 (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 3.18.28 (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 3.18.29 (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 3.18.30 (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 (3.4.60) 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 (3.18.40) T is finite. Further by (3.18.15) 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. □

3.18.3 Polynomials

In this section we consider the polynomial ring with coefficients in a field, $k[X]$.

Proposition 3.18.31
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 3.18.32
The units of $k[X]$ are precisely the non-zero polynomials of degree 0.

Proposition 3.18.33 (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 3.18.34
A polynomial $f \in k[X]$ is associate to precisely one monic polynomial g. If f is irreducible so is g.

Proof. **TODO** □

Proposition 3.18.35 (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 (3.8.9) to $g/\ell(g)$, and multiply by $\ell(g)$ again. □

Proposition 3.18.36 (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 3.18.37 (Unique Factorisation of Polynomials)
For the ring $k[X]$ the set of irreducible monic polynomials constitutes a representative set (Definition (3.15.24)). 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. (3.18.34) shows that the irreducible monic polynomials constitute a representative set. Therefore the result follows from (3.15.26). 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 3.18.38 (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 3.18.39 (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 3.18.40
A polynomial f has at most $\deg(f)$ *roots*

Corollary 3.18.41
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 (3.18.37) each g_i must be appear in the factorization of f, that is to say g splits completely. □

Proposition 3.18.42 (Formal derivative)
Let k be a field. Then there exists a unique k-vector space homomorphism

$$(-)' : k[X] \to k[X]$$

such that

$$(X^r)' = \begin{cases} 0 & r = 0 \\ rX^{r-1} & r > 0 \end{cases}$$

It satisfies the product rule

$$(fg)' = f'g + fg'$$

for all $f, g \in k[X]$. Define recursively $f^{(0)} = f$ and $f^{(n)} := f^{(n-1)\prime}$.

Proof. The monomials $\{1, X, X^2, \ldots\}$ form a k-basis of $k[X]$, so $(-)'$ exists and is unique.

Suppose $f(X) = \sum_{i=0}^{n} a_i X^i$ and $g(X) = \sum_{i=0}^{m} b_i X^i$. Then

$$(fg)(X) = \sum_{i=0}^{n+m} \left(\sum_{k+l=i} a_k b_l \right) X^i$$

and

$$\begin{aligned}
f'(X) &= \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i \\
g'(X) &= \sum_{i=0}^{m-1} (i+1) b_{i+1} X^i \\
(fg)'(X) &= \sum_{i=0}^{n+m-1} (i+1) \left(\sum_{k+l=i+1} a_k b_l \right) X^i \\
&= \sum_{i=0}^{n+m-1} \left(\sum_{k+l=i+1} (k+l) a_k b_l \right) X^i \\
&+ \sum_{i=0}^{n+m-1} \left(\sum_{k+l=i} (k+1) a_{k+1} b_l \right) X^i + \sum_{i=0}^{n+m-1} \left(\sum_{k+l=i} (l+1) a_k b_{l+1} \right) X^i \\
&= f'(X) g(X) + f(X) g'(X)
\end{aligned}$$

□

Proposition 3.18.43 (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 (3.18.38) and (3.18.42)

$$f^{(1)}(X) = (X - \alpha)^{r-1} [r g(X) + (X - \alpha) g'(X)]$$

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 3.18.44 (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 3.18.45
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 (3.18.43). □

Proposition 3.18.46
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 (3.14.5) 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 (3.14.5). □

We can provide a partial converse to (3.18.45) by working in a large enough extension field

Proposition 3.18.47 (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 (3.18.43) $b) \iff c)$

Proposition (3.18.45) shows that $a) \implies b)$. Conversely suppose f is not separable, then by (3.14.5) f and f' must have a non-trivial common divisor h. By (3.18.41) we see that h splits in K. Any root of h is a common root of f and f' in K, which by (3.18.43) is a multiple root of f in K. □

3.18.4 Algebraic Extensions

Proposition 3.18.48 (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 (3.18.33) $m_{\alpha,k} = \lambda p$. In particular $\deg(m_{\alpha,k}(X)) = \deg(p(X))$ so $\deg(q(X)) = 0$ and $q(X)$ is a unit (3.18.32). 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 3.18.49
Let $K/E/k$ be extensions and $\alpha \in K$ algebraic over k. Then α is algebraic over E.

Definition 3.18.50 (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 3.18.51
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 (3.18.15). □

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 3.18.52 (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 $\{1, \alpha, \dots, \alpha^{n-1}\}$.*

Example 3.18.53
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 (3.15.22) so K is a field by (3.4.58). 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 $\pi(p(X)) \overset{(3.18.15)}{=} p(\pi(X)) = p(\alpha)$. By (3.18.18) we see $K = k[\alpha]$. Since K is a field then $K = k[\alpha] = k(\alpha)$ is simple by (3.18.24).

Similarly $f(\alpha) = f(\pi(X)) \overset{(3.18.15)}{=} \pi(f(X)) = 0$, so α is a root of f. By (3.18.33) $f/\ell(f)$ is irreducible and by uniqueness in (3.18.48) 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 $m_\alpha \mid g$, which is 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 3.18.54 (Simple extension)
Let $k(\alpha)/k$ be a simple extension. Then there is a canonical isomorphism of k-algebras

$$k[X]/(m_\alpha) \longrightarrow k(\alpha)$$

under which $X + (m_\alpha) \to \alpha$. Further $k(\alpha)$ is a finite-dimensional vector space with basis

$$\{1, \alpha, \dots, \alpha^{n-1}\}$$

where $n = \deg(m_\alpha) = [k(\alpha) : k]$ and $k(\alpha) = k[\alpha]$.

Proof. By (3.18.48), Definition (3.18.18) and (3.4.56) there is a canonical isomorphism $k[X]/(m_\alpha) \to k[\alpha]$ of k-algebras induced by the evaluation homomorphism $\mathrm{ev}_\alpha : k[X] \to K$. (3.18.52) shows that the image of this isomorphism, $k[\alpha]$, is a field, whence $k[\alpha] = k(\alpha)$ by (3.18.24). Since a k-algebra isomorphism is a-fortiori a k-vector space isomorphism it maps a basis to a basis. The result follows from (3.18.52) as the basis thus defined is the image of the basis in the proposition under the specified isomorphism. □

Definition 3.18.55 (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 3.18.56 (Finitely generated by algebraic $\implies$ finite and algebraic)
Let $K = k(\alpha_1, \ldots, \alpha_n)/k$ be a field extension such that α_i is algebraic. Then K/k is a finite algebraic extension. Furthermore

$$k[\alpha_1, \ldots, \alpha_n] = k(\alpha_1, \ldots, \alpha_n)$$

In particular a finitely-generated algebraic extension is finite.

Proof. We write $K_i = k(\alpha_1, \ldots, \alpha_i)$. Then we have a tower

$$K = K_n/\ldots/K_0 = k$$

such that $K_i = K_{i-1}(\alpha_i)$ is a simple algebraic extension. By (3.18.54) K_i/K_{i-1} is finite. Therefore by (3.18.12) K/k is finite. By (3.18.29) it's also algebraic. For the second statement we may proceed inductively. Note we have

$$k[\alpha_1, \ldots, \alpha_{i+1}] \overset{(3.18.19)}{=} k[\alpha_1, \ldots, \alpha_i][\alpha_{i+1}] = k(\alpha_1, \ldots, \alpha_i)[\alpha_{i+1}] \overset{(3.18.54)}{=} k(\alpha_1, \ldots, \alpha_i)(\alpha_{i+1}) \overset{(3.18.23)}{=} k(\alpha_1, \ldots, \alpha_{i+1})$$

The second equality is simply the inductive hypothesis. □

Corollary 3.18.57
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 3.18.58 (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

$$m_{\alpha,E}(X) = a_0 + a_1 X + \ldots a_n X^n$$

Then define $E_0 = i_{kE}(k)(a_0, \ldots, a_n)$. By (3.18.56) E_0/k is finite. Clearly α is algebraic over E_0 as it is a root of $m_{\alpha,E}$. By (3.18.48) $m_{\alpha,E_0} \mid m_{\alpha,E}$ as elements of $E_0[X]$ and $m_{\alpha,E} \mid m_{\alpha,E_0}$. Therefore $m_{\alpha,E_0} = m_{\alpha,E}$.

By (3.18.54) $E_0(\alpha)/E$ is finite, therefore $E_0(\alpha)/k$ is finite. By (3.18.29) $E_0(\alpha)/k$ is algebraic, whence α is algebraic over k. The last statement follows from (3.18.48) again. □

Corollary 3.18.59
K/E and E/k are both algebraic if and only if K/k is.

Proof. One direction is (3.18.49). The converse follows from the previous result. □

We may prove the first lifting theorem

Proposition 3.18.60 (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

$$\begin{array}{ccc} \mathrm{Mor}_k(k(\alpha), L) & \longrightarrow & \{\beta \in L \mid m_{\alpha,k}(\beta) = 0\} \\ \sigma & \to & \sigma(\alpha) \end{array}$$

and $\sigma(k(\alpha)) = k(\sigma(\alpha))$. In particular if $m_{\alpha,k}$ is separable and splits completely in L then there are precisely $\deg(m_\alpha) \overset{(3.18.54)}{=} [k(\alpha) : k]$ such extensions.

Proof. Observe $m_{\alpha,k}(\sigma(\alpha)) \overset{(3.18.15)}{=} \sigma(m_{\alpha,k}(\alpha)) = 0$. Therefore the mapping is well-defined. By (3.18.26) it is injective. We claim it is also surjective. By (3.18.54) 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 (3.18.48). The final statement follows from (3.18.47) □

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 3.18.61 (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 (3.18.60) 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 (3.18.41) $m_{\alpha,K'}(X)$ splits in L (because $m_{\alpha,k}(X)$ does). Therefore by (3.18.60) 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 (3.18.60) the poset is non-empty, and the same argument works. □

3.18.5 Galois Theory Summary

Definition 3.18.62 (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 (3.18.47)).*

In the case of a Galois extension we denote the group of automorphisms by $\mathrm{Gal}(K/k)$.

To summarize the main results

a) The group of automorphism of a normal extension K/k acts transitively on the roots of a given irreducible polynomial.

b) For K/k finite we have $\#\operatorname{Aut}(K/k) \leq [K : k]$ with equality if and only if K/k is Galois.

c) An algebraic extension K/k is automatically separable whenever either $\mathrm{char}(k) = 0$ or k is finite.

d) When K/k is finite and Galois then we have an order-reversing bijection between subfields and subgroups

$$\begin{aligned} \{H \leq \mathrm{Gal}(K/k)\} &\longleftrightarrow \{F \subseteq K\} \\ H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \mathrm{Gal}(K/F) &\longleftarrow F \end{aligned}$$

3.18.6 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 3.18.63 (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 (3.18.56) K/k is necessarily algebraic, and if S is finite then so is K/k.

Definition 3.18.64 (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 3.18.65 (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 generated by the roots of every polynomial $f \in S$, that is*

$$K = k\left(\bigcup_{f \in S} T_{f,K}\right)$$

- *Any subfield $K' \subset K$ in which S splits completely is equal to K*

Proof. For all $f \in S$ there is a factorisation

$$f = \prod_{\alpha \in T_{f_i,K}} (X - \alpha)$$

Suppose $K = k(\bigcup_{f\in S} T_{f,K})$ and let K' be a subfield in which all $f \in S$ split completely. Then by unique factorization in $K[X]$ we have $T_{f,K} \subset K'$ for all $f \in S$ and therefore $K' = K$.

Conversely it's clear that S splits completely in $k(\bigcup_{f\in S} T_{f,K})$, therefore by hypothesis this equals K. □

Lemma 3.18.66
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 3.18.67 (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 (3.18.66) 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 (3.18.25). □

Proposition 3.18.68 (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 (3.18.41). Therefore the morphism $\sigma : K/k \to L/k$ exists by (3.18.61).

Note by (3.18.67) 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 (3.18.65) and therefore σ is an isomorphism as required. □

Proposition 3.18.69 (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 3.18.70 (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 3.18.71 (Existence of Algebraic Closure)
Given a field k there exists an algebraic closure $\bar{k}/k$

Proposition 3.18.72 (Algebraic extensions embed into Algebraic Closure)
Let K/k be an algebraic extension and M/k be field such that every polynomial $f \in k[X]$ splits completely then there exists a morphism $\sigma : K/k \to M/k$.

In particular this holds when M is algebraically closed.

Proof. A straightforward application of (3.18.61) since every $m_{\alpha,k}(X)$ splits in M. □

Corollary 3.18.73 (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 3.18.74 (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 (3.18.52). □

Remark 3.18.75
Note if K/k is an algebraic extension then (3.18.72) 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 $i_{k_{i+1}} \circ i_{k_i,k_{i+1}} = i_{k_i}$.

3.18.7 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 3.18.76
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 (3.18.48). Apply i_{KL} and then we may use (3.18.41). □

Proposition 3.18.77 (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 (3.18.61) with $K = L$. □

Proposition 3.18.78 (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 (3.18.67).

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 (3.18.77) 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 (3.18.66) $m_{\alpha,k}(X)$ splits completely in K. Therefore K/k is normal as required. □

Corollary 3.18.79 (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 (3.18.68) there is a morphism $\sigma : K/k \to L/k$ with $\sigma(\alpha) = \beta$. By (3.18.67) 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 (3.18.66) $m_{\alpha,k}(X)$ splits completely in K. As α was arbitrary then K/k is normal. □

Proposition 3.18.80 (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 (3.18.61) 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 (3.18.30) 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 3.18.81 (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 (3.18.80) this composition is surjective, whence the result follows. □

Corollary 3.18.82 (Quotient of automorphism group)
Let $L/K/k$ be a tower of extensions such that L/k and K/k are normal. Then L/K is normal and there is an isomorphism of groups.

$$\begin{array}{rcl} \operatorname{Aut}(L/k)/\operatorname{Aut}(L/K) & \longrightarrow & \operatorname{Aut}(K/k) \\ \sigma & \to & i_{KL}^{-1} \circ \sigma \circ i_{KL} \end{array}$$

Proof. The given map is well-defined by (3.18.78) since $(\sigma \circ i_{KL})(K) = i_{KL}(K)$, and σ fixes K precisely when $\sigma \circ i_{KL} = i_{KL}$, that is $\sigma \in \operatorname{Aut}(L/k)$. Given $\tau \in \operatorname{Aut}(K/k)$, by (3.18.80) there exists $\sigma \in \operatorname{Aut}(L/k)$ 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 3.18.83 (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 3.18.84 (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 (3.18.79) L/k is normal and by (3.18.61) 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 (3.18.65). 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 (3.18.79). By assumption $L' = L$ and therefore L/k is the splitting field for S'. Uniqueness follows from the uniqueness of splitting fields (3.18.68). □

3.18.8 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 3.18.85 (Separable element)
*We say $\alpha \in K/k$ is **separable** over k if it is algebraic and $m_{\alpha,k}(X)$ is a separable polynomial.*

*We say K/k is **separable algebraic** (or just separable if K/k is assumed to be algebraic) if every $\alpha \in K$ is **separable**.*

Lemma 3.18.86
$\alpha \in K/k$ 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 $i_{kK}(k) \subset E \subset K$.

Proof. One direction is obvious. Conversely suppose $f(\alpha) = 0$ with f separable. Then $m_{\alpha,k} \mid f$ so the result follows from (3.18.46). □

Proposition 3.18.87 (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 3.18.88 (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 (3.18.60), the final equality from (3.18.54). The inequality follows from (3.18.40). The final statement follows from (3.18.47). □

The main results of this section are the following

Proposition 3.18.89 (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

$$\psi := \mathrm{Mor}_k(i_{FK}, L) : \mathrm{Mor}_k(K, L) \to \mathrm{Mor}_k(F, L)$$

It is surjective by (3.18.81). Consider $\sigma \in \mathrm{Mor}_k(F, L)$ and the fibre $\psi^{-1}(\sigma) = \mathrm{Mor}_F(K, (L/F, \sigma))$. 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 $\mathrm{Mor}_k(K, L)$ 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 (3.18.88) 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 (3.18.86) 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 3.18.90 (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 (3.18.86).

Conversely the finite case follows from (3.18.89) by multiplicativity. For the general case, consider $\alpha \in K$. Then (3.18.58) 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 (3.18.88) 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 (3.18.89) $[E_0 : k]_s = [E_0 : k]$. 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 3.18.91
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 (3.18.86) α_i is separable over K_{i-1}. Therefore $[K_i : K_{i-1}]_s = [K_i : K_{i-1}]$ by (3.18.88) and $[K:k]_s = [K:k]$ by multiplicativity. (3.18.89) shows that K/k is separable. □

Proposition 3.18.92 (Equivalent definition of separability)
Let K/k be an algebraic extension. 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 (3.18.89). We need only show *b)* $\implies$ *a)*.

Consider $\alpha \in K$. Then by (3.18.58) 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. □

3.18.9 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 3.18.93
*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.*

*We say an extension K/k is **purely inseparable** if every $x \in K/k$ is purely inseparable.*

*Further K/k is **purely inseparable of height** $\leq n$ if additionally every $x \in K$ has height at most n.*

Lemma 3.18.94
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 (3.18.6) we have $f(X) = (X-b)^{p^e}$. Then evidently b is the unique root. □

Lemma 3.18.95
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 (3.18.6) $f(X) = (X-b)^{p^e}$ 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 3.18.96
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 given polynomial is irreducible by (3.18.95) and therefore is the minimal polynomial by uniqueness. The first relation follows from (3.18.54) and the second from (3.18.88). □

Corollary 3.18.97
Let $x \in K/k$. Then the following are equivalent

a) *x is purely inseparable*

b) *$m_x(X) = (X-x)^r$ for some r*

In this case we must have $r = p^n$ where n is the height of x.

Corollary 3.18.98
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 (3.18.47) $e = 0$ which means precisely $x \in k$. □

Proposition 3.18.99 (Relative Separable Closure)
Let K/k be a field extension. The subextension $K_s/k \subset K/k$ of separable elements form a separable algebraic subfield. Furthermore if K/k is algebraic then K/K_s is purely inseparable and the restriction map

$$\mathrm{Mor}_k(K, L) \to \mathrm{Mor}_k(K_s, L)$$

is bijective for every normal extension L/K. 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 algebraic then the field $k(\alpha, \beta)$ is separable algebraic by (3.18.91). As this contains $\alpha \pm \beta$ and $\alpha\beta$ then K_s is a subfield which is by definition separable. Then by (3.18.89) 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 (3.18.101) 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. Consider the mapping

$$\mathrm{Mor}_k(K, L) \to \mathrm{Mor}_k(K_s, L)$$

obtained by restriction. By (3.18.81) 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 (3.18.96). This shows that $\widehat{\psi}$ is unique and the mapping is bijective. □

This relied on the following results

Lemma 3.18.100 (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 3.18.101 (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 (3.18.100) □

Definition 3.18.102 (Degree of Inseparability)
Let K/k be a finite extension. Then in light of (3.18.99) we may define the ***degree of inseparability*** *to be the integer*

$$[K : k]_i := \frac{[K : k]}{[K : k]_s}$$

By (3.18.11) and (3.18.89) it is multiplicative in the sense that for a tower of finite extensions

$$[L : k]_i = [L : K]_i [K : k]_i$$

3.18.10 Separable closure

Proposition 3.18.103 (Relatively Separably Closed)
Let K/k be an extension. The following are equivalent

a) *Every separable $x \in K/k$ lies in k*

b) *Every separable algebraic subextension is trivial*

c) *K_s/k is trivial*

*In this case we say K/k is **relatively separably closed**.*

If K/k is algebraic then this is equivalent to being purely inseparable.

Proof. The final statement follows from (3.18.99). □

Definition 3.18.104
*We say a field k is **separably closed** if every separable algebraic extension is trivial.*

*We say an extension k^{sep}/k is a **separable closure** if it is separable algebraic and separably closed.*

Proposition 3.18.105
Let $\bar{k}/k$ be an algebraic closure, then the subextension $\bar{k}_s/k$ is a separable closure for k.

Furthermore every separable closure is isomorphic to $\bar{k}_s/k$ and $\bar{k}/\bar{k}_s$ is purely inseparable.

Proof. By (3.18.99) $\bar{k}_s/k$ is separable and algebraic. Suppose $K/\bar{k}_s$ is separable and algebraic then by (...) there exists an embedding $i : K/\bar{k}_s \to \bar{k}/\bar{k}_s$. As $\bar{k}_s$ is relatively separably closed in $\bar{k}$ we see that $i(K) = \bar{k}_s$ and therefore $K = \bar{k}_s$.

Let k^{sep}/k be a separable closure, then by (3.18.72) there is an embedding $\phi : k^{sep}/k \to \bar{k}/k$. Then by definition $\phi(k^{sep}) \subset \bar{k}_s$, so this defines an extension $\bar{k}_s/k^{sep}$ which is by definition separable. By assumption it is trivial which means precisely $\phi(k^{sep}) = \bar{k}_s$.

It follows from (3.18.99) that $\bar{k}/\bar{k}_s$ is purely inseparable. □

Proposition 3.18.106
Let k^{sep}/k be a separable closure and k'/k a separable algebraic extension. Then there exists a morphism

$$k'/k \to k^{sep}/k$$

Proof. By (3.18.105) we may identify k^{sep}/k with $\bar{k}_s/k$. By (3.18.72) there exists a morphism $k'/k \to \bar{k}/k$ which by definition has image in $\bar{k}_s/k$. □

3.18.11 Perfect Fields

Proposition 3.18.107 (Perfect Closure)
Let k be a field with characteristic exponent p contained in an algebraically closed field Ω (e.g. $\bar{k}$). Define

$$k^{p^{-n}} := \{x \in \Omega \mid x^{p^n} \in k\}$$

Then $k^{p^{-n}}$ is a subfield of Ω/k, which is purely inseparable of height $\leq n$. Furthermore it is a splitting field for the family of polynomials $\{X^{p^r} - a \mid a \in k\,, r \leq n\}$ which characterizes it up to isomorphism. Furthermore

$$k^{p^{-\infty}} := \{x \in \Omega \mid x^{p^n} \in k \text{ some } n \geq 1\} = \bigcup_{n \geq 1} k^{p^{-n}}$$

is the smallest perfect subfield of Ω containing k and is also a splitting field for the family of polynomials $\{X^{p^n} - a \mid a \in k\,, n \in \mathbb{N}\}$.

Proof. Suppose $\alpha, \beta \in k^{p^{-n}}$ then applying the Frobenius homomorphism (...) we see $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ and so $k^{p^{-n}}$ is an additive subgroup. Furthermore $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n}$ whence it is a multiplicative subgroup as this demonstrates $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} \in k$. Therefore it is a subfield which is by definition purely inseparable of height $\leq n$.

By definition $k^{p^{-n}}$ is precisely the set of roots of the given polynomials and it is therefore the corresponding splitting field by (...). This also shows that $n \leq m \implies k^{p^{-n}} \subseteq k^{p^{-m}}$ which shows that the union $k^{p^{-\infty}}$ is a subfield of Ω.

To demonstrate it's perfect we need to show every element $x \in k^{p^{-n}}$ has a p-th root. By definition $x^{p^n} \in k$ and there exists a root α to the polynomial $X^{p^{n+1}} - x^{p^n}$ in $k^{p^{-(n+1)}}$. Therefore $(\alpha^p - x)^{p^n} = 0$ whence $\alpha^p = x$ as required.

Let k' be another perfect subfield containing k. We claim by induction that $k^{p^{-n}} \subseteq k'$. For given $\alpha \in k^{p^{-(n+1)}}$ by definition $\alpha^p \in k^{p^{-n}}$ whence $\alpha^p \in k'$ by the inductive hypothesis, and by assumption $\alpha \in k'$. Therefore $k^{p^{-\infty}}$ is the smallest perfect subfield. Furthermore by definition it is the set of roots of the given family of polynomials and therefore the corresponding splitting field. □

Proposition 3.18.108
Let k'/k be a purely inseparable extension of height $\leq n$, then there exists an embedding

$$k'/k \to k^{p^{-n}}/k$$

If k'/k is purely inseparable and K/k is perfect then there also exists an embedding

$$k'/k \to K/k$$

Proof. For the first part let $\alpha \in k'$ then by (3.18.96) the minimal polynomial of α is $g(X) = X^{p^e} - \alpha^{p^e}$ for $e \leq n$ which splits completely in $k^{p^{-n}}$ by (3.18.107). Then the embedding exists by (3.18.61).

Suppose K/k is perfect then we claim that $X^{p^n} - a$ splits completely for every $a \in K$. By induction there is $b \in K$ such that $b^{p^n} = a$. Then $X^{p^n} - a = (X-b)^{p^n}$ splits completely. In particular for every $\alpha \in k'$ the minimal polynomial splits completely in K/k and the embedding follows from (3.18.61). □

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 3.18.109 (Finite fields are perfect)
Any finite field is perfect.

Proof. The Frobenius homomorphism is injective and therefore surjective by counting. □

Proposition 3.18.110 (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 (3.18.48) 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 (3.18.90).

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 (3.18.95) 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 (3.18.101) 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 (3.18.101) $\text{char}(k) = p > 1$ and $f \in k[X^p]$. By assumption all the coefficients are p-th powers and therefore $f = h^p$ by (3.18.6) for some $h \in k[X]$. This contradicts irreducibility of f, and so f must be separable. □

3.18.12 Applications of Separability

Definition 3.18.111 (Bounds on $\text{Aut}(K/k)$)
Let K/k be an algebraic extension and L/K an extension such that L/k is normal. Then there is a natural injection

$$\begin{aligned} \text{Mor}_k(K, i_{KL}) : \text{Aut}(K/k) &\to \text{Mor}_k(K, L) \\ \sigma &\to i_{KL} \circ \sigma \end{aligned}$$

In particular in the case $[K : k] < \infty$

$$\#\operatorname{Aut}(K/k) \leq [K:k]_s \leq [K:k] < \infty$$

If i_{KL} is inclusion, then we may regard $\operatorname{Aut}(K/k)$ as a subset of $\operatorname{Mor}_k(K,L)$

As an application of the concept of separability degree we prove

Proposition 3.18.112 (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 $\operatorname{Mor}_k(K,\bar{k}) = \{\sigma_1,\dots,\sigma_n\}$ which by (3.18.92) 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 $\#\operatorname{Mor}_k(k(\alpha+c\beta),\bar{k}) \geq n$ 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. □

3.18.13 Normal Extensions II

We provide some more straightforward criteria based on $[K:k]_s$

Proposition 3.18.113 (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

$$\operatorname{Mor}_k(K, i_{KL}) : \operatorname{Aut}(K/k) \to \operatorname{Mor}_k(K,L)$$

is a bijection. In particular if K/k is finite, then it is normal if and only if

$$\#\operatorname{Aut}(K/k) = [K:k]_s$$

Proof. Suppose K/k is normal and consider $\sigma \in \operatorname{Mor}_k(K,L)$. Then by NOR1 $\sigma(K) = i_{KL}(K)$ and we may define $\tau := i_{KL}^{-1} \circ \sigma$ with $\tau \in \operatorname{Aut}(K/k)$. The converse is similar.

For the final part we've already observed (3.18.111) that in the finite case $\#\operatorname{Aut}(K/k) \leq [K:k]_s = \#\operatorname{Mor}_k(K,L) \leq [K:k] < \infty$. Therefore the embedding $\operatorname{Mor}_k(K, i_{KL})$ is a bijection precisely when the orders are the same. □

Corollary 3.18.114 (Galois Criteria)
Let K/k be a finite extension. Then

$$\#\operatorname{Aut}(K/k) \leq [K:k]_s \leq [K:k]$$

with equalities if and only if K/k is Galois.

Proof. We've seen the inequalities (3.18.111)

$$\#\operatorname{Aut}(K/k) \leq [K:k]_s \leq [K:k] < \infty$$

with equality if and only if K/k is both normal (3.18.113) and separable (3.18.89) □

3.18.14 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 3.18.115 (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 ((3.18.40)) 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 (3.18.40). Therefore the fact $K^\star$ is cyclic follows from (3.3.24). □

Proposition 3.18.116 (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 (3.18.30). □

Further we can show existence and uniqueness of finite fields.

Proposition 3.18.117 (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 (3.18.47) $f(X)$ has p^n distinct roots and the splitting field of $f(X)$ is exactly the set of roots.

Furthermore every subfield of order p^n must satisfy this polynomial by Lagrange's (3.3.12), so it is the unique such subfield.

Since every algebraic extension of $\mathbb{F}_p$ is isomorphic to a subfield of $\overline{\mathbb{F}_p}$ it's also the unique algebraic extension of order p^n up to isomorphism.

Clearly if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ we see that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p]$, so we must have $m \mid n$. Conversely if $\alpha \in \mathbb{F}_{p^m}$ then $\alpha^{p^m} = \alpha \implies \alpha^{p^{rm}} = \alpha$ for all $r > 0$, so $\alpha \in \mathbb{F}_{p^n}$. □

It is usually most convenient to work in $\overline{\mathbb{F}_p}$ and consider the finite fields of the form $\mathbb{F}_{p^n}$ as in the Proposition. We've seen in (3.18.109) that every finite field $\mathbb{F}_q := \mathbb{F}_{p^n}$ is perfect and therefore every algebraic extension is separable (3.18.110). In fact we may show that every finite extension is Galois.

Proposition 3.18.118
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 ((3.18.40)) so we must have $d \geq n$, and therefore $d = n$. Clearly ϕ generates a cyclic subgroup of order n. However by (3.18.114) 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 3.18.119 (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 $m \mid n$ (and no such subfield otherwise). 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 (3.18.117) 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 (3.18.114) $\#H \leq [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$, whence we have equality and so the extension is Galois by (3.18.114) and $H = \langle \phi^m \rangle$. □

Lemma 3.18.120
Let $x \in \mathbb{F}_{p^n}$. Then $\deg(x) = n \iff \mathrm{Fix}(x) = \{1\} \subset \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

In other words $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ *acts freely on the elements of degree n.*

Proof. Observe that $\deg(x) = n \iff [\mathbb{F}_p(x) : \mathbb{F}_p] = n \iff \mathbb{F}_p(x) = \mathbb{F}_{p^n} \overset{(3.18.122)}{\iff} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p(x)) = \{1\}$ which is equivalent to the statement. □

3.18.15 Galois Theory

We've seen that for K/k a finite extension

$$\#\,\mathrm{Aut}(K/k) \leq [K : k]_s \leq [K : k]$$

with equality if and only if K/k is Galois, by (3.18.114).

Remark 3.18.121
If k is perfect then $\bar{k}/k$ is Galois.

The main result of Galois Theory is

Proposition 3.18.122
Let K/k be a finite Galois extension then there is an order-reversiing bijection between subgroups and subfields

$$\begin{aligned} \{H \leq \mathrm{Gal}(K/k)\} &\longleftrightarrow \{F/k \subseteq K/k\} \\ H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \mathrm{Gal}(K/F) &\longleftarrow F \end{aligned}$$

Proof. This is proved in a series of Propositions in the rest of this section. Firstly we show it is well-defined in (3.18.123). The maps are mutual inverses by (3.18.124) and (3.18.125). □

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 3.18.123
If K/k is Galois and $F \subset K/k$ then K/F is Galois.

Proof. This follows from (3.18.76) and (3.18.90). □

Proposition 3.18.124 (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 (3.18.77) there is an element $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\alpha) = \beta$. In other words $\alpha \notin K^{\mathrm{Gal}(K/F)}$, which shows the reverse inclusion. □

Proposition 3.18.125
Let K/k be a field extension and $H \subseteq \mathrm{Aut}(K/k)$ a finite subgroup then K/K^H is finite Galois with

$$H = \mathrm{Gal}(K/K^H)$$

and order equal to $[K : K^H]$. When K/k is finite then H is automatically finite.

Proof. Firstly observe that trivially $H \subseteq \mathrm{Aut}(K/K^H)$. If we know that $[K : K^H] < \infty$, then by (3.18.114) we have

$$\#H \leq \#\,\mathrm{Aut}(K/K^H) \leq [K : K^H]_s \leq [K : K^H]$$

We can prove equality everywhere if we show that $[K : K^H] \leq \#H$, which is shown either by (3.18.126) or (3.18.127). Note equality also shows that K/K^H is finite Galois by the same result.

Finally when K/k is finite, then $\#\,\mathrm{Aut}(K/k) < \infty$. So in this case H is always finite. □

We present two approaches to showing the inequality $[K : K^H] \leq \#H$. The first uses independence of characters style argument (see Garling, JMilne), and the second which is more straightforward uses the action of H to show that every element has degree at most $\#H$ (Artin).

Lemma 3.18.126 (Bound degree of fixed field I)
Let K/k be a field extension and $H \subset \mathrm{Aut}(K/k)$ a finite subgroup. Then $[K : K^H] \leq \#H$

Proof. Let $H = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}$ and $\alpha_1, \ldots, \alpha_m$ a K^H-basis for K.

Consider the vector space K^n and the elements $\hat{\alpha}_j = (\sigma_1(\alpha_j), \ldots, \sigma_n(\alpha_j))$ for $j = 1 \ldots m$. It's enough to show that these are linearly independent over K, as that implies $m \leq n$ by (3.4.137).

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 3.18.127 (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 (3.18.47). 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 (3.18.46).

If K/k is finite, then a-fortiori K/K^H is finite, so we may apply the Primitive Element Theorem (3.18.112) 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 (3.18.112), 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 3.18.128
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 (3.18.78) 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 (3.18.122) $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/F') \iff F = F'$. 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 (3.18.82). □

3.18.16 Transcendental Field Extensions

Definition 3.18.129 (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 $x_1, \dots, x_n \in S$ 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 3.18.130
Let K/k be a field extension and S, T subsets of 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 $a) \iff b)$.

Suppose $a)$ holds, then a-fortiori S is algebraically independent over k. Suppose T is algebraically dependent over $k(S)$, then there exists $t_1, \dots, t_n \in T$ such that $F(x_1, \dots, x_n) = 0$ for some $0 \neq F \in k(S)[X_1, \dots, X_n]$. By clearing denominators we may assume that $F \in k[S][X_1, \dots, X_n]$. As there are only finitely many coefficients we may also take $S = \{s_1, \dots, s_m\}$ to be finite. Explicitly

$$F(X_1, \dots, X_n) = \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

and

$$\lambda_\alpha = G_\alpha(s_1, \dots, s_m)$$

for some $G_\alpha \in k[Y_1, \dots, Y_m]$. We may then define $\widehat{F} \in k[X_1, \dots, X_n, Y_1, \dots, Y_m]$ by

$$\widehat{F}(X_1, \dots, X_n, Y_1, \dots, Y_m) := \sum_{\alpha \in \mathbb{N}^n} G_\alpha(Y_1, \dots, Y_m) X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

Then $\widehat{F}(t_1, \dots, t_n, s_1, \dots, s_m) = 0$, and by assumption this is an algebraic dependence (as $S \cap T = \emptyset$). Therefore by assumption $\widehat{F} = 0$ and in particular $G_\alpha(s_1, \dots, s_m) = 0$ for all α. This implies $F = 0$, a contradiction.

$b) \implies a)$ Evidently $S \cap T = \emptyset$ otherwise there is a trivial algebraic dependence of T on $k(S)$. Suppose there is an algebraic dependence of $S \cup T$ on k. We may assume wlog that $S = \{s_1, \dots, s_m\}$ and $T = \{t_1, \dots, t_n\}$ are finite. Then the evaluation homomorphism

$$k[X_1, \dots, X_n, Y_1, \dots, Y_m] \to K$$

may be written as a composite

$$k[X_1, \dots, X_n, Y_1, \dots, Y_m] \to k(S)[X_1, \dots, X_n] \to K$$

which are both injective by hypothesis. □

Corollary 3.18.131 (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 (3.18.130) by considering $S = \{x\}$ and $T = \{y\}$. □

Corollary 3.18.132 (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 (3.18.130). □

Corollary 3.18.133 (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 (3.18.130).

$b) \implies a)$ 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 (3.18.132) it satisfies the extension property. Therefore by (2.3.6) it is precisely the family of matroid independent sets. □

Proposition 3.18.134 (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 3.18.135 (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 3.18.136
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 3.18.137
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 3.18.138
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 (3.18.135)

b) A-fortiori $K/k(\Gamma)$ is finitely generated and by assumption algebraic so by (...) it is finite □

3.18.17 Separating Transcendence Base

In applications the existence of a separating transcendence base is important, and is guaranteed when k is perfect, or a weaker condition.

Definition 3.18.139 (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.*

Definition 3.18.140 (Maclane's Criterion)
*We say that an algebra A/k of characteristic exponent p satisfies **Maclane's Criterion** if it is reduced and and for all $a_1, \ldots, a_n \in K$ the following property holds*

$$\{a_1, \ldots, a_n\} \text{ } k\text{-linearly independent} \implies \{a_1^p, \ldots, a_n^p\} \text{ } k\text{-linearly independent}$$

When $p = 1$ this is trivially always satisfied and when $p > 1$ such an algebra is automatically reduced by the following result

Lemma 3.18.141
Let A be a k-algebra and $m > 1$ an integer. Then the following are equivalent

a) *A is reduced*

b) $x^m = 0 \implies x = 0$

In particular if A has characteristic exponent $p > 1$ then it is reduced iff the Frobenius homomorphism is injective.

Proof. *a)* $\implies$ *b)* is trivial. Conversely suppose $x^n = 0$. Then there exists $a > 0$ such that $n \leq am$. In particular $x^{am} = 0$ and therefore by induction $x = 0$ as required. □

This is a generalization of the case of a perfect base field by the following result.

Proposition 3.18.142 (Perfect $\implies$ Maclane)
Let A/k be a reduced algebra with k perfect. Then it satisfies Maclane's Criterion.

In particular this holds for every field extension K/k of a perfect base field.

Proof. By assumption A is reduced so we may consider only the case $p > 1$.

Suppose $0 = \sum_i \lambda_i a_i^p$ then by hypothesis $\lambda_i = \mu_i^p$. By (3.18.6) $0 = (\sum_i \mu_i a_i)^p$. As A is reduced we find $0 = \sum_i \mu_i a_i$ as required. □

Lemma 3.18.143
Let $n \geq 0$ an integer and $K = k(x_1, \ldots, x_{n+1})$ an extension of k such that

- $\mathrm{char}(k) \neq 0$
- $\{x_1, \ldots, x_n\}$ *is a transcendence base*
- K/k *satisfies Maclane's Criterion*

Then for some x_i the set $\{x_1, \ldots, \widehat{x_i}, \ldots, x_{n+1}\}$ is a ***separating transcendence base*** *for K/k.*

Note when $n = 0$ this means precisely that a simple algebraic extension satisfying Maclane's Criterion is separable.

Proof. By assumption x_{n+1} is algebraic over $k(x_1, \ldots, x_n)$, and therefore there exists a non-zero $F \in k[X_1, \ldots, X_{n+1}]$ such that $F(x_1, \ldots, x_{n+1}) = 0$. 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 $(x_1, \ldots, x_{n+1})$, and this factor would have smaller total degree.

We wish to show that not all powers of X_i appearing in F are multiples of p. Suppose this were the case then the monomials

$$\{x_1^{\alpha_1} \ldots x_{n+1}^{\alpha_{n+1}} \mid \lambda_\alpha \neq 0\}$$

are k-linearly dependent where λ_α are the coefficients of F and $\alpha \in \mathbb{N}^{n+1}$. Then by Maclane's Criterion the set

$$\{x_1^{\alpha_1/p} \ldots x_{n+1}^{\alpha_{n+1}/p} \mid \lambda_\alpha \neq 0\}$$

is linearly dependent. This contradicts the minimality of F.

Choose X_i for which a non p-th power appears in F and define

$$F_i(T) := F(x_1, \ldots, x_{i-1}, T, x_i, \ldots, x_{n+1}) \in k[S_i][T]$$

where $S_i := \{x_1, \ldots, \widehat{x_i}, \ldots, x_{n+1}\}$. By assumption $F_i(T)$ is non-zero and clearly $F_i(x_i) = 0$ so that x_i, and therefore by (3.18.56) K is algebraic over $k(S_i)$. By (3.18.137) S_i is a transcendence base for K and in particular algebraically independent. Therefore $k[S_i][T]$ may be identified with $k[X_1, \ldots, X_{n+1}]$ and we may conclude that $F_i(T)$ is irreducible. Further $k[S_i]$ is a UFD so by (3.15.33) $F_i(T)$ is irreducible as a polynomial in $k(S_i)[T]$. By construction $F_i(T) \notin k(S_i)[T^p]$ so by (3.18.101) F_i is separable. Therefore x_i is separable over $k(S_i)$, and $K/k(S_i)$ is separable by (3.18.91) as required. □

Proposition 3.18.144
Let K/k be a finitely-generated field extension which satisfies Maclane's Criterion (e.g. 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 (3.18.135). Every subfield of K also has characteristic 0, so then we are done by (3.18.110). So we may only consider the positive characteristic case, $p > 1$.

Suppose $K = k(x_1, \ldots, x_n)$. By (3.18.134) there is a (possibly empty) subset which is a transcendence base, say $\{x_1, \ldots, x_d\}$ after renumbering. By (3.18.56) $[K : K'] < \infty$ where $K' = k(x_1, \ldots, x_d)$, and we may choose K' such that the degree of inseparability $[K : K']_i$ is minimal. If K/K' is separable then we are done. Otherwise we may

assume by renumbering that $K'(x_{d+1})/K$ is not separable (3.18.91) and therefore $[K'(x_{d+1}) : K']_i > 1$. Then by (3.18.143) $[K'(x_{d+1}) : K'']_i = 1$ where $K'' := k(x_1, \ldots, \widehat{x}_j, \ldots, x_{d+1})$. By multiplicativity $[K : K'']_i < [K : K']_i$ which contradicts minimality. □

3.19 Local Rings

Local rings arise quite naturally when localizing at a prime ideal (see (3.6.32) and Example 3.19.4) so we recall some basic properties here.

Definition 3.19.1 (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 3.19.2 (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 3.19.3 (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 3.19.4
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 3.19.5 (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. □

3.20 Modules over Local Rings (Nakayama's Lemma)

The main result of this section ((3.20.7)) 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 3.20.1 (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 3.20.2
The Jacobson Radical $\sqrt{0}^J$ is a proper ideal

Example 3.20.3
When $(A, \mathfrak{m}_A)$ is a local ring then $\sqrt{0}^J = \mathfrak{m}_A$.

Lemma 3.20.4 (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 3.20.5 (Nakayama's Lemma)
Let M be a finitely generated A-module and $\mathfrak{a} \lhd A$ an ideal. Then the following holds

a) *If $M = \mathfrak{a}M$ then there exists $a \in \mathfrak{a}$ such that $m = am$ for all $m \in M$*

Suppose in addition that $\mathfrak{a} \subseteq \sqrt{0}^J$ (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 3.16.4 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 3.16.3 (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 (3.20.4) $(1-a)$ is invertible, whence $m = 0$ as required.

c) Observe $\mathfrak{a}(M/N) \overset{(3.4.101)}{=} (N + \mathfrak{a}M)/N = M/N$ 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 3.16.3

$$m_1 = \sum_j a_j m_j \quad a_j \in \mathfrak{a}$$

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 (3.20.4). 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 3.20.4 $S^{-1}\mathfrak{a} \subseteq J(S^{-1}A)$. 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 (3.4.102) 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 3.20.6
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 (3.20.5).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 3.20.7 (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 $\widetilde{M}$ and $\widetilde{\cdot}|_S$ 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 $\widetilde{\cdot}|_S$ is injective so $\#S = \#\widetilde{S} = n$).*

Proof. a) By (3.4.102) $\widetilde{M}$ is a k-module, and it's clearly finite.

b) By the (3.20.6) 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 (3.20.6) $\widetilde{S}$ spans $\widetilde{M}$. Suppose $\widetilde{T} \subset \widetilde{S}$ also spans $\widetilde{M}$. By (3.20.6) 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.

□

3.21 Lying over, Incomparability, Going Up and Going Down

Definition 3.21.1 (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 3.21.2 (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 3.21.3
It's possible to interpret these geometrically in terms of the map $\phi_\star : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$.

- *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 3.21.5. 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 3.21.4 (Lieing over criteria)
Let $\phi : A \to B$ be a ring map, $\mathfrak{p} \lhd A$ prime such that $\ker(\phi) \subseteq \mathfrak{p}$ 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 (3.4.51) that in general $\mathfrak{p} \subseteq \mathfrak{q}^c \iff \mathfrak{p}^e \subseteq \mathfrak{q}$. The first equivalence is then clear because $x \in \mathfrak{q}^c \setminus \mathfrak{p} \iff \phi(x) \in \mathfrak{q} \cap \phi(A \setminus \mathfrak{p})$. For $\phi(x) \in \mathfrak{q} \cap \phi(A \setminus \mathfrak{p}) \implies \phi(x) = \phi(y)$ for $y \notin \mathfrak{p}$ and $x \in \mathfrak{q}^c$. This implies $x - y \in \ker(\phi) \subseteq \mathfrak{p}$ whence $x \notin \mathfrak{p}$ as required.

The final statement follows by considering $\mathfrak{q} = \mathfrak{p}^e$. □

Proposition 3.21.5 (Lieing over correspondence)
Let $\phi : A \to B$ be a ring map and $\mathfrak{p} \lhd A$ a prime ideal s.t. $\ker(\phi) \subseteq \mathfrak{p}$. Then there is a order-preserving correspondence of prime ideals

$$\begin{array}{ccccc} \{\mathfrak{q} \mid \mathfrak{q} \text{ lies above } \mathfrak{p}\} & \longleftrightarrow & \{\mathfrak{q}' \lhd B_{\mathfrak{p}} \mid \mathfrak{p}B_{\mathfrak{p}} \subseteq \mathfrak{q}'\} & \longleftrightarrow & \{\mathfrak{q}'' \lhd B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}\} \\ \mathfrak{q} & \longrightarrow & \mathfrak{q}B_{\mathfrak{p}} & & \longrightarrow \mathfrak{q}B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \end{array}$$

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 3.21.4 $\mathfrak{q}$ 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 (3.4.55).

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 $\mathfrak{p} = \mathfrak{p}^{ec} \overset{3.21.4}{\iff} \mathfrak{p}^e \cap S = \emptyset \overset{3.6.17.e)}{\iff} \mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$ □

Remark 3.21.6
Geometrically this is an explicit representation of the fiber as a prime spectrum

$$\mathrm{Spec}(\phi)^{-1}(\mathfrak{p}) \longleftrightarrow \mathrm{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p})$$

Proposition 3.21.7 (Injective Ring Maps are Dense)
Let $\phi : A \to B$ be a ring map and $\mathfrak{p} \lhd A$ a minimal prime over $\ker(\phi)$. Then there exists a prime ideal $\mathfrak{q} \lhd B$ such that $\mathfrak{q}^c = \mathfrak{p}$. Furthermore $\mathfrak{q}$ may be taken to be minimal.

Proof. We may reduce to the case ϕ is injective by replacing A with $A/\ker(\phi)$. We have the commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle i_S} & & \downarrow{\scriptstyle i_T} \\ A_\mathfrak{p} & \overset{\tilde{\phi}}{\dashrightarrow} & T^{-1}B \end{array}$$

where $S := A \setminus \mathfrak{p}$ and $T := \phi(S)$. By (3.6.6) there exists a homomorphism $\tilde{\phi}$. Define $\mathfrak{m} := \mathfrak{p}A_\mathfrak{p}$ to be the unique maximal ideal of $A_\mathfrak{p}$. By (3.6.17) it is a minimal prime ideal and therefore the unique prime ideal. By assumption $0 \notin T$ and so $T^{-1}B \neq 0$. $T^{-1}B$ has a maximal ideal $\mathfrak{n}$ by (3.4.36). By uniqueness we find $\tilde{\phi}^{-1}(\mathfrak{n}) = \mathfrak{m}$. Therefore $\mathfrak{q} := i_T^{-1}(\mathfrak{n})$ is a prime ideal such that $\mathfrak{q}^c = \mathfrak{p}$.

By (3.4.43) there is a minimal prime $\mathfrak{r} \subset \mathfrak{q}$ which by minimality also satisfies $\mathfrak{r}^c = \mathfrak{p}$. □

3.22 Integral Ring Extensions

Definition 3.22.1 (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 3.22.2 (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 3.22.3
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 3.16.4 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 3.22.4 (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 (3.13.4)).

For any $b \in A[b_1, \ldots, b_n]$ we have $A[b] \subset A[b_1, \ldots, b_n]$ so by (3.22.3) 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 (3.22.3). □

Proposition 3.22.5 (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 (3.22.3) B' is a finite A-module and $B'[c]$ is a finite B'-module. Therefore $B'[c]$ is a finite A-module and by (3.22.3) we have c is integral over A. □

Definition 3.22.6 (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 3.22.7 (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 (3.22.4) the subring $A[\alpha, \beta]$ is a finite A-module containing $\alpha \pm \beta$ and $\alpha\beta$. Therefore by (3.22.3) they are also integral over A.

Clearly $\bar{A}$ is integral over A so by (3.22.5) it is integrally closed. □

Proposition 3.22.8 (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 (3.22.7) $\bar{A}$ 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 (3.22.4). Let $\phi \in \mathrm{End}_A(M)$ denote multiplication by b^n then $\phi(M) \subseteq \mathfrak{a}M$ so by Theorem 3.16.4 ϕ satisfies a monic polynomial with coefficients in $\mathfrak{a}$. In particular b^n is integral over $\mathfrak{a}$. □

Proposition 3.22.9
A UFD is integrally closed.

In particular polynomial ring over a UFD is integrally closed.

Proof. □

The following criterion is also useful :

Lemma 3.22.10 (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 3.22.11 (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 3.22.12
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 (3.4.55)) 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 3.22.13 (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 (3.4.55). By (3.22.12) 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 (3.4.58). Then we may apply (3.22.11) to show the equivalence. □

Proposition 3.22.14 (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 (3.22.12) 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 (3.22.13) $\widetilde{\phi}^{-1}(\mathfrak{n})$ 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 (3.21.5) 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 (3.22.4) 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 (3.20.5) $B' = 0$, 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 (3.22.13) 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

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow & & \downarrow \\ A/\mathfrak{p} & \xhookrightarrow{\tilde{\phi}} & B/\mathfrak{q} \end{array}$$

The induced map $\tilde{\phi}$ is integral (3.22.13). 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 (3.4.55). Then from the diagram we see $\phi^{-1}(\mathfrak{q}') = \mathfrak{p}'$ as required.

□

Proposition 3.22.15 (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 $\mathfrak{a} \lhd A$ 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 (3.22.8) 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 (3.18.77) 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 3.22.16 (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 (3.21.5) $\mathfrak{p}$ 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 (3.22.8) we have y is integral over $\mathfrak{p}$ whence by (3.22.15) 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. □

Proposition 3.22.17
Let B, C be commutative A-algebras such that B is integral over A. Then $C \otimes_A B$ is integral over C.

Proof. Let $\overline{C}$ be the subring of $C \otimes_A B$ of elements which are integral over C (3.22.7). Consider an elementary tensor $c \otimes b$ then by definition there is $P \in A[X]$ such that $P(b) = 0$. Then

$$P(c \otimes b) = \sum_{i=0}^{n} a_i (c \otimes b)^i = \sum_{i=0}^{n} c^i \otimes a_i b^i = c^i \otimes \sum_i a_i b^i = c^i \otimes P(b) = 0$$

This shows that $\overline{C}$ contains the elementary tensors and therefore is equal to $C \otimes_A B$. □

3.23 Valuation Rings and Places

Definition 3.23.1 (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 3.23.2 (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) $x \in A \setminus A^\star \iff x \in \mathfrak{m} \iff x^{-1} \notin A$

c) *A is integrally closed in K*

Proof. We prove each in turn

a) By (3.19.3) 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 $x^{-1} \notin A \iff x \in A \setminus A^\star \iff x \in \mathfrak{m}$.

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 (3.22.10) $x \in A[x^{-1}] \subseteq A$ as required.

□

Proposition 3.23.3 (Domination between Local Rings)
Let $A \subset B$ be local rings. Then the following are equivalent

a) $\mathfrak{m}_A \subset \mathfrak{m}_B$

b) $\mathfrak{m}_A = A \cap \mathfrak{m}_B$

c) $\mathfrak{m}_A B \subsetneq B$

*We say that B **dominates** A.*

Proof. *a)* $\iff$ *b)* Suppose $\mathfrak{m}_A \subset \mathfrak{m}_B$ then $\mathfrak{a} := A \cap \mathfrak{m}_B$ is an ideal which contains $\mathfrak{m}_A$. As $\mathfrak{m}_B$ is proper we have $1 \notin \mathfrak{a}$ whence it is proper. By maximality we conclude it is equal to $\mathfrak{m}_A$ as required. The converse is obvious.

a) $\implies$ *c)* Clearly $\mathfrak{m}_A B \subset \mathfrak{m}_B B = \mathfrak{m}_B \subsetneq B$

c) $\implies$ *a)* By (3.4.15) $\mathfrak{m}_A B \subset \mathfrak{m}_B$ and trivially $\mathfrak{m}_A \subset \mathfrak{m}_A B$. □

Definition 3.23.4 (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 3.23.5 (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 3.23.6
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 3.23.7 (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 3.23.8 (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 (3.23.7) we may assume without loss of generality that A is a local ring with unique maximal ideal $\mathfrak{m} = \ker(\phi)$. By (3.23.6) we may also suppose that $\mathfrak{m}A[x]$ is proper. Then it's contained in a maximal ideal $\mathfrak{B} \triangleleft A[x]$. 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

$$\begin{array}{ccccc} & & \overset{\phi}{\frown} & & \\ A & \twoheadrightarrow & k & \hookrightarrow & \Omega \\ \downarrow & & \downarrow & \nearrow & \\ A[x] & \twoheadrightarrow & K & & \end{array}$$

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 (3.18.72) 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 (3.23.7) may extend $\tilde{\phi}$ to $B_{\mathfrak{B}}$ and so by maximality $B = B_{\mathfrak{B}}$. Finally (3.19.5) 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 3.23.9
Let $A \subset K$ be a subring of a field and $\mathfrak{a} \triangleleft A$ 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 (3.4.36) there is a maximal ideal $\mathfrak{m}_A \triangleleft A$ 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 (3.23.8), such that $\mathfrak{m}_B \cap A = \ker(\phi) = \mathfrak{m}_A$. □

Proposition 3.23.10 (Alternative Characterisation of Valuation Rings)
Let K be a field and $A \subset K$ a subring. Then the following are equivalent

a) *A is a valuation ring for K*

b) *A is a local ring maximal under the relation "B dominates A"*

c) *$K = \mathrm{Frac}(A)$ and the principal ideals of A are totally ordered*

d) *$K = \mathrm{Frac}(A)$ and the ideals of A are totally ordered*

Proof. Let $(A, \mathfrak{m}_A) \preccurlyeq (B, \mathfrak{m}_B)$ denote the relation B dominates A.

a) $\implies$ *b)* Suppose that $(A, \mathfrak{m}_A) \preccurlyeq (B, \mathfrak{m}_B)$ with B local and A a valuation ring. We claim that $A = B$; suppose for a contradiction that $x \in B \setminus A$. Then $x^{-1} \in A \implies x^{-1} \in B \implies x \in B^\star$. Therefore $A \subset B \setminus B^\star = \mathfrak{m}_B$. In particular $1 \in \mathfrak{m}_B$ which is a contradiction as $\mathfrak{m}_B$ is proper.

b) $\implies$ *a)* Let $(A, \mathfrak{m}_A)$ be a maximal local ring. By (3.23.9) there exists a valuation ring $(B, \mathfrak{m}_B)$ such that $(A, \mathfrak{m}_A) \preccurlyeq (B, \mathfrak{m}_B)$. By maximality $A = B$ and A is a valuation ring.

a) $\implies$ *c)* Evidently $K = \mathrm{Frac}(A)$. Suppose $(a) \not\subset (b)$, then $a \notin (b) \implies b^{-1}a \notin A \implies a^{-1}b \in A \implies b \in (a) \implies (b) \subset (a)$.

c) $\implies$ *d)* Suppose $\mathfrak{a} \not\subset \mathfrak{b}$ then there exists $a \in \mathfrak{a} \setminus \mathfrak{b}$. In particular for all $b \in \mathfrak{b}$ we have $a \notin (b)$, whence by assumption $b \in (a)$. Therefore we conclude $\mathfrak{b} \subset (a) \subset \mathfrak{a}$.

d) $\implies$ *b)* As A is a non-zero ring it has a maximal ideal $\mathfrak{m}_A$, which by assumption must be the unique maximal ideal. So $(A, \mathfrak{m}_A)$ is a local ring. Suppose that $(A, \mathfrak{m}_A) \preccurlyeq (B, \mathfrak{m}_B)$ and given $x \in B$ we have by assumption $x = a_1 a_2^{-1}$ for some $a_1, a_2 \in A$. If $a_1 \in (a_2)$ then $x \in A$. Otherwise $a_2 \in (a_1)$ whence $x^{-1} \in A \implies x^{-1} \in B^\star \overset{(3.23.2)}{\implies} x^{-1} \notin \mathfrak{m}_B \overset{(3.23.3)}{\implies} x^{-1} \notin \mathfrak{m}_A \implies x^{-1} \in A^\star \implies x \in A$. Consequently $A = B$ and *b)* holds. □

Corollary 3.23.11
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 (3.22.10) 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 (3.23.9) there is a valuation ring $(V, \mathfrak{m}_V)$ such that $x^{-1} \in \mathfrak{m}_V$ which implies $x \notin V$ by (3.23.2). □

Definition 3.23.12 (Valuation)
*Let K be a field and Γ an abelian ordered group. A function $v : K^\star \to \Gamma$ is said to be a **valuation** if it satisfies the following properties*

a) $v(ab) = v(a) + v(b)$ *for all* $a, b \in K^\star$

b) $v(a+b) \geq \min(v(a), v(b))$ *with the convention that* $v(0) = \infty$

Note $v(1) = 0$. We say that two valuations v, v' are equivalent if there is an order-preserving isomorphism $\phi : v(K^\star) \to v'(K^\star)$ such that $\phi \circ v = v'$. Clearly this is an equivalence relation.

If $k \subset K$ and $v(k) = 0$ then we say v is a valuation for K/k.

Proposition 3.23.13 (Correspondence between Valuations Rings and Valuations)
Let K be a field with $k \subset K$. Then there is a bijection

$$\begin{array}{rcl} \{k \subset A \subset K \mid A \text{ is a valuation ring }\} & \longleftrightarrow & \{v : K^\star \to \Gamma \mid v \text{ is a valuation over } k\}/\sim \\ A & \to & v_A : K^\star \to K^\star/A^\star) \\ v^{-1}(\Gamma_{\geq 0}) & \leftarrow & v : K^\star \to \Gamma \end{array}$$

Under this map v_A is just the quotient map and $\bar{x} \leq \bar{y} \iff yx^{-1} \in A^\star$. Furthermore

a) $v_A(\overline{x}) \geq 0 \iff x \in A$.

b) $v_A(\overline{x}) = 0 \iff x \in A^\star$

c) $v_A(\overline{x}) > 0 \iff x \in \mathfrak{m}_A$

Proof. Given a valuation ring we may define the abelian group $\Gamma := K^\star/A^\star$ under multiplication with $\overline{x} \leq \overline{y} \iff yx^{-1} \in A$. This is easily verified to be a total ordering. Then $v_A : K^\star \to K^\star/A^\star$ is simply the quotient map and we clearly $v_A(\overline{x}) \geq 0 \iff x \in A^\star$. To demonstrate the additive condition we may consider the case $x, y \neq 0$ and suppose wlog that $xy^{-1} \in A$

$$v(x+y) = v((xy^{-1}+1)y) = v(xy^{-1}+1) + v(y) \geq v(y) \geq \min(v(x), v(y))$$

The case that one of $x, y = 0$ is trivial. Observe $A = v_A^{-1}(\Gamma_{\geq 0}) \cup \{0\}$. We may therefore construct a one-sided inverse; given a valuation $v : K' \to \Gamma$ we may define $A_v := v^{-1}(\Gamma_{\geq 0}) \cup \{0\}$. It's evident from the two properties of v that A is an additive and multiplicative subgroup. Further by total ordering we see that A is a valuation ring. We only need to demonstrate that the given constructions are mutually inverse, namely $v \sim v_{A_v}$. However this is immediate because the composite $v(K^\star) \to K^\star/{A_v}^\star \to v_{A_v}(K^\star)$ is an abelian group isomorphism, which preserves the positive segments, and therefore is an order isomorphism. □

Proposition 3.23.14 (Bezout Domain)
Let A be an integral domain. Then the following are equivalent

a) *Every finitely generated ideal is principal*

b) *Every ideal generated by two elements is principal*

*In this case we say A is a **Bezout Domain**. Further in this case every pair of elements has a greatest common divisor d which satisfies $d = ax + by$ for some $x, y \in A$.*

Proof. By assumption $(a, b) = (d)$. Immediately we have $d \mid a$ and $d \mid b$. Similarly $d = \lambda a + \mu b$. Suppose $a = xe$ and $b = ye$ then $d = (\lambda x + \mu y)e$ whence $e \mid d$. □

Lemma 3.23.15 (Valuation Ring = Local Bezout Domain)
Let A be an integral domain. Then the following are equivalent

a) *A is a valuation ring*

b) *A is a local Bezout domain.*

In particular A is a Noetherian valuation ring iff it is a local principal ideal domain.

Proof. Suppose A is a valuation ring and $\mathfrak{a} = (x, y)$. Without loss of generality $xy^{-1} \in A$ whence $x \in (y)$ so $\mathfrak{a} = (y)$ as required.

Conversely suppose A is a local Bezout domain and let $x = \frac{y}{z} \in K$. We may divide by the greatest common divisor so that $\lambda y + \mu z = 1$. We claim one of λy and μz is a unit, for suppose not then by (3.19.3) we have $\lambda y, \mu z \in \mathfrak{m} \implies 1 \in \mathfrak{m}$ a contradiction. Therefore one of y, z is a unit which implies $x \in A$ or $x^{-1} \in A$, and A is a valuation ring. □

3.24 Derivations

Definition 3.24.1 (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 3.24.2 (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 3.24.3 (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 3.24.4 (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 3.24.5
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 3.24.6 (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

$$\frac{\partial F}{\partial X_k} := \sum_{\substack{i \in \mathbb{N}^n \\ i_k \neq 0}} a_i i_k X_1^{i_1} \ldots X_k^{i_k - 1} \ldots X_n^{i_n} \tag{3.4}$$

We observe that

$$\frac{\partial X_l}{\partial X_k} = \delta_{lk}$$

Note this condition uniquely determines Equation (3.4)*, see (3.24.8).*

We show that these form a basis for $\mathrm{Der}_k(A)$.

Lemma 3.24.7 (Product Rule)
For $F, G \in A[X_1, \ldots, X_n]$ *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 $A[X_1, \ldots, X_n] \cong A[X_1, \ldots, \widehat{X_k}, \ldots, X_n][X_k]$ under which $\frac{\partial}{\partial X_k}$ corresponds to $\frac{\partial}{\partial X}$. □

Lemma 3.24.8 (Multivariate Chain Rule)
Let $D \in \mathrm{Der}_k(A, M)$ *be a derivation,* $x_1, \ldots, x_n \in A$ *and* $F \in A[X_1, \ldots, X_n]$*. Then*

$$D(F(x_1, \ldots, x_n)) = \sum_{k=1}^{n} \frac{\partial F}{\partial X_k}(x_1, \ldots, x_n) D(x_k)$$

As a special case we find

$$\begin{aligned} D(F(x)) &= F'(x) D(x) \\ D(x^n) &= n x^{n-1} D(x) \end{aligned}$$

Proof. First we observe that by induction on n

$$D(x_1 \ldots x_n) = \sum_{k=1}^{n} x_1 \ldots \widehat{x_k} \ldots x_n D(x_k)$$

and in particular

$$D(x^n) = \begin{cases} n x^{n-1} D(x) & n > 0 \\ 0 & n = 0 \end{cases}$$

Then for $F \in k[X_1, \ldots, X_n]$ we have

$$\begin{aligned} D(F(x_1, \ldots, x_n)) &= \sum_{i \in \mathbb{N}^n} a_i D(x_1^{i_1} \ldots x_n^{i_n}) \\ &= \sum_{i \in \mathbb{N}^n} a_i \sum_{k=1}^{n} x_1^{i_1} \ldots \widehat{x_k^{i_k}} \ldots x_n^{i_n} D(x_k^{i_k}) \\ &= \sum_{k=1}^{n} \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \ldots \widehat{x_k^{i_k}} \ldots x_n^{i_n} D(x_k^{i_k}) \\ &= \sum_{k=1}^{n} \sum_{\substack{i \in \mathbb{N}^n \\ i_k \neq 0}} i_k a_i x_1^{i_1} \ldots x_k^{i_k - 1} \ldots x_n^{i_n} D(x_k) \end{aligned}$$

which gives the required result.

□

Proposition 3.24.9 (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 (3.24.5) the following definition is clearly related to the existence of derivations.

Definition 3.24.10 (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 3.24.11
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 (3.4.65) as required. □

Lemma 3.24.12
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 (3.24.11). □

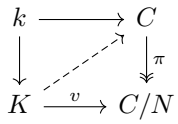
Lemma 3.24.13
The polynomial ring $k[X_1, \ldots, X_n]$ and function field $k(X_1, \ldots, X_n)$ is formally smooth.

Proof. The first follows by definition and the second by (3.24.12). □

Lemma 3.24.14
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 3.24.15 (Separable algebraic extensions are "formally unramified")
A separable algebraic extension K/k is formally uramified.

Proof. Consider the following commutative diagram



We suppose first that K is a finite extension. By (3.18.112) 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 $m'(x)$ is a unit we argue as follows. As α is separable, $m'(\alpha) \neq 0$, hence is a unit in K. As v is injective $v(m'(\alpha)) = m'(v(\alpha)) = m'(\pi(x)) = \pi(m'(x))$ is a unit in C/N. By (3.24.11) $m'(x) \in C^\star$. 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 3.24.16
A separably generated extension K/k is formally smooth.

Proof. This follows from (3.24.13), (3.24.15) and (3.24.14). □

3.25 Krull Dimension

Definition 3.25.1 (Krull Dimension)
Let A be a commutative ring. We say that a chain of distinct prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

*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 3.25.2
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 3.25.3
Let A be a ring then the lattice of radical ideals $\operatorname{Rad}(A)$ 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 3.25.4
This is easier to see in light of the dual isomorphism in (6.3.10), 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 3.25.5 (Simple properties)
The following properties of Krull dimension hold

a) $\dim A = \dim A/N(A)$

b) $\operatorname{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}}$

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*** $\operatorname{ht}(\mathfrak{p}) \geq \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) + \operatorname{ht}(\mathfrak{q})$

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 (3.4.55) there is an order-isomorphism between prime ideals of A containing $N(A)$ and prime ideals of $A/N(A)$. However by (3.4.46) 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 (3.4.55).

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 3.25.6 (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 (3.22.14). □

Corollary 3.25.7
Let $\phi : A \to B$ be integral and $\mathfrak{b} \lhd B$, then $\dim \phi^{-1}(\mathfrak{b}) = \dim(\mathfrak{b})$.

Lemma 3.25.8
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 (3.15.9). 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 3.25.9
Let A be a Noetherian ring and $\mathfrak{a}$ a proper ideal. Then there are only finitely many minimal primes containing $\mathfrak{a}$, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. 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 (3.25.3) applied to the radical ideal $\sqrt{a}$. □

Remark 3.25.10
This is essentially the proof of [Kap74, Theorem 87, 88].

We've noted in general (3.25.5) that the so-called codimension formula does not hold. However it holds in the following case, for essentially trivial reasons.

Proposition 3.25.11 (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 $\mathrm{ht}(\mathfrak{a}) = 1$.

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 3.25.12 (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*

$$\mathrm{ht}(\mathfrak{p}/\mathfrak{r}) = \mathrm{ht}(\mathfrak{p}/\mathfrak{q}) + \mathrm{ht}(\mathfrak{q}/\mathfrak{r})$$

When A is irreducible this is equivalent to the following condition

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q}) + \mathrm{ht}(\mathfrak{p}/\mathfrak{q})$$

Proof. This is restatement of (2.5.9). □

Proposition 3.25.13 (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*

$$\dim \mathfrak{q} = \dim \mathfrak{p} + \mathrm{ht}(\mathfrak{p}/\mathfrak{q}) \quad \forall \mathfrak{q} \subseteq \mathfrak{p}$$

d) *A satisfies c) whenever $\mathrm{ht}(\mathfrak{p}/\mathfrak{q}) = 1$ (i.e. $\mathfrak{q} \subsetneq \mathfrak{p}$ is saturated)*

Furthermore

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}/\mathfrak{q}) + \mathrm{ht}(\mathfrak{q})$$

Proof. This is a restatement of (2.5.11). □

Proposition 3.25.14 (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*

$$\dim \mathfrak{q} = \dim \mathfrak{p} + \mathrm{ht}(\mathfrak{p}/\mathfrak{q}) \quad \forall \mathfrak{q} \subseteq \mathfrak{p}$$

e) *A satisfies d) whenever $\mathrm{ht}(\mathfrak{p}/\mathfrak{q}) = 1$ (i.e. $\mathfrak{q} \subsetneq \mathfrak{p}$ is saturated)*

Proof. This is a restatement of (2.5.14). □

Proposition 3.25.15 (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

$$\begin{aligned} \dim A &= \dim \mathfrak{a} + \mathrm{ht}(\mathfrak{a}) \\ \mathrm{ht}(\mathfrak{a}) &= \mathrm{ht}(\mathfrak{a}/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}) \\ \dim \mathfrak{p} &= \dim \mathfrak{a} + \mathrm{ht}(\mathfrak{a}/\mathfrak{p}) \end{aligned}$$

Proof. This is a restatement of (2.5.13). □

3.25.1 Local Rings of Dimension 0

Lemma 3.25.16 (Dimension 0 local ring)
Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then the following are equivalent

a) $\dim A = 0$ *(i.e. every prime ideal is maximal)*

b) $\mathfrak{m}^n = 0$ *for some* n

c) $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ *for some* n

If A is an integral domain then this is equivalent to A being a field.

Proof. *a)* $\implies$ *b)* By (3.25.9) $\mathfrak{r} := \sqrt{(0)} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$ is a decomposition into minimal prime ideals. By assumption these are also maximal, and therefore by uniqueness $\sqrt{(0)} = \mathfrak{m}$ and the result follows from (3.4.48) as $\mathfrak{m}$ is finitely generated.

b) $\implies$ *a)* Let $\mathfrak{p}$ be a prime ideal then trivially $\mathfrak{m}^n \subset \mathfrak{p}$ so by (3.27.1) it is $\mathfrak{m}$-primary i.e. $\mathfrak{m}$ is a minimal prime of $\mathfrak{p}$ whence $\mathfrak{m} = \mathfrak{p}$.

b) $\iff$ *c)* One direction is obvious, and the converse follows from Nakayama's Lemma (3.20.5) because $\mathfrak{m}^n$ is finitely generated. □

3.26 Hauptidealsatz

The main result of this section is the following result due to Krull

Proposition 3.26.1 (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 $\mathfrak{a} := (x_1, \ldots, x_n)$. 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*

$$\operatorname{ht}(\mathfrak{p}) = \min\{n \mid \mathfrak{p} \text{ minimal over } (x_1, \ldots, x_n)\}$$

In particular if $\mathfrak{p}$ is minimal over $(x_1, \ldots, x_n)$ 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 3.26.2 (Hauptidealsatz Ring)
*We say a ring A is a **generalized hauptidealsatz** ring if for all $x_1, \ldots, x_n \in A$ and $\mathfrak{p}$ prime ideals minimal over $(x_1, \ldots, x_n)$ 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 3.26.3
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 3.26.4 (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 integral (which means it is hauptidealsatz by assumption because (0) is prime) and assume wlog that $n > 1$. Let $\mathfrak{p}$ be a minimal prime of $(x_1, \ldots, x_n)$ and $\mathfrak{q}$ a minimal prime of $(x_1, \ldots, x_{n-1})$. 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 (3.25.12) we see $\operatorname{ht}(\mathfrak{p}) \leq n$ as required.

For the general case, suppose $\mathfrak{p}$ is minimal over $(x_1, \ldots, x_n)$ and let $\mathfrak{r} \subseteq \mathfrak{p}$ be a minimal prime. Then the ring $A/\mathfrak{r}$ is integral and we see that $\operatorname{ht}(\mathfrak{p}/\mathfrak{r}) \leq n$ by the first part. Taking the supremum over all minimal primes $\mathfrak{r}$ shows that $\operatorname{ht}(\mathfrak{p}) \leq n$.

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 (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 by the previous Lemma. □

The catenary assumption may be relaxed by making a more complicated argument.

Proposition 3.26.5 (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 $(x_1, \dots, x_n)$. Suppose $\operatorname{ht}(\mathfrak{p}) > n$ then we may choose a saturated chain $\mathfrak{q} \subsetneq \mathfrak{p}$ such that $\operatorname{ht}(\mathfrak{q}) \geq n$. By minimality of $\mathfrak{p}$ we have $\mathfrak{q} \cap \{x_1, \dots, x_n\} = \{x_1, \dots, x_r\}$ 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 $(x_1, \dots, x_r)$ and there is a chain

$$(x_1, \dots, x_r) \subseteq \mathfrak{r} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$$

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 $\operatorname{ht}(\mathfrak{p}/\mathfrak{r}) \leq 1$. 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 3.26.6
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 3.26.7
Let $\mathfrak{q} \subseteq \mathfrak{p}$ be prime ideals then

$$\operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{p})$$

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 3.26.8
Suppose $\mathfrak{a} \subseteq \mathfrak{b}$. Then

$$\operatorname{ht}(\mathfrak{a}) \leq \operatorname{ht}(\mathfrak{b})$$

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 $\operatorname{ht}(\mathfrak{a}) \leq \operatorname{ht}(\mathfrak{p}')$. Furthermore by the previous Lemma $\operatorname{ht}(\mathfrak{p}') \leq \operatorname{ht}(\mathfrak{p})$, which yields the required result.

Suppose $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{a})$ then by definition $\operatorname{ht}(\mathfrak{a}) \leq \operatorname{ht}(\mathfrak{p}') \leq \operatorname{ht}(\mathfrak{p})$ and therefore we conclude $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}')$. 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 3.26.9
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

$$\operatorname{ht}(\mathfrak{a}) < \operatorname{ht}(\mathfrak{b})$$

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 (3.26.8) is a minimal prime of $\mathfrak{a}$. This must contain x which then contradicts the assumption. □

Proposition 3.26.10 (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 3.26.11
*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 (3.25.1) we may take the infimum over only minimal prime ideals. □

Proposition 3.26.12 (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 (3.26.7) $\operatorname{ht}(\mathfrak{p}_i) < \operatorname{ht}(\mathfrak{p}_{i+1})$ 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 (3.25.9) 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 (3.26.11). In particular $\mathfrak{p}_i \not\subseteq \mathfrak{q}_k$.

By prime avoidance (3.26.10) 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 (3.26.8) and (3.26.9) 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 (3.26.8) 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. □

3.27 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 3.27.1 ($\mathfrak{m}$-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. In this case we say $\mathfrak{a}$ is $\mathfrak{m}$-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 $\mathfrak{m} = \sqrt{\mathfrak{a}} \subseteq \mathfrak{p}$ by (3.4.46). In particular $\mathfrak{m}$ is a minimal prime.

b) $\implies$ *a)* Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{a}$. By (3.4.36) $\mathfrak{p} \subseteq \mathfrak{m}$ and by assumption $\mathfrak{p} = \mathfrak{m}$. The result then follows from (3.4.46).

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 $\mathfrak{m}^n \subset \mathfrak{a}$ is clearly sufficient, and necessary in the finitely generated case by (3.4.48). □

An ideal satisfying one of the equivalent conditions above is called **$\mathfrak{m}$-primary**, though some authors require the stronger condition.

Proposition 3.27.2 (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 (3.26.12) and the equivalent definitions of $\mathfrak{m}$-primary (3.27.1). 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 $\mathfrak{m}/\mathfrak{m}^2$ (3.20.7). □

Definition 3.27.3
Let $(A, \mathfrak{m})$ be a Noetherian local ring. We say A is ***regular*** *if*

$$\dim A = \mu(\mathfrak{m}) = \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$$

3.28 Discrete Valuation Rings

A Discrete Valuation Ring (DVR) corresponds to a regular local ring of dimension 1 and therefore regular (or in the case of perfect base field, smooth) points on a curve. There are a number of equivalent conditions which are summarised here (see also [AM69, Proposition 9.2]).

Lemma 3.28.1
Let $(A, \mathfrak{m})$ be a local domain such that $\mathfrak{m}$ is finitely generated and $\dim A = 1$. Then for every non-zero ideal $\mathfrak{a}$ there exists some n such that $\mathfrak{m}^n \subseteq \mathfrak{a}$.

Proof. As $\dim A = 1$ every minimal prime over $\mathfrak{a}$ is equal to $\mathfrak{m}$, whence $\sqrt{\mathfrak{a}} = \mathfrak{m}$ (i.e. $\mathfrak{a}$ is $\mathfrak{m}$-primary). As $\mathfrak{m}$ is finitely generated there is some n such that $\mathfrak{m}^n \subseteq \mathfrak{a}$. □

Proposition 3.28.2 (DVR Criteria)
Let A be an integral domain which is not a field. Then the following are equivalent.

a) *A is a valuation ring whose valuation group is order-isomorphic to $\mathbb{Z}$*

b) *A is a local principal ideal domain*

c) *A is a Noetherian local ring with maximal ideal $\mathfrak{m} = (\pi)$ and $\dim A = 1$*

d) *A is a local ring such that every ideal is of the form (π^k) for some $k \geq 0$ (and these are distinct)*

e) *A is a Noetherian valuation ring*

f) *A is a Noetherian integrally closed local domain with* $\dim A = 1$

g) *A is a Noetherian regular local ring with* $\dim A = 1$

In this case we say A is a ***discrete valuation ring*** *and let $K = \mathrm{Frac}(A)$. For every generator π of $\mathfrak{m}$, the ideals (π^n) are distinct and there is a valuation $v : K^\star \to \mathbb{Z}$ determined uniquely by the relation*

$$\begin{aligned}(x) &= (\pi^{v(x)}) \quad x \in A \\ (x^{-1}) &= (\pi^{-v(x)}) \quad x \notin A\end{aligned}$$

for which A is the valuation ring. Furthermore for every $x \in K^\star$ there exists a unit $u \in A^\star$ such that $x = u\pi^{v(x)}$.

Proof. *a)* $\implies$ *b)* Consider a valuation $v : K \to \mathbb{Z}$ with $v^{-1}(\mathbb{Z}_{\geq 0}) = A$. For any ideal $\mathfrak{a}$ choose $f \in \mathfrak{a}$ such that $v(f)$ is minimal. For $g \in \mathfrak{a}$ we have $v(g) \geq v(f) \implies v(gf^{-1}) \geq 0 \implies gf^{-1} \in A \implies g \in (f)$. Therefore $\mathfrak{a} = (f)$ is principal. Further by (3.23.2) A is a local ring.

b) $\implies$ *c)* By (3.25.5) $\dim A = 1$ and by assumption $\mathfrak{m} = (\pi)$. Evidently A is Noetherian.

c) $\implies$ *d)* By (3.25.16) the sequence (π^k) is strictly decreasing. Assume wlog that $\mathfrak{a}$ is proper and non-zero, then as $\dim A = 1$ every prime ideal is maximal and we find $\sqrt{\mathfrak{a}} = (\pi)$ by (3.4.46).

Suppose that $\mathfrak{a} \subseteq (\pi^k)$ for all k. Then $\pi \in \sqrt{\mathfrak{a}} \implies (\pi^k) = \mathfrak{a}$ for all sufficiently large k which contradicts the fact the sequence is strictly decreasing. Therefore we may assume $\mathfrak{a} \subseteq (\pi^k)$ for some k and there exists $a \in \mathfrak{a} \setminus (\pi^{k+1})$. Therefore $a = u\pi^k$ and by construction $u \notin (\pi) \implies u \in A^\star \implies \pi^k \in \mathfrak{a}$. Therefore $(\mathfrak{a}) = (\pi^k)$ as required.

d) $\implies$ *a)* Define $v(a)$ to be the unique integer such that $(a) = (\pi^{v(a)})$. We need to show that v is a valuation. By uniqueness we deduce $v(ab) = v(a)+v(b)$. Suppose that $a, b, a+b \in A\setminus\{0\}$. Then $(\pi^{v(a+b)}) = (a+b) \subseteq (\pi^{\min(v(a),v(b))})$. As the sequence (π^k) is strictly decreasing we find $v(a+b) \geq \min(v(a), v(b))$ as required. We may extend to $K^\star$ by $v(ab^{-1}) := v(a) - v(b)$. Then $v(ab^{-1}) \geq 0 \iff v(a) \geq v(b) \iff (a) \subseteq (b) \iff b \mid a \iff ab^{-1} \in A$. Further $v(a) = 0 \iff a \notin (\pi) \iff a \in A^\star$. Therefore A is the valuation ring associated to v.

d) $\implies$ *e)* $\implies$ *b)* This follows from (3.23.15).

e) $\implies$ *f)* A valuation ring is integrally closed (3.23.2) and we've already shown A is local with dimension 1.

f) $\implies$ *c)* Let $0 \neq a \in \mathfrak{m}$. As $\dim A = 1$ from (3.28.1) we know $\mathfrak{m}^n \subseteq (a)$ for some $n \geq 1$. Choose n minimal and $b \in \mathfrak{m}^{n-1} \setminus (a)$. Let $x = a^{-1}b \in K = \mathrm{Frac}(A)$. Evidentally $x \notin A$, for otherwise $b \in (a)$; further $x\mathfrak{m} = a^{-1}b\mathfrak{m} \subseteq a^{-1}\mathfrak{m}^n \subseteq a^{-1}(a) \subseteq A$ is an ideal of A.

We claim that $x\mathfrak{m} = A$. Suppose not then $x\mathfrak{m} \subseteq \mathfrak{m}$ by (3.4.36). Then $\mathfrak{m}$ is a faithful finite $A[x]$-module and x is integral over A (3.22.3). By asssumption A is integrally closed so $x \in A$ which is a contradiction. Therefore $x\mathfrak{m} = A \implies \mathfrak{m} = x^{-1}A$ (which in particular shows $x^{-1} \in A$).

c) $\implies$ *g)* By assumption A is a Noetherian local ring with $\dim A = 1$. So it remains to show that $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$. As $\mathfrak{m}$ is principal then $\dim \mathfrak{m}/\mathfrak{m}^2 \leq 1$. If it is zero then $\mathfrak{m} = \mathfrak{m}^2$ and $\dim A = 0$ by (3.25.16), a contradiction.

g) $\implies$ *c)* By assumption $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$ and so by (3.20.7) $\mathfrak{m} = (\pi)$ for some $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$.

The final statements have already been proven. □

Corollary 3.28.3
Let A be a principal ideal domain which is not a field. Then every localisation of A at a non-zero prime ideal is a DVR.

In particular $\mathbb{Z}_{(p)}$ and $k[X]_f$ are DVRs where p is prime and $f(X)$ is an irreducible polynomial.

3.29 Affine Algebras

Definition 3.29.1 (Affine Domain)
We call a finitely-generated k-algebra an ***affine algebra****. If in addition it's integral we call it an* ***affine domain****.*

3.29.1 Normalisation

References

- Commutative Algebra, Nicolas Bourbaki [Bou98a, Chap. V §3.1]
- Steps in Commutative Algebra, R. Sharp [Sha00]

The following normalisation results can be seen as a refinement of results on transcendence bases (Section 3.18.16).

Definition 3.29.2 (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 3.29.3 (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 3.29.4 (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 (3.18.57) 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 (3.18.137). □

The following is useful as it removes the necessity of showing algebraic independence in certain cases.

Corollary 3.29.5
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 (3.18.137). □

There are a few forms of the Normalisation Lemma which we prove, of progressively stronger form.

Lemma 3.29.6 (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 3.29.7
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 3.29.8 (Nagata Normalisation Lemma)
Let $A = k[x_1, \ldots, x_n]$ be a finitely-generated k-algebra such that k is infinite. Then there exists a ***normalising family*** *$y_1, \ldots, y_d \in A$ such that each y_i is a k-linear combination of $x_1, \ldots, x_n$. Further if $\mathfrak{a}_1 \lhd A$ is a proper ideal, then these may be chosen such that*

$$\mathfrak{a}_1 \cap k[y_1, \ldots, y_d] = (y_1, \ldots, y_h)k[y_1, \ldots, y_d]$$

for some $0 \leq h \leq d$, where $h = 0$ denotes the zero ideal.

Proposition 3.29.9 (Bourbaki Normalisation Lemma)
Let $A = k[x_1, \ldots, x_n]$ be a finitely-generated k-algebra such that k is infinite. Then there exists a ***normalising family*** *$y_1, \ldots, y_d \in A$ such that each y_i is a k-linear combination of $x_1, \ldots, x_n$.*

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

$$\mathfrak{a}_j \cap k[y_1, \ldots, y_d] = (y_1, \ldots, y_{h(j)})k[y_1, \ldots, y_d] \quad 1 \leq j \leq p\,.$$

for some non-decreasing sequence of integers $h(j)$, where $h(j) = 0$ denotes the zero ideal.

Remark 3.29.10 (Geometric Interpretation)
Note the normalisation here is equivalent to a commutative diagram

$$\begin{array}{ccc} k[Y_1, \ldots, Y_d] & \hookrightarrow & A \\ \uparrow & & \downarrow \\ k[Y_{h(1)+1}, \ldots, Y_d] & \hookrightarrow & A/\mathfrak{a}_1 \\ \uparrow & & \downarrow \\ \vdots & & \vdots \\ \uparrow & & \downarrow \\ k[Y_{h(p)+1}, \ldots, Y_d] & \hookrightarrow & A/\mathfrak{a}_p \end{array}$$

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 $\phi^{-1}(\mathfrak{a}_i) = (Y_1, \ldots, Y_{h(i)})$

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 (3.29.6). 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

$$F' := F(X_1 + \lambda_1 X_n, \ldots, X_{n-1} + \lambda_{n-1} X_n, X_n)$$

Furthermore in terms of homogenous polynomials

$$F'_m = F_m(X_1 + \lambda_1 T, \ldots, X_{n-1} + \lambda_{n-1} X_n, X_n)$$

and the coefficient of X_n^m in F' is simply $F'_m(0, \ldots, 0, 1) = F_m(\lambda_1, \ldots, \lambda_{n-1}, 1) \in k$. 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 $F'(x_1, \ldots, x_{n-1}, X_n) = 0$, with the leading coefficient in X_n constant.

Let $B := k[x_1, \ldots x_{n-1}, F]$. Then clearly $B[X_n] = A$ and X_n is integral over B. Therefore by (3.22.4) A is a finite B-module. As $\operatorname{trdeg}(A/k) = n$ by (3.29.5) $\{x_1, \ldots, x_{n-1}, F\}$ is a normalising family, and B is isomorphic to a polynomial ring.

As B is a polynomial ring it is integrally closed (3.22.9). Then the final statement is a consequence of the following lemma (3.29.11) (essentially to prove that $V(F) \to \mathbb{A}^{n-1}$ is surjective). □

Lemma 3.29.11
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 $K = \operatorname{Frac}(A)$ and $L = \operatorname{Frac}(B)$, 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 3.29.12
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 3.29.13
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 (3.29.8), (3.29.9). 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 (3.29.8) 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 (3.29.6) 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 (3.14.4).

Otherwise $B' := k[t_2, \ldots, t_n]$ is a polynomial ring and $\mathfrak{a}'_1 := \mathfrak{a}_1 \cap B'$ is proper by (3.29.12). 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 (3.22.4), and A is integral over C (3.22.5), so by (3.29.5) $x_1, \ldots, x_n$ 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 (3.29.13) applied to the ring C'. Then (3.29.13) applied to the ring C demonstrates the claim. □

Proof of (3.29.9) 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 (3.22.7). Then A is integral over C by (3.22.5), and this is a normalising family by (3.29.5), and in particular algebraically independent.

For $j \leq p-1$ and $h := h(j) \leq r$, apply (3.29.13) 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 (3.29.13) that $\mathfrak{a}_j \cap C = (t_1, \ldots, t_h)C$ as required.

Similarly by (3.29.13) $\mathfrak{a}_p \cap k[x_{s+1}, \ldots, x_n] = \{0\}$ and clearly $t_1, \ldots, t_r, x_{r+1}, \ldots, x_s \in \mathfrak{a}_p$. Then by (3.29.13) again $\mathfrak{a}_p \cap C = (t_1, \ldots, t_r, x_{r+1}, \ldots, x_s)C$ as required . □

Remark 3.29.14
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. Here we use a simplified argument from [Sha00].

3.29.2 Nullstellensatz

Definition 3.29.15 (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 3.29.16 (Zeros are homomorphisms)
Let $\mathfrak{a} \triangleleft k[X_1, \ldots, X_n]$ be an ideal then there is a bijection

$$\begin{array}{rcl} \mathrm{AlgHom}_k(k[X_1, \ldots, X_n]/\mathfrak{a}, K) & \longleftrightarrow & \{ \text{ zeros of } \mathfrak{a} \text{ in } K^n \} \\ \phi & \longrightarrow & (\phi(\bar{X}_1), \ldots, \phi(\bar{X}_n)) \end{array}$$

The following notion is useful in future

Definition 3.29.17 (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 3.29.18 (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 (3.10.3). Any subring of a field is an integral domain, which means $\mathfrak{p}_x$ is prime by (3.4.58).

By (3.18.56) 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 (3.4.58).

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 (3.18.72). 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 3.29.2.1. □

The final part is what is usually known as the **Weak Nullstellensatz**. It can be rephrased in multiple forms

Proposition 3.29.19 (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* $\mathfrak{m} \lhd k[X_1, \ldots, X_n]$ *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 (3.18.56).

c) $\implies$ *a)* By (3.18.72) there is an embedding $K \to \bar{k}$. Therefore by (3.29.16) every maximal ideal has a root.

c) $\implies$ *d)* Every finitely generated k-algebra A is of the form $k[X_1, \ldots, X_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$. If A is a field then $\mathfrak{a}$ is maximal by (3.4.58) and so by assumption A/k is a finitely-generated algebraic field extension and therefore finite by (3.18.56).

d) $\implies$ *c)*. This is clear.

Finally even if k is finite, it's always the case that $\bar{k}$ is infinite, so we can reduce to the case k is infinite by considering $\mathfrak{a}\bar{k}[X_1, \ldots, X_n]$ in a). □

When $K = \bar{k}$ is an algebraic closure we may use these results to make the connection more precise

Proposition 3.29.20 (Weak Nullstellensatz II)
There is a bijective map

$$\begin{array}{rcl} \bar{k}^n / \operatorname{Aut}(\bar{k}/k) & \longrightarrow & \{\mathfrak{m} \lhd k[X_1, \ldots, X_n] \text{ maximal } \} \\ x & \longrightarrow & \mathfrak{m}_x \end{array}$$

When $x \in k^n$ *then*

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

Proof. The map is surjective by (3.29.19). It's well-defined because $\mathfrak{m}_{\sigma(x)} = \mathfrak{m}_x$.

By (3.29.18) we have an isomorphism $k[X_1, \ldots, X_n]/\mathfrak{m}_x \xrightarrow{\sim} k[x_1, \ldots, x_n] \subset \bar{k}$. If $\mathfrak{m}_x = \mathfrak{m}_y$ then these compose to yield an isomorphism $\sigma : k[x_1, \ldots, x_n] \xrightarrow{\sim} k[y_1, \ldots, y_n] \subset \bar{k}$ such that $\sigma(x_i) = y_i$. By (3.18.80) this extends to $\sigma \in \operatorname{Aut}(\bar{k}/k)$. Therefore the given mapping is injective. □

3.29.2.1 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 $A := k[X_1, \ldots, X_n]/\mathfrak{a}$ is integral over $B := k[z_1, \ldots, z_d]$ where $z_1, \ldots, z_d$ are algebraically independent.

If $\mathfrak{a}$ is maximal then A is a field and by (3.22.11) 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 (3.22.14) 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 (3.29.16) 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 $k(x) = k(x_1, \dots, x_n) := \mathrm{Frac}(A)$.

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 (3.23.8). 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 (3.29.16) as required. □

3.29.3 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 (3.29.28). Further there's a geometric proof of the "Hauptidealsatz" (3.29.25). We first show that it is equal to transcendence degree in the integral case.

Proposition 3.29.21
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 $\dim A = \mathrm{trdeg}(\mathrm{Frac}(A)/k)$, 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 (3.25.6).

$\dim A \geq n$). 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 (3.29.9) 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 (3.25.8). By (3.29.6) 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 (3.29.8) and (3.29.4)

□

Corollary 3.29.22
Let A be a finitely-generated k-algebra. Then $\dim A[T] = \dim A + 1$.

Proof. By (3.29.8) there is an injective integral ring homomorphism

$$\phi : k[X_1, \ldots, X_n] \hookrightarrow A$$

where $\dim A = n$. By (3.8.5) there is a ring homomorphism

$$k[X_1, \ldots, X_n][T] \hookrightarrow A[T]$$

which is injective. Further by assumption $A = k[y_1, \ldots, y_r]$ so $A[T] = k[y_1, \ldots, y_r, T]$ and by (3.22.4) the ring homomorphism is integral. This shows that $\phi(x_1), \ldots, \phi(x_n), T$ is a normalising family and the result follows from (3.29.21). □

Corollary 3.29.23
The ideal $(X_1, \ldots, X_r) \triangleleft k[X_1, \ldots, X_n]$ *has dimension* $n - r$.

Corollary 3.29.24
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 3.29.25 (Hypersurface has pure codimension 1)
Let A *be an affine domain of dimension* n *and* $0 \neq f \in A$*. Then*

$$\dim((f)) = n - 1$$
$$\mathrm{ht}((f)) = 1$$

More precisely if $\mathfrak{p}$ *is minimal over* (f) *then it has dimension* $n - 1$ *and height* 1.

Proof. Consider the case $A = k[X_1, \ldots, X_n]$. Suppose first that f is prime, then $\mathfrak{p} = (f)$ and by (3.29.6) there is an integral injective map

$$k[Y_1, \ldots, Y_{n-1}] \hookrightarrow A/(f)$$

Therefore

$$\dim((f)) = \dim(A/(f)) \overset{(3.25.6)}{=} \dim(k[Y_1, \ldots, Y_{n-1}]) \overset{(3.29.21)}{=} n - 1$$

When f is not prime then, as $k[X_1, \ldots, X_n]$ 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 (3.4.46).

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 (3.29.8) 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 (3.25.7). 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 (3.25.11) we have $\mathrm{ht}((f)) = 1$. □

Remark 3.29.26
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 (3.25.11)

Corollary 3.29.27 (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 (3.29.25). Alternatively by (3.29.8) 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 $\mathrm{ht}(\mathfrak{q}) = 1$. By (3.25.8) $\mathfrak{q}$ is principal and by (3.29.6) 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 (3.25.7) 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 $\mathrm{ht}(\mathfrak{p}_2/\mathfrak{p}_1) = 1$. Therefore

$$\dim(\mathfrak{p}_2) = \dim(\mathfrak{p}_2/\mathfrak{p}_1) = \dim(A/\mathfrak{p}_1) - 1 = \dim(\mathfrak{p}_1) - 1$$

□

Corollary 3.29.28 (Biequidimensionality)
*Let A be an affine algebra. Then it is **quasi-biequidimensional** and satisfies the **codimension formulae** for $\mathfrak{p} \subset \mathfrak{a}$*

$$\begin{aligned} \dim A &= \dim \mathfrak{a} + \mathrm{ht}(\mathfrak{a}) \\ \dim \mathfrak{a} &= \dim \mathfrak{p} + \mathrm{ht}(\mathfrak{a}/\mathfrak{p}) \\ \mathrm{ht}(\mathfrak{a}) &= \mathrm{ht}(\mathfrak{a}/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}) \end{aligned}$$

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 (3.29.27) A satisfies the criteria in (3.25.13).e) and so is quasi-biequidimensional. The codimension formulas follow from (3.25.15). □

We may also consider the following result

Proposition 3.29.29 (Generalized Hauptidealsatz for Affine Algebras)
Let A be an affine algebra and $\mathfrak{p}$ a prime ideal. Then

a) *If $\mathrm{ht}(\mathfrak{p}) = n$ then it is minimal over some ideal $\mathfrak{a} := (x_1, \dots, x_n)$. Furthermore $\mathfrak{a}$ may be chosen such that $\mathrm{ht}(\mathfrak{a}) = n$ and every minimal prime is of height n*

b) *We have the following characterization of height of a prime ideal*

$$\mathrm{ht}(\mathfrak{p}) = \min\{n \mid \mathfrak{p} \text{ minimal over } (x_1, \dots, x_n)\}$$

In particular if $\mathfrak{p}$ is minimal over $(x_1, \dots, x_n)$ then $\mathrm{ht}(\mathfrak{p}) \leq n$.

Furthermore the same result holds for localization of A at any prime ideal.

Proof. This is largely restatement of results in Section 3.26. By (3.29.25) we have $A/\mathfrak{p}$ is hauptidealsatz for every prime ideal $\mathfrak{p}$. Furthermore by (3.29.28) A is quasi-biequidimensional and so catenary (3.25.13). Then by (3.26.4) this means A is a generalized hauptidealsatz ring (and so is every localization $A_{\mathfrak{p}}$).

Then *a*) and *b*) follows from (3.26.12). □

Corollary 3.29.30
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

$$\dim A_{\mathfrak{p}} = \min\{n \mid \sqrt{(x_1, \dots, x_n)} = \mathfrak{m}\} \leq \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$$

with equality iff $A_{\mathfrak{p}}$ is a regular local ring.

Proof. By (3.29.29) $A_{\mathfrak{p}}$ is a Noetherian local ring satisfying the generalized hauptidealsatz. Therefore the result follows by (3.27.2). □

3.29.3.1 ** Biequidimensionality by Strong Normalisation **

We may prove more directly the biequidimensionality property by using the strong form of the Normalisation Lemma (3.29.9) and Going Down (3.22.16). First we prove a technical result

Lemma 3.29.31 (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 (3.22.14). The second follows by applying Going Down (3.22.16) 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 3.29.32
*Let A be an affine domain, then every maximal chain has order $n = \dim A$, i.e. A is **irreducible** and **biequidimensional**.*

Proof of (3.29.32). 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 (3.29.9) 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 (3.29.21). Clearly $h(0) = 0$ and by (3.22.13) $\mathfrak{q}_m$ 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 (3.22.9). Therefore we may apply (3.29.31) 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 $m = n$. □

3.29.4 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 3.29.33 (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 (3.24.8) 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 3.29.34 (Derivations = Tangent Vectors)
Let $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ be a f.g. k-algebra and M an A-module. Then we have an A-module isomorphism

$$\begin{array}{rcl} \mathrm{Der}_k(A,M) & \cong & \left\{v \in M^n \mid \sum_{i=1}^n \overline{\frac{\partial F}{\partial X_i}} v_i = 0 \quad \forall F \in \mathfrak{a}\right\} \subset M^n \\ D & \longrightarrow & (D(\overline{X}_1), \ldots, D(\overline{X}_n)) \\ \sum_{i=1}^n \overline{\frac{\partial}{\partial X_i}} \cdot v_i & \longleftarrow & v \end{array}$$

If $\mathfrak{a} = \langle F_1, \ldots, F_m \rangle$ 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 (3.24.8) we have the following relationship for all $F \in k[X_1, \ldots, X_n]$

$$D(\overline{F}) = D(F(\overline{X}_1, \ldots, \overline{X}_n)) = \sum_{i=1}^n \frac{\partial F}{\partial X_i}(\overline{X}_i) D(\overline{X}_i) = \sum_{i=1}^n \overline{\frac{\partial F}{\partial X_i}} D(\overline{X}_i)$$

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

$$\sum_{i=1}^n \frac{\partial}{\partial X_i} \cdot v_i$$

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 $H_j \in k[X_1, \ldots, X_n]$. 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 3.29.35 (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 (3.24.5) 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 (3.24.15) there is a unique homomorphism $\phi_{\hat{D}} : L \to L[V]$ completing the diagram, and in particular by (3.24.5) there is a derivation $\widetilde{D} : L \to V$ extending D. Uniqueness follows from that of $\phi_{\hat{D}}$. □

Corollary 3.29.36
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 (3.24.1) 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 (3.29.35). □

Proposition 3.29.37
*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

$$\mathrm{Der}_k(K) \overset{(3.29.35)}{\cong} \mathrm{Der}_k(k(\eta_1, \ldots, \eta_n), K) \overset{(3.24.9)}{\cong} \mathrm{Der}_k(k[\eta_1, \ldots, \eta_n], K)$$

which then has dimension n by (3.29.33). □

Lemma 3.29.38
Let A be a k-algebra and $\mathfrak{m}$ an ideal. Then $\mathfrak{m}/\mathfrak{m}^2$ is a $k(\mathfrak{m})$-module with action given by

$$(a + \mathfrak{m}) \cdot (b + \mathfrak{m}^2) = (ab + \mathfrak{m}^2)$$

for all $a \in A$ and $b \in \mathfrak{m}$.

Proof. Suppose $a - a' \in \mathfrak{m}$ and $b - b' \in \mathfrak{m}^2$ then

$$ab - a'b' = (a - a')(b - b') + a'(b - b') + b'(a - a') \in \mathfrak{m}^2$$

this shows that the action is well-defined. The properties of a module are straightforward. □

Lemma 3.29.39
Let A be a k-algebra and $\mathfrak{m}$ an ideal. Then there is an isomorphism of A-algebras

$$\begin{array}{ccc} A & \longrightarrow & A/\mathfrak{m}^2 \\ \downarrow \pi_1 & \searrow^{\pi_2} & \downarrow \\ k(\mathfrak{m}) & \overset{\psi}{\dashrightarrow}_{\sim} & k(\mathfrak{m}/\mathfrak{m}^2) \end{array}$$

Further there is an isomorphism of A-modules

$$\begin{array}{rcl} \mathrm{Der}_k(A/\mathfrak{m}^2, k(\mathfrak{m}/\mathfrak{m}^2)) & \to & \mathrm{Der}_k(A, k(\mathfrak{m})) \\ D & \to & x \to \psi^{-1}(D(\overline{x})) \end{array}$$

Proof. The first statement follows from (3.4.57) with $\mathfrak{a} = \mathfrak{m}^2$ and $\mathfrak{b} = \mathfrak{m}$.

Define $\widehat{D}(x) := \psi^{-1}(D(\overline{x}))$. By hypothesis $D(\overline{xy}) = \pi_2(x)D(\overline{y}) + \pi_2(y)D(\overline{x})$. Therefore

$$\widehat{D}(xy) = \pi_1(x)\psi^{-1}(D(\overline{y})) + \pi_1(y)\psi^{-1}(D(\overline{x})) = \pi_1(x)\widehat{D}(\overline{y}) + \pi_1(y)\widehat{D}(\overline{x})$$

and so $\widehat{D}$ is a well-defined derivation. Suppose $\widehat{D} \in \mathrm{Der}_k(A, k(\mathfrak{m}))$ then by the product rule $\mathfrak{m}^2 \subset \ker(\widehat{D})$ so there is a derivation $D' : A/\mathfrak{m}^2 \to k(\mathfrak{m})$ such that $D'(\overline{x}) = \widehat{D}(x)$. Define $D := \psi \circ D'$, then evidentally the image of this derivation is $\widehat{D}$ and so the map is surjective.

Suppose $\widehat{D} = 0$ then as ψ is an isomorphism $D \circ \bar{\cdot} = 0$. As the reduction map is surjective we deduce that $D = 0$. Therefore the map is injective, bijective and an isomorphism. □

Lemma 3.29.40
Let A be a k-algebra and $\mathfrak{m}$ an ideal. Then there is an isomorphism of A-modules

$$\begin{array}{rcl} \mathrm{Hom}_{k(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2, k(\mathfrak{m})) & \to & \mathrm{Hom}_{k(\mathfrak{m}/\mathfrak{m}^2)}((\mathfrak{m}/\mathfrak{m}^2)/(\mathfrak{m}^2/\mathfrak{m}^2), k(\mathfrak{m}/\mathfrak{m}^2)) \\ \theta & \to & \psi \circ \theta \circ i^{-1} \end{array}$$

where $i : \mathfrak{m}/\mathfrak{m}^2 \to (\mathfrak{m}/\mathfrak{m}^2)/(\mathfrak{m}^2/\mathfrak{m}^2)$ is a ring isomorphism such that

$$i(\pi_1(a) \cdot x) = \pi_2(a) \cdot i(x)$$

Proof. Then for $x \in (\mathfrak{m}/\mathfrak{m}^2)/(\mathfrak{m}^2/\mathfrak{m}^2)$, $a \in A$ and $\theta \in \mathrm{Hom}_{k(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2, k(\mathfrak{m}))$

$$\begin{array}{rcl} (\psi \circ \theta \circ i^{-1})(\pi_2(a) \cdot x) & = & (\psi \circ \theta)(\pi_1(a) \cdot i^{-1}(x)) \\ & = & \psi\left(\pi_1(a)\theta(i^{-1}(x))\right) \\ & = & \pi_2(a)(\psi \circ \theta \circ i^{-1})(x) \end{array}$$

so that the map is well-defined. Similarly if $\theta' \in \mathrm{Hom}_{k(\mathfrak{m}/\mathfrak{m}^2)}((\mathfrak{m}/\mathfrak{m}^2)/(\mathfrak{m}^2/\mathfrak{m}^2), k(\mathfrak{m}/\mathfrak{m}^2))$

$$\begin{array}{rcl} (\psi^{-1} \circ \theta' \circ i)(\pi_1(a) \cdot x) & = & (\psi^{-1} \circ \theta')(\pi_2(a) \cdot i(x)) \\ & = & \psi^{-1}(\pi_2(a)\theta'(i(x))) \\ & = & \pi_1(a)(\psi^{-1} \circ \theta' \circ i)(x) \end{array}$$

so the inverse map is well-defined. □

Proposition 3.29.41 (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 (3.29.19)).*

Proof. The map θ_D is well-defined because D annihilates $\mathfrak{m}^2$ by the product rule. It remains to show the map is bijective when $k(\mathfrak{m})/k$ is separable algebraic.

We first 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 of A-module homomorphisms

$$\begin{array}{ccc} \mathrm{Der}_k(A', k(\mathfrak{m}')) & \longrightarrow & \mathrm{Hom}_{k(\mathfrak{m}')}(\mathfrak{m}'/\mathfrak{m}'^2, k(\mathfrak{m}')) \\ \wr\downarrow & & \wr\downarrow \\ \mathrm{Der}_k(A, k(\mathfrak{m})) & \longrightarrow & \mathrm{Hom}_{k(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2, k(\mathfrak{m})) \end{array}$$

The horizontal maps have already been defined and the vertical maps are defined in (3.29.39) and (3.29.40). The diagram evidentally commutes, so therefore it is sufficient to show that the top map is an isomorphism.

We revert to the original notation, but with the additional assumption that $\mathfrak{m}^2 = 0$. By (3.24.16) 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. 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

$$\begin{aligned} D_\theta((\lambda + x)(\lambda' + x')) &= \theta(\lambda' x + \lambda x') \\ &= \pi(\lambda')\theta(x) + \pi(\lambda)\theta(x') \\ &= \pi(\lambda' + x')\theta(x) + \pi(\lambda + x)\theta(x') \\ (\lambda' + x') \cdot D_\theta(\lambda + x) + (\lambda + x) \cdot D_\theta(\lambda' + x') & \end{aligned}$$

Therefore the given map is surjective.

As $k(\mathfrak{m})/k$ is separable then by (3.29.36) 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 3.29.42
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.

3.29.5 Linearly Disjoint Algebras

Definition 3.29.43
*Let A/k, B/k be k-algebras and homomorphisms $i : A/k \to \Omega/k$, $j : B/k \to \Omega/k$ (typically being inclusion). Then we say that A and B are **linearly disjoint in** Ω if the canonical map*

$$\begin{aligned} A \otimes_k B &\to \Omega \\ a \otimes b &\to i(a)j(b) \end{aligned}$$

is injective. As the canonical maps $A, B \to A \otimes_k B$ are injective by (3.5.40) this implies i, j must be injective. In the case that Ω is integral (resp. reduced) then A, B are also necessarily integral (resp. reduced).

Recall that every k-module is free (3.4.137), 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 3.29.44
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 3.29.45
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 3.29.46
Let $i : A/k \to \Omega/k$ and $j : B/k \to \Omega/k$ be algebra homomorphisms. Then the following are equivalent

a) A/k and B/k are linearly disjoint in Ω/k

b) If $S \subset A$ is linearly independent over k then $i(S)$ is linearly independent over B

b') If $T \subset B$ is linearly independent over k then $j(T)$ is linearly independent over A

c) There is a k-basis $\{a_\lambda\}_{\lambda \in \Lambda}$ of A for which $\{i(a_\lambda)\}_{\lambda \in \Lambda}$ is linearly independent over B

c') There is a k-basis $\{b_\lambda\}_{\lambda \in \Lambda}$ of B for which $\{j(b_\lambda)\}_{\lambda \in \Lambda}$ is linearly independent over A

Proof. *a)* $\implies$ *b)* By (3.5.29) and (3.5.30) 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 (3.4.137) 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 $(b_\lambda)_{\lambda\in\Lambda} \to \sum i(a_\lambda)j(b_\lambda)$. The hypothesis means precisely that this map is injective.

We immediately have the symmetric result *a)* $\iff$ *b′)* $\iff$ *c′)*. □

In cases where both algebras are fields and one is algebraic then linear disjointness can be characterized by a property of the tensor product. In particular it does not depend on the *ambient* algebra Ω/k.

Proposition 3.29.47
Let K/k be a field extension and k'/k an algebraic *field extension. Then the following are equivalent*

a) *K and k' are linearly disjoint with respect to every embedding into an algebra Ω/k*

b) *K and k' are linearly disjoint with respect to some common field extension Ω/k*

c) *$K \otimes_k k'$ is an integral domain*

d) *$K \otimes_k k'$ is a field*

Proof. *a)* $\implies$ *b)* We may take $\Omega := (K \otimes_k k')/\mathfrak{m}$.

b) $\implies$ *c)* As Ω is assumed to be a field it is certainly integral, and therefore so is $K \otimes_k k'$ being a subring.

c) $\implies$ *d)* As every element of the tensor product is a finite linear combination of elementary tensors we may reduce to the case k' is finitely generated. Then by (3.18.56) k' is finite over k and therefore by (3.5.22) $K \otimes_k k'$ is finite over K. By assumption multiplication by an element x is injective and K-linear. Therefore by (3.4.148) it is surjective and x has an inverse as required.

d) $\implies$ *a)* This is immediate because the kernel is an ideal which must be (0). □

3.30 Jacobson Rings

Definition 3.30.1 (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 (3.4.46) and (3.4.59)

$$\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}}^J$$

Proposition 3.30.2 (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 (3.4.46)

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

as required □

We prove the Weak Nullstellensatz implies the following result

Proposition 3.30.3 (Strong Nullstellensatz)
Let A be a finitely-generated k-algebra. Then it is a Jacobson ring.

Proof. □

3.31 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 [Sta15] but large parts of exposition are from [Bou89].

Definition 3.31.1 (Geometrically Reduced / Integral Algebra)
A k-algebra A is

- ***geometrically integral*** *(resp.* ***irreducible***, ***reduced****) if the ring $A \otimes_k L$ is* ***integral*** *(resp.* ***irreducible***, ***reduced****) for every field extension L/k.*
- ***algebraically integral*** *(resp.* ***irreducible***, ***reduced****) if the ring $A \otimes_k \bar{k}$ is* ***integral*** *(resp.* ***irreducible***, ***reduced****).*

A few remarks about the important results and notation in the literature

- *As in (3.4.63) we see that* ***integral*** $\iff$ ***irreducible*** *and* ***reduced****.*
- *These are shown to be equivalent (3.31.23), (3.31.33) and (3.31.39). In fact it is sufficient to check the properties for all finite extensions.*
- *[Liu06] uses the "algebraic" form*
- *[Bou89] uses the term "separable" for "geometrically reduced", as this coincides with the notion of separable for algebraic extensions (3.31.17)*
- *Similarly [Bou89] and [Lan11] use the term "regular" for geometrically integral*

We make implicit use of the following results throughout

Proposition 3.31.2
Let A, B be k-algebras, then the structural morphisms $A \to A \otimes_k B$ and $B \to A \otimes_k B$ are injective. Furthermore if A' and B' are k-subalgebras then the canonical homomorphism

$$A' \otimes_k B' \to A \otimes_k B$$

is injective.

Proof. This is (3.5.29) and (3.5.40) □

Proposition 3.31.3
Let A, B be k-algebras. Let $\{a_i\}_{i \in I}$ be a k-linearly independent subset (resp. basis) of A and $\{b_j\}_{j \in I}$ be a k-linearly independent subset (resp. basis) of B. Then $\{a_i \otimes b_j\}_{(i,j) \in I \times J}$ is a k-linearly independent subset (resp. basis) of $A \otimes_k B$.

Furthermore $\{a_i \otimes 1\}_{i \in I}$ is a B-linearly independent subset (resp. basis) of $A \otimes_k B$.

Proof. The first statement is (3.5.30). For the last statement extend $\{a_i\}_{i \in I}$ to a basis (2.3.7) and apply (3.5.25). □

Proposition 3.31.4
Let A, B be k-algebras. Then $A \otimes_k B$ is the union of subrings of the form a) $A \otimes_k B'$, b) $A' \otimes_k B$ or c) $A' \otimes_k B'$ where A' and B' are finitely-generated k-subalgebras of A and B respectively.

If K/k is an algebraic field extension then $A \otimes_k K$ is the union of subrings of the form $A \otimes_k k'$ where k'/k are finite subextensions.

Proof. An arbitrary element $z \in A \otimes_k B$ is a finite sum of elementary tensors. Therefore the result follows from (3.31.2).

The final statement follows from recalling finitely generated algebraic extensions are finite (3.18.56). □

3.31.1 Etale Algebras

Definition 3.31.5
*Let A be a finite-dimensional k-algebra. Then define the **separable degree** as follows*

$$[A : k]_s := \#\,\mathrm{AlgHom}_k(A, \bar{k})$$

*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 (3.18.89).*

Lemma 3.31.6
Let A be a finite-dimensional k-algebra and K/k a field extension. Then

$$[\mathrm{Hom}_k(A, K) : K] = [A^\vee : k] = [A : k]$$

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 $\mathrm{Hom}_k(A, K)$.

Proof. This is simply a special case of (3.5.26). □

Lemma 3.31.7 (Dedekind's Lemma)
Let K/k be a field extension and A a k-algebra. The set of k-algebra homomorphisms

$$\mathrm{AlgHom}_k(A, K)$$

is K-linearly independent as a subset of $\mathrm{Hom}_k(A, K)$.

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 3.31.8 (Separable degree is finite)
Let A be a finite-dimensional k-algebra then $\#\,\mathrm{AlgHom}_k(A, K) \leq [A : k]$ for every field extension K/k.

Proposition 3.31.9 (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

$$\mathrm{AlgHom}_k(A, K) = \mathrm{AlgHom}_k(A, \Omega)$$

If Ω contains $\bar{k}$ then these are both equal to $\mathrm{AlgHom}_k(A, \bar{k})$.

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 (3.18.56).

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

$$\mathrm{AlgHom}_k(A, K) \subseteq \mathrm{AlgHom}_k(A, \bar{k}) \subseteq \mathrm{AlgHom}_k(A, \Omega)$$

whence they are all equal. □

Proposition 3.31.10 (Etale-ness is preserved under base extension)
Let A be a finite-dimensional k-algebra and K/k a field extension then

$$\begin{aligned} [A \otimes_k K : K] &= [A : k] \\ [A \otimes_k K : K]_s &= [A : k]_s \end{aligned}$$

In particular A is etale if and only if $A \otimes_k K$ is.

Proof. The first equality follows from (3.5.25) and (3.4.103).

For the second equality we see that by (3.31.9) and (3.5.37)

$$\mathrm{AlgHom}_k(A, \bar{k}) = \mathrm{AlgHom}_k(A, \overline{K}) \cong \mathrm{AlgHom}_K(A \otimes_k K, \overline{K})$$

□

Lemma 3.31.11
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

$$\mathrm{AlgHom}_k(A_1 \times \ldots \times A_d, \bar{k}) \cong \mathrm{AlgHom}_k(A_1, \bar{k}) \times \ldots \times \mathrm{AlgHom}_k(A_d, \bar{k})$$

and a similar consideration for the dimension over k. □

Lemma 3.31.12
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. If $\dim_k A = 1$ then any proper ideal must have strictly lower dimension and therefore A is a field. It is therefore sufficient to show (by induction on dimension) 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 (3.20.5) 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 $a_1 e + a_2 f$ is $(a_1 e, a_2 f)$. 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 (3.31.11) and (3.18.110). □

Lemma 3.31.13
Let A be a finite-dimensional k-algebra and Ω/k a field extension containing $\bar{k}$. Then the following are equivalent

a) *A is etale*

b) *$A \otimes_k \Omega \cong \Omega^n$ as an Ω-algebra*

Proof. *a)* $\implies$ *b)* By (3.31.9) $\#\operatorname{AlgHom}_k(A,\Omega) = \#\operatorname{AlgHom}_k(A,\bar{k}) =: [A:k]_s = [A:k]$ with the last equality because A is assumed etale. Then defining $B := A \otimes_k \Omega$

$$\#\operatorname{AlgHom}_\Omega(B,\Omega) \overset{(3.5.37)}{=} \#\operatorname{AlgHom}_k(A,\Omega) = [A:k] \overset{(3.5.16)}{=} [B:\Omega] = [B^\vee:\Omega]$$

By (3.31.7) and (3.4.138) we see that $\operatorname{AlgHom}_\Omega(B,\Omega)$ is a Ω-basis for $B^\vee$. Denote this basis by $\phi_1,\dots,\phi_n$ then by (3.4.103) this corresponds to a basis $e_1,\dots,e_n$ of B. Then the algebra isomorphism is exhibited explicitly by

$$\begin{aligned} B &\cong \Omega^n \\ b &\to (\phi_1(b),\dots,\phi_n(b)) \end{aligned}$$

b) $\implies$ *a)* We may show that the algebra homomorphisms are just the projections $\pi_i : \Omega^n \to \Omega$, so that $\#\operatorname{AlgHom}_\Omega(B,\Omega) = [B:\Omega]$. As before then $[A:k]_s = \#\operatorname{AlgHom}_k(A,\bar{k}) = \#\operatorname{AlgHom}_k(A,\Omega) = \#\operatorname{AlgHom}_\Omega(B,\Omega) = [B:\Omega] = [A:k]$ which shows that A is etale. □

Proposition 3.31.14 (Etale Criteria)
Let A be a finite-dimensional k-algebra. The following are equivalent

a) *A is etale*

b) *A is geometrically reduced*

c) *$A \otimes_k \bar{k}$ is reduced*

d) *$A \otimes_k K$ is reduced for some perfect field extension K/k*

e) *$A \cong L_1 \times \ldots \times L_n$ for L_i/k finite separable extensions*

In particular A is reduced.

Proof. *a)* $\implies$ *b)* Consider a field extension L/k and the tower of extensions $\overline{L}/L/k$. Then by (3.31.13) $A \otimes_k \overline{L} \cong \overline{L}^n$ is evidently reduced. By (...) $A \otimes_k L \subset A \otimes_k \overline{L}$ is a subring and therefore also reduced.

b) $\implies$ *c)* immediate.

c) $\implies$ *d)* immediate as $\bar{k}$ is perfect.

d) $\implies$ *a)* By (3.31.12) $A \otimes_k K$ is an etale K-algebra so by (3.31.10) A is etale.

e) $\implies$ *a)* Follows immediately from (3.31.11).

a) $\implies$ *e)* We know that A is reduced so the result follows from (3.31.12). □

Corollary 3.31.15
Let A be a finite-dimensional k-algebra and k perfect. Then the following are equivalent

a) *A is etale*

b) *A is reduced*

c) *A is geometrically reduced*

d) *$A \otimes_k \bar{k}$ is reduced.*

For completeness we summarize the relationship between the different notions of separability

Corollary 3.31.16 (Equivalent definitions of separability)
Let K/k be a finite extension. Then the following are equivalent

a) *K/k is separable algebraic (3.18.62)*

b) *K/k is etale*

c) *K/k is geometrically reduced*

d) *$K \otimes_k \bar{k}$ is reduced*

When k is perfect every field extension is separable.

Proof. We have already shown *b)* $\iff$ *c)* $\iff$ *d)*. Furthermore *a)* $\iff$ *b)* is (3.18.89). □

Corollary 3.31.17 (Equivalent definitions of separability)
Let K/k be an algebraic extension. Then the following are equivalent

a) *K/k is separable algebraic (3.18.62)*

b) *Every finite subextension of K/k is etale*

c) *K/k is geometrically reduced*

d) *$K \otimes_k \bar{k}$ is reduced*

In particular an algebraic extension of a perfect field k is geometrically reduced.

Proof. This follows directly from (3.31.16) because each property has "finite character", i.e. holds if and only if it holds for every finite subextension.

The last statement follows from (3.18.110). □

3.31.2 Geometrically Reduced Algebras

Reference is [Bou89, Section V.15.4]. The main results of this section are (3.31.23) and (3.31.25). Observe that if k is perfect every extension K/k satisfies Maclane's Criterion and is therefore Geometrically Reduced.

Lemma 3.31.18
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 (3.4.46) 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 (3.5.24) and the second by (...). □

Proposition 3.31.19
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 3.31.20
Let A be a geometrically reduced k-algebra and K the total ring of fractions. Then K is geometrically reduced.

Conversely if A is integral and K is geometrically reduced, then A is geometrically reduced.

Proof. Let L/k be a field extension and consider a nilpotent element $x \in K \otimes L$. Then by definition

$$x = \sum_{i=1}^{n} (a_i s_i^{-1}) \otimes \lambda_i \quad a_i \in A, s_i \notin Z(A), \lambda_i \in L$$

Let $s = s_1 \dots s_n$ then $x \cdot (s \otimes 1) \in A \otimes L \subset K \otimes L$. Then $x \cdot (s \otimes 1)$ is nilpotent and so by definition zero. As $(s \otimes 1)$ is invertible we see $x = 0$ as required.

For the converse $A \subset K$ and therefore $A \otimes_k L \subset K \otimes_k L$. □

Lemma 3.31.21
Let K/k be a separably generated field extension. Then K/k is geometrically reduced.

Proof. Consider first the case $K = k(\mathcal{B})$ is purely transcendental. Then 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.

For the general case

$$K \otimes_k L \cong K \otimes_{k(\mathcal{B})} (k(\mathcal{B}) \otimes_k L)$$

We have shown that $k(\mathcal{B}) \otimes_k L$ is reduced and by (3.31.17) $K/k(\mathcal{B})$ is geometrically reduced as by assumption it is separable. By (3.31.19) $K \otimes_k L$ is reduced and K is geometrically reduced as required. □

Lemma 3.31.22
Let A be a reduced k-algebra for which k is perfect. Then A is geometrically reduced.

Proof. We prove the result in increasing generality

a) We first consider the case $A = K/k$ is a finitely generated field extension. By (3.18.144) K/k is separably generated and so by (3.31.21) it is geometrically reduced.

b) When A is a finitely-generated k-algebra by (3.31.18) 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 as required.

c) The general case follows from b) and the reduction to the finitely generated case (3.31.4).

□

Proposition 3.31.23 (Maclane's Criterion for Algebras)
Let A be a k-algebra. Then the following are equivalent

a) *A is geometrically reduced*

b) *$A \otimes_k \bar{k}$ is reduced*

c) *$A \otimes_k k^{p^{-\infty}}$ is reduced*

d) *$A \otimes_k K$ is reduced for some perfect extension K/k*

e) *$A \otimes_k k^{p^{-1}}$ is reduced*

f) *$A \otimes_k k'$ is reduced for every finite subextension k'/k of $k^{p^{-1}}/k$*

g) *The following k-module homomorphism*

$$\begin{aligned} m : A \otimes_k k^{p^{-1}} &\to A \\ a \otimes \lambda &\to \lambda^p a^p \end{aligned}$$

is injective (that is $k^{p^{-1}}$ and A are linearly disjoint with respect to the p-th power embedding into A)

h) *A satisfies Maclane's Criterion (3.18.140)*

In particular when k is perfect then this is equivalent to A being reduced.

Proof. The case $p = 1$ is simply (3.31.22) because $k^p = k = k^{p^{-1}} = k^{p^{-\infty}}$ is perfect and g) is equivalent to A being reduced. Therefore we assume $p > 1$.

a) $\implies$ *b)* By definition

b) $\implies$ *c)* By (3.18.72) there is an embedding $k^{p^{-\infty}} \hookrightarrow \bar{k}$ whence an embedding $A \otimes_k k^{p^{-1}} \hookrightarrow A \otimes_k \bar{k}$

c) $\implies$ *d)* By (3.18.107) $k^{p^{-\infty}}$ is perfect

d) $\implies$ *e)* By (3.18.108) there is an embedding $k^{p^{-1}} \hookrightarrow K$ whence an embedding $A \otimes_k k^{p^{-1}} \hookrightarrow A \otimes_k K$.

e) $\implies$ *f)* this is immediate as we have an embedding $A \otimes_k k' \hookrightarrow A \otimes_k k^{p^{-1}}$

f) $\iff$ *g)* Suppose $x := \sum_i \lambda_i \otimes a_i \in A \otimes_k k^{p^{-1}}$ is a finite sum then we may consider the finite subextension $k' := k(\{a_i\}_i)$. Observe that

$$x^p = \sum_i \lambda_i^p \otimes a_i^p = \sum_i 1 \otimes \lambda_i^p a_i^p = 1 \otimes \left(\sum_i \lambda_i^p a_i^p \right) =: 1 \otimes m(x)$$

Therefore we see $A \otimes_k k'$ is reduced for every such k' iff $m(x)$ is injective.

g) $\iff$ *h)* Consider the Frobenius morphisms $i : k^{p^{-1}} \to A$ and $j : A \to A$. Then *g)* is equivalent to $k^{p^{-1}}$ and A being linearly disjoint in A with respect to i, j and the result follows from the characterization of linear disjointness (3.29.46).

h) $\implies$ *a)* Let $\{a_i\}_{i \in I}$ be a k-basis for A then by (3.5.25) $\{a_i \otimes 1\}_{i \in I}$ is an L-basis for $A \otimes_k L$. Given $x \in A \otimes_k L$ we have

$$x = \sum_{i \in I} a_i \otimes \lambda_i \quad \lambda_i \in L$$

and

$$x^p = \sum_{i \in I} \lambda_i^p \otimes a_i^p = \sum_{i \in I} \lambda_i^p (a_i^p \otimes 1)$$

By assumption $\{a_i^p\}_{i \in I}$ is k-linearly independent and therefore $\{a_i^p \otimes 1\}_{i \in I}$ is L-linearly independent. Therefore $x^p = 0 \implies \lambda_i^p = 0$ for all $i \in I \implies \lambda_i = 0$ for all $i \in I \implies x = 0$, as L is reduced. It follows from (3.18.141) that $A \otimes_k L$ is reduced, as we assumed that $p > 1$. □

Corollary 3.31.24 (Maclane's Criterion for Fields)
Let K/k be a field extension with characteristic exponent p. Then the following are equivalent

a) *K/k is geometrically reduced*

b) *$K \otimes_k \bar{k}$ is reduced*

c) *$K \otimes_k k^{p^{-1}}$ is reduced*

d) *$K \otimes_k k^{p^{-\infty}}$ is reduced*

e) *$K \otimes_k k'$ is reduced for some perfect extension k'/k*

f) *K and $k^{p^{-1}}$ are linearly disjoint (with respect to some common field extension)*

g) *$K \otimes_k k^{p^{-1}}$ is an integral domain*

h) *$K \otimes_k k^{p^{-1}}$ is a field*

i) *K/k satisfies Maclane's Criterion (3.18.140)*

Observe i) has finite character *in the sense it holds if and only if it holds for every finitely-generated subextension.*

In particular when k is perfect every extension is geometrically reduced.

Proof. By (3.31.23) $a) - f), i)$ are equivalent (using (3.29.47) to generalise the linear disjoint condition to any ambient field) and by (3.29.47) again $f) - h)$ are equivalent. □

Proposition 3.31.25 (Separable Field Extensions)
Let K/k be a field extension. Then the following are equivalent

a) *K/k is geometrically reduced*

b) *$K \otimes_k \bar{k}$ is reduced*

c) *K/k satisfies Maclane's Criterion (3.18.140)*

d) *Every finitely generated subextension K/k is separably generated*

In particular if k is perfect every field extension satisfies these properties.

Proof. By (3.31.24) we have *a)* $\iff$ *b)* $\iff$ *c)*. Further *c)* $\implies$ *d)* is Lemma (3.18.144), since every subextension satisfies Maclane's Criterion. For *d)* $\implies$ *a)* observe that every finitely generated subextension is geometrically reduced by (3.31.21). We may use (3.31.2) to argue that K/k is geometrically reduced. □

Corollary 3.31.26
Let K/k be a finitely generated field extension. Then the following are equivalent.

a) *K/k is geometrically reduced*

b) *$K \otimes_k \bar{k}$ is reduced*

c) *K/k satisfies Maclane's Criterion (3.18.140)*

d) *Every finitely generated subextension of K/k is separably generated*

e) *K/k is separably generated*

Proof. We've already shown equivalence of $a) - d)$ and clearly $d) \implies e)$. Finally $e) \implies a)$ is simply (3.31.21). □

3.31.3 Geometrically Irreducible Algebras

The reference for this section is [Sta15, 00I2] presented here with more elementary proof of Proposition (3.31.31).

Lemma 3.31.27
Let A, B be k-algebras. If $a \otimes 1 \in A \otimes_k B$ is a zero-divisor then so is a.

Proof. Consider a basis $\{a_i\}_{i\in I}$ for A such that $a_{i_0} = a$. If a is not a zero-divisor then we may show directly that $\{aa_i\}_{i\in I}$ is linearly independent. Then by extending to a basis of A we may use (3.5.25) to show that $\{(aa_i) \otimes 1\}_{i\in I}$ is B-linearly independent. We see immediately that $a \otimes 1$ is not a zero-divisor as required. □

Lemma 3.31.28
Let A be a ring and $\mathfrak{a} \subset N(A)$ a locally nilpotent ideal. Then A is irreducible iff $A/\mathfrak{a}$ is irreducible.

Lemma 3.31.29
Let $A \subset B$ be a subring of an irreducible ring. Then A is irreducible.

In particular if B is a geometrically irreducible k-algebra, then so is any subalgebra.

Proof. By (3.21.7) every minimal prime in A is the contraction of a minimal prime. As there is precisely one minimal prime of B then we are done.

The final statement follows because the canonical map $A \otimes_k L \to B \otimes_k L$ is injective. □

When k is algebraically closed then nothing interesting happens.

Lemma 3.31.30
Let A be an irreducible (resp. integral) k-algebra, k algebraically closed and K/k a field extension. Then $A \otimes_k K$ is irreducible (resp. integral).

In other words A is geometrically irreducible (resp. integral).

Proof. Observe that $N(A) \otimes_k K \subset N(A \otimes_k K)$. For $(n \otimes \lambda)^m = n^m \otimes \lambda^m = 0$ and we may use (...) to argue any linear combination of such elements is nilpotent. By (...) we have an isomorphism

$$A/N(A) \otimes_k K \cong (A \otimes_k K)/(N(A) \otimes_k K)$$

Then by (3.31.28) $A/N(A) \otimes_k K$ is irreducible iff $A \otimes_k K$ is. Therefore we may consider only the case A is reduced and therefore integral, and show that $A \otimes_k K$ is integral and a-fortiori irreducible.

If $A \otimes_k K$ were not integral it would contain a non-trivial zero divisor, and this would also be true for $A' \otimes_k K$ for some finitely generated subalgebra A'. Therefore we may assume wlog that A is finitely generated.

To simplify the argument choose a basis $\{\lambda_i\}_{i\in I}$ for K/k. By (...) $\{1 \otimes \lambda_i\}_{i\in I}$ is an A-basis for $A \otimes_k K$. Therefore if we have a product of elements equal to 0 then may write it as follows

$$\left(\sum_i a_i \otimes \lambda_i\right)\left(\sum_i a_i' \otimes \lambda_i\right) = 0$$

for some $a_i, a_i' \in A$ all but finitely many zero. Let $\mathfrak{m} \triangleleft A$ be a maximal ideal, then by the Weak Nullstellensatz (3.29.19) the structural morphism $k \to A/\mathfrak{m}$ is an isomorphism. Reduce the equation to $A/\mathfrak{m} \otimes_k K \cong K$ to find

$$\left(\sum_i \overline{a}_i \lambda_i\right)\left(\sum_i \overline{a}_i' \lambda_i\right) = 0$$

As K is an integral domain, and λ_i are linearly independent we find $\overline{a}_i, \overline{a}_i' = 0$. As $\mathfrak{m}$ was arbitrary we find $a_i, a_i' \in \bigcap \mathfrak{m}$ for all i. By assumption (0) is prime and so by the Strong Nullstellensatz (3.30.3) we find $a_i = a_i' = 0$. This shows that $A \otimes_k K$ is integral as required. □

Proposition 3.31.31 (Extension of Scalars is Flat)
Let A be a k-algebra and $L/K/k$ a tower of field extensions. Then the canonical ring homomorphism

$$A \otimes_k K \to A \otimes_k L$$

satisfies Going Down. Further we have a well-defined surjective map of minimal primes

$$\mathrm{MinPrime}(A \otimes_k L) \to \mathrm{MinPrime}(A \otimes_k K)$$

given by the inverse image.

Proof. By (...) there is a commutative diagram

$$\begin{array}{ccc} A \otimes_k K & \longrightarrow & A \otimes_k L \\ & \searrow & \downarrow \sim \\ & & (A \otimes_k K) \otimes_K L \end{array}$$

Therefore it is enough to show that $A \to A \otimes_k K$ satisfies going down. Suppose $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 = \mathfrak{q}_2^c$. There is a commutative diagram

$$\begin{array}{ccc} A/\mathfrak{p}_1 & \xrightarrow{\alpha} & A/\mathfrak{p}_1 \otimes_k K \\ {\scriptstyle\pi}\uparrow & & \uparrow{\scriptstyle\pi\otimes 1} \\ A & \xrightarrow{\beta} & A \otimes_k K \end{array}$$

where (3.5.41) shows that $\ker(\pi \otimes 1) = \mathfrak{p}_1^e$.

Let $\widetilde{\mathfrak{q}}_1$ be a minimal prime of $A/\mathfrak{p}_1 \otimes_k K$ contained in $\widetilde{\mathfrak{q}}_2 := (\pi \otimes 1)(\mathfrak{q}_2)$ by (3.4.43). Define $\mathfrak{q}_1 := (\pi \otimes 1)^{-1}(\widetilde{\mathfrak{q}}_1)$ then $\mathfrak{q}_1$ is a prime minimal over $\mathfrak{p}_1^e$. As $\pi \otimes 1$ is surjective it is contained in $\mathfrak{q}_2$. We require to prove that $\beta^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$, which we readily see is implied by $\alpha^{-1}(\widetilde{\mathfrak{q}}_1) = (0)$.

By (3.4.44) $\widetilde{\mathfrak{q}}_1$ consists of zero divisors and by (3.31.27) so does $\alpha^{-1}(\widetilde{\mathfrak{q}}_1)$. As $A/\mathfrak{p}_1$ is an integral domain we see that this equals (0) and we are done.

This immediately shows that the inverse image of a minimal prime is again a minimal prime. By (3.21.7) every minimal prime is a contracted minimal prime. □

Lemma 3.31.32 (Purely Inseparable Extensions of Scalars are Homeomorphisms)
Let k be a field with characteristic exponent p, A a k-algebra and k'/k a purely inseparable field extension. Consider the structural algebra homomorphism

$$\phi : A \to A \otimes_k k'$$

Then ϕ induces an order-preserving bijection between prime ideals

$$\mathfrak{q}^c \quad \leftarrow \quad \mathfrak{q}$$

In particular A is irreducible iff $A \otimes_k k'$ is.

Futhermore a purely inseparable extension is geometrically irreducible.

Proof. If $p = 1$ then k'/k is trivial and the statement is obvious. So we may assume wlog that $p > 1$.

If ϕ were surjective then we would have equality $\mathfrak{q}^{ce} = \mathfrak{q}$ and which would imply the map of prime ideals is injective. However we note that ϕ is "almost" surjective, namely for every $z = \sum_{i=1}^N a_i \otimes \lambda_i$ there exists $n \geq 0$ such that $z^{p^n} \in \phi(A)$. For k'/k is purely inseparable so by definition there is some $n \geq 0$ such that $\lambda_i^{p^n} \in k$ for all $i = 1 \dots N$. In this case $z^{p^n} = \sum_{i=1}^n a^{p^n} \lambda_i^{p^n} \otimes 1$ which is in the image of A as required.

This allows us to argue the map is injective for suppose $\mathfrak{p} := \mathfrak{q}^c = (\mathfrak{q}')^c$ and $z \in \mathfrak{q} \setminus \mathfrak{q}'$. Then by the previous argument $z^{p^n} = \phi(x) \implies z^{p^n} \in \mathfrak{q} \implies z^{p^n} \in \mathfrak{q}' \implies z \in \mathfrak{q}'$ which is a contradiction. Therefore contraction of prime ideals is injective.

Finally we may observe that ϕ is integral (3.22.17) and injective (3.31.2). Therefore it satisfies the lying over property (3.22.14) and so every prime ideal in A is contracted and the given map is surjective. □

The following result shows it is sufficient to ensure that A remains irreducible under a finite separable base change.

Proposition 3.31.33
Let A be an k-algebra. Then the following are equivalent

a) *A is geometrically irreducible*

b) *$A \otimes_k k'$ is irreducible for every finite separable extension k'/k*

c) *$A \otimes_k k^{sep}$ is irreducible*

d) *$A \otimes_k \bar{k}$ is irreducible*

Proof. *a)* $\implies$ *b)* immediate

b) $\implies$ *c)* Suppose $\mathfrak{q}_1, \mathfrak{q}_2$ are minimal prime ideals of $A \otimes_k k^{sep}$. Let $k^{sep}/k'/k$ be a fixed finite separable extension and consider the subring

$$A \otimes_k k' \subset A \otimes_k k^{sep}$$

together with the prime ideals $\mathfrak{p}_i := \mathfrak{q}_i \cap (A \otimes_k k')$. By (3.31.31) the prime ideals $\mathfrak{p}_i$ are minimal and therefore $\mathfrak{p}_1 = \mathfrak{p}_2$ by assumption. As k'/k was an arbitrary finite subextension we may conclude by (3.31.4) that $\mathfrak{q}_1 = \mathfrak{q}_2$ and $A \otimes_k k^{sep}$ is irreducible.

c) $\implies$ *d)* By (...) $A \otimes_k \bar{k} \cong (A \otimes_k k^{sep}) \otimes_{k^{sep}} \bar{k}$ and so is irreducible by (3.31.32), since $\bar{k}/k^{sep}$ is purely inseparable (3.18.105).

d) $\implies$ *a)* Let K/k be a field extension then we may identify $\bar{k}$ and K as subextensions of $\overline{K}/k$. Then $A \otimes_k \overline{K} \cong (A \otimes_k \bar{k}) \otimes_{\bar{k}} \overline{K}$. By (3.31.30) $A \otimes_k \overline{K}$ is irreducible. Finally from (3.31.31) we see that $A \otimes_k K$ is irreducible as required. □

Proposition 3.31.34
Let A be a geometrically irreducible K-algebra and K/k a geometrically irreducible field extension. Then A/k is geometrically irreducible.

Proof. It is sufficient by (3.31.33) to consider base change by a finite separable extension k'/k. Observe by transitivity

$$A \otimes_k k' \cong A \otimes_K (K \otimes_k k')$$

so it would be sufficient to show that $K \otimes_k k'$ is a field. By hypothesis $K \otimes_k k'$ is irreducible. Furthermore k'/k is geometrically reduced (3.31.16) whence $K \otimes_k k'$ is reduced and therefore an integral domain. Using the fact k'/k is algebraic we may conclude from (3.29.47) that $K \otimes_k k'$ is a field. and we are done. □

Proposition 3.31.35 (Primary Extension)
Let K/k be a field extension. Then K/k is geometrically irreducible if and only if it is relatively separably closed.

In this case the subfield of algebraic elements is purely inseparable over k. In particular an algebraic extension is geometrically irreducible if and only if it is purely inseparable.

*We say such an extension is **primary**.*

Proof. Suppose that K/k is relatively separably closed. By (3.31.33) it is enough to show that $K \otimes_k k'$ is irreducible for every finite separable extension k'/k.

Let $K/K'/k$ be the relative algebraic closure then K/K' is relatively algebraically closed (3.18.58) and K'/k is purely inseparable because $K_s = k$ by hypothesis (3.18.103). Observe K'/k is geometrically irreducible (3.31.32) so by (3.31.34) it is enough to show that K/K' is geometrically irreducible. This reduces to the case that K/k is relatively algebraically closed.

As before it is sufficient to consider base change by a finite separable extension k'/k. By (3.18.88) $k' = k(\alpha)$ is simple. Let $m(X)$ be the minimal polynomial for α then $k(\alpha) \cong k[X]/(m)$. From (3.31.36) $m(X)$ remains irreducible in $K[X]$ and therefore

$$K \otimes_k k(\alpha) \cong K[X]/(m)$$

is a field and in particular irreducible.

Conversely suppose that K/k is geometrically irreducible and $\alpha \in K$ is separable. Then $k(\alpha)$ is geometrically irreducible by (3.31.29). Therefore by the Chinese Remainder Theorem (...)

$$k(\alpha) \otimes_k \bar{k} \cong k[X]/(m_\alpha) \otimes_k \bar{k} \cong \bar{k}[X]/(m_\alpha) \cong \bar{k}[X]/(X - \alpha_1)^{n_1} \times \ldots \times \bar{k}[X]/(X - \alpha_r)^{n_r}$$

is irreducible where $\alpha_1, \ldots, \alpha_r$ are the distinct roots in $\bar{k}$. This implies $r = 1$ and therefore α is purely inseparable (3.18.97). Being both separable and purely inseparable $\alpha \in k$ (3.18.98) as required. □

We made use of

Lemma 3.31.36
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 $K[X]$. □

3.31.4 Geometrically Integral Algebras

Clearly a geometrically (resp. algebraically) integral algebra is integral, we are interested in providing sufficient conditions for the reverse implication.

Proposition 3.31.37
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 3.31.38 (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 (3.29.46), 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. □

Proposition 3.31.39 (Criteria to be Geometrically Integral)
Let A be a k-algebra. Then the following are equivalent

a) *A is geometrically integral*

b) *A is geometrically reduced and irreducible*

c) *$A \otimes_k \bar{k}$ is an integral domain*

d) *$A \otimes_k k'$ is an integral domain for every finite extension k'/k*

Note we may restrict d) to only finite separable, and finite purely inseparable extensions of height at most 1.

Proof. This is largely a collection of existing results. *a)* $\iff$ *b)* is by definition and (3.4.64). Then *b)* $\iff$ *c)* $\iff$ *d)* is from the reduced (3.31.23) and irreducible (3.31.33) cases, together with the trivial observation that reduced + irreducible $\iff$ integral (3.4.64). □

Proposition 3.31.40 (Regular Extension)
Let K/k be a field extension. Then the following are equivalent

a) *K/k is geometrically integral*

b) *K/k is geometrically reduced (e.g. separably generated) and relatively separably closed*

c) *K/k is geometrically reduced (e.g. separably generated) and relatively algebraically closed*

d) *$K \otimes_k \bar{k}$ is an integral domain*

We say such an extension is ***regular****.*

Proof. $a) \implies b)$ is by definition and (3.31.35). $c) \implies b)$ is immediate. For the converse suppose $\alpha \in K/k$ is algebraic then $k(\alpha)/k$ is geometrically reduced and therefore separable algebraic (3.31.16). By hypothesis $\alpha \in k$ as required. $a) \iff d)$ was already proven. □

Corollary 3.31.41 (Criteria to be Geometrically Integral II)
Let A be a geometrically reduced k-algebra and K the total ring of fractions. Then the following are equivalent

a) *A is geometrically integral*

b) *$A \otimes_k \bar{k}$ is integral*

c) *$A \otimes_k k'$ is integral for every finite separable extension k'/k*

d) *A is integral and K/k is geometrically integral*

e) *A is integral and K/k is relatively separably closed*

f) *A is integral and K/k is relatively algebraically closed*

Proof. For $a) - c)$ we know that integral $\iff$ irreducible and we may apply (3.31.33). For $a) \iff d)$ we may apply (3.31.38). Note $\mathrm{Frac}(A)$ is also geometrically reduced by (3.31.20). Therefore $d) - f)$ follows from (3.31.40). □

Chapter 4

Topology and Sheaves

4.1 Topological Spaces

References :

- General Topology [Kel71, Chap. 1]
- General Topology [Wil70]

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 (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 4.1.4 (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 4.1.5 (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 4.1.6 (Base generating topology)
A base $\mathcal{B}$ satisfies $\mathcal{T}_{\mathcal{B}} = \mathcal{T}_X$ if and only if

a) $\mathcal{B} \subset \mathcal{T}_X$

b) *or 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 (the topology on)* X.

Proposition 4.1.7 (Subbase for a topology)
Let X *be a set and* $\mathcal{B}$ *be an arbitrary family of subsets. Then there exists a topology* $\mathcal{T}_\mathcal{B}$ *such that*

a) $\mathcal{B} \subset \mathcal{T}_\mathcal{B}$

b) *For every topology* $\mathcal{T}'$ *containing* $\mathcal{B}$ *we have* $\mathcal{T}_\mathcal{B} \subset \mathcal{T}'$.

We say that $\mathcal{B}$ *is a* ***subbase*** *for the topology* $\mathcal{T}_\mathcal{B}$. *Explicitly* $\mathcal{T}_\mathcal{B}$ *consists of arbitrary unions of finite intersections of elements of* $\mathcal{B}$.

Proposition 4.1.8 (Base for subspace topology)
Let $(X, \mathcal{T})$ *be a topological space, and* $Y \subset X$ *has the subsapce topology* $\mathcal{T}_Y$ *(4.1.3). If* $\mathcal{B}$ *is a base for* $(X, \mathcal{T})$ *then*

$$\mathcal{B}_Y := \{U \cap Y \mid U \in \mathcal{B}\}$$

is a base for $(Y, \mathcal{T}_Y)$.

Definition 4.1.9 (Adherent point)
For $Y \subset X$ *we say* x *is an* ***adherent point*** *of* Y *if every open neighbourhood of* x *intersects* Y.

Similarly we say x *is a* ***limit point*** *(or* ***accumulation point****) for* Y *if every open neighbourhood of* x *intersects* Y *at a point other than* x.

Proposition 4.1.10 (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 4.1.11
For a topological space X *let* X° *denote the subset of closed points.*

4.1.1 Axioms of Countability

Definition 4.1.12 (Neighbourhood)
Let X *be a topological space and* $x \in X$. *We say a set* $V \subset X$ *is a* ***neighbourhood*** *of* x *if* $x \in U \subset V$ *for some open set* U. *We write* $\mathscr{U}_x$ *for the neighbourhoods of* x, *and* $\mathscr{O}_x$ *for the open neighbourhoods of* x.

We say that a collection of neighbourhoods $\mathscr{B}_x$ *is a* ***local base*** *for* x *if every neighbourhood* $U \in \mathscr{U}_x$ *contains some neighbourhood* $V \in \mathscr{B}_x$. *For example* $\mathscr{O}_x$ *is a local base.*

Definition 4.1.13 (First-Countable)
Let X *be a topological space.* X *is* ***first countable*** *if every point* $x \in X$ *has a countable local base.*

Definition 4.1.14 (Secound-Countable)
Let X *be a topological space.* X *is* ***second countable*** *if there exists a countable basis. Evidently this is stronger than first countability.*

Example 4.1.15
For example a metric space is always first countable as we may consider balls of radius $1/n$.

Further $\mathbb{R}$ *is second countable as we may consider open intervals with rational endpoints.*

4.1.2 Closure

Definition 4.1.16 (Adherent Point)
Let X *be a topological space and* $Y \subset X$. *We say that* $x \in X$ *is an* ***adherent point*** *of* Y, *if* $U \in \mathscr{U}_x \implies U \cap Y \neq \emptyset$.

We say that x *is a* ***sequential limit point*** *of* Y *if there exists a sequence* $x_n \in Y$ *such that* $x_n \to x$.

Proposition 4.1.17 (Adherent Point)
Let X *be a topological space. Then every sequential limit point is an adherent point. If* X *is first countable the converse holds.*

Proof. The first implication is straightforward. For the latter, consider a countable local base at x given by U_n. We may assume wlog that it is decreasing. Then by assumption we may choose $x_n \in U_n \cap Y$. For any $V \in \mathscr{B}_x$ we have $U_N \subset V$ for some N, and therefore $n \geq N \implies x_n \in U_n \implies x_n \in V$. Therefore $x_n \to x$. □

Proposition 4.1.18 (Topological Closure)
Let $Y \subset X$ then the following equality holds

$$\bigcap_{\substack{Z \supseteq Y \\ Z \text{ closed}}} Z = \{x \in X \mid x \text{ adherent point of } Y\}$$

*We denote this by $\overline{Y}$ (or $\mathrm{cl}_X(Y)$ to emphasise the ambient space X) and refer to it as the **closure** of Y in X. Furthermore the following properties hold*

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*

When X is first countable then $\overline{Y}$ is the set of sequential limit points of Y.

Proof. Suppose Z is a closed set containing Y and x is an adherent point of Y. Then $x \notin Z \implies x \in X \setminus Z \implies (X \setminus Z) \cap Y \neq \emptyset$ a contradiction. Conversely assume $x \notin \overline{Y}$ then there exists $Z \supseteq Y$ closed such that $x \notin Z \implies x \in X \setminus Z$. This means x is not an adherent 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.

□

Corollary 4.1.19
Let X be a first countable topological space. Then $\mathrm{cl}_X(Y)$ is the set of sequential limit points of Y.

Proposition 4.1.20 (Closure in Subspace Topology)
Let X be a topological space and Y a subset. For $Z \subset Y$ we have

$$\mathrm{cl}_Y(Z) = \mathrm{cl}_X(Z) \cap Y$$

Proof. By (4.1.18) $\mathrm{cl}_X(Z)$ is a closed subset of X and therefore $\mathrm{cl}_X(Z) \cap Y$ is a closed subset of Y in the subspace topology. Therefore $\mathrm{cl}_Y(Z) \subset \mathrm{cl}_X(Z) \cap Y$ by minimality. Similarly $\mathrm{cl}_Y(Z) = W \cap Y$ for W closed in X.By minimality $\mathrm{cl}_X(Z) \subset W \implies \mathrm{cl}_X(Z) \cap Y \subset W \cap Y = \mathrm{cl}_Y(Z)$. □

Proposition 4.1.21
Let $Y_1, \ldots, Y_n$ be subsets of a topological space X. Then

$$\overline{Y_1 \cup \ldots \cup Y_n} = \overline{Y_1} \cup \ldots \cup \overline{Y_n}$$

Proof. By induction it is sufficient to demonstrate the case $n = 2$. $\overline{Y_1 \cup Y_2}$ is a closed set containing both Y_1 and Y_2. Therefore by definition

$$\overline{Y_1} \cup \overline{Y_2} \subset \overline{Y_1 \cup Y_2}$$

On the other hand $\overline{Y_1} \cup \overline{Y_2}$ is closed and contains $Y_1 \cup Y_2$. Therefore the reverse inclusion follows immediately. □

Proposition 4.1.22 (Dense subset)
Let $Y \subset X$ then the following are equivalent

a) *$\overline{Y} = X$*

b) *$Y \cap U \neq \emptyset$ for any $U \subset X$ open*

*In this case we say Y is **dense**.*

Proof. 1 $\implies$ 2) Follows from (4.1.18).c)

2 $\implies$ 1). Suppose $Y \subseteq \overline{Y} \subsetneq X$ then $X \setminus \overline{Y}$ is an open set not intersecting Y a contradiction. □

4.1.3 Continuous Maps

Proposition 4.1.23 (Continuous at a point)
Let $f : X \to Y$ a map of topological spaces and $x \in X$. Then the following are equivalent

a) $V \in \mathscr{U}_{f(x)} \implies f^{-1}(V) \in \mathscr{U}_x$

b) $V \in \mathscr{B}_{f(x)} \implies f^{-1}(V) \in \mathscr{U}_x$

c) $V \in \mathscr{U}_{f(x)} \implies \exists U \in \mathscr{U}_x \text{ s.t. } f(U) \subseteq V$

d) $V \in \mathscr{B}_{f(x)} \implies \exists U \in \mathscr{B}_x \text{ s.t. } f(U) \subseteq V$

*where $\mathscr{B}_{f(x)}$ is any local base at $f(x)$ and $\mathscr{B}_x$ is any local base at x. We say that f is **continuous** at x.*

Proof. *a)* $\implies$ *b)* is obvious. Suppose *b)* holds and $V \in \mathscr{U}_{f(x)}$ then by definition there exists $V' \in \mathscr{B}_{f(x)}$ such that $V' \subset V$. By hypothesis $f^{-1}(V') \in \mathscr{U}_x$ from which it follows that $f^{-1}(V) \in \mathscr{U}_x$.

a) $\implies$ *c)* $f(f^{-1}(V)) \subseteq V$

c) $\implies$ *d)* By definition there exists $U' \in \mathscr{B}_x$ such that $U' \subseteq U \implies f(U') \subseteq f(U) \subseteq V$

d) $\implies$ *b)* Observe that $f(U) \subseteq V \implies U \subseteq f^{-1}(V)$ whence $f^{-1}(V) \in \mathscr{U}_x$ as required. □

Proposition 4.1.24
Let $f : X \to Y$ and $g : Y \to Z$ be maps of topological spaces such that f is continuous at x and g is continuous at $f(x)$. Then $g \circ f$ is continuous at x.

Proposition 4.1.25 (Characterisation of Continuous Maps)
Let $f : X \to Y$ be a map of topological spaces. Then the following are equivalent

a) *f is continuous at all points $x \in X$*

b) *$V \subset Y$ open $\implies f^{-1}(V) \subset X$ is open*

c) *$Z \subset Y$ closed $\implies f^{-1}(Z) \subset X$ is closed*

Let $\mathcal{B}_1, \mathcal{B}_2$ be bases of open sets for X and Y respectively. Then this is equivalent to the following condition

$$\forall V \in \mathcal{B}_2, \text{ s.t. } x \in f^{-1}(V), \exists U \in \mathcal{B}_1 \text{ s.t. } x \in U \subset f^{-1}(V)$$

4.1.4 Quasi-Homeomorphism

Proposition 4.1.26 (Quasi-Homeomorphism)
Let $f : X \to Y$ be a map. The following are equivalent

a) *The map $W \to f^{-1}(W)$ is a bijection between open sets*

b) *The map $Z \to f^{-1}(Z)$ is a bijection between closed sets*

*In this case we say f is a **quasi-homeomorphism**. Such a map induces a bijection between irreducible sets, respectively irreducible components.*

Proof. This follows by taking complements and observing $X \setminus f^{-1}(A) = f^{-1}(Y \setminus A)$. □

4.1.5 Separation Axioms

Definition 4.1.27
Let X be a topological space. We say that X is

- ***Hausdorff** If for all distinct pairs $x, y \in X$ there exists open neighbourhoods U, V of x and y respectively such that $U \cap V = \emptyset$*
- ***Kolmogorov** If for all distinct pairs $x, y \in X$ there exists an open set U such that either $x \in U$ and $y \notin U$, or $x \notin U$ and $y \in U$*

*Observe that **Hausdorff** $\implies$ **Kolmogorov**, but not conversely (e.g. co-finite topology).*

Proposition 4.1.28 (Indistinguishable points)
Let X be a topological space and $x, y \in X$. The following are equivalent

a) $\overline{\{x\}} = \overline{\{y\}}$

b) $x \in \overline{\{y\}}$ *and* $y \in \overline{\{x\}}$

c) *Every closed $Z \subset X$ contains both or neither of x, y*

d) *Every open $U \subset X$ contains both or neither of x, y*

We say x, y are ***topologically indistinguishable****, otherwise we say x and y are* ***distinguishable****.*

X is Kolmogorov iff every pair of points are distinguishable.

Being indistinguishable determines an equivalence relation on X, and we denote by $X_0 := X/\sim$ the ***Kolmogorov Quotient****.*

Proof. *a)* $\implies$ *b)* Clear

b) $\implies$ *a)* By definition of closure $x \in \overline{\{y\}} \iff \overline{\{x\}} \subset \overline{\{y\}}$.

c) $\iff$ *d)* Follows by taking complements

c) $\implies$ *b)* Suppose $x \in Z$ for Z closed then by hypothesis $y \in Z$. As Z was arbitrary we see that $y \in \overline{\{x\}}$, and symmetrically $x \in \overline{\{y\}}$.

b) $\implies$ *c)* By assumption $x \in Z \implies y \in Z$ for Z closed and symmetrically $y \in Z \implies x \in Z$. □

Proposition 4.1.29 (Kolmogorov Quotient)
Let X be a topological space and X_0 be the Kolmogorov Quotient with quotient map $\pi : X \to X_0$. Relative to the quotient topology

$$\mathcal{T}_{X_0} := \{W \subset X_0 \mid \pi^{-1}(W) \in \mathcal{T}_X\}$$

π is a quasi-homeomorphism and an open and closed map. More precisely $\pi^{-1}(\pi(U)) = U$ for all U open and closed. Further X_0 is Kolmogorov.

Proof. As arbitrary intersections and unions commute with inverse image we see that $\mathcal{T}_{X_0}$ is a well-defined topology. As π is surjective $\pi(\pi^{-1}(W)) = W$ for any subset $W \subset X_0$. Similarly if $U \subset X$ is open (resp. closed) then we claim $\pi^{-1}(\pi(U)) = U$. Generically $U \subset \pi^{-1}(\pi(U))$. Suppose $x \in \pi^{-1}(\pi(U))$ then $\pi(x) = \pi(y)$ for some $y \in U$. Then by definition of π, x and y are indistinguishable and so $x \in U$. This shows that π is a quasi-homeomorphism.

Suppose $\pi(x) \neq \pi(y)$ then by definition there exists an open set $U \subset X$ such that $x \in U$ and $y \notin U$. As π is open then $\pi(U)$ is open. By construction $\pi(x) \in \pi(U)$ and $\pi(y) \notin \pi(U)$. This shows that X_0 is Kolmogorov. □

Proposition 4.1.30 (Kolmogorv Quotient Functioriality)
Let $f : X \to Y$ be a continuous map, then there is a unique (continuous) map $f_0 : X_0 \to Y_0$.such that the following diagram commutes

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ X_0 & \xrightarrow{f_0} & Y_0 \end{array}$$

Proof. Given $x, x' \in X$ and suppose $f(x) \not\sim f(x')$. Then there exists an open set U such that $f(x') \in U$ and $f(x) \notin U$. Therefore $x' \in f^{-1}(U)$ and $x \notin f^{-1}(U)$ and $x \not\sim x'$. Equivantly $x \sim x' \implies f(x) \sim f(x')$. Therefore the map

$$f_0([x]) = [f(x)]$$

is well-defined.

For $W_0 \subset Y_0$ we have $\pi^{-1}(f_0^{-1}(W_0)) = f^{-1}(\pi^{-1}(W_0))$ is open. As π is surjective and open $f_0^{-1}(W) = \pi(\pi^{-1}(f_0^{-1}(W_0))$ is open, and therefore f_0 is continuous.

Any such f_0 satisfies $\{f_0(x_0)\} = \pi(f(\pi^{-1}(\{x_0\})))$ and so is unique. □

4.1.6 Convergent Sequences

Proposition 4.1.31 (Convergent Sequence)
Let X be a topological space, (x_n) a sequence in X and $x \in X$. Let $\mathscr{B}_x$ be a local base for x. Then the following are equivalent

a) *For every $V \in \mathscr{U}_x$ there exists N such that*

$$n \geq N \implies a_n \in V$$

b) *For every $V \in \mathscr{B}_x$ there exists N such that*

$$n \geq N \implies a_n \in V$$

c) *The function*

$$\begin{aligned} \mathbb{N} \cup \{\infty\} &\to X \\ n &\to x_n \\ \infty &\to x \end{aligned}$$

is continuous at ∞ with respect to the topology on $\mathbb{N} \cup \{\infty\}$ given by open sets of the form $\{N, N+1, \dots, \} \cup \{\infty\}$ and arbitrary subsets of $\mathbb{N}$.

In this case we say that $x_n \to x$.

Proposition 4.1.32 (Continuous $\implies$ Sequentially Continuous)
Let $f : X \to Y$ be a continuous map and $x_n \to x$ a sequence in X. Then $f(x_n) \to f(x)$.

Proof. If we regard the sequence as a continuous map $\mathbb{N} \cup \infty$ (4.1.31) then the result follows from (4.1.24). □

Proposition 4.1.33 (Limits are Unique in Kolmogorov Spaces)
Let X be a Kolmogorov topological space. Then limits of sequences are unique.

Proposition 4.1.34 (Sequentially Continuous $\implies$ Continuous)
Let X, Y be topological spaces, $f : X \to Y$ a map and $x \in X$ a point with a countable *local base $\mathscr{B}_x$. Suppose that for all sequences $x_n \to x$ we have $f(x_n) \to f(x)$. Then f is continuous at x.*

In particular if X is first countable then $f : X \to Y$ is continuous iff it is sequentially continuous.

Proof. Consider a point $x \in X$ and $y := f(x)$. By hypothesis $\mathscr{B}_x = \{U_n\}$ is countable. By replacing with the base $U'_n := \bigcap_{k=1}^{n} U_k$ we may suppose that

$$U_1 \supseteq U_2 \dots \supseteq U_n \supseteq \dots$$

is decreasing. Suppose f is not continuous at x then by (4.1.23).d) there exists $V \in \mathscr{U}_{f(x)}$ such that $f(U_n) \setminus V \neq \emptyset$ for all n. Therefore we may choose $x_n \in U_n$ such that $f(x_n) \notin V$. Consider $U \in \mathscr{U}_x$ then by definition there is some N such that $U_N \subseteq U$. Furthermore $n \geq N \implies U_n \subseteq U_N \subseteq U \implies x_n \in U$. Therefore $x_n \to x$. By construction $f(x) \in V$ but $f(x_n) \notin V$ for all n and in particular $f(x_n) \not\to f(x)$. □

4.1.7 Irreducible Topological Spaces

References :

a) [Bou98a, Chapter II §4.2]

b) [Sta15, 004U]

Proposition 4.1.35 (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. *a)* $\implies$ *b)* Suppose U, V are open sets such that $U \cap V = \emptyset$. Then $X = (X \setminus U) \cup (X \setminus V)$. By hypothesis $X = (X \setminus U)$ or $X = (X \setminus V)$ whence either U or V is empty.

b) $\implies$ *a)* Similar.

c) $\iff$ *b)* Follows directly from (4.1.22) □

Proposition 4.1.36 (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 4.1.37
*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 (4.1.36). □

Remark 4.1.38
Singletons $\{x\}$ are always irreducible.

Definition 4.1.39 (Irreducible Component)
We say that Y is an irreducible component if it is a maximal irreducible subset.

Proposition 4.1.40
Let $f : X \to Y$ be a continuous map and $Z \subset X$ irreducible. Then $f(Z)$ is irreducible in Y.

Proof. Suppose $f(Z) \subset Y_1 \cup Y_2$ for Y_1, Y_2 closed. Then $Z \subset f^{-1}(f(Z)) \subset f^{-1}(Y_1) \cup f^{-1}(Y_2)$. Then by (4.1.36).b) wlog $Z \subset f^{-1}(Y_1)$ therefore $f(Z) \subset f(f^{-1}(Y_1)) \subset Y_1$. Therefore by the same criterion $f(Z)$ is irreducible. □

Proposition 4.1.41
Let $Y \subset X$. Then Y is irreducible iff $\overline{Y}$ is.

Proof. This follows from (4.1.36).b) and (4.1.18) that $Y \subset Z \iff \overline{Y} \subset Z$. □

Proposition 4.1.42 (Decomposition into Irreducible Components)
A topological space X may be decomposed into irreducible components. More precisely

a) *Every irreducible component is closed*

b) *Every irreducible closed subset is contained in an irreducible component*

c) *X is the union of irreducible components*

Proof. We prove each in turn

a) By (4.1.41) $\overline{Y}$ is irreducible and closed, so by maximality $Y = \overline{Y}$ is closed.

b) We may show that the lattice of closed subsets is chain complete so we may use to show that the lattice of irreducible closed subsets is also chain complete (2.4.4). Therefore we may apply Theorem 2.1.55 to find an irreducible component.

c) As $\{x\}$ is irreducible every element is contained in an irreducible component by b).

□

Corollary 4.1.43
For $x \in X$ the closure $\overline{\{x\}}$ is an irreducible closed subset.

Corollary 4.1.44
X is irreducible if and only if it has a single irreducible component.

Definition 4.1.45 (Generic Point)
Let Z be an irreducible closed subset of X, then we say $\eta \in X$ is a generic point of Z if

$$Z = \overline{\{\eta\}}$$

Proposition 4.1.46
Let X be an irreducible space then every open subset U is irreducible.

Proof. By (4.1.35) U is dense in X. Therefore by (4.1.41) U is irreducible. □

Proposition 4.1.47
Let $X = \bigcup_{i=1}^{n} X_i$ where X_i are irreducible closed subsets, and mutually incomparable. Then the X_i are the irreducible components of X.

Proof. For any irreducible closed subset E we have by (4.1.42) $E \subset X_i$ for some i. In particular every irreducible component is contained in some X_i. On the other hand every X_j is contained in an irreducible component. By incomparability we deduce that each X_i is an irreducible component, and that the set is complete. □

Proposition 4.1.48
Let $Y \subset X$ such that $Y = \bigcup_{i=1}^{n} Y_i$ where Y_i are the irreducible components of Y. Then the set of irreducible components of $\overline{Y}$ is $\{\overline{Y_i}\}_{i=1\dots n}$, and these are distinct.

Proof. By (4.1.41) $\overline{Y_i}$ are irreducible subsets which, by (4.1.21) cover $\overline{Y}$. By (4.1.42) Y_i is closed in Y and so by (4.1.20) $\overline{Y_i} \cap Y = Y_i$. This shows that the $\overline{Y_i}$ are distinct and also incomparable. Then (4.1.47) shows that these must be the irreducible components. □

Proposition 4.1.49
Let $U \subset X$ be an open subset. There is an order isomorphism

$$\begin{array}{ccc} \{Y \subset U \mid Y \text{ irreducible, closed and non-empty}\} & \longleftrightarrow & \{Z \subset X \mid Z \text{ irreducible and closed and } Z \cap U \neq \emptyset\} \\ Y & \to & \mathrm{cl}_X(Y) \\ Z \cap U & \leftarrow & Z \end{array}$$

which restricts to irreducible components.

Proof. By (4.1.41) the first map is well-defined. Conversely $Z \cap U$ is closed in Y and open in Z, so irreducible by (4.1.46).

By (4.1.35) $Z \cap U$ is dense in Z, that is $Z = \mathrm{cl}_Z(Z \cap U) \overset{(4.1.20)}{=} \mathrm{cl}_X(Z \cap U) \cap Z \implies Z \subset \mathrm{cl}_X(Z \cap U)$, and so by minimality they are equal.

By (4.1.20) $\mathrm{cl}_X(Y) \cap U = \mathrm{cl}_U(Y) = Y$. Therefore the maps are mutually inverse and order preserving. □

4.1.8 Noetherian Topological Spaces

Definition 4.1.50 (Noetherian)
*A topological space X is **Noetherian** if the lattice of closed subsets is Artinian (i.e. satisfies the descending chain condition).*

Proposition 4.1.51 (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 (4.1.37) and (2.4.7). □

Proposition 4.1.52
Let X be a Noetherian topological space and $Y \subset X$. Then Y is Noetherian.

Proposition 4.1.53
Let $X = \bigcup_{i=1}^{n} X_i$ be topological space such that X_i is Noetherian. Then X is Noetherian.

Proposition 4.1.54
Let X be a Noetherian topological space and $U \subset X$ an open subset. Then there is a bijection

$$\begin{array}{ccc} \{Y \subset U \mid Y \text{ closed and non-empty}\} & \longleftrightarrow & \{Z \subset X \mid Z \text{ closed and every irreducible component meets } U\} \\ Y & \to & \mathrm{cl}_X(Y) \\ Z \cap U & \leftarrow & Z \end{array}$$

which is order preserving and restricts to closed irreducible subsets and irreducible components.

Proof. By (4.1.52) and (4.1.51) $Y = Y_1 \cup \ldots \cup Y_n$ where Y_i are the irreducible components of Y. Then by (4.1.48) the irreducible components of $\overline{Y}$ are $\overline{Y_i}$, which evidentally intersect U. Furthermore by definition $Z \cap U$ is closed in U and the maps are well-defined.

By (4.1.49) the maps restricts to closed irreducible subsets (resp. components) and are bijections, in particular for Z irreducible closed we have $\overline{Z \cap U} = Z$.

By (4.1.20) $\overline{Y} \cap U = Y$. For the case Z is closed then as before $Z = Z_1 \cup \ldots \cup Z_n$ is a decomposition into irreducible components. By assumption $Z_i \cap U \neq \emptyset$. Therefore by (4.1.21)

$$\overline{Z \cap U} = \overline{Z_1 \cap U} \cup \ldots \cup \overline{Z_n \cap U} = Z_1 \cup \ldots \cup Z_n = Z$$

as required. □

4.1.9 Krull Dimension

References :

- Éléments de géométrie algébrique IV [Gro64, Chap. 0 §**14.4.1**]
- Some remarks on biequidimensionality of topological spaces and Noetherian schemes [Hei17]

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 (4.1.37). Therefore we may use the notions of Krull Lattice developed in Section 2.5.

Definition 4.1.55 (Chain of irreducibles)
*Let X be a Noetherian topological space. A **chain** of irreducible closed 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 4.1.56 (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 closed subsets. Note this may be ∞.*
- *The **height** or **codimension** of an irreducible closed subset $Y \subseteq X$, denoted $\mathrm{codim}(Y, X)$, 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 closed 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 4.1.57 (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 4.1.58 (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 4.1.59 (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* $\operatorname{codim}(Y, Z)$

*Observe that **quasi-biequidimensional** + **equidimensional** $\iff$ **biequidimensional** and **irreducible** $\implies$ **equidimensional***

Proposition 4.1.60 (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 (2.5.11) to the topological case. □

Proposition 4.1.61 (Codimension Formula)
Suppose X is a quasi-biequidimensional topological space. Then for $Z \subset Y$ closed subsets

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

Further every closed subset is also quasi-biequidimensional.

Proof. This follows from (2.5.13) and (2.5.15). □

Proposition 4.1.62
Suppose $X = \bigcup_{i \in I} U_i$. Then $\dim X = \sup_{i \in I} \dim U_i$.

Proof. By (4.1.49) a chain of irreducible closed subsets of U_i lifts to a chain of the same length in X. Therefore $\dim U_i \leq \dim X$ for all $i \in I$ whence $\sup_{i \in I} \dim U_i \leq \dim X$. Similarly given a chain of irreducible closed subsets

$$X_0 \subsetneq \ldots \subsetneq X_n \subseteq X$$

choose i such that $X_0 \cap U_i \neq \emptyset$. Then (4.1.54) shows that this restricts to a chain of the same length in U_i. Therefore $\dim X \leq \dim U_i \leq \sup_{i \in I} \dim U_i$. □

4.1.10 Product Topology

Definition 4.1.63 (Product Topology)
*Let $\{X_i\}_{i \in I}$ be a family of topological spaces. The **product topology** is the topology generated by the base of open sets of the form*

$$\prod_{i \in I} U_i$$

where $U_i \subset X_i$ is open and only finitely many are proper subsets of X.

Proposition 4.1.64
Let $\{X_i\}_{i \in I}$ be family of topological spaces. The family of sets given in (4.1.63) is a base. The topology generated is the smallest family of subsets for which the projection maps

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

are continuous. Furthermore if each X_i is Hausdorff (resp. Kolmogorov), then so is the product.

Proposition 4.1.65 (Product of Sequences)
Let $X_1, \ldots, X_m$ be a family of topological spaces and $a_n^i \to \alpha^i$ for $i = 1 \ldots m$. Then $(a_n^1, \ldots, a_n^m) \to (\alpha^1, \ldots, \alpha^m)$.

Proposition 4.1.66 (Diagonal is Closed)
Let X be a topological space. Then X is Hausdorff if and only if $\{(x, x) \mid x \in X\}$ is closed in $X \times X$.

Proposition 4.1.67
Let $f, g : X \to Y$ be continuous maps and Y a Hausdorff space. Then

$$\{x \in X \mid f(x) = g(x)\}$$

is closed.

Proof. The level set is $(f \times g)^{-1}(\Delta_Y)$ which by (4.1.66) is closed. □

4.1.11 Compactness

Definition 4.1.68 (Cluster Point of a Sequence)
Let (x_n) be a sequence in a topological space X. We say that $x \in X$ is

a) *a **cluster point** (or **accumulation point**) of x_n if for every $U \in \mathscr{O}_x$ the set $\{m \in \mathbb{N} \mid x_m \in U\}$ is infinite*

b) *a **subsequential limit** of x_n if there exists some subsequence $x_{n_k} \to x$*

In general the the latter implies the former, and if X is first countable the concepts are equivalent as we will see.

Lemma 4.1.69 (Cluster Point is Subsequential Limit Point)
Let X be a first countable topological space and x a cluster point of a sequence (x_n). Then there exists some subsequence x_{n_k} such that $x_{n_k} \to x$.

Proof. Let (U_n) be a local base at x. By replacing it with $U'_n := U_1 \cap \ldots \cap U_n$ we may assume it is without loss of generality decreasing. Define $n_0 = 0$ and n_k inductively by

$$n_k := \min\{m > n_{k-1} \mid x_m \in U_k\}$$

which is well-defined precisely because x is a cluster point. Then $x_{n_k} \in U_k$ which shows that $x_{n_k} \to x$ as required. □

Definition 4.1.70
Let X be a topological space. We say it is

a) ***Compact*** *if every open cover of X has a finite subcover*

b) ***Countably Compact*** *if every* countable *open cover of X has a finite subcover*

c) ***Sequentially Compact*** *if every sequence (x_n) in X has a convergent subsequence*

Proposition 4.1.71 (Criteria for Countable Compactness)
Let X be a topological space. Then the following are equivalent

a) *X is countably compact*

b) *Let $\{Z_n\}_{n\in\mathbb{N}}$ be a countable collection of closed subsets such that every finite set has non-empty intersection. Then the intersection $\bigcap_{n\in\mathbb{N}} Z_n$ is non-empty*

c) *For every increasing sequence of proper open subsets*

$$U_1 \subseteq U_2 \subseteq \ldots \subseteq U_n \subseteq \ldots$$

the union $\bigcup_{n=1}^{\infty} U_n$ is proper.

d) *For every decreasing sequence of non-empty closed subsets*

$$Z_1 \supseteq Z_2 \supseteq \ldots \supseteq Z_n \supseteq \ldots$$

the intersection $\bigcap_{n=1}^{\infty} Z_n$ is non-empty

Proof. *a)* $\iff$ *b)* and *c)* $\iff$ *d)* are just demorgans law. For *a)* $\implies$ *c)* suppose $\bigcup_{n=1}^{\infty} U_n = X$ then by assumption $U_{n_1} \cup \ldots \cup U_{n_k} = X$, and by the increasing assumption $U_{n_k} = X$ which is a contradiction.

For *c)* $\implies$ *a)*, suppose we have an open cover $X = \bigcup_{n=1}^{\infty} U_n$ define the increasing open cover

$$U'_n := \bigcup_{i=1}^{n} U_i$$

by the contrapositive U'_n is not proper for some n, which means precisely that there is a finite subcover. □

Proposition 4.1.72
Let X be a topological space. Then sequentially compact $\implies$ countably compact. Under the assumption of first countability the converse holds.

Proof. $\implies$) Consider a countable open cover $X = \bigcup_{n=1}^{\infty} U_n$ with no finite subcover. Then there exists $x_n \in X \setminus \bigcup_{i=1}^{n} U_i$. By assumption there is a convergent subsequence $x_{n_k} \to x$. We have $x \in U_N$ for some N but $n_k \geq N \implies x_{n_k} \notin U_N$.

$\impliedby$) Consider a sequence (x_n) and define

$$Z_n := \overline{\{x_k : k > n\}}$$

which is a decreasing sequence of non-empty closed subsets. By the countable compactness criteria (4.1.71) $Z := \bigcap_{n=1}^{\infty} Z_n$ is non-empty. However we may show this is precisely the set of cluster points of (x_n), i.e. there exists a cluster point $x \in Z$. By (4.1.69) there exists a subsequence such that $x_{n_k} \to x$ as required. □

Lemma 4.1.73 (Lindelof Lemma)
Let X be a second countable topological space. Then every open cover has a countable subcover.

Proof. Let $\mathcal{B}$ be a countable base and $\{U_\alpha\}_{\alpha\in\mathcal{A}}$ an open cover of X. Note for every U_α we have some subfamily $\mathcal{B}_\alpha \subset \mathcal{B}$ such that $U_\alpha = \bigcup \mathcal{B}_\alpha$. Consider $\mathcal{B}' := \bigcup\{B_\alpha \mid \alpha \in \mathcal{A}\} \subset \mathcal{B}$. By definition for every $V \in \mathcal{B}'$ we have $V \subset U_\alpha$ for some $\alpha \in \mathcal{A}$. In otherwords there exists a map $f : \mathcal{B}' \to \mathcal{A}$ such that $V \subset U_{f(V)}$. We may verify that $\{U_\alpha\}_{\alpha\in \mathrm{Im}(f)}$ is a countable subcover. □

We summarise the relationships between the concepts

Proposition 4.1.74
Let X be a topological space. Then

a) *Compact, Sequentially Compact $\implies$ Countably compact*

b) *First Countable and (Countably) Compact $\implies$ Sequentially Compact*

c) *Second Countable and Countably or Sequentially Compact $\implies$ Compact*

Proof. a) The first implication is obvious and the second implication is (4.1.72)

b) This is (4.1.72)

c) This follows from (4.1.73) and a)

□

Proposition 4.1.75 (Compact subsets of Hausdorff Spaces are Closed)
Let X be a Hausdorff topological space and $Y \subset X$ a subset compact with respect to the subspace topology. Then Y is closed.

Proof. Fix $x \in X \setminus Y$. Then for every $y \in Y$ by assumption there exists disjoint open subsets $x \in U_y$ and $y \in V_y$. Then $\{V_y \cap Y \mid y \in Y\}$ is an open cover for Y, so there exists a finite set of points $y_1, \ldots, y_n$ such that $Y \subseteq V_{y_1} \cup \ldots \cup V_{y_n}$. Furthermore

$$U := U_{y_1} \cap \ldots \cap U_{y_n}$$

is an open neighbourhood of x disjoint from each V_{y_i} and therefore disjoint from Y. By (4.1.18) we see that $x \notin \overline{Y}$, which shows $Y = \overline{Y}$, i.e. Y is closed. □

Proposition 4.1.76 (Closed subsets of Compact Spaces are Compact)
Let X be a compact topological space and $Y \subset X$ a closed subset. Then Y is compact under the subspace topology.

Proof. Let $\mathcal{U} := \{U_\alpha\}_{\alpha\in\mathcal{A}}$ be an open cover for Y. Then by definition $U_\alpha = U'_\alpha \cap Y$. where $U'_\alpha \subset X$ are open. Evidently

$$\mathcal{U}' : \{U'_\alpha\}_{\alpha\in\mathcal{A}} \cup \{X \setminus Y\}$$

is an open cover of X. Therefore by assumption it has a finite subcover, which immediately yields a finite subcover of X as required. □

Proposition 4.1.77 (Image of a Compact Space is Compact)
Let $f : X \to Y$ be a continuous map of topological spaces where X is compact. Then the image $f(X)$ is compact.

Further if Y is Hausdorff then f is an open map (i.e. $f(U)$ is open for every open $U \subset X$). If in addition f is injective then it is a homeomorphism onto its image.

Proof. We may assume without loss of generality that $f(X) = Y$. Let $\{U_\alpha\}_{\alpha\in\mathcal{A}}$ be an open cover of Y. In otherwords $f(X) \subseteq \bigcup_{\alpha\in\mathcal{A}} U_\alpha \implies X \subseteq \bigcup_{\alpha\in\mathcal{A}} f^{-1}(U_\alpha)$. By assumption we have a finite subcover

$$X \subseteq f^{-1}(U_{\alpha_1}) \cup \ldots \cup f^{-1}(U_{\alpha_n})$$

which implies

$$f(X) \subseteq U_{\alpha_1} \cup \ldots \cup U_{\alpha_n}$$

since f is assumed to be surjective, and we see that $f(X)$ is compact. □

Analogously we have similar results for sequentially compact spaces, which may be conceptually simpler.

Proposition 4.1.78
Let X be a first countable Kolmogorov space and $Y \subset X$ a subset of a sequentially compact with respect to the subspace topology. Then Y is closed.

Proof. Consider $x \in \overline{Y}$ then by (4.1.18) there is some sequence $x_n \to x$. Further by assumption there is some subsequence $x_{n_k} \to y \in Y$. By uniqueness of limits (4.1.33) we have $x = y$, and in particular $\overline{Y} = Y$ is closed. □

Proposition 4.1.79
Let X be a sequentially compact topological space, and $Y \subset X$ a closed subset. Then Y is sequentially compact.

Proof. Let $x_n \in Y$ be a sequence. By assumption it has a convergent subsequence $x_{n_k} \to x$ where $x \in X$. By (4.1.17) x is an adherent point of Y and therefore lies in Y by (4.1.18). □

Proposition 4.1.80
Let $f : X \to Y$ be a continuous map of topological spaces where X is sequentially compact. Then the image $f(X)$ is sequentially compact.

Proof. Let $y_n = f(x_n)$ be a sequence in $f(X)$. Then by assumption $x_{n_k} \to x$, and therefore by (...) $y_{n_k} \to f(x)$. □

4.1.12 Connectedness

Definition 4.1.81
*We say a topological space X is **disconnected** if $X = U \cup V$ for two non-empty, disjoint open subsets U, V. Otherwise we say X is connected.*

Proposition 4.1.82
Let X be a topological space. The following are equivalent

a) *X is connected*

b) *The only subsets which are both open and closed are X and $\emptyset$*

Proposition 4.1.83
Let $f : X \to Y$ be a continuous map and X connected. Then $f(X)$ is also connected.

4.1.13 Order Topology

Definition 4.1.84 (Order Topology)
*Let $(X, \leq)$ be a totally ordered set. Then the **order topology** is the topology generated by the subbase of half-open intervals*

$$\{y \in X \mid y < x\} \text{ and } \{y \in X \mid y > x\}$$

for $x \in X$.

Proposition 4.1.85 (Base for order topology)
Let $(X, \leq)$ be a totally ordered set. Then the sets of the form

$$\{y \in X \mid y < x\}, \{y \in X \mid y > x\} \text{ and } \{y \in X \mid x < y < z\}$$

for $x, z \in X$ constitute a base for the order topology.

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 and $Z \subset X$ an irreducible subset. Define the stalk $\mathcal{F}_Z$ to be the directed limit

$$\mathcal{F}_Z := \varinjlim_{Z\cap U\neq\emptyset} \mathcal{F}(U)$$

under the directed system $\{\mathcal{F}(U) \to \mathcal{F}(V)\}_{V\subseteq U}$. Note this is directed by (4.1.36).c) because open sets intersecting Z are closed under finite intersection. Explicitly this may be constructed as

$$\mathcal{F}_Z := \{(U, \sigma) \mid \sigma \in \mathcal{F}(U)\}/\sim$$

where $(U, \sigma) \sim (V, \tau)$ if there is an open set W such that $Z \subset W \subset U \cap V$ and $\sigma|_W = \tau|_W$. It comes equipped with a family of morphisms $\rho_{U,Y} : \mathcal{F}(U) \to \mathcal{F}_Z$ such that

$$\rho_{V,Z} \circ \rho_{UV} = \rho_{U,Z}$$

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 $\phi_Z : \mathcal{F}_Z \to A$ such that $\phi_U = \phi_Y \circ \rho_{U,Z}$.

As a special case we may consider $Z = \{x\}$ and write this as $\mathcal{F}_x$.

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 (4.1.6) 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 (4.1.6) 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 $Z \subset X$ irreducible there is a unique morphism

$$\rho_Z : (f_\star \mathcal{F})_{f(Z)} \to \mathcal{F}_Z$$

such that $\rho_Z(\sigma_{f(Z)}) = \sigma_Z$ for all $\sigma \in \mathcal{F}(f^{-1}V)$ and V nbhds of $f(Z)$.

Proposition 4.2.11 (Sheafification)
Given a $\mathcal{B}$-presheaf $\mathcal{F}$ define the sheafification $\mathcal{F}^+$ on $\mathcal{T}_X$ by

$$\mathcal{F}^+(U) := \left\{(s_x)_{x\in U} \mid s_x \in \mathcal{F}_x \text{ s.t. } s_x = (\sigma_i)_x \quad \forall x \in U_i \text{ and some } \sigma_i \in \mathcal{F}(U_i) \text{ where } U = \bigcup_{i\in I} U_i\right\}$$

We say the section s is determined by the sections $\{(U_i, \sigma_i)\}_{i\in I}$. 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

$$\begin{array}{rcl} \eta : \mathcal{F} & \longrightarrow & \left(\mathcal{F}^+\right)|_{\mathcal{B}} \\ \sigma & \to & (\sigma_x)_{x\in U} \end{array}$$

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

$$\begin{array}{rcl} \mathrm{Mor}(\mathcal{F}^+, \mathcal{G}) & \xrightarrow{\sim} & \mathrm{Mor}(\mathcal{F}, \mathcal{G}|_{\mathcal{B}}) \\ \alpha & \longrightarrow & \alpha|_{\mathcal{B}} \circ \eta_{\mathcal{F}} \\ \epsilon_{\mathcal{G}} \circ \beta^+ & \longleftarrow & \beta \end{array}$$

where we have used the counit natural transformation, which is infact an isomorphism,

$$\begin{array}{rcl} \epsilon_{\mathcal{G}} : (\mathcal{G}|_{\mathcal{B}})^+ & \xrightarrow{\sim} & \mathcal{G} \\ (\rho_x(\sigma_x)) & \longleftarrow & \sigma \end{array}$$

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

$$\mathrm{Sh}(X; \mathcal{B}) \underset{(-)^+}{\overset{(-)|_{\mathcal{B}}}{\leftrightarrows}} \mathrm{Sh}(X)$$

Proposition 4.2.15
Let $\mathcal{F}$ be a sheaf on X, $U \subset X$ an open subset and $W \subset X$ an irreducible subset such that $U \cap W \neq \emptyset$. Then $U \cap W$ is irreducible and there is a canonical isomorphism

$$\begin{aligned} (\mathcal{F}|_U)_{U \cap W} &\xrightarrow{\sim} \mathcal{F}_W \\ (V, \sigma) &\to [(V, \sigma)] \end{aligned}$$

Proof. The set $Z := X \setminus U$ is closed. Suppose that $U \cap W \subset Z_1 \cup Z_2$ for Z_1, Z_2 closed in X. Then

$$W \subset (U \cap W) \cup Z \subset (Z_1 \cup Z) \cup (Z_2 \cup Z)$$

By hypothesis $W \subset Z_1 \cup Z$ say. Then evidentally $U \cap W \subset Z_1$. Therefore we deduce $U \cap W$ is irreducible by (4.1.36).

Let $(V, \sigma) \in \mathcal{O}_{X,W}$ then by definition $V \cap W \neq \emptyset$. So by (4.1.36) $U \cap V \cap W \neq \emptyset$. Therefore $(V \cap U, \sigma|_{V \cap U}) \in \mathcal{O}_{U,U \cap W}$ and the image is (V, σ), so the map is surjective. Injectivity is straightforward, as is the fact it is an isomorphism. □

4.3 Locally Ringed Spaces

It's possible to abstract the notion of differentiable functions on a manifold 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 $\mathcal{O}_{X,Z}$ are local rings for all irreducible subsets $Z \subset X$.

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 irreducible $Z \subset X$ the composite map

$$f^\sharp_Z : \mathcal{O}_{Y,f(Z)} \longrightarrow (f_\star \mathcal{O}_X)_{f(Z)} \overset{4.2.10}{\longrightarrow} \mathcal{O}_{X,Z}$$

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

Analysis

The first task is to define the field of real numbers $\mathbb{R}$, having already constructed the rational numbers $\mathbb{Q} = \text{Frac}(\mathbb{Z})$. Typically this is done by some axiomatisation as an ordered field containing $\mathbb{Q}$ for which every bounded subset has a supremum (**Dedekind Completeness**). We show $\mathbb{R}$ is unique such ordered field.

5.1 Real Numbers

Definition 5.1.1 (Ordered Ring / Field)
*An **ordered ring** is a ring $(A, +, \cdot)$ such that the additive group $(A, +)$ is an ordered abelian group with ordering $\leq$ which also satisfies*

$$x, y \geq 0 \implies x \cdot y \geq 0$$

*An **ordered field** is a field with the structure of an ordered ring.*

Proposition 5.1.2 (Extension to Field of Fractions)
Let A be an ordered ring with no zero-divisors. The $K = \text{Frac}(A)$ is an ordered ring with the order given by

$$\frac{x}{y} \leq \frac{w}{z} \iff xz \leq wy$$

Example 5.1.3
$\mathbb{Z}$ is an ordered ring and $\mathbb{Q} := \text{Frac}(\mathbb{Z})$ is an ordered field.

Proposition 5.1.4 (Trichotomy Law)
Let G be an ordered abelian group. Then G is the disjoint union of $\{0\}$, G^+ and G^-.

More generally precisely one of $x = y$, $x < y$ and $x > y$ holds.

Lemma 5.1.5 (Elementary Properties)
Let G be an ordered abelian group. Then

a) $x \in G^+ \iff -x \in G^-$

b) $x \in G^+$ *and* $x \leq y \implies y \in G^+$

c) $x \in G^-$ *and* $y \leq x \implies x \in G^-$

d) $x, y \in G^+ \implies x + y \in G^+$

e) $x, y \in G^- \implies x + y \in G^-$

f) $x, y \in G^+ \implies xy \in G^+$

Proof. a) $x \in G^+ \implies 0 \leq x \implies -x \leq 0$. Furthermore $x \neq 0 \implies -x \neq 0$ by assumption so $-x \in G^-$.

b) By transitivity $0 \leq y$. Suppose $y = 0$ then $0 \leq x \leq 0$ so $x = 0$ a contradiction.

c) Similarly

d) Follows from *b*) since $0 \leq x \implies 0 \leq y \leq x + y$.

e) Follows from *c*) since $x \leq 0 \implies x + y \leq y \leq 0$.

f) If $xy = 0 \implies x = 0$ or $y = 0$ which is a contradiction. Therefore $xy > 0$.

□

Proposition 5.1.6 (Ordered Rings are Torsion Free)
Let A be a non-zero ordered ring. Then the canonical map $\mathbb{Z} \to A$ is injective, in other words A has characteristic 0.

In particular every ordered field K contains $\mathbb{Q}$ as a subring.

Proof. Follows immediately by induction, since if $n.1 = 0$ then $(n-1) > n \implies 1 < 0 \implies -1 > 0 \implies 1 = -1 * -1 < 0$ a contradiction. □

Proposition 5.1.7 (Archimedean Field)
Let K be an ordered field. Then the following are equivalent

a) *$\mathbb{Q}$ is dense in K i.e. for all $x, y \in K$ there exists $z \in \mathbb{Q}$ such that $x < z < y$*

b) *For all $x, y \in K$ there exists $n \in \mathbb{N}$ such that $ny > x$*

*In this case we say K is **Archimedean**.*

In particular for every $\epsilon \in K^+$ there exists $n \in \mathbb{N}^+$ such that $\frac{1}{n} < \epsilon$.

Proof. Suppose the second property is satisfied then choose $n > \frac{1}{y-x}$. By definition $0 < \frac{1}{n} < y - x$. Let

$$S = \left\{ m \in \mathbb{Z} \mid \frac{m}{n} \leq x \right\}$$

By the Archimedean property (applied to $\frac{1}{n}$ and $-x$) S is non-empty. By the well-ordering principle it has a maximal element. By maximality $\frac{m+1}{n} > x$. Furthermore

$$x < \frac{m+1}{n} \leq x + \frac{1}{n} < x + (y - x) = y$$

and therefore $z := \frac{m+1}{n}$ satisfies the required property.

Conversely suppose K satisfies the first property and assume wlog that $x, y > 0$. Choose $\frac{m}{n}$ such that

$$0 < \frac{m}{n} < \frac{y}{x}$$

which implies $ny > mx \geq x$. □

Definition 5.1.8 (Absolute Value)
*Let G be an **ordered abelian group**. Define the absolute value as*

$$|x| := \begin{cases} x & x \in G^+ \\ -x & x \in G^- \\ 0 & x = 0 \end{cases}$$

Then this satisfies the following properties

a) $|x| \geq 0$

b) $|-x| = |x|$

c) $|x| = 0 \iff x = 0$

d) $||x| - |y|| \leq |x + y| \leq |x| + |y|$

Proposition 5.1.9 (Topology of Ordered Abelian Group)
Let G be an ordered abelian group. Then $U \subset G$ is open in the order topology iff

$$\forall x \in U \exists \epsilon \in G^+ \text{ s.t. } |y - x| < \epsilon \implies y \in U$$

Proof. Let $\mathcal{B}$ be the basis defined in (4.1.85). Recall (...) that U is open iff for all $x \in U$ there exists $V \in \mathcal{B}$ such that $x \in V \subseteq U$. If $U \subset G$ satisfies the given condition holds then evidently $x \in \{g \in G \mid y - \epsilon < g < y + \epsilon\}$ which is an element of $\mathcal{B}$. Conversely if $x \in V$ with $V = \{g \in G \mid y < g < z\}$, then we may define $\epsilon = \min(z - x, x - y)$. □

5.1.1 Sequences in an Ordered Field

Proposition 5.1.10
The order topology on an ordered field K is Hausdorff.

Proposition 5.1.11 (Convergent Sequence)
Let K be an ordered field and (a_n) in K a sequence. Then the following are equivalent

a) $a_n \to \alpha$ *in the sense of (4.1.31)*

b) *For all $\epsilon \in K^+$ there exists $N(\epsilon) \in \mathbb{N}$ such that $n \geq N(\epsilon) \implies |a_n - \alpha| < \epsilon$*

As K is Hausdorff limits are unique. When K is Archimedean it is sufficient to consider the case $\epsilon := \frac{1}{N}$ for all positive integers N.

Definition 5.1.12 (Convergent Sequence)
*Let K be an ordered field. We say that a sequence $(a_n)_{n\in\mathbb{N}^+}$ is **cauchy** if for all $\epsilon > 0$ there exists $N(\epsilon) > 0$ such that*

$$\forall m, n \in \mathbb{N} : (m, n \geq N(\epsilon) \implies |a_n - a_m| < \epsilon)$$

If K is Archimedean then it is sufficient to demonstrate this only for ϵ of the form $\frac{1}{N}$.

Proposition 5.1.13
Let K be an ordered field. Then every convergent sequence is cauchy.

Proof. Given $\epsilon > 0$ then $\frac{\epsilon}{2} > 0$. Therefore there exists N such that

$$n \geq N \implies |a_n - \alpha| < \frac{\epsilon}{2}$$

Then by the triangle inequality

$$n, m \geq N \implies |a_n - a_m| < \epsilon$$

□

Definition 5.1.14 (Sequentially Completeness)
*We say an ordered field K is **sequentially complete** if every cauchy sequence is convergent.*

Proposition 5.1.15 (Completeness)
Let K be an ordered field. The following conditions are equivalent

a) *Every non-empty subset $X \subset K$ bounded above admits a supremum $\sup X \in K$*

b) *Every non-empty subset $X \subset K$ bounded below admits an infimum $\inf X \in K$*

*In this case we say that K is **complete**.*

Proof. $\inf X = -\sup(-X)$ and vice versa. □

Lemma 5.1.16
*Let K be a complete ordered field. Then K is also **Archimedean***

Proof. Suppose K is not Archimedean then $\mathbb{Z}^+$ is bounded above and in particular has a supremum α. Then for every $n \in \mathbb{Z}^+$ we have $n + 1 \leq \alpha \implies n \leq \alpha - 1$, which contradicts maximality. □

Lemma 5.1.17
Let $X \subset K$ be a subset of an Archimedean ordered field which is "upwards closed" and bounded below (resp. " downwards closed" and bounded above).

Then for every $\epsilon \in K^+$ there exists an $x \in X$ such that $x - \epsilon \notin X$ (resp. $x + \epsilon \notin X$)

Proof. By (5.1.7) there is some $n \in \mathbb{N}^+$ such that $0 < \frac{1}{n} < \epsilon$. Consider the set

$$\mathcal{S} := \{k \in \mathbb{Z} \mid \frac{k}{n} \in X\}$$

As X is bounded below then so is $\mathcal{S}$. By the well ordering principle it has a minimal element, say k. Define $x := \frac{k}{n}$ and then $x - \epsilon < x - \frac{1}{n} = \frac{k-1}{n}$ which by minimality is not in X, whence neither is $x - \epsilon$. □

Lemma 5.1.18
Let $X \subset K$ be a non-empty subset for which $x := \sup X$ exists. Then there exists a sequence (a_n) in X such that $a_n \uparrow x$.

Proof. For every $n \in \mathbb{N}^+$ there exists some $a_n \in X$ such that $a_n > x - \frac{1}{n}$ (otherwise $x - \frac{1}{n}$ would be a smaller upper bound). Then evidently a_n is increasing. For every $\epsilon \in K^+$ there exists some N such that $0 < \frac{1}{N} < \epsilon$ by (5.1.7). Consequently

$$n \geq N \implies a_n > x - \frac{1}{N} \implies x \geq a_n > x - \epsilon \implies |a_n - x| < \epsilon$$

□

Definition 5.1.19 (Extended Real Line)
Let K be an ordered field and define the set

$$K^\sharp := K \cup \{-\infty\} \cup \{\infty\}$$

with the obvious total ordering and induced order topology. $K \subset K^\sharp$ has the subspace topology and every open subset is of the form

$$U, U \cup (x, \infty], U \cup [-\infty, x), U \cup [-\infty, x) \cup (y, \infty] .$$

If $X \subset K$ is a subset which is unbounded above (resp. below) then define $\sup X$ (resp. $\inf X$) to be ∞ (resp. $-\infty$).

Proposition 5.1.20 (Convergence to infinity)
Let K be an ordered field and $a_n \in K^\sharp$ a sequence. Then the following are equivalent

a) $a_n \to \infty$

b) *For all $\lambda \in K$ there exists N such that $n \geq N \implies a_n \geq \lambda$*

A similar statement holds for $-\infty$.

Lemma 5.1.21 (Limit of Bounded Sequence)
Let $a_n \leq b_n$ be sequences in $K^\sharp$ converging to α and β respectively. Then $\alpha \leq \beta$.

In particular if $a_n \downarrow \alpha$ then $\alpha \leq a_n$.

Proof. If $\beta = \infty$ then the result is vacuously true. If $\beta = -\infty$ then evidently $\alpha = -\infty$ also. Therefore we may assume that β is finite without loss of generality.

Suppose $\alpha > \beta$ and define $\epsilon = (\alpha - \beta)$. By assumption there exists some N such that

$$n \geq N \implies |a_n - \alpha| < \frac{\epsilon}{2} \wedge |b_n - \beta| < \frac{\epsilon}{2}$$

Then $a_n > \frac{\alpha+\beta}{2}$ and $b_n < \frac{\alpha+\beta}{2}$ which is a contradiction. □

5.1.2 Sequential Completeness

Lemma 5.1.22 (Monotone Convergence Theorem)
Let K be a complete ordered field and (a_n) an increasing (resp. decreasing) sequence in $K^\sharp$. Then $a_n \to \sup a_n$. This is finite if and only if a_n is bounded above (resp. below).

Proof. Suppose first that (a_n) is bounded above and define $\alpha := \sup\{a_n\}$. Then for every $\epsilon \in K^+$ there exists N such that $a_N > \alpha - \epsilon$ (for otherwise $\alpha - \epsilon$ would be an upper bound). By assumption $n \geq N \implies \alpha - \epsilon < a_n \leq \alpha$ whence $|\alpha - a_n| < \epsilon$. Therefore $a_n \to \alpha$.

The case that (a_n) is unbounded above is trivial. □

Proposition 5.1.23 (Complete $\implies$ Sequentially Complete)
*Let K be an ordered field which is **complete**. Then it is **sequentially complete**.*

Proof. Let (a_n) be a cauchy sequence. There exists N such that $n \geq N \implies |a_n - a_N| < 1 \implies |a_n| \leq 1 + |a_N|$. Then $|a_n|$ is bounded by $\max(|a_1|, \ldots, |a_N| + 1)$. Consider the sequence

$$a_n^- := \inf_{k \geq n} a_k$$

Then a_n^- is bounded and increasing. Therefore $a_n^- \uparrow \alpha := \sup a_n^- < \infty$ by (5.1.22). For every $\epsilon \in K^+$ there exists N_1 such that $n \geq N_1 \implies \alpha - a_n^- < \epsilon$. There exists N_2 such that $n, m \geq N_2 \implies |a_n - a_m| < \epsilon$. By definition of a_n^-, for every $n \geq N_1$ there exists $m \geq N_1$ such that $|a_m - a_n^-| < \epsilon$. Consequently every $n \geq \max(N_1, N_2)$ there is some m such that

$$|\alpha - a_n| \leq \left|\alpha - a_n^-\right| + \left|a_n - a_n^-\right| \leq \left|\alpha - a_n^-\right| + |a_n - a_m| + \left|a_m - a_n^-\right| < 3\epsilon$$

As this is independent of m we see that $a_n \to \alpha$ as required. □

Proposition 5.1.24 (Sequentially Complete $\implies$ Complete)
*Let K be an Archimedean ordered field which is **sequentially complete**. Then K is **complete**.*

Proof. Let $X \subset K$ be a non-empty subset bounded above, and $\mathcal{U}$ the set of upper bounds for X, which in particular is bounded below. By assumption $\mathcal{U}$ is non-empty. For each $n \in \mathbb{N}^+$ we may choose $a_n \in \mathcal{U}$ such that $a_n - \frac{1}{2^n} \notin \mathcal{U}$ by (5.1.17). We may assume without loss of generality that a_n is decreasing by setting $a_n := \min_{n' \leq n} a_{n'}$. We argue that

$$a_n - a_{n+1} < \frac{1}{2^n}$$

for otherwise we see that $a_{n+1} \leq a_n - \frac{1}{2^n}$ which implies $a_{n+1} \notin \mathcal{U}$. Therefore by the triangle inequality applied repeatedly

$$m \geq n \implies |a_n - a_m| \leq \sum_{i=n}^{m-1} \frac{1}{2^i} < \frac{1}{2^{n-1}} < \frac{1}{n-1}$$

By the Archimedean property we see that the sequence is cauchy and therefore convergences to $\alpha \in K$. By (5.1.21) $\alpha \leq a_n$. We claim that $\alpha \in \mathcal{U}$. For suppose not then there exists $x \in X$ such that $x > \alpha$. Then there exists n such that $a_n - \alpha < x - \alpha \implies a_n < x$ which contradicts $a_n \in \mathcal{U}$. Suppose $\exists \alpha' \in \mathcal{U}$ such that $\alpha' < \alpha$. Then for some n we have $\frac{1}{n} < \alpha - \alpha'$ therefore $a_n - \frac{1}{2^n} \geq a_n - \frac{1}{n} \geq \alpha - \frac{1}{n} > \alpha'$. This would imply $a_n - \frac{1}{2^n} \in \mathcal{U}$, a contradiction. Therefore $\alpha' \geq \alpha$ and $\alpha = \sup X$ as required. □

5.1.3 Uniqueness of Reals

Lemma 5.1.25
Let K be a complete ordered field. Then every $x \in K$ satisfies

$$x = \sup \left\{ \frac{m}{n} \in \mathbb{Q} \mid \frac{m}{n} \leq x \right\}$$

Similarly for every $x \in K$ there is a sequence $a_n \in \mathbb{Q}$ such that $a_n \uparrow x$.

Proof. By assumption the supremum α exists. By definition x is an upper bound for the set so $\alpha \leq x$. Suppose $\alpha < x$ then by (5.1.7) there exists $\frac{m}{n}$ such that $\alpha < \frac{m}{n} < x$. On the other hand by definition $\frac{m}{n} \leq \alpha$, which is a contradiction. Therefore $\alpha = x$ as required.

The final statement follows from (5.1.18). □

Lemma 5.1.26
Let $\tau : K_1 \hookrightarrow K_2$ be an embedding of ordered fields with K_2 Archimedean. Suppose $x = \sup X$ for some subset $X \subset K_1$. Then $\tau(x) = \sup \tau(X)$.

Proof. Clearly $x' \in X \implies x' \leq x \implies \tau(x') \leq \tau(x) \implies \tau(x) \in \tau(X)^\uparrow$. Suppose $y \in \tau(X)^\uparrow$ and $y < \tau(x)$. Then by (5.1.7) there exists $z \in \mathbb{Q}$ such that $y < z < \tau(x)$. By the order preserving property we have $z \in X^\uparrow$ and $z < x$ which is a contradiction. Therefore $y \in \tau(X)^\uparrow \implies y \geq \tau(x)$ and $\tau(x) = \sup \tau(X)$. □

Proposition 5.1.27 (Uniqueness of Reals)
Let K_1, K_2 be complete ordered fields. Then there exists a unique ordered field embedding $K_1 \hookrightarrow K_2$, which is an isomorphism.

Proof. Let $\tau, \tau' : K_1 \to K_2$ be order embeddings. Then they agree on $\mathbb{Q}$. By (5.1.25) every x is the supremum of a set $X \subset \mathbb{Q}$. Then uniqueness follows from (5.1.26). The same result shows it is surjective.

For existence we claim that

$$\tau(x) := \sup \left\{ \frac{m}{n} \cdot 1_{K_2} \mid \frac{m}{n} \cdot 1_{K_1} \leq x \right\}$$

is a well-defined, order-preserving field isomorphism. Firstly x is bounded by some integer N so the supremum is well-defined. Similarly suppose $x' > x$ then by (5.1.7) we have $x < \frac{m}{n} < x'$. This shows that $\tau(x) \leq \frac{m'}{n'} \leq \tau(x')$ as required, whence τ is order preserving.

By (5.1.25) there exists $a_n, b_n \in \mathbb{Q}$ such that $a_n \uparrow x$, $b_n \uparrow y$ and by the triangle inequality $a_n + b_n \uparrow x + y$. We may show using the definition of τ that $a_n \uparrow \tau(x), b_n \uparrow \tau(y), a_n + b_n \uparrow \tau(x+y)$. Uniqueness of limits shows that $\tau(x+y) = \tau(x) + \tau(y)$. Similarly we may show that $\tau(xy) = \tau(x)\tau(y)$. □

5.1.4 Existence of Reals

Proposition 5.1.28 (Construction of the Reals)
There exists a (sequentially) complete ordered field $\mathbb{R}$ which is unique up to a unique order-preserving isomorphism.

*Furthermore it has characteristic zero and the subfield $\mathbb{Q}$ is **order-dense** (5.1.7) and **sequentially dense** (5.1.25).*

*It is **Archimedean** in the sense that for all pairs $x, y \in \mathbb{R}$ there exists $n \in \mathbb{Z}$ such that $nx > y$. Equivalently for all $\epsilon > 0$ there exists n such that $\frac{1}{n} < \epsilon$.*

The canonical (order) topology has base the open intervals (a, b), where a, b may be taken to be rational. In particular the order topology on $\mathbb{R}$ is second countable.

Proof. TODO. □

5.1.5 n-th Root

For technical reasons it is convenient to introduce the n-th root function at an early stage in an elementary fashion. Other special functions may be defined by similar considerations but it is convenient to wait until there is more machinery available.

Lemma 5.1.29 (Binomial Theorem)
Let K be a field of characteristic 0 and $x, y \in K$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

where $\binom{n}{k}$ is a positive integer given by the formula

$$\binom{n}{k} := \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1}$$

In particular if K is an ordered field and $x \geq 0$ then for every $0 \leq k \leq n$

$$(1+x)^n \geq \binom{n}{k} x^k$$

Lemma 5.1.30
Let K be a field of characteristic zero, $a, b \in K$ and n a positive integer. Then

$$a^n - b^n = (a-b)\left(a^{n-1}b + a^{n-2}b^2 + \ldots + ab^{n-2} + b^{n-1}\right)$$

In particular if $a > b \geq 0$ then

$$(a-b)nb^{n-1} < a^n - b^n < (a-b)na^{n-1}$$

Proposition 5.1.31 (n-th root over the Reals)
Let n be a positive integer. Then there exists a function

$$\sqrt[n]{\cdot} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$$

such that

$$\sqrt[n]{x}^n = \sqrt[n]{x^n} = x$$

It is bijective and strictly increasing.

Proof. Let $a > 0$ be a positive real number. There can be at most one solution because $x > y \implies x^n > y^n$. Let

$$X = \{y \in \mathbb{R}_{\geq 0} \mid y^n \leq a\}$$

then we may see that X is bounded by $\max(1, a)$, for $y > \max(1, a) \implies y^n \geq y > a$.

Define $\alpha = \sup X$. Suppose $\alpha^n > a$ then we claim there is an $h > 0$ such that $(\alpha - h)^n > a$. Then $y > \alpha - h \implies y^n > a$, or contrapositively $y^n \leq a \implies y \leq \alpha - h$, and $\alpha - h$ is an upper bound of X, which is a contradiction. By (5.1.30) we have

$$\alpha^n - (\alpha - h)^n \leq hn\alpha^{n-1}$$

therefore we may choose h such that

$$0 < h < \frac{\alpha^n - a}{n\alpha^{n-1}}.$$

Suppose $\alpha^n < a$ then we claim there is $h > 0$ such that $(\alpha + h)^n < a$, which is a contradiction. As before

$$(\alpha + h)^n - \alpha^n \leq hn(\alpha + h)^{n-1}$$

therefore we may choose h such that

$$0 < h < \frac{a - \alpha^n}{n(\alpha + h)^{n-1}}$$

to demonstrate the required property.

By the trichotomy law we deduce that $\alpha^n = a$ as required, and the n-th root function is well-defined and satisfies $\sqrt[n]{x}^n = x$.

Suppose that $a^n = b^n = x > 0$ then evidently $a, b > 0$ and we deduce from (5.1.30) that $a = b$. Therefore the function is unique and injective. It is evidently surjective as $\sqrt[n]{a^n} = a$ by uniqueness. Finally we may deduce from (5.1.30) that for $y > x \geq 0$

$$\sqrt[n]{y} - \sqrt[n]{x} > \frac{y - x}{n\sqrt[n]{y}^{n-1}} > 0$$

and so the function is strictly increasing. □

5.1.6 Limsup and Liminf

Proposition 5.1.32 (Limsup and Liminf)
Let K be a complete ordered field and (a_n) a sequence. Define the associated sequences in $K^\sharp$

$$\begin{aligned} a_n^+ &:= \sup_{n' \geq n} a_{n'} \\ a_n^- &:= \inf_{n' \geq n} a_{n'} \end{aligned}$$

which are decreasing and increasing sequences respectively. Define

$$\begin{aligned} \limsup a_n &= \lim_{n\to\infty} a_n^+ \\ \liminf a_n &:= \lim_{n\to\infty} a_n^- \end{aligned}$$

Then

a) *a_n is bounded above* $\iff$ *a_n^+ is bounded above* $\iff \limsup a_n^+ < \infty$

b) *a_n is bounded below* $\iff$ *a_n^- is bounded above* $\iff \liminf a_n^- > -\infty$

c) $\limsup a_n \geq \liminf a_n$

d) $a_n \to \alpha \iff \limsup a_n = \liminf a_n = \alpha$

Proof. Clearly a_n^+ is decreasing and a_n^- is increasing. Therefore by (5.1.22) the definition of $\limsup a_n$ and $\liminf a_n$ is well-defined, the same result also demonstrates *a*) and *b*). By definition $a_n^+ \geq a_n \geq a_n^-$ so the inequality *c*) follows from (5.1.21).

Suppose $\alpha \to \infty$ then for every $L > 0$ there exists N such that

$$n \geq N \implies a_n > L \implies a_n^- \geq L$$

whence $\liminf a_n = \infty$. Conversely suppose $\liminf a_n = \infty$ we see by definition that $a_n \to \infty$ as required. The case of $-\infty$ follows similarly.

Suppose that $\alpha = \limsup a_n = \liminf a_n$ is finite, then there exists N_1 such that

$$n \geq N_1 \implies a_n \geq a_n^- > \alpha - \frac{\epsilon}{2}$$

and N_2 such that

$$n \geq N_2 \implies a_n \leq a_n^+ < \alpha + \frac{\epsilon}{2}$$

Then

$$n \geq \max(N_1, N_2) \implies |a_n - \alpha| < \epsilon$$

and we conclude $\lim_{n\to\infty} a_n = \alpha$.

Conversely suppose $a_n \to \alpha$. Then for every $\epsilon > 0$ there exists some N such that

$$n \geq N \implies \alpha - \epsilon < a_n < \alpha + \epsilon$$

and therefore

$$n \geq N \implies \alpha - \epsilon \leq a_n^- \leq a_n \leq a_n^+ \leq \alpha + \epsilon$$

Evidentally then

$$\alpha - \epsilon \leq \liminf a_n \leq \limsup a_n \leq \alpha + \epsilon$$

As ϵ was arbitrary then this shows $\alpha = \liminf a_n = \limsup a_n$. □

Proposition 5.1.33 (Arithmetic Properties of limsup and liminf)
Let K be a complete ordered field and $(a_n), (b_n)$ bounded sequences. Then

a) $\limsup(a_n + b_n) \leq \limsup a_n + \limsup b_n$

b) $\liminf(a_n + b_n) \leq \liminf a_n + \liminf b_n$

If $b_n \to b$ then

c) $\limsup(a_n + b_n) = \limsup a_n + b$

d) $\liminf(a_n + b_n) = \liminf a_n + b$

and if in addition $b \geq 0$ then

e) $\limsup(a_n b_n) = b \limsup a_n$

f) $\liminf(a_n b_n) = b \liminf a_n$

Proof. We prove each in turn

a) By definition $n' \geq n \implies a_{n'} + b_{n'} \leq a_n^+ + b_n^+$, whence $(a_n + b_n)^+ \leq a^+ + b_n^+$. The result follows from (5.1.21).

b) Similarly

c) By $a)$ we have $\limsup(a_n + b_n) \leq \limsup a_n + b$. Furthermore $\limsup(a_n) = \limsup(a_n + b_n + (-b_n)) \leq \limsup(a_n + b_n) + \limsup(-b_n) = \limsup(a_n + b_n) - b$, and the result follows.

d) Similarly

e), f) Suppose first that $b = 0$. Then for sufficiently large n

$$0 \leq b_n \leq \epsilon \implies -\epsilon \left|a_n^-\right| \leq (a_n b_n)^+ \leq \left|a_n^+\right| \epsilon \implies \left|(a_n b_n)^+\right| \leq \max\left(\left|\sup_k a_k^+\right|, \left|\inf_k a_k^-\right|\right) \epsilon$$

as (a_n) is assumed bounded then this shows that $(a_n b_n)^+ \to 0$ as required. In this case $f)$ follows similarly. For the general case then

$$a_n b_n = a_n(b_n - b) + a_n b$$

Obviously $b_n - b \to 0$, so by the case already proven we have

$$\limsup(a_n(b_n - b)) = \liminf(a_n(b_n - b)) = 0$$

and in particular $a_n(b_n - b) \to 0$ by (5.1.32).d). Consequently by $c)$

$$\limsup(a_n b_n) = \limsup(a_n b) = b \limsup(a_n)$$

as required. The case $f)$ follows similarly. □

Proposition 5.1.34
Let K be a complete ordered field and (a_n) a bounded sequence. Then every subsequence (a_{n_k}) satisfies

$$\limsup_k a_{n_k} \leq \limsup_n a_n$$

and there in fact exists a convergent subsequence a_{n_k} such that

$$a_{n_k} \downarrow \limsup_n a_n$$

A similar statement applies to $\liminf a_n$.

Proof. Define $b_k := \sup_{k' \geq k} a_{n_{k'}}$, then by definition

$$b_k^+ \leq a_{n_k}^+$$

Taking limits as $k \to \infty$ and considering we find that

$$\limsup_k a_{n_k} \overset{(5.1.21)}{\leq} \lim_{k\to\infty} a_{n_k}^+ \overset{??}{=} \lim_{n\to\infty} a_n^+ =: \limsup_n a_n$$

Recall that $a_n^+ \downarrow \limsup a_n$. Therefore for every $k > 0$ there exists N_k such that $a_{N_k}^+ \leq \limsup a_n + \frac{1}{2k}$. Then by definition there exists some $n_k \geq N_k$ such that $a_{n_k} \leq a_{N_k}^+ + \frac{1}{2k} \leq \limsup a_n + \frac{1}{k}$. We see that a_{n_k} has the required property. □

5.2 Complex Numbers

Proposition 5.2.1 (Existence of Complex Numbers)
Let K be a field for which -1 has no square root (and in particular $\operatorname{char}(K) \neq 2$). Then

$$K[i] := K[X]/(X^2+1)$$

is a field with a K-basis $\{1, i\}$ such that $i^2 = -1$. Multiplication in $K[i]$ is defined as follows

$$(a+bi)(c+di) = (ac-bd) + (bc+ad)i$$

and the inverse is given by

$$(a+bi)^{-1} = \frac{a-bi}{a^2+b^2}$$

The field extension $K(i)/K$ is Galois of degree two with

$$\operatorname{Gal}(K(i)/K) = \{1, \bar{\cdot}\}$$

*where $\bar{\cdot}$ is the **complex conjugation** automorphism given by*

$$\overline{a+bi} = a - bi$$

In particular we see that $\bar{\cdot}$ satisfies the following properties

$$\begin{aligned} \overline{\alpha+\beta} &= \overline{\alpha} + \overline{\beta} \\ \overline{\alpha\beta} &= \overline{\alpha}\,\overline{\beta} \end{aligned}$$

Proof. The polynomial X^2+1 is of degree 2 so it is irreducible if and only if has no root. Therefore the quotient ring is a field by (3.18.52). $\mathbb{R}$ satisfies this property by (5.1.5), so $\mathbb{C}$ is a field.

Observe that as polynomials in $K[X]$

$$(a+bX)(c+dX) = ac + (bc+ad)X + bdX^2 = (ac-bd) + (bc+ad)X + bd(X^2+1)$$

from which the multiplication identity follows immediately.

For the inverse we claim that $a \neq 0$ or $b \neq 0 \implies a^2+b^2 \neq 0$. For otherwise either a/b or b/a would be a square root of -1. Therefore the expression for the inverse is well-defined and it may be verified directly to be an inverse.

The complex conjugation operator exists by (3.18.60). Therefore $\operatorname{Aut}(K(i)/K)$ has order at least $[K(i):K] = 2$, and we deduce $K(i)/K$ is Galois (3.18.114). □

Definition 5.2.2 (Complex Numbers)
*Define the **complex numbers** $\mathbb{C}$ to be the field $\mathbb{R}[i]$ and identify $\mathbb{R}$ with the subfield $\{a + 0i \mid a \in \mathbb{R}\}$.*

*Define the **absolute value** on $\mathbb{C}$ as follows*

$$|a+bi| := \sqrt{a^2+b^2} \in \mathbb{R}_{\geq 0}$$

*Define the **real part** and **imaginary part** as follows*

$$\begin{aligned} \operatorname{Re}(a+bi) &= a \\ \operatorname{Im}(a+bi) &= b \end{aligned}$$

Observe that

$$\alpha + \overline{\alpha} = 2\operatorname{Re}(\alpha)$$

Proposition 5.2.3 (Complex Absolute Value)
Let $\alpha, \beta \in \mathbb{C}$ be complex numbers. The following properties hold

$$\begin{aligned} |\alpha| &= |\overline{\alpha}| \\ |\alpha|^2 &= \alpha\overline{\alpha} \\ |\alpha\beta| &= |\alpha|\,|\beta| \\ |\alpha+\beta| &\leq |\alpha| + |\beta| \end{aligned}$$

Furthermore this agrees with the usual notion of absolute value on $\mathbb{R}$.

Proof. The first two relations follow by direct calculation. Then

$$|\alpha\beta|^2 = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = |\alpha|^2\,|\beta|^2$$

and the third relation follows by taking square roots. Further

$$\begin{aligned} |\alpha+\beta|^2 &= (\alpha+\beta)(\overline{\alpha}+\overline{\beta}) = \alpha\overline{\alpha} + (\alpha\overline{\beta} + \overline{\alpha}\beta) + \beta\overline{\beta} \\ &= |\alpha|^2 + 2\,\mathrm{Re}(\alpha\beta) + |\beta|^2 \\ &\leq |\alpha|^2 + 2\,|\alpha\beta| + |\beta|^2 \\ &= (|\alpha| + |\beta|)^2 \end{aligned}$$

and the result follows by taking square roots (and this being an increasing function). □

Proposition 5.2.4 (Complex Numbers are Complete)
$\mathbb{C}$ is complete as a normed vector space.

Proof. Let (α_n) be a cauchy sequence in $\mathbb{C}$, and consider the decomposition into real and imaginary parts

$$\alpha_n = a_n + b_n i$$

Then

$$|a_n| \leq |\alpha_n|$$
$$|b_n| \leq |\alpha_n|$$

Therefore we see both (a_n) and (b_n) are cauchy sequences of reals, which therefore have limits a and b respectively. We may verify directly that $\alpha_n \to \alpha$ where $\alpha := a + bi$. □

5.3 Metric Spaces

Definition 5.3.1 (Metric Space)
*Let X be a set and $d : X \times X \to \mathbb{R}_{\geq 0}$ a function. We say that (X, d) is a **metric space** if the following properties hold*

a) *$d(x, y) = 0 \iff x = y$ for all $x, y \in X$*

b) *$d(x, y) = d(y, x)$*

c) *$d(x, z) \leq d(x, y) + d(x, z)$ for all $x, y, z \in X$*

*Given $x \in X$ and $\epsilon > 0$ we define the **open ball** at x to be*

$$B(x; \epsilon) := \{y \in X \mid d(x, y) < \epsilon\}$$

Proposition 5.3.2
Let (X, d) be a metric space. Then we say that a subset $U \subset X$ is open if

$$\forall x \in X\ \exists \epsilon > 0 \text{ s.t. } B(x; \epsilon) \subset U$$

The open sets form a topology with open balls forming a base.

For each $x \in X$ a local base consists of open balls of the form $B(x; \epsilon)$. Further we may also consider the countable local base

$$\mathscr{B}_x := \left\{ B\left(x; \frac{1}{n}\right) \mid n \in \mathbb{N} \right\}$$

*In particular every metric space is **first countable**.*

Proposition 5.3.3 (Convergent Sequence)
Let (X,d) be a metric space and (x_n) a sequence in X and $x \in X$. Then the following are equivalent

a) *For every $\epsilon > 0$ there exists N such that $n \geq N \implies d(x_n, x) < \epsilon$*

b) *The function*

$$\begin{aligned} \mathbb{N} \cup \{\infty\} &\to X \\ n &\to x_n \\ \infty &\to x \end{aligned}$$

is continuous at ∞ with respect to the topology on $\mathbb{N} \cup \{\infty\}$ given by open sets of the form $\{N, N+1, \dots, \} \cup \{\infty\}$ and arbitrary subsets of $\mathbb{N}$. Note this function is automatically continuous at every n.

*In this case we say that $x_n \to x$ is a **convergent sequence**.*

Proposition 5.3.4 (Continuous at a Point)
Let $f : (X,d) \to (Y,d')$ be a map of metric spaces. Then for $x \in X$ and $y := f(x)$ the following are equivalent

a) *For all $\epsilon > 0$ there exists $\delta > 0$ such that*

$$d(y,x) < \delta \implies d'(f(y), f(x)) < \epsilon$$

b) *$f : X \to Y$ is continuous at x in the sense of topological spaces (4.1.23)*

c) *For every sequence $x_n \to x$ we have $f(x_n) \to f(x)$*

Proposition 5.3.5 (Continuous Criteria)
Let $f : X \to Y$ be a map of metric spaces. Then the following are equivalent

a) *f is continuous at every $x \in X$ (5.3.4)*

b) *f is continuous in the topological sense (4.1.25)*

c) *For every convergent sequence $x_n \to x$ we have $f(x_n) \to f(x)$*

Definition 5.3.6 (Product Metric Space)
Let (X_i, d_i) be metric spaces for $i = 1 \dots n$. Define the metric space on $X_1 \times \dots \times X_n$ by

$$d((x_1, \dots, x_n), (y_1, \dots, y_n)) = \max(d_1(x_1, y_1), \dots, d_n(x_n, y_n))$$

Then the topology induced on (X,d) coincides with the product topology.

5.3.1 Completeness

Definition 5.3.7 (Cauchy Sequence)
*Let (X,d) be a metric space. A sequence (x_n) in X is said to be **cauchy** if*

$$\forall \epsilon \, \exists N \text{ s.t. } n, m \geq N \implies d(x_n, d_m) < \epsilon$$

Definition 5.3.8
*A metric space (X,d) is said to be **complete** if every cauchy sequence is convergent.*

Proposition 5.3.9
Let (x_n) be a Cauchy sequence in a metric space (X,d) with $x \in X$ a cluster point (equivalently, subsequential limit point). Then $x_n \to x$.

Proposition 5.3.10
Let (X,d) be a complete metric space. A closed subset $Y \subset X$ is complete iff it is closed in X.

Proposition 5.3.11
Let (X_i, d_i) be complete metric spaces for $i = 1 \dots n$. Then the product metric space is $(X_1 \times \dots \times X_n, d)$ is complete.

Corollary 5.3.12
The metric space $\mathbb{R}^k$ induced by the product metric is complete.

A subset $X \subset \mathbb{R}^k$ is complete if and only if it is closed.

Proof. This is simply (5.3.11) and (5.3.10). □

5.3.2 Compactness

Definition 5.3.13
*We say a metric space (X, d) is **separable** if there exists a countable dense subset X_0.*

Proposition 5.3.14
Suppose X is a separable metric space. Then it is second countable.

Proof. We may show that the family

$$\mathcal{B} := \left\{ B\left(x_0; \frac{1}{n}\right) \mid x_0 \in X_0,\, n \in \mathbb{N} \right\}$$

is a countable base. □

Proposition 5.3.15 (Precompact)
Let (X, d) be a metric space. The following are equivalent

a) *For all $\epsilon > 0$ there exists a finite covering $X = U_1 \cup \ldots \cup U_n$ such that $\operatorname{diam}(U_i) < \epsilon$*

b) *For all $\epsilon > 0$ there exists a finite set of points $x_1, \ldots, x_n$ such that $X = \bigcup_{i=1}^{n} B(x_i; \epsilon)$*

c) *Every sequence has a cauchy subsequence.*

*In this case we say X is **precompact** or **totally bounded**.*

Proof. *a)* $\iff$ *b)* is straightforward. For *c)* $\implies$ *b)* suppose X did not satisfy this property, then we could inductively choose a sequence x_n such that

$$x_n \in X \setminus \bigcup_{i=1}^{n-1} B(x_i; \epsilon)$$

Then evidently $d(x_n, x_{n+1}) \geq \epsilon$ for all n and it can have no cauchy subsequence.

For *b)* $\implies$ *c)* Let (x_n) be a sequence. If $\{x_n\}$ is finite then we are done. Otherwise assuming it is infinite, we construct a decreasing sequence of sets

$$A_1 \supset \ldots \supset A_k \supset \ldots$$

such that $\operatorname{diam}(A_k) < \frac{1}{k}$ and $A_k \cap \{x_n\}$ is infinite. For suppose $A_1, \ldots, A_k$ are constructed, then evidently A_k itself satisfies *b)* so we may find $A_k = \bigcup_{i=1}^{m} B(x_i; \frac{1}{k+1})$. For at least one i we must have $B(x_i; \frac{1}{k+1}) \cap A_k \cap \{x_n\}$ is infinite. Therefore we may define $A_{k+1} := B(x_i; \frac{1}{k+1}) \cap A_k$. Finally choosing an increasing sequence n_k such that $x_{n_k} \in A_k$ yields the required cauchy subsequence.

c) $\implies$ *b)* On the contrary suppose this doesn't hold. Then for some $\epsilon > 0$ we may find a sequence $\{x_n\}$ such that

$$x_{n+1} \notin \bigcup_{i=1}^{n} B(x_i; \epsilon)$$

□

Corollary 5.3.16 (Compactness Criteria)
Let (X, d) be a metric space then the following are equivalent

a) *X is compact*

b) *X is countably compact*

c) *X is sequentially compact*

d) *X is complete and precompact*

Proof. *a), c)* $\implies$ *b)* This is (4.1.74).a)

a), b) $\implies$ *c)* This is (4.1.74).b)

c) $\implies$ *d)* By (5.3.9) every cauchy sequence is convergent. Therefore X is complete, and precompact by (5.3.15).

d) $\implies$ *a)* We show that (X, d) is sequentially compact and second countable, and the result follows from (4.1.74).c). Sequential compactness is a consequence of (5.3.15) and (5.3.9). To show that X is second countable we may for each n find a finite cover

$$X = \bigcup_{i=1}^{N_n} B\left(x_{ni}; \frac{1}{n}\right)$$

We claim that

$$\left\{B\left(x_{ni};\frac{1}{n}\right)\right\}$$

is a base. For given $y \in X$ and a nbhd $U \in \mathscr{U}_y$ we have $B(y;\epsilon) \subset U$ for some $\epsilon > 0$. Choose n such that $\frac{1}{n} < \frac{\epsilon}{2}$. Then for some $1 \leq i \leq N_n$, $y \in B(x_{ni};\frac{1}{n})$. We may show that $B(x_{ni};\frac{1}{n}) \subset B(y;\epsilon) \subset U$ which shows that the given collection is a base. □

5.3.3 Uniform Continuity

Definition 5.3.17 (Uniformly Continuous)
*Let (X,d) and (Y,d') be metric spaces and $f : X \to Y$ a function. We say that f is **uniformly continuous** if*

$$\forall \epsilon > 0\, \exists \delta > 0 \text{ s.t. } d(x,y) < \delta \implies d'(f(x),f(y)) < \epsilon$$

Proposition 5.3.18 (Compact & Continuous $\implies$ Uniformly Continuous)
Let $f : X \to Y$ be a continuous map of metric spaces and suppose X is (sequentially) compact. Then f is uniformly continuous.

Proof 1. Fix $\epsilon > 0$ then for every $x \in X$ there exists δ_x such that $f(B(x;\delta_x)) \subseteq B(f(x);\epsilon)$. Evidently $X = \bigcup_x B(x;\frac{\delta_x}{2})$ whence there is a finite subcover associated to $x_1,\ldots,x_n$. Define

$$\delta := \min\left(\frac{\delta_{x_1}}{2},\ldots,\frac{\delta_{x_n}}{2}\right)$$

Given $y \in X$ then $y \in B\left(x_i;\frac{\delta_{x_i}}{2}\right)$ for some $i = 1\ldots n$. Furthermore suppose $d(y,z) < \delta$ then

$$d(x_i,z) \leq d(x_i,y) + d(y,z) < \delta_{x_i}$$

whence $y,z \in B(x_i;\delta_{x_i})$. Therefore by construction $d(f(y),f(z)) < \epsilon$, as required. □

Proof 2. By (5.3.16) we know that X is sequentially compact. Suppose that f is not uniformly continuous, then there exists $\epsilon > 0$ and sequences $\{x_n\},\{y_n\}$ such that $d(x_n,y_n) < \frac{1}{n}$ and $d(f(x_n),f(y_n)) > \epsilon$. By assumption there is a subsequence n_k such that $x_{n_k} \to x$ and $y_{n_k} \to y$. Evidently

$$d(x,y) \leq d(x,x_{n_k}) + d(x_{n_k},y_{n_k}) + d(y_{n_k},y) \to 0$$

whence $d(x,y) = 0$ and $x = y$. By (...) $f(x_{n_k}) \to f(x)$ and $f(y_{n_k}) \to f(x)$ which is a contradiction. □

5.4 Normed Vector Spaces

Definition 5.4.1 (Valued Field)
*Let K be a field. A **valuation** on K is a function*

$$|\cdot| : K \to \mathbb{R}_{\geq 0}$$

such that for all $x,y \in K$ the following relations are satisfied

a) $|x| = 0 \iff x = 0$

b) $|xy| = |x|\,|y|$

c) $|x+y| \leq |x| + |y|$

*We say that this valuation is **non-archimedean** if it satisfies the ultrametric inequality*

$$|x+y| \leq \max(|x|,|y|)$$

*for all $x,y \in K$. Otherwise it is **archimedean**.*

*We say the pair $(K,|\cdot|)$ is a **valued field**.*

Definition 5.4.2 (Banach Space)
*A normed vector space which is complete as a metric space is called a **Banach Space**.*

Example 5.4.3
Any subfield of $\mathbb{C}$ (and therefore $\mathbb{R}$) is an archimedean valued field, using the complex absolute value $|\cdot|$ (5.2.2).

Definition 5.4.4 (Normed Vector Space)
Let $(K, |\cdot|)$ be a valued field and X a K-vector space. A norm $\|\cdot\|$ is a function

$$\|\cdot\| : X \to \mathbb{R}_{\geq 0}$$

satisfying the following properties

a) $\|x\| = 0 \iff x = 0$

b) $\|\lambda x\| = |\lambda| \, \|x\|$

c) $\|x + y\| \leq \|x\| + \|y\|$

*We say the pair $(X, \|\cdot\|)$ is a **normed vector space** over the valued field $(K, |\cdot|)$.*

Example 5.4.5
A valued field (e.g. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$) is a normed vector space over itself.

$\mathbb{C}$ is a normed vector space over $\mathbb{R}$.

For any valued field K the vector space K^n is a normed vector space with the following definition of norm

$$\|v\| := \sqrt{v_1^2 + \ldots + v_n^2}$$

(the triangle inequality requires proof).

Proposition 5.4.6
Let $(X, \|\cdot\|)$ a normed vector space. Then it is naturally a metric space with induced metric

$$d(x, y) := \|x - y\|$$

and in particular a topological space with base the open balls

$$B(x; \epsilon) := \{y \in X \mid \|y - x\| < \epsilon\}$$

Furthermore the open balls $B(x; \epsilon)$ and $B(x; \frac{1}{n})$ form a local base at x.

The same statement applies to valued fields and in particular $\mathbb{R}$.

5.4.1 Continuous Functions

Proposition 5.4.7 (Continuous maps of Normed Vector Spaces)
Let $S \subset X$ be a subset of a normed vector space and $f : S \to Y$ be a map to a normed vector space Y and $x \in S$. Then the following are equivalent

a) *For all $\epsilon > 0$ there exists $\delta > 0$ such that for all $x' \in S$, $\|x - x'\| < \delta \implies \|f(x) - f(x')\| < \epsilon$*

b) *f is continuous at x with respect to the subspace topology on S*

*In this case we say the map f is **continuous** at x.*

Example 5.4.8
For X a normed vector space then $\|\cdot\| : X \to \mathbb{R}$ is evidently continuous.

5.4.2 Product Space

Definition 5.4.9 (Product Norm)
*Let $X_1, \ldots, X_n$ be normed vector spaces over the same valued field K. Then we may define the **product norm** on the vector space $X_1 \times \ldots \times X_n$ by*

$$\|(x_1, \ldots, x_n)\| := \max(\|x_1\|, \ldots, \|x_n\|)$$

The metric induced by the product norm is the same as the product metric (5.3.6).

Proposition 5.4.10
Let $X_1, \ldots, X_n$ be normed vector spaces over the same valued field K. Then the metric (resp. topology) induced by product norm is the same as product metric (resp. product topology).

Proof. Consider a point $x = (x_1, \ldots, x_n)$ then

$$B(x; \epsilon) = \{(x_1, \ldots, x_n) \mid \|x_i\| \leq \epsilon\} = B(x_1; \epsilon) \times \ldots \times B(x_n; \epsilon)$$

Therefore the open balls are open in the product topology, and being a base for the norm topology, this a subset of the product topology (...). To show that the product topology is a subset of the norm topology it is sufficient to show that open sets of the form

$$U := U_1 \times \ldots \times U_n$$

are open in the product norm topology. For given $y \in U$ then by definition $B(y_i; \epsilon_i) \subset U_i$. Consider $\epsilon := \min(\epsilon_1, \ldots, \epsilon_n)$ and $z \in B(y; \epsilon)$. Then

$$\|z - y\| < \epsilon \implies \max_i(\|z_i - y_i\|) < \epsilon \leq \epsilon_i \implies z_i \in B(y_i; \epsilon_i) \implies z \in U$$

in other words $B(y; \epsilon) \subset U$ as required. □

Proposition 5.4.11 (Arithmetic Operations are Continuous)
Let X be a normed vector space over a valued field K. Then the addition map

$$+ : X \times X \to X$$

is continuous with respect to the product topology. Similarly the scalar multiplication operation is continuous

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

Finally all the arithmetic operations of a valued field K are continuous

$$+ : K \times K \to K$$

$$\cdot : K \times K \to K$$

$$(-)^{-1} : K \setminus \{0\} \to K$$

Proof. For by the triangle inequality

$$\|(x_1, x_2) - (y_1, y_2)\| < \epsilon \implies \|x_1 - y_1\| < \epsilon \wedge \|x_2 - y_2\| < \epsilon \implies \|(x_1 + x_2) - (y_1 + y_2)\| < 2\epsilon$$

Therefore we may apply the criterion given by (5.4.7), and using the product norm.

For scalar multiplication observe

$$\begin{aligned} \|(\lambda_1, x_1) - (\lambda_2, x_2)\| < \delta \quad &\implies \quad |\lambda_1 - \lambda_2| < \delta \wedge \|x_1 - x_2\| < \delta \\ &\implies \quad \|\lambda_1 x_1 - \lambda_2 x_2\| \leq |\lambda_1| \, \|x_1 - x_2\| + \|x_2\| \, |\lambda_1 - \lambda_2| \\ &\implies \quad \|\lambda_1 x_1 - \lambda_2 x_2\| \leq |\lambda_1| \, \|x_1 - x_2\| + (\|x_1\| + \delta) \, |\lambda_1 - \lambda_2| \\ &\implies \quad \|\lambda_1 x_1 - \lambda_2 x_2\| \leq \delta^2 + (\|x_1\| + \delta)\delta \end{aligned}$$

Therefore choose $\delta < \min(1, \frac{\epsilon}{\|x_1\|+1})$ to find $\|\lambda_1 x_1 - \lambda_2 x_2\| < 3\epsilon$. □

5.4.3 Convergent Sequences

Proposition 5.4.12 (Convergent Sequence)
Let X be a normed vector space and (a_n) a sequence in X. Then the following are equivalent

a) *$a_n \to \alpha$ in the topological sense (4.1.31)*

b) *For all $\epsilon > 0$ there exists $N(\epsilon) \in \mathbb{N}^+$ such that*

$$n \geq N(\epsilon) \implies \|a_n - \alpha\| < \epsilon$$

c) *The function*

$$\begin{aligned} \mathbb{N} \cup \{\infty\} &\to X \\ n &\to a_n \\ \infty &\to \alpha \end{aligned}$$

is continuous with respect to the topology on $\mathbb{N} \cup \{\infty\}$ given by open sets of the form $\{N, N+1, \ldots, \} \cup \{\infty\}$ and arbitrary subsets of $\mathbb{N}$.

*In this case we say the sequence (a_n) is **convergent**. If this doesn't hold it is **divergent**.*

Proposition 5.4.13 (Uniqueness of Limits)
Let X be a normed vector space. Then it is Hausdorff and limits are unique.

Proposition 5.4.14 (Continuous Image of Convergent Sequence)
Let X, Y be normed vector spaces, $S \subset X$ and $f : S \to Y$ a map. Then the following are equivalent

a) *f is continuous in the topological sense*

b) *For every convergent sequence $a_n \to \alpha$ we have $f(a_n) \to f(\alpha)$.*

Proof. Recall that X is first-countable and so the equivalence follows from (4.1.32) and (4.1.34). □

Proposition 5.4.15 (Arithmetic of Convergent Sequences in an NVS)
Let X be a normed vector space and (a_n) and (b_n) be convergent sequences in X. Then

$$\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$$

$$\lim_{n\to\infty} \lambda a_n = \lambda \lim_{n\to\infty} a_n$$

In particular $a_n \to \alpha \iff a_n - \alpha \to 0$.

Proposition 5.4.16 (Arithmetic of Convergent Sequences in a valued field)
Let K be a valued field and (a_n) and (b_n) be convergent sequences. Then

$$\lim_{n\to\infty} a_n b_n = \left(\lim_{n\to\infty} a_n\right)\left(\lim_{n\to\infty} b_n\right)$$

Further if both b_n and $\lim_{n\to\infty} b_n$ is non-zero then

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{\lim_{n\to\infty} a_n}{\lim_{n\to\infty} b_n}$$

Proposition 5.4.17 (Arithmetic of Convergent Sequences in an ordered field)
Let K be an ordered field and (b_n) a sequence of non-negative elements. Then $b_n \to \infty \iff b_n^{-1} \to 0$.

Proposition 5.4.18
Let K be a valued field and $x \in K$ such that $|x| < 1$. Then

$$\lim_{n\to\infty} x^n = 0$$

Proof. We may reduce to the case that $x \in \mathbb{R}$ and $0 < x < 1$. Let $y = \frac{1-x}{x} > 0$, then it is enough to show that $(1+y)^n \to \infty$ by (5.4.17). However from (5.1.29) $(1+y)^n \geq 1+ny$, and the result follows from Archimedean property (...). □

Definition 5.4.19 (Cauchy Sequence)
*Let X be a normed vector space and $(a_n)_{n\in\mathbb{N}}$ a sequence in X. We say (a_n) is a **cauchy sequence** if for all $\epsilon > 0$ there exists $N(\epsilon)$ such that*

$$n, m \geq N(\epsilon) \implies \|a_n - a_m\| < \epsilon$$

*Every **convergent sequence** is **cauchy**. If the converse holds then we say X is **complete**.*

5.4.4 Finite-Dimensional Normed Spaces

Definition 5.4.20 (Equivalent Norms)
*Let X be a vector space over a valued field K. Consider two norms $\|\cdot\|_1$ and $\|\cdot\|_2$. We say that they are **equivalent** if there exists constants $c_1, c_2 > 0$ such that*

$$c_1 \|x\|_1 \leq \|x\|_2 \leq c_2 \|x\|_2$$

We may prove easily that this is an equivalence relation on norms.

Proposition 5.4.21
Let X be a vector space over a valued field K. Suppose that $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent norms for X. Then the following derived quantities are the same

- *Induced topology*
- *Convergent sequences*
- *Cauchy sequences*

Proposition 5.4.22 (Supremum Norm)
Let X be a finite-dimensional vector space with basis $(e_1, \ldots, e_n)$. Then the supremum norm defined by

$$\left\| \sum_{i=1}^{n} \lambda_i e_i \right\|_\infty := \max(|\lambda_1|, \ldots, |\lambda_n|)$$

is well-defined (it is the product norm on $X \cong \mathbb{R} \times \ldots \times \mathbb{R}$). If K is complete then so is X.

Proposition 5.4.23 (Equivalence of Norms)
Let X be a non-zero finite-dimensional vector space over a complete valued field K. Then every norm is equivalent to the infinity norm (and therefore complete

Proof. Fix a basis $(e_1, \ldots, e_n)$. Then for any norm $\|\cdot\|$ we have by the triangle inequality

$$\left\| \sum_{i=1}^{n} \lambda_i e_i \right\| \leq \sum_{i=1}^{n} |\lambda_i| \, \|e_i\| \leq \left(\sum_{i=1}^{n} \|e_i\| \right) \left\| \sum_{i=1}^{n} \lambda_i e_i \right\|_\infty$$

The reverse inequality we prove by induction. The case $n = 1$ we may take $c_1 = \|e_1\|$. Suppose $n > 1$ and there is no such constant C. Then there are vectors $v_k \in X$ such that

$$\|v_k\| < \frac{1}{k} \|v_k\|_\infty$$

Suppose

$$v_k = \sum_{i=1}^{n} \lambda_{ki} e_i$$

Consider the sets of integers

$$S_i := \{k \in \mathbb{N} \mid \|v_k\|_\infty = |\lambda_{ki}|\} \quad i = 1 \ldots n$$

Then at least one of $S_1, \ldots, S_n$ is infinite, since the union is $\mathbb{N}$. Without loss of generality we assume it is S_n.

Therefore by passing to a subsequence, and scaling, we may assume that $\|v_k\|_\infty = \lambda_{kn} = 1$ and $\|v_k\| < \frac{1}{k}$. Define the vector $w_k := v_k - e_n$. Then by definition $w_k \to e_n$ with respect to $\|\cdot\|$.

Let W be the $(n-1)$-dimensional subspace spanned by $\{e_1, \ldots, e_{n-1}\}$. We prove also that $w_k \to w \in W$ with respect to $\|\cdot\|$, which contradicts uniqueness of limits. Evidentally w_k is a cauchy sequence with respect to $\|\cdot\|$ restricted to W. By induction $\|\cdot\|_\infty$ is equivalent to $\|\cdot\|$ on W, and therefore w_k is cauchy with respect to $\|\cdot\|_\infty$. As W is complete (5.4.22) we see that $w_k \to w$ with respect to $\|\cdot\|_\infty$, and therefore with respect to $\|\cdot\|$. □

5.4.5 Convergent Series

Definition 5.4.24 (Series)
Let X be a normed vector space and (a_n) a sequence in X. The formal expression

$$\sum_{n=1}^{\infty} a_n$$

*is called the **series** associated to this sequence. For such a sequence define the **partial sum** sequence as follows*

$$s_n := \sum_{k=1}^{n} a_k$$

*If the partial sum sequence converges then we say that the series **converges** and write*

$$\sum_{n=1}^{\infty} a_n := \lim_{n \to \infty} s_n$$

If the series

$$\sum_{n=1}^{\infty} \|a_n\|$$

*converges then we say the original series **converges absolutely**.*

The choice of terminology is justified in the case that X is complete.

Proposition 5.4.25 (Absolute Convergence $\implies$ Convergence)
Let X be a complete normed vector space and $\sum_{n=0}^{\infty} a_n$ a series which converges absolutely. Then the series converges in the usual sense.

Proof. The partial sums of the series $\sum_{n=1}^{\infty} \|a_n\|$ are cauchy by (5.4.19). By the triangle inequality we may demonstrate that the partial sums of the series $\sum_{n=1}^{\infty} a_n$ are cauchy. Then by completeness of X the partial sums must also converge. □

Proposition 5.4.26
Let X be a normed vector space and $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ two convergent sequences. Then the following series are convergent with limits

$$\sum_{n=1}^{\infty}(a_n + b_n) = \sum_{n=1}^{\infty} a_n + \sum_{n=1}^{\infty} b_n$$

$$\sum_{n=1}^{\infty} \lambda a_n = \lambda \sum_{n=1}^{\infty} a_n$$

where $\lambda \in K$.

Proposition 5.4.27
Let X be a normed vector space and $\sum_{n=1}^{\infty} a_n$ a convergent series. Then $\|a_n\| \to 0$.

Proof. Let $\alpha := \sum_{n=1}^{\infty} a_n$. Then by definition there exists N such that $n \geq N \implies \|\sum_{k=1}^{n} a_k - \alpha\| < \epsilon$. As this holds for $n+1$ we may use the triangle inequality to find that $n \geq N+1 \implies \|a_n\| < 2\epsilon$. As ϵ was arbitrary we find $\|a_n\| \to 0$ as required. □

Proposition 5.4.28 (Comparison Test)
Let X be a complete normed vector space. Suppose (a_n) is a sequence in X and (c_n) is a sequence in $\mathbb{R}$ such that

a) *The series $\sum_{n=0}^{\infty} c_n$ converges*

b) *$\|a_n\| \leq c_n$ for $n \geq N_0$*

then the series $\sum_{n=0}^{\infty} a_n$ converges absolutely.

Proof. By assumption *b*) (c_n) is non-negative, and by (5.4.29) the sequence of partial sums $\sum_{k=0}^{n} c_k$ is bounded. therefore so is the sequence $\sum_{k=0}^{n} \|a_k\|$, and by the same result the series $\sum_{n=0}^{\infty} \|a_n\|$ converges, in other words $\sum_{n=0}^{\infty} a_n$ converges absolutely. □

Proposition 5.4.29 (Series of Positive Reals)
Let (a_n) be a sequence of non-negative real numbers. Then the following are equivalent

a) *The sequence of partial sums $A_n := \sum_{k=0}^{n} a_k$ is bounded*

b) *The series $\sum_{n=0}^{\infty} a_n$ converges (absolutely)*

Proof. By (5.1.22) we always have $A_n \to \sup A_n \in \mathbb{R}^\sharp$, and the limit is finite iff A_n is bounded. □

Proposition 5.4.30 (Geometric Series)
Suppose $0 \leq x < 1$ is a real number, then

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

and in particular the partial sums are bounded by $\frac{1}{1-x}$.

Proof. It's straightforward to show by induction that the partial sums are given explicitly by

$$\sum_{n=0}^{N} x^n = \frac{1-x^N}{1-x}.$$

Then the result follows from (5.4.18). □

Proposition 5.4.31 (Root Test)
Let X be a normed vector space. Given a series $\sum_{n=0}^{\infty} a_n$, define

$$\alpha := \limsup_n \sqrt[n]{\|a_n\|}$$

Then

a) *if $\alpha < 1$ then the series converges absolutely*

b) *if* $\alpha > 1$ *then the series diverges*

Proof. a) Define $\alpha := \limsup_n \sqrt[n]{\|a_n\|}$ and $\beta := \frac{1+\alpha}{2} < 1$. Then by definition there is an integer N such that

$$n \geq N \implies \sqrt[n]{\|a_n\|} \leq \alpha + \frac{1-\alpha}{2} = \beta \implies \|a_n\|^n \leq \beta^n$$

In particular for $n \geq N$

$$\sum_{k=0}^{n} \|a_k\| \leq \sum_{n=0}^{N-1} \|a_k\| + \sum_{k=N}^{n} \|a_k\| \leq \sum_{k=0}^{N-1} \|a_k\| + \sum_{k=N}^{n} \beta^k \leq \sum_{k=0}^{N-1} \|a_k\| + \sum_{k=0}^{\infty} \beta^k$$

where the last step follows from by (5.4.30). We conclude from (5.4.29) that the series converges absolutely.

b) By (5.1.34) there exists a subsequence a_{n_k} such that $\sqrt[n_k]{\|a_{n_k}\|} \to \alpha > 1$. Therefore we may find a subsequence such that $\sqrt[n_k]{\|a_{n_k}\|} \geq \frac{1+\alpha}{2} > 1 \implies \|a_{n_k}\| > 1$. This shows that $\|a_{n_k}\| \not\to 0$, whence $\|a_n\| \not\to 0$ by (...), and the series diverges by (5.4.27).

□

Proposition 5.4.32 (Ratio Test)
Let X *be a valued field and consider a series* $\sum_{n=1}^{\infty} a_n$*. If*

$$\limsup_n \left| \frac{a_{n+1}}{a_n} \right| < 1$$

then the series is convergent.

Proof. Let $\alpha := \limsup \left| \frac{a_{n+1}}{a_n} \right|$ and $\beta = \frac{1+\alpha}{2}$. Then by assumption $\beta < 1$, and there exists N such that $n \geq N \implies \left| \frac{a_{n+1}}{a_n} \right| \leq \beta \implies |a_{N+k}| \leq |a_N| \beta^k$. We then see by Comparison Test (5.4.28) that the series is convergent. □

Proposition 5.4.33 (Cauchy Product of Series)
Let X *be a complete valued field and* $\sum_{n=1}^{\infty} a_n$, $\sum_{n=1}^{\infty} b_n$, $\sum_{n=1}^{\infty} c_n$ *series such that*

a) *one of* $\sum_{n=1}^{\infty} a_n$ *and* $\sum_{n=1}^{\infty} b_n$ *are absolutely convergent*

b) $c_n := \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} a_{n-k} b_k$

then $\sum_{n=0}^{\infty} c_n$ *is absolutely convergent and*

$$\sum_{n=0}^{\infty} c_n = \left(\sum_{n=1}^{\infty} a_n \right) \left(\sum_{n=1}^{\infty} b_n \right)$$

Proof. Denote the partial sums by A_n, B_n and C_n, and the limits by A, B respectively. Then evidently

$$C_n = \sum_{i=0}^{n} a_{n-i} B_i$$

therefore

$$C_n = \sum_{i=0}^{n} a_{n-i}(B_i - B) + A_n B$$

Then it's sufficient to show that the first term tends to 0. Observe that $\beta_n := B_n - B \to 0$. **TODO** □

5.4.6 Function Spaces

Definition 5.4.34 (Uniform Convergence)
Let S *be a metric space and* Y *a normed vector space. Suppose* $\{f_n : S \to Y\}$ *is a sequence of functions and* $f : S \to Y$ *is a function. We say that* $f_n \to f$ ***converges uniformly*** *if*

$$\forall \epsilon > 0 \, \exists N \text{ s.t. } n \geq N \implies \|f_n(x) - f(x)\| < \epsilon \, \forall x \in S$$

Note this implies, but is strictly stronger than, pointwise convergence that is $f_n(x) \to f(x)$ *for all* $x \in S$*, as* N *may be chosen independently of* x*.*

Proposition 5.4.35 (Uniform Limit of Continuous Functions is Continuous)
Let S be a metric space and Y a normed vector space. Suppose that $\{f_n : S \to Y\}$ is a sequence of continuous functions converging uniformly to a limit $f : S \to Y$. Then f is continuous.

Proof. Fix $\epsilon > 0$. There exists N such that

$$n \geq N \implies \|f_n(x) - f(x)\| < \epsilon \, \forall x \in S$$

Fix $x \in S$ then there exists $\delta > 0$ such that

$$\|y - x\| < \delta \implies \|f_n(y) - f_n(x)\| < \epsilon$$

Therefore

$$\|y - x\| < \delta \implies \|f(x) - f(y)\| \leq \|f(x) - f_n(x)\| + \|f_n(x) - f_n(y)\| + \|f(y) - f_n(y)\| < 3\epsilon$$

Consequently f is also continuous. □

Definition 5.4.36 (Bounded Function Space)
Let S be a metric space and Y a normed vector space. Define the vector space of ***bounded functions*** *by*

$$\mathscr{B}(S, Y) := \{f : S \to Y \mid \exists C > 0 \text{ s.t. } \|f(x)\| \leq C \text{ for all } x \in S\}$$

This is a normed vector space under the ***sup norm*** *given by*

$$\|f\|_\infty := \sup_{x \in S} \|f(x)\|$$

Evidently convergence in this norm is equivalent to uniform convergence.

Proposition 5.4.37 (Bounded Functions are Complete)
Suppose Y is a Banach Space, then $\mathscr{B}(S, Y)$ is also a Banach Space.

Proof. Let $\{f_n\}$ be a cauchy sequence of maps $S \to Y$ with respect to the sup norm. Then for every $\epsilon > 0$ there exists N such that

$$n, m \geq N \implies \|f_n - f_m\| < \epsilon$$

In particular for every $x \in S$ we have $\{f_n(x)\}$ is cauchy. As Y is complete it is a convergent sequence, for which we denote the limit by $f(x)$. For every $x \in S$ we may also choose some $m \geq N$ such that

$$\|f_m(x) - f(x)\| < \epsilon$$

then

$$\|f(x) - f_n(x)\| \leq \|f(x) - f_m(x)\| + \|f_m(x) - f_n(x)\| < 2\epsilon$$

As this inequality is independent of m we find that $\|f - f_n\| \to 0$ as required. We may also show easily that it is bounded. □

5.4.7 Continuous Linear Maps

Proposition 5.4.38 (Continuous Linear Maps)
Let $f : X \to Y$ be a linear map of normed vector spaces. Then the following are equivalent

a) *f is continuous*

b) *There exists a constant $C > 0$ such that*

$$\|f(x)\| \leq C \|x\|$$

c) *f is bounded on the unit sphere*

$$\sup\{\|f(x)\|_Y \mid \|x\|_X = 1\} < \infty$$

Proof. Suppose *b*) holds then f is even uniformly continuous because

$$\|x - y\| < \frac{\epsilon}{C} \implies \|f(x) - f(y)\| < \epsilon$$

Conversely given *a*) there exists δ such that

$$\|x\| \leq \delta \implies \|f(x)\| < 1$$

Therefore

$$\left\| f\left(\frac{\delta x}{\|x\|}\right) \right\| < 1 \implies \|f(x)\| < \frac{1}{\delta} \|x\|$$

and we may take $C = \frac{1}{\delta}$. Given *b*) evidently $\|f\| \leq C < \infty$, and conversely $\|f(x)\| \leq \|f\| \, \|x\|$. □

Proposition 5.4.39
Let X, Y be normed vector spaces. Denote by $L(X,Y)$ the set of continuous linear maps. It is a normed vector space, with norm given by

$$\|\theta\| := \sup\{\|\theta(x)\|_Y \mid \|x\|_X = 1\}$$

Furthermore if Y is complete, so is $L(X,Y)$.

Proof. Evidently $\|\lambda\theta\| = |\lambda| \, \|\theta\|$ and $\|\theta_1 + \theta_2\| \leq \|\theta_1\| + \|\theta_2\| < \infty$. Let $\{\theta_n\}$ be a cauchy sequence in $L(X,Y)$. Given $x \in X$ then

$$\|\theta_n(x) - \theta_m(x)\| \leq \|\theta_n - \theta_m\| \, \|x\|$$

whence $\{\theta_n(x)\}$ is a cauchy sequence, and therefore converges to $\theta(x)$. By uniqueness of limits we see that θ is linear. Furthermore by the reverse triangle inequality (...)

$$|\|\theta_n\| - \|\theta_m\|| \leq \|\theta_n - \theta_m\|$$

in otherwords $\|\theta_n\|$ is a cauchy sequence and converges to some limit C. Suppose that $\|x\| = 1$ then

$$\|\theta(x)\| \leq \|\theta(x) - \theta_n(x)\| + \|\theta_n(x)\| \leq \|\theta(x) - \theta_n(x)\| + \|\theta_n\|$$

Choose N_1 such that $n \geq N_1 \implies \|\theta_n\| \leq C + \epsilon$ and N_2 such that $n \geq N_2 \implies \|\theta(x) - \theta_n(x)\| < \epsilon$. As ϵ was arbitrary we see that $\|\theta\| \leq C$ and in particular is finite. □

Proposition 5.4.40 (Finite-Dimensional Linear Maps are continuous)
Suppose that $\theta : X \to Y$ is a linear map of normed vector spaces and X is finite-dimensional. Then θ is continuous.

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis. By (5.4.23) we know that $\|\cdot\|_X$ is equivalent to the infinity norm $\|\cdot\|_\infty$. therefore it is sufficient to show that θ is continuous with respect to this norm. However

$$\left\| \theta(\sum_{i=1}^n \lambda_i e_i) \right\| \leq \sum_{i=1}^n |\lambda_i| \, \|\theta(e_i)\| \leq n \left\| \sum_{i=1}^n \lambda_i e_i \right\|_\infty \max_i \|\theta(e_i)\|$$

□

Proposition 5.4.41 (Continuous Bilinear Maps)
Let $\psi : X \times Y \to Z$ be a bilinear map of normed vector spaces. Then the following are equivalent

a) *ψ is continuous*

b) *There exists a constant $C > 0$ such that*

$$\|\psi(x,y)\| \leq C \, \|x\| \, \|y\|$$

c) *The following quantity is finite*

$$\sup\{\|\psi(x,y)\| \mid \|x\| = \|y\| = 1\} < \infty$$

In this case $L(X,Y;Z)$ is a normed vector space with norm given by expression in c). Furthermore if Z is complete so is $L(X,Y;Z)$. Finally there is a canonical linear isomorphism which has norm ≤ 1

$$L(X, L(Y,Z)) \to L(X,Y;Z)$$

Proof. *a)* $\implies$ *b)* Suppose there is no such constant C, then exists $(x_n, y_n) \in X \times Y$ such that

$$\|\psi(x_n, y_n)\| > n^2 \, \|x_n\| \, \|y_n\|$$

Define $\hat{x}_n := \frac{x_n}{n\|x_n\|}$ and $\hat{y}_n := \frac{y_n}{n\|y_n\|}$. Evidently $(\hat{x}_n, \hat{y}_n) \to 0$ but $B(\hat{x}_n, \hat{y}_n) > 1$, which is a contradiction for (...).

b) $\implies$ *a)* Observe

$$\begin{aligned} \|B(x+h, y+k) - B(x,h)\| &\leq \|B(x+h, y+k) - B(x+h, y)\| + \|B(x+h, y) - B(x,y)\| \\ &= \|B(x+h, k)\| + \|B(h,y)\| \\ &\leq C \, \|x+h\| \, \|k\| + C \, \|h\| \, \|y\| \\ &\leq C(\|x\| + \|h\|) \, \|k\| + C \, \|h\| \, \|y\| \end{aligned}$$

Therefore choose $\|h\| < \min(1, \frac{\epsilon}{2C\|y\|})$ and $\|k\| < \frac{\epsilon}{2C(\|x\|+1)}$.

b) $\iff$ *c)* Straightforward

The supremum is evidently a norm, and the verification of completeness follows as before.

The given map is clearly a bijection. Furthermore

$$\|\theta(x)(y)\| \leq \|\theta(x)\| \, \|y\| \leq \|\theta\| \, \|x\| \, \|y\|$$

which shows the last statement. □

Proposition 5.4.42
Let X, Y be normed vector spaces and $\psi : X \times Y \to Z$ a bilinear continuous map. Then for each $x \in X$ (resp. $y \in Y$) the map

$$y \to \psi(x, y)$$

resp.

$$x \to \psi(x, y)$$

is a continuous linear map.

Proof. This is clear from (5.4.41).b) and (5.4.38).b) as we may choose $C := \|\psi\| \, \|x\|$. □

Proposition 5.4.43
Let X, Y be normed vector spaces then the following map

$$\begin{array}{rcl} L(X,Y) \times X & \to & Y \\ (\theta, x) & \to & \theta(x) \end{array}$$

is bilinear and continuous

Proof. Bilinearity is trivial. As θ is continuous we have

$$\|\theta(x)\| \leq \|\theta\| \, \|x\|$$

and so the relation is continuous by (5.4.41).b). □

Corollary 5.4.44
Let X, Y be normed vector spaces and $x \in X$. Then the evaluation map

$$L(X, Y) \to Y$$

is a continuous linear map.

5.5 Differentiable Functions

Definition 5.5.1 (Differentiable Scalar Function)
*Let K be a complete valued field, $U \subset K$ an open subset, Y a normed vector space over K and $f : U \to Y$ a function. We say that f is **differentiable** at $x \in U$ if the following relation holds*

$$\forall \epsilon > 0 \, \exists \delta > 0 \ s.t. \ 0 < |y - x| < \delta \implies \left\| \frac{f(y) - f(x)}{y - x} - f'(x) \right\| < \epsilon$$

for some $f'(x) \in K$.

*We say that f is simply **differentiable** if it is differentiable at every point of U.*

Proposition 5.5.2
Let K be a valued field, $U \subset K$ an open subset and $f : U \to Y$ a function which is differentiable at $x \in U$. Suppose $x_n \to x$ is a sequence such that $x_n \neq x$. Then

$$\frac{f(x_n) - f(x)}{x_n - x} \to f'(x)$$

Proposition 5.5.3
Let K be a valued field, $U \subset K$ an open subset and $f : U \to Y$ a function which is differentiable at $x \in U$. Then f is continuous at x.

Proposition 5.5.4 (Arithmetic of Differentiable Functions)
Let K be a valued field, $U \subset K$ an open subset and $f, g : U \to Y$ be functions differentiable at $x \in U$. Then

a) $(f + g)'(x) = f'(x) + g'(x)$

b) $(\lambda f)'(x) = \lambda f'(x)$

If Y has continuous algebra structure (e.g. $Y = K$) then

$$(fg)'(x) = f'(x)g(x) + f(x)g'(x)$$

Corollary 5.5.5
Let K be a valued field of characteristic zero and n a positive integer. Then the derivative of x^n is nx^{n-1}.

5.6 Power Series

Definition 5.6.1 (Convergent Power Series)
*Let K be a field. Then a **power series** is a formal expression of the form*

$$P(X) := \sum_{n=0}^{\infty} a_n X^n$$

where $a_n \in K$. We denote the ring of power series by $K[[X]]$. If K is a valued field then, we say this converges at $z \in K$ if the series

$$\sum_{n=0}^{\infty} a_n z^n$$

converges in K.

Proposition 5.6.2 (Radius of convergence)
Let K be a complete valued field and consider the formal power series

$$\sum_{n=0}^{\infty} a_n X^n \quad a_n \in K\,.$$

*Define the **radius of convergence** to be*

$$R := \left(\limsup \sqrt[n]{|a_n|}\right)^{-1}$$

where we understand $0^{-1} = \infty$ and $\infty^{-1} = 0$. Then

a) *For every $|z| < R$ the series $\sum_{n=0}^{\infty} a_n z^n$ is absolutely convergent, and we denote this function by $f(z)$.*

b) *For every $|z| > R$ the series $\sum_{n=0}^{\infty} a_n z^n$ is divergent*

c) *R is the unique value such that $a), b)$ hold.*

d) *The limit $f(z)$ is continuous and differentiable in the open set $B(0,R)$ with derivative*

$$f'(z) = \sum_{n=1}^{\infty} n a_n z^{n-1}$$

which has radius of convergence at least R

Proof. a) First consider the case $R < \infty$. Define $c_n := a_n z^n$ then $\sqrt[n]{|c_n|} = |z| \sqrt[n]{|a_n|}$. Then clearly $|z| < R \implies \limsup \sqrt[n]{|c_n|} < 1$ whence the result follows from (5.4.31). In the case $R = \infty$ we see that $\limsup \sqrt[n]{|c_n|} = 0$ for all z and the result follows similarly.

b) This follows similarly by (5.4.27).

c) This is evident for suppose $R' \neq R$ satisfies the same properties and consider z such that $|z| = \frac{R'+R}{2}$ for a contradiction.

d) Let R' be the radius of convergence for the given series, we claim that $R' \geq R$, or in otherwords that $|z| < R$ implies $\sum_{n=0}^{\infty}(n+1)a_{n+1}z^n$ converges. For we may choose w such that $|z| < |w| < R$. Then by definition

$$\sum_{n=0}^{\infty} a_n w^n$$

converges. In particular by (...) $|a_n w^n| \to 0$ and therefore $|a_n w^n|$ is bounded, by M. Therefore

$$\sum_{n=1}^{\infty} \left|n a_n z^{n-1}\right| = \sum_{n=1}^{\infty} n \left|a_n w^{n-1}\right| \left|\frac{z}{w}\right|^{n-1} \leq \frac{M}{|w|} \sum_{n=1}^{\infty} n \left|\frac{z}{w}\right|^{n-1}$$

The latter series converges by the Ratio Test (5.4.32) and therefore the series converges by the Comparison Test (5.4.28). Consider distinct $z, w \in B(0,R)$ then

$$\frac{f(w)-f(z)}{w-z} - f'(z) = \sum_{n=2}^{\infty} a_n \left[\frac{w^n - z^n}{w-z} - nz^{n-1}\right]$$

Observe that for $n \geq 1$

$$\frac{w^n - z^n}{w-z} = w^{n-1} + w^{n-2}z + \ldots + wz^{n-2} + z^{n-1}$$

Therefore for $n \geq 2$

$$\begin{aligned}\frac{w^n - z^n}{w-z} - nz^{n-1} &= (w^{n-1} - z^{n-1}) + z(w^{n-2} - z^{n-2}) + \ldots + z^{n-2}(w-z) \\ &= (w-z)\left[w^{n-2} + 2w^{n-3}z + \ldots + (n-1)z^{n-2}\right]\end{aligned}$$

For any w such that $|w-z| < \frac{R-|z|}{2}$ we have $|w| \leq \frac{R+|z|}{2} =: r < R$. Then

$$\left|\frac{w^n - z^n}{w-z} - nz^{n-1}\right| \leq |w-z| \frac{n(n-1)}{2} r^{n-2}$$

which implies

$$\left|\frac{f(w)-f(z)}{w-z} - f'(z)\right| \leq |w-z| \sum_{n=2}^{\infty} |a_n| \frac{n(n-1)}{2} r^{n-2}$$

The sum is finite because the second formal derivative is absolutely convergent at r, by the part already demonstrated. Therefore we see that f is differentiable at z with derivative $f'(z)$. This also shows that f is continuous at z (...).

□

5.7 Real Analysis

5.7.1 Closed Intervals

Proposition 5.7.1 (k-cells are closed)
Subsets of the form

$$[a_1, b_1] \times \ldots \times [a_k, b_k] \subset \mathbb{R}^k$$

are closed.

Proof. By definition of the product topology we may reduce to the case $k = 1$. Then $[a,b]$ is sequentially closed by (5.1.21), which is equivalent to being closed by (4.1.18) as $\mathbb{R}$ is first countable. □

5.7.2 Power Function

Proposition 5.7.2 (Power function)
Let $\alpha \in \mathbb{Q}$ and $x \in \mathbb{R}$ be non-negative numbers. Suppose $\alpha = \frac{m}{n}$ for integers m, n, where $n > 0$. Then the function

$$x^\alpha := \sqrt[n]{x^m} = \left(\sqrt[n]{x}\right)^m$$

is continuous and strictly increasing/decreasing (according to the sign of α). Furthermore

$$x^\alpha x^\beta = x^{\alpha+\beta}$$

Proof. We first consider the case $\alpha > 0$ and $m, n > 0$. The two definitions are equivalent because x^α is the unique function satisfying $(x^\alpha)^n = x^m$, the latter being an injective function. We may consider the cases $\alpha = m$ and $\alpha = \frac{1}{n}$ separately (since the composition of continuous and increasing functions is continuous and increasing). In light of (5.1.31) and (5.4.11) then it remains to show that $\sqrt[n]{x}$ is continuous. However by (5.1.30)

$$\left|\sqrt[n]{y} - \sqrt[n]{x}\right| \leq \frac{|y-x|}{n\sqrt[n]{x}^{n-1}}.$$

Suppose $\alpha = \frac{m}{n}$ and $\beta = \frac{p}{q}$ then $\alpha + \beta = \frac{mq+np}{nq}$ and

$$\left(x^\alpha x^\beta\right)^{nq} = (x^\alpha)^{nq}(x^\beta)^{nq} = x^{mq}x^{np} = x^{mq+np}$$

whence by uniqueness $x^\alpha x^\beta = x^{\alpha+\beta}$.

We may define $x^0 = 1$ and $x^{-\alpha} = (x^\alpha)^{-1}$, and verify that the addition formula still holds. □

5.7.3 Countability

Proposition 5.7.3 (ℝ is separable and second countable)
The subset $\mathbb{Q} \subset \mathbb{R}$ is dense. Furthermore $\mathbb{R}$ is second countable, with a base formed by open balls with rational center and radius.

Similarly $\mathbb{Q}^k$ is dense in $\mathbb{R}^k$, which is second countable.

Proof. We only need to show that $\mathbb{Q} \subset \mathbb{R}$ is dense, and the rest follows from (5.3.14) because $\mathbb{Q}$ is countable.

By (5.1.25) for every $x \in \mathbb{R}$ there is a sequence $x_n \in \mathbb{Q}$ such that $x_n \to x$. Then (4.1.18) shows that $x \in \overline{\mathbb{Q}}$ as required. □

5.7.4 Bolzano-Weierstrass Theorem

Proposition 5.7.4 (Monotone Subsequence Theorem)
Let (a_n) be a sequence in an ordered field. Then it has a monotone subsequence.

Proof. Define the set of peaks to be

$$X = \{n \in \mathbb{N} \mid m \geq n \implies x_n \geq x_m\}$$

If X is infinite then the elements determine a decreasing subsequence. Suppose X is finite and define $n_1 := \max(X)+1$. We claim inductively that there is a sequence of integers

$$n_1 < n_2 < \ldots < n_k < \ldots$$

such that a_{n_k} is increasing. Evidently $n_k \notin X$ whence there exists $n_{k+1} > n_k$ such that $a_{n_{k+1}} > a_{n_k}$. □

Proposition 5.7.5 (Bolzano-Weierstrass Theorem)
Let (a_n) be a bounded sequence in $\mathbb{R}$. Then it contains a convergent subsequence.

Proof 1. By (5.7.4) a_n has a monotone subsequence. By (5.1.22) this subsequence is convergent. □

Proof 2. Define two sequences of real numbers (l_n), (u_n) recursively as follows

$$(l_n, u_n) \quad := \begin{cases} (L, U) & n = 1 \\ (l_{n-1}, \frac{l_{n-1}+u_{n-1}}{2}) & \{a_n\} \cap [l_{n-1}, \frac{l_{n-1}+u_{n-1}}{2}] \text{ is infinite} \\ (\frac{l_{n-1}+u_{n-1}}{2}, u_{n-1}) & \text{otherwise} \end{cases}$$

Then by definition

a) (l_n) is increasing and (u_n) is decreasing

b) $l_n \leq u_m$ for all n, m

c) $|u_n - l_n| = \frac{U-L}{2^n} \to 0$

d) $[l_n, u_n]$ contains infinitely elements of the sequence (a_n)

We claim that

$$\bigcap_{n \in \mathbb{N}} [l_n, u_n] = \{\sup l_n\} = \{\inf u_n\}$$

Suppose x, y lie in the intersection then by c) we have $|x - y| < \epsilon$ for all ϵ, whence they are equal. So the set consists of at most one element. We claim $\sup l_n$ lies in the intersection. For $l_n \uparrow \sup l_n$ by (...) and $l_n \leq u_m$ whence $\sup l_n \leq u_m$ by (...) as required.

Finally let (a_{n_k}) be a subsequence such that $a_{n_k} \in [l_k, u_k]$ consequently by c) we have $|a_{n_k} - \alpha| \to 0$ where $\alpha := \sup l_n$. □

Corollary 5.7.6 (Bolzano-Weierstrass in $\mathbb{R}^k$)
Let (a_n) be a bounded sequence in $\mathbb{R}^k$. Then it contains a convergent subsequence.

Proof. Observe that $(a_n) = (a_n^1, \ldots, a_n^k)$ where a^i is a bounded sequence in $\mathbb{R}$. By applying (5.7.5) to each coordinate in turn we may find a subsequence n_j such that $a^i_{n_j} \to a^i$ for $i = 1 \ldots k$. By definition of the product norm it is clear that $a_{n_j} \to (a^1, \ldots, a^k)$. □

Proposition 5.7.7 (Heine-Borel Theorem)
Let X be a subset of $\mathbb{R}^k$. Then the following are equivalent

a) *X is closed and bounded*

b) *X is sequentially compact*

c) *X is compact*

In particular every closed k-cell $[\mathbf{a}, \mathbf{b}]$ is compact.

Proof 1. Recall from (5.7.3) that $\mathbb{R}^k$ is second countable, and therefore so is X. Therefore the equivalences $b) \iff c)$ follows from (4.1.74).

$b), c) \implies a)$ We may use (4.1.78) to show that X is closed, observing that $\mathbb{R}^k$ is both first countable and Kolmogorov. Alternatively we may observe $\mathbb{R}^k$ is Hausdorff and appeal to (4.1.75).

To show that it is bounded we may assume it is not to find a sequence x_n such that $\|x_n\| \geq n$. By assumption this has a convergent subsequence $x_{n_j} \to x$. Further there is some N_1 such that $N_1 > \|x\|$ and some N_2 such that $n \geq N_2 \implies \|x_n - x\| < N_1 - |x| \implies \|x_n\| < N_1$. Then taking $n = \max(N_1, N_2)$ implies $\|f(x_n)\|$ is both less and greater than N_1, a contradiction.

Alternatively we may reduce to the case $k = 1$ by noting that $\pi_i(X)$ is compact (4.1.77). The family $\{B(n; 1) \mid n \in \mathbb{N}\}$ forms an open cover, for which there must exist a finite subcover. This immediately shows that $\pi_i(X)$, and therefore X, is bounded.

$a) \implies b), c)$ By assumption $X \subset [-M, M] \times \ldots \times [-M, M]$ for some M, which by (5.7.6) is sequentially compact. We may then use either (4.1.76) or (4.1.79). □

Proof 2. Firstly X is complete iff it is closed by (5.3.12). Evidentally a subset of $\mathbb{R}$ is totally bounded iff it is bounded, and the same argument may be extended to $\mathbb{R}^k$. Therefore the equivalence follows from (5.3.16). □

5.7.5 Boundedness Theorem

Proposition 5.7.8
Let X be a compact topological space and $f : X \to \mathbb{R}^k$ be a continuous function. Then f is bounded and attains its bounds.

Proof 1. We may prove directly the case $X = [a, b]$ and $k = 1$.

Suppose f is not bounded, then there is some sequence (x_n) in X such that $|f(x_n)| \geq n$. By choosing a convergent subsequence (5.7.5) we may assume that $x_n \to x$. Further X is closed so $x \in X$ (4.1.18). By continuity (5.4.14) $f(x_n) \to f(x)$. Choose $N_1 > |f(x)|$ and N_2 such that $n \geq N_2 \implies |f(x_n) - f(x)| < N_1 - |f(x)| \implies |f(x_n)| < N_1$. Then $n := \max(N_1, N_2) \implies |f(x_n)| < N_1$ and $|f(x_n)| > N_1$ a contradiction. □

Proof 2. We may reduce to the case $k = 1$ by considering the composition with the norm $\|\cdot\|$.

By (4.1.77) (or (4.1.80)) $f(X)$ is (sequentially) compact. Then by (5.7.7) $f(X)$ is closed and bounded.

Let $y = \sup f(X)$. By (5.1.18) there exists $y_n \to y$ with $y_n \in f(X)$. Since $f(X)$ is closed we see $y \in f(X)$ by (4.1.18) as required. □

5.7.6 Intermediate Value Theorem

Proposition 5.7.9 (Intervals are connected)
Let $X \subset \mathbb{R}$. Then the following are equivalent

a) *X is connected*

b) *For every $x < y < z$ such that $x, z \in X$, we have $y \in X$*

In particular $(a, b], (a, b), [a, b)$ are connected.

Proof. $b) \implies a)$ Suppose X is disconnected, then $X = U \sqcup V$ with U, V non-empty open and closed subsets of X. Let $x \in U$ and $z \in V$, and assume wlog that $x < z$. Define

$$\alpha := \sup(U \cap (x, z))$$

By (5.1.21) $\alpha \in [x, z] \subset X$. By (5.1.18) there exists $\alpha_n \in U \cap (x, z)$ such that $\alpha_n \uparrow \alpha$. Then by (4.1.19) we have $\alpha \in \mathrm{cl}_{\mathbb{R}}(U) \cap X \overset{(4.1.20)}{=} \mathrm{cl}_X(U) \overset{(4.1.18)}{=} U$. If $\alpha = z$ then we reach a contradiction as U and V were assumed to be

disjoint. Similarly if $\alpha < z$, as U is open in X, we may choose $0 < \epsilon < z - \alpha$ such that $(\alpha - \epsilon, \alpha + \epsilon) \cap X \subset U$. By assumption $\alpha + \epsilon \in X$ whence $\alpha + \epsilon \in U$, which contradicts maximality of α.

$a) \implies b)$ Suppose we have $x < y < z$ such that $x, z \in X$ but $y \notin X$. Then define the open subsets $U = (-\infty, y) \cap X$ and $V = (y, \infty) \cap X$. Then

$$U := (-\infty, y) \cap X = (-\infty, y] \cap X$$

is both open and closed. □

Proposition 5.7.10 (Intermediate Value Theorem)
Let $a < b$ be real numbers and $f : [a, b] \to \mathbb{R}$ continuous such that $f(a) < f(b)$. Then for every $f(a) < c < f(b)$ there exists $x \in (a, b)$ such that $f(x) = c$.

Proof 1. Consider

$$X := \{x' \in [a, b] \mid f(x') < c\}$$

By definition X is bounded, and $a \in X$, so it is non-empty, so we may define $x := \sup X$. We claim that $f(x) = c$. By (5.1.18) there is a sequence $x_n \in X$ such that $x_n \to x$. By (5.4.14) $f(x_n) \to f(x)$ and by (5.1.21) $x \leq b$ and $f(x) \leq c$. Further by assumption $x \neq b$.

To show $f(x) \geq c$ consider the sequence $x_n := x + \min(\frac{1}{n}, b - x) \in [a, b]$. Evidently $x_n \to x$ so by continuity $f(x_n) \to f(x)$. By construction $f(x_n) \geq c$ whence $f(x) \geq c$.

Therefore we conclude $f(x) = c$ as required. □

Proof 2. By (5.7.9) $[a, b]$ is connected, whence by (4.1.83) $f([a, b])$ is connected. The result follows from (5.7.9) again. □

5.7.7 Mean-Value Theorem

Proposition 5.7.11 (Mean-Value Theorem)
Let $f : [a, b] \to \mathbb{R}$ be a continuous function which is differentiable on (a, b). Then there exists $c \in (a, b)$ such that

$$f'(c) = \frac{f(b) - f(a)}{b - a}$$

Proof 1. Define the function

$$g(x) := f(x) - \frac{f(b) - f(a)}{b - a}(x - a)$$

Then g satisfies the same conditions with $g(a) = g(b) = f(a)$ and $g'(x) = f'(x) - \frac{f(b)-f(a)}{b-a}$. Evidently it is sufficient to find $c \in (a, b)$ such that $g'(c) = 0$.

By (5.7.8) g is bounded and attains its maximum and minimum, say at c, d respectively. If both $c, d \in \{a, b\}$ then g must be the constant function whence g' is exactly zero. Otherwise we may assume for example that $c \in (a, b)$. By (5.5.2)

$$\lim_{n \to \infty} \frac{g(c \pm \frac{1}{n}) - g(c)}{\pm \frac{1}{n}} = g'(c)$$

As c is an extremum we may deduce from (5.1.21) that both $g'(c) \leq 0$ and $g'(c) \geq 0$, whence $g'(c) = 0$. □

Corollary 5.7.12
Let $f : [a, b] \to \mathbb{R}$ a continuous function which is differentiable on (a, b). If $f'(x)$ is positive (resp. strictly positive, negative, strictly negative) then $f(x)$ is increasing (resp. strictly increasing, decreasing, strictly decreasing).

Proposition 5.7.13
Let $f : (a, b) \to \mathbb{R}$ be a strictly increasing (resp. decreasing) continuous function. Then f is a homeomorphism onto its image.

Proof. Evidently f is injective, therefore it is only required to show that the map

$$f^{-1} : f(U) \to U$$

is continuous. Without loss of generality we may assume that f is strictly increasing. Suppose $y = f(x)$ then we require to show for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$|y' - y| < \delta \implies \left|f^{-1}(y') - f^{-1}(y)\right| < \epsilon$$

Define $\epsilon' \leq \epsilon$ such that $(x - \epsilon', x + \epsilon') \subset (a, b)$. Define $\delta := \min(f(x + \epsilon') - f(x), f(x) - f(x - \epsilon'))$. Then

$$|y' - y| < \delta \implies f(x - \epsilon') < y' < f(x + \epsilon') \implies x - \epsilon' < f^{-1}(y') < x + \epsilon' \implies \left|f^{-1}(y') - f^{-1}(y)\right| < \epsilon' \leq \epsilon$$

as f^{-1} is also monotonic. □

5.8 Integration

5.8.1 Algebras of Sets

Definition 5.8.1
Let Ω be a set and $\mathcal{F}$ a family of subsets of Ω. We consider the following types of families

a) *$\mathcal{F}$ is a **semi-ring** if the following properties hold*

i) $\emptyset \in \mathcal{F}$

ii) $A_1, \ldots, A_n \in \mathcal{F} \implies A_1 \cap \ldots \cap A_n \in \mathcal{F}$

iii) *For all $A, B \in \mathcal{F}$ there is a family of disjoint subsets $C_1, \ldots, C_n \in \mathcal{F}$ such that*

$$B \setminus A = C_1 \sqcup \ldots \sqcup C_n$$

b) *$\mathcal{F}$ is a **ring** (resp. **algebra**) if the following properties hold*

i) $\emptyset \in \mathcal{F}$ *(resp. $\Omega \in \mathcal{F}$)*

ii) $A_1, \ldots, A_n \in \mathcal{F} \implies A_1 \cup \ldots \cup A_n \in \mathcal{F}$

iii) $A, B \in \mathcal{F} \implies A \setminus B \in \mathcal{F}$

c) *$\mathcal{F}$ is a σ-**ring** (resp. σ-**algebra**) if the following properties hold*

i) $\emptyset \in \mathcal{F}$ *(resp. $\Omega \in \mathcal{F}$)*

ii) $A_1, \ldots, A_n, \ldots \in \mathcal{F} \implies \bigcup_{i=1}^{\infty} A_i \in \mathcal{F}$

iii) $A, B \in \mathcal{F} \implies A \setminus B \in \mathcal{F}$

Evidently σ-ring $\implies$ ring $\implies$ semi-ring.

Example 5.8.2
The family of half-open intervals $\mathcal{F} = \{[a, b) \mid a < b\}$ forms a semi-ring on $\mathbb{R}$.

More generally the family of products of half-open intervals $\{[a_1, b_1) \times \ldots \times [a_n, b_n) \mid a_i < b_i\}$ forms a semi-ring on $\mathbb{R}^n$.

Lemma 5.8.3
Let Ω be a set and $\{\mathcal{F}_\alpha\}_{\alpha \in \mathcal{A}}$ a family of rings (resp. algebras, σ-rings, σ-algebras). Then the family of subsets

$$\bigcap_{\alpha \in \mathcal{A}} \mathcal{F}_\alpha$$

is a ring (resp. algebra, σ-ring, σ-algebra). In particular every family of subsets is contained in a smallest ring (resp. algebra, σ-ring, σ-algebra).

Definition 5.8.4 (Borel Algebra)
*Let X be a topological space. We say that the family of **borel sets** $\mathcal{B}(X)$ is the smallest σ-algebra containing the family of open sets.*

Proposition 5.8.5
Let $\mathcal{R}$ be a semi-ring (resp. semi-algebra). Then the family of finite disjoint unions

$$\mathcal{F} := \{A_1 \sqcup \ldots \sqcup A_n \mid A_1, \ldots, A_n \in \mathcal{R} \text{ pairwise disjoint}\}$$

is a ring (resp. algebra), and indeed the smallest ring (resp. algebra) containing $\mathcal{R}$.

Lemma 5.8.6 (Semi-Ring Extended Set Difference)
Let $\mathcal{R}$ be a semi-ring and $A_0, A_1, \ldots, A_n \in \mathcal{R}$. Then

$$A_0 \setminus \bigcup_{i=1}^{n} A_i = \bigsqcup_{k=1}^{m} B_k$$

for some disjoint sets $B_k \in \mathcal{R}$.

Proof. We proceed by induction, the case $n = 1$ holding by definition. Suppose the relation holds for n. Then

$$A_0 \setminus \bigcup_{i=1}^{n+1} A_i = \left(\bigsqcup_{k=1}^{m} B_k \right) \setminus A_{n+1} = \bigsqcup_{k=1}^{m} (B_k \setminus A_{n+1})$$

and by definition of $\mathcal{R}$ we have

$$B_k \setminus A_{n+1} = \bigsqcup_{j=1}^{N} C_{kj} \quad k = 1 \dots m$$

and $C_{kj} \in \mathcal{R}$. As B_k are disjoint we see that the C_{kj} are disjoint for all j, k and the result follows immediately. □

5.8.2 Set Functions

Definition 5.8.7 (Finitely Additive Set Function)
*Let $\mathcal{F}$ be a family of subsets of Ω containing $\emptyset$. A **set function***

$$\mu : \mathcal{F} \to [0, \infty]$$

*is **finitely additive** if it satisfies*

a) $\mu(\emptyset) = 0$

b) $\mu(A_1 \sqcup \dots \sqcup A_n) = \sum_{i=1}^{n} \mu(A_i)$ *whenever this is well-defined*

*We say a set $A \in \mathcal{F}$ is **finite** if $\mu(A) < \infty$, and μ is **finite** if $\mu(\mathcal{F}) < \infty$.*

*We say that μ is σ-**finite** if for every set $A \in \mathcal{F}$ there exists a sequence A_i such that $A \subset \bigcup_{i=1}^{\infty} A_i$ and $\mu(A_i) < \infty$. If $\Omega \in \mathcal{F}$ then it is sufficient for this condition to hold for Ω.*

Proposition 5.8.8 (Extension Theorem I)
Let $\mathcal{R}$ be a semi-ring, and $\mathcal{F}$ the ring generated by $\mathcal{R}$. Given a finitely additive set function $\mu : \mathcal{R} \to [0, \infty]$ there exists a unique extension to $\mathcal{F}$ given by

$$\mu(A_1 \sqcup \dots \sqcup A_n) = \sum_{i=1}^{n} \mu(A_i)$$

which is finitely additive.

Proof. In order to ensure the definition is well-defined suppose

$$A_1 \sqcup \dots \sqcup A_n = B_1 \sqcup \dots \sqcup B_m$$

Then in particular

$$A_i = (A_i \cap B_1) \sqcup \dots \sqcup (A_i \cap B_m)$$

We may deduce by the additive property that

$$\sum_{i=1}^{n} \mu(A_i) = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu(A_i \cap B_j)$$

Evidentally this is symmetric in A and B so this also equals $\sum_{j=1}^{m} \mu(B_j)$. This shows that the measure μ is well-defined. The additivity property is straightforward. □

Proposition 5.8.9 (Properties of finitely-additive set functions)
*Let $(\Omega, \mathcal{R})$ be a **semi-ring** and $\mu : \mathcal{R} \to [0, \infty]$ a finitely additive set function. Then*

a) *μ is **monotone**, that is for sets $A \subset B$ we have*

$$\mu(A) \leq \mu(B)$$

b) *Suppose $A_1 \sqcup \dots \sqcup A_n \subset A_0$ for $A_i \in \mathcal{R}$ then*

$$\sum_{i=1}^{n} \mu(A_i) \leq \mu(A_0)$$

c) *Suppose* $A_0 \subset A_1 \cup \ldots \cup A_n$ *for* $A_i \in \mathcal{R}$ *then*

$$\mu(A_0) \leq \sum_{i=1}^{n} \mu(A_i)$$

Proof. a) By definition $B \setminus A = C_1 \sqcup \ldots \sqcup C_n$ and therefore by finite additivity

$$\mu(B) = \mu(C_1 \sqcup \ldots \sqcup C_n \sqcup A) = \mu(C_1) + \ldots + \mu(C_n) + \mu(A) \geq \mu(A)$$

b) By (5.8.6)

$$A_0 \setminus \bigsqcup_{i=1}^{n} A_i = \bigsqcup_{k=1}^{m} B_k$$

for some $B_k \in \mathcal{R}$ disjoint. Observe they are by construction disjoint from A_i therefore

$$A_0 = A_1 \sqcup \ldots \sqcup A_n \sqcup B_1 \sqcup \ldots \sqcup B_m$$

The result follows from finite additivity.

c) By replacing A_i with $A_i \cap A_0$ we may assume that $A_0 = A_1 \cup \ldots \cup A_n$ by a). Observe that by (5.8.6)

$$\widehat{A}_i := A_i \setminus \bigcup_{j=1}^{i-1} A_j = \bigsqcup_{k=1}^{m} C_{ik}$$

for $C_{ik} \in \mathcal{R}$ (if necessary padding out by $\emptyset$). Therefore

$$A_0 = \bigsqcup_{i=1}^{n} \widehat{A}_i = \bigsqcup_{i,k} C_{ik}$$

and by finite additivity

$$\mu(A_0) = \sum_{i=1}^{n} \sum_{k=1}^{m} \mu(C_{ik})$$

By b)

$$\sum_{k=1}^{m} \mu(C_{ik}) \leq \mu(A_i)$$

from which the result follows.

□

Definition 5.8.10 (Simple Functions)
Let $(\Omega, \mathcal{F})$ *be a family of subsets and* X *a normed vector space over* $\mathbb{R}$*. We define the space of simple functions to be*

$$\mathrm{Simple}(\mathcal{F}, \mathrm{X}) := \left\{ \sum_{\mathrm{i}=1}^{\mathrm{n}} \lambda_{\mathrm{i}} \mathbf{1}_{\mathrm{A_i}} \mid \mathrm{A}_1 \sqcup \ldots \sqcup \mathrm{A_n} = \Omega, \lambda_1, \ldots, \lambda_{\mathrm{n}} \in \mathrm{X} \right\}$$

Proposition 5.8.11 (Integration of Simple Functions)
Let $(\Omega, \mathcal{F})$ *be a ring and* μ *a finitely additive measure and* X *a vector space over* $\mathbb{R}$*. There is a well-defined linear map*

$$\begin{aligned} \int d\mu : \mathrm{Simple}(\mathcal{F}, \mathrm{X}) &\to X \\ \sum_{i=1}^{n} \alpha_i \mathbf{1}_{A_i} &\to \sum_{i=1}^{n} \alpha_i \mu(A_i) \end{aligned}$$

Proof. Suppose that $\sum_{i=1}^{n} \alpha_i \mathbf{1}_{A_i} = \sum_{j=1}^{m} \beta_j \mathbf{1}_{B_j}$ where both $\{A_i\}$ and $\{B_j\}$ are *disjoint* partitions of X. Then

$$A_i = (A_i \cap B_1) \sqcup \ldots \sqcup (A_i \cap B_m)$$

whence

$$\mu(A_i) = \sum_{j=1}^{m} \mu(A_i \cap B_j)$$

Therefore

$$\sum_{i=1}^{n} \alpha_i \mu(A_i) = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_i \mu(A_i \cap B_j)$$

By the same argument

$$\sum_{j=1}^{m} \beta_j \mu(B_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} \beta_j \mu(A_i \cap B_j)$$

Evidently $\{A_i \cap B_j\}$ is a disjoint partition of X. If $A_i \cap B_j \neq \emptyset$ then the first equality requires that $\alpha_i = \beta_j$. This shows that the integrals are equal as required. □

Proposition 5.8.12
Let $(\Omega, \mathcal{F})$ be a ring, μ a finitely additive measure and X a normed vector space over $\mathbb{R}$. Then we have the following properties

a) $\int (f+g)d\mu = \int f d\mu + \int g d\mu$

b) $\int \lambda f d\mu = \lambda \int f d\mu$

c) $\left\| \int f d\mu \right\| \leq \int \|f\| \, d\mu$

If μ is finite then

$$\left\| \int f d\mu \right\| \leq \mu(\Omega) \left\| f \right\|_\infty$$

Proof. For the last part observe that

$$\left\| \sum_{i=1}^{n} \alpha \mathbf{1}_{A_i} \right\| \leq \sum_{i=1}^{n} \left\| \alpha \right\|_i \mu(A_i) \leq \left\| f \right\|_\infty \sum_{i=1}^{n} \mu(A_i) \leq \mu(\Omega) \left\| f \right\|_\infty$$

□

5.8.3 Integration of Regulated Functions

Definition 5.8.13 (SubBorel Measure)
Let $\Omega = \mathbb{R}$ and $\mathcal{F}$ the ring generated by the half-open subintervals. Then there is a finitely additive measure $\mu : \mathcal{F} \to \mathbb{R}$ determined by

$$\mu([b, a)) = (b - a)$$

By (...) this determines a bounded linear map

$$\int : \text{Simple}(\mathbb{R}, X) \to X$$

for any real vector space X.

Definition 5.8.14 (Regulated Function)
*Let X be a Banach space. A **regulated function** is a map*

$$f : \mathbb{R} \to X$$

*of **compact** support for which there exists a sequence (f_n) of* simple *functions (with respect to the ring generated by the half-open subintervals) such that*

$$f_n \to f$$

converges uniformly. We denote this by

$$\text{Reg}(\mathbb{R}, X)$$

Lemma 5.8.15
A uniform limit of bounded functions is bounded. In particular a regulated function is bounded.

Proof. There is some N such that $n \geq N \implies \|f_n(x) - f(x)\| < 1$. Then

$$\|f(x)\| \leq \|f_n(x) - f(x)\| + \|f_n(x)\| \leq 1 + \|f_n(x)\|$$

We may take supremum over x to show that f is bounded. □

Proposition 5.8.16 (Continuous Functions are Regulated)
Let X be a Banach space and $f : [a, b] \to X$ a continuous function. Then f is regulated.

Proof. We may define

$$\begin{aligned} f_n(x) &:= \sum_{i=1}^{N} f(a_i)\mathbf{1}_{[a_i,b_i)}(x) + \mathbf{1}\{x=b\}f(b) \\ a_i &:= a_i + \frac{j-1}{N}(b-a) \\ b_i &:= a_i + \frac{j}{N}(b-a) \end{aligned}$$

By (...) f is uniformly continuous so that for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$|x-y| < \delta \implies \|f(x) - f(y)\| < \epsilon$$

Choose N such that

$$\max_i \frac{b_i - a_i}{N} < \delta$$

For every $x \in [a,b]$ we have $x \in [a_i, b_i)$ for some i and by construction $\|f(x) - f(a_i)\| < \epsilon$ whence $\|f(x) - f_n(x)\| < \epsilon$. As this applies for any $x \in [a,b]$ we see that the convergence is uniform. □

Proposition 5.8.17 (Integration of Regulated Functions)
Let X be a Banach space and $f : [a,b] \to X$ a function for which $f_n \to f$ converges uniformly. Then the sequence

$$\int_a^b f_n$$

converges in X. Furthermore the limit is independent of the choice of f_n, and we denote the limit by $\int_a^b f$.

In particular the integration of continuous functions with compact support is well-defined.

Proof. Let $x_n := \int f_n$. Then by (...) we have

$$\|x_n - x_m\| \leq (b-a)\|f_n - f_m\|_\infty$$

By the uniform convergence of f_n we see that x_n is a cauchy sequence, and so by assumption $x_n \to x$. The uniqueness is straightforward. □

Lemma 5.8.18
Let X be a Banach space and $f \in \mathrm{Reg}([a,b], X)$. Then $\|f\| \in \mathrm{Reg}([a,b], \mathbb{R})$.

Proposition 5.8.19 (Properties of the Integral)
Let X be a Banach space. Then the following properties hold

a) $\int_a^b (\lambda f + \mu g) = \lambda \int_a^b f + \mu \int_a^b g$

b) $\int_a^b f + \int_b^c f = \int_a^c f$

c) $\left\| \int_a^b f \right\| \leq \int_a^b \|f\|$

In the case $X = \mathbb{R}$ then we also have the following properties

d) $f \geq 0 \implies \int_a^b f \geq 0$

e) $f \leq g \implies \int_a^b f \leq \int_a^b g$

f) *f continuous, positive such that $\int_a^b f = 0$ implies $f \equiv 0$*

Proposition 5.8.20 (Fundamental Theorem of Calculus)
Let $f \in \mathrm{Reg}([a,b], X)$ where X is a Banach space. Suppose $c \in (a,b)$ is a point where f is continuous. Define

$$F(x) := \int_a^x f$$

Then F is differentiable at c and $F'(c) = f(c)$

Proof. Observe that for $0 < h < b - c$

$$\begin{aligned}\left\| \frac{F(c+h) - F(c)}{h} - f(c) \right\| &= \frac{1}{h} \left\| \int_c^{c+h} (f(t) - f(c)) dt \right\| \\ &\leq \frac{1}{h} \int_c^{c+h} \|f(t) - f(c)\| \, dt \\ &\leq \sup_{|t-c|<h} \|f(t) - f(c)\|\end{aligned}$$

and similarly for $a - c < h < 0$. As f is regulated it is bounded (...) and so the supremum is finite. As f is assumed continuous we find $F'(c) = f(c)$. □

Proposition 5.8.21
Suppose $f_i \in \mathrm{Reg}([a,b], X_i)$ for $i = 1 \ldots n$. Then $(f_1, \ldots, f_n) \in \mathrm{Reg}([a,b], X)$ where $X := X_1 \times \ldots X_n$ and

$$\int_a^b f = \left(\int_a^b f_1, \ldots, \int_a^b f_n \right)$$

5.8.4 Measure Spaces

To create a robust theory of integration it is necessary to replace finite additivity with countably additivity, and further show that such set functions can be defined over σ-algebras and not just algebras.

Definition 5.8.22 (Countably Additive Set Function)
Let $\mathcal{F}$ be a family of subsets of Ω containing $\emptyset$. A function

$$\mu : \mathcal{F} \to [0, \infty]$$

*is a **countably additive set function** (or **measure**) if it satisfies*

a) $\mu(\emptyset) = 0$

b) $\mu\left(\bigsqcup_{n=1}^{\infty} A_n\right) = \sum_{i=1}^{\infty} \mu(A_i)$ *whenever this is well-defined*

*We say it is **countably subadditive** if it satisfies*

$$\mu\left(\bigcup_{i=1}^{\infty} A_i \right) \leq \sum_{i=1}^{\infty} \mu(A_i)$$

whenever this is well-defined. We show in (5.8.25) that these conditions are almost equivalent.

Definition 5.8.23 (Measurable Space)
*Let $(\Omega, \mathcal{F})$ be a measurable space and $\mu : \mathcal{F} \to [0, \infty]$ a measure. Then the triplet $(\Omega, \mathcal{F}, \mu)$ is a **measurable space**.*

The following are standard results which are somewhat more awkward to prove in the case of semi-rings. However the proofs follow precisely the same lines and semi-ring extension theorem may be more directly applicable.

Proposition 5.8.24 (Continuity of Measures)
Let $\mathcal{R}$ be a semi-ring of subsets of Ω and $\mu : \mathcal{R} \to [0, \infty]$ a countably additive measure. Then for any sequence of sets $A_1, A_2, \ldots \in \mathcal{R}$ we have

$$\lim_{n \to \infty} \mu\left(\bigcup_{i=1}^{n} A_i \right) = \mu\left(\bigcup_{n=1}^{\infty} A_n \right)$$

whenever this is well-defined.

Proof. Define the increasing sequence

$$B_n := \bigcup_{i=1}^{n} A_i$$

then wish to show

$$\lim_{n \to \infty} \mu(B_n) = \mu\left(\bigcup_{n=1}^{\infty} B_n \right).$$

By definition we have (with the convention $B_0 = \emptyset$)

$$B_i \setminus \bigcup_{j=1}^{i-1} B_j = B_i \setminus B_{i-1} = \bigsqcup_{k=1}^{N_i} C_{ik} \quad i = 1, 2, \ldots$$

for $C_{ik} \in \mathcal{R}$ whence

$$B_n = \bigsqcup_{i=1}^{n} B_i \setminus B_{i-1} = \bigsqcup_{i=1}^{n} \bigsqcup_{k=1}^{N_n} C_{ik}$$

for $n = 1, 2, \ldots, \infty$. Then by additivity

$$\lim_{n\to\infty} \mu(B_n) = \lim_{n\to\infty} \sum_{i=1}^{n} \sum_{k=1}^{N_i} \mu(C_{ik}) = \sum_{i=1}^{\infty} \sum_{k=1}^{N_i} \mu(C_{ik})$$

and

$$\mu\left(\bigcup_{n=1}^{\infty} B_n\right) = \mu\left(\bigsqcup_{i=1}^{\infty} \bigsqcup_{k=1}^{N_i} C_{ik}\right) = \sum_{i=1}^{\infty} \sum_{k=1}^{N_i} \mu(C_{ik})$$

□

Proposition 5.8.25 (Finitely additive + Countably subadditive $\iff$ Countably additive)
Let $\mathcal{R}$ be a semi-ring of subsets of Ω and $\mu : \mathcal{R} \to [0, \infty]$ a finitely additive set function. Then

$$\mu\left(\bigsqcup_{i=1}^{\infty} A_i\right) \geq \sum_{i=1}^{\infty} \mu(A_i)$$

whenever this is well-defined. In particular μ is a measure iff it is countably subadditive.

Proof. By (5.8.9).b) we have

$$\sum_{i=1}^{n} \mu(A_i) \leq \mu\left(\bigsqcup_{i=1}^{\infty} A_i\right)$$

and the result follows by taking $n \to \infty$ (5.1.21).

Therefore if μ is countably subadditive it must also be countably additive. Conversely if μ is countably additive then we aim to show

$$\mu\left(\bigcup_{i=1}^{\infty} A_i\right) \leq \sum_{i=1}^{\infty} \mu(A_i)$$

for a not necessarily disjoint sequence $A_i \in \mathcal{R}$. By assumption μ is finitely additive, so by (5.8.9).c)

$$\mu\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} \mu(A_i) \leq \sum_{i=1}^{\infty} \mu(A_i)$$

Using continuity of measures (5.8.24) we deduce that

$$\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = \lim_{n\to\infty} \mu\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{\infty} \mu(A_i)$$

as required. □

Proposition 5.8.26 (Extension Theorem II)
Let $\mathcal{R}$ be a semi-ring of sets over Ω and $\mu : \mathcal{R} \to [0, \infty]$ a measure. Suppose that Ω is denumerable union of sets in $\mathcal{R}$. Then there exists an extension

$$\widetilde{\mu} : \sigma(\mathcal{R}) \to [0, \infty]$$

to the σ-algebra generated by $\mathcal{R}$. When μ is σ-finite then this extension is unique. More precisely it is given by

$$\widetilde{\mu}(A) := \inf\left\{\sum_{i=1}^{\infty} \mu(A_i) \mid A \subset \bigcup_{i=1}^{\infty} A_i \,, A_i \in \mathcal{R}\right\}$$

Proof. Define first the "outer measure"

$$\begin{aligned} \mu^\star : \mathcal{P}(\Omega) &\to [0, \infty] \\ \mu^\star(A) &:= \inf\{\sum_{i=1}^{\infty} \mu(E_i) \mid A \subset \bigcup_{i=1}^{\infty} E_i \quad E_i \in \mathcal{F}\} \end{aligned}$$

Note that the infimum is well-defined precisely by the hypothesis. Further define the family of subsets

$$\widehat{\mathcal{R}} := \{A \subset \Omega \mid \mu^\star(B) = \mu^\star(A \cap B) + \mu^\star(A^c \cap B) \quad \forall B \subset \Omega\}$$

We make a number of claims

a) $\mu^\star(A) = \mu(A)$ for all $A \in \mathcal{R}$

b) $\mu^\star$ is countably subadditive and monotone

$$\mu^\star\left(\bigcup_{i=1}^{\infty} A_i\right) \leq \sum_{i=1}^{\infty} \mu^\star(A_i) \quad A_i \subset \Omega$$

c) $\mathcal{R} \subset \widehat{\mathcal{R}}$

d) $\widehat{\mathcal{R}}$ is a σ-algebra containing $\sigma(\mathcal{R})$ and $\mu^\star$ is a measure on $\widehat{\mathcal{R}}$

and prove each in turn

a) Evidently $\mu^\star(A) \leq \mu(A)$ as $A \subset A \cup \emptyset \ldots \cup \emptyset \ldots$. Conversely suppose that $A \subset \cup_{i=1}^{\infty} A_i$ for $A_i \in \mathcal{R}$ and $\mu^\star(A) < \infty$ (otherwise the reverse inequality is clear). Then evidently

$$A = \bigcup_{i=1}^{\infty} (A_i \cap A)$$

As μ is countably subadditive (5.8.25) and monotone (5.8.9) we see

$$\mu(A) \leq \sum_{i=1}^{\infty} \mu(A_i \cap A) \leq \sum_{i=1}^{\infty} \mu(A_i)$$

By definition of the infimum we find $\mu(A) \leq \mu^\star(A)$.

b) Let $A_1, \ldots, A_n, \ldots$ be subsets of Ω such that $A \subset \bigcup_{i=1}^{\infty} A_i$. For a given $\epsilon > 0$, choose $A_{ij} \in \mathcal{R}$ such that $A_i \subset \bigcup_{j=1}^{\infty} A_{ij}$ and

$$\sum_{j=1}^{\infty} \mu(A_{ij}) \leq \mu^\star(A_i) + \frac{\epsilon}{2^i}$$

Then evidently $A \subset \bigcup_{i,j=1}^{\infty} A_{ij}$ and so by definition

$$\mu^\star(A) \leq \sum_{i,j=1}^{\infty} \mu(A_{ij}) \leq \sum_{i=1}^{\infty} \mu^\star(A_i) + \epsilon$$

As ϵ was arbitrary we deduce that $\mu^\star$ is countably subadditive. Monotonicity is straightforward from the definition.

c) Suppose $A \in \mathcal{R}$ and $B \subset \Omega$ then we require to prove that

$$\mu^\star(B) = \mu^\star(A \cap B) + \mu^\star(A^c \cap B)$$

By subadditivity it is sufficient so show that

$$\mu^\star(B) \geq \mu^\star(A \cap B) + \mu^\star(A^c \cap B)$$

Let $B \subset \bigcup_{i=1}^{\infty} B_i$ be an arbitrary cover with $B_i \in \mathcal{R}$, then by definition of $\mu^\star$ it is sufficient to show that

$$\mu^\star(A \cap B) + \mu^\star(A^c \cap B) \leq \sum_{i=1}^{\infty} \mu(B_i)$$

Recall by definition of semi-ring that

$$A^c \cap B_i = \bigsqcup_{k=1}^{n_i} C_{ik}$$

for some disjoint sets $C_{ik} \in \mathcal{R}$ and evidently

$$A \cap B \subset \bigcup_{i=1}^{\infty} (A \cap B_i)$$

$$A^c \cap B \subset \bigcup_{i=1}^{\infty} \bigsqcup_{k=1}^{n_i} C_{ik}$$

Therefore by monotonicity and countable subadditivity of $\mu^\star$

$$\begin{aligned}\mu^\star(A\cap B)+\mu^\star(A^c\cap B) &\leq \mu^\star\left(\bigcup_{i=1}^\infty (A\cap B_i)\right)+\mu^\star\left(\bigcup_{i=1}^\infty\bigsqcup_{k=1}^{n_i} C_{ik}\right)\\ &\leq \sum_{i=1}^\infty \mu^\star(A\cap B_i)+\sum_{i=1}^\infty\sum_{k=1}^{n_i}\mu(C_{ik})\\ &= \sum_{i=1}^\infty \mu(A\cap B_i)+\sum_{i=1}^\infty\sum_{k=1}^{n_i}\mu(C_{ik})\\ &= \sum_{i=1}^\infty\left(\mu(A\cap B_i)+\sum_{k=1}^{n_i}\mu(C_{ik})\right)\\ &= \sum_{i=1}^\infty \mu(B_i)\end{aligned}$$

where the last step follows from finite additivity of μ.

d) We prove the various properties in turn

i) Evidently $\mu^\star(\emptyset)=0$ and therefore $\emptyset,\Omega\in\widehat{\mathcal{R}}$

ii) Given $A_1,A_2\in\widehat{\mathcal{R}}$ and $B\subset\Omega$. Observe that we may apply the measurability condition to B and A_1, and then to $B\cap A_1$ and A_2, and $B\cap A_1^c$ and A_2 to find

$$\begin{aligned}\mu^\star(B) &= \mu^\star(B\cap A_1)+\mu^\star(B\cap A_1^c)\\ &= \mu^\star(B\cap A_1\cap A_2)+\mu^\star(B\cap A_1\cap A_2^c)+\mu^\star(B\cap A_1^c\cap A_2)+\mu^\star(B\cap A_1^c\cap A_2^c)\end{aligned}$$

We may also consider the relationship with B replaced with $B\cap(A_1\cup A_2)$ to find

$$\mu^\star(B\cap(A_1\cup A_2)) = \mu^\star(B\cap A_1\cap A_2)+\mu^\star(B\cap A_1\cap A_2^c)+\mu^\star(B\cap A_1^c\cap A_2) \tag{5.1}$$

Combining these two relations we deduce

$$\mu^\star(B)=\mu^\star(B\cap(A_1\cup A_2))+\mu^\star(B\cap(A_1\cup A_2)^c)$$

As B was arbitrary then we deduce $A_1\cup A_2\in\widehat{\mathcal{R}}$. Evidently by definition $A^c\in\widehat{\mathcal{R}}$ and therefore by de-morgan $A_1\cap A_2\in\widehat{\mathcal{R}}$. Therefore $\widehat{\mathcal{R}}$ is closed under finite unions and intersections.

iii) Let $A_1,\ldots,A_n\in\widehat{\mathcal{R}}$ be disjoint then we claim that

$$\mu^\star\left(B\cap\left(\bigsqcup_{i=1}^n A_i\right)\right)=\sum_{i=1}^n\mu^\star\left(B\cap A_i\right)$$

From (5.1) we have

$$\mu^\star\left(B\cap(A_1\sqcup A_2)\right)=\mu^\star(B\cap A_1)+\mu^\star(B\cap A_2)$$

and the result follows by induction.

iv) Let $A_1,A_2,\ldots\in\widehat{\mathcal{R}}$ be a countable family and $B\subset\Omega$. We require to prove that

$$\mu^\star(B)=\mu^\star\left(B\cap\bigcup_{i=1}^\infty A_i\right)+\mu^\star\left(B\cap\left(\bigcup_{i=1}^\infty A_i\right)^c\right)$$

By (5.8.6) we may consider the decomposition

$$A_i\setminus\bigcup_{j=1}^{i-1}A_j=\bigsqcup_{k=1}^{n_i}C_{ik}$$

where $C_{ik}\in\mathcal{R}$ are disjoint. Observe

$$\bigcup_{i=1}^n A_i=\bigsqcup_{i=1}^n\bigsqcup_{k=1}^{n_i}C_{ik}\text{ for }n=1,2,\ldots,\infty$$

We have shown in ii) that $\bigcup_{i=1}^{n} A_i \in \widehat{\mathcal{R}}$, therefore

$$\begin{aligned}\mu^\star(B) &= \mu^\star\left(B \cap \left(\bigcup_{i=1}^{n} A_i\right)\right) + \mu^\star\left(B \cap \left(\bigcup_{i=1}^{n} A_i\right)^c\right) \\ &= \mu^\star\left(B \cap \left(\bigsqcup_{i=1}^{n}\bigsqcup_{k=1}^{n_i} C_{ik}\right)\right) + \mu^\star\left(B \cap \left(\bigcup_{i=1}^{n} A_i\right)^c\right)\end{aligned}$$

Recall from iii) that $\mu^\star(B \cap -)$ is finitely additive on $\widehat{\mathcal{R}}$. Additionally by monotonicity we may deduce that

$$\begin{aligned}\mu^\star(B) &= \sum_{i=1}^{n}\sum_{k=1}^{n_i} \mu^\star(B \cap C_{ik}) + \mu^\star\left(B \cap \left(\bigcup_{i=1}^{n} A_i\right)^c\right) \\ &\geq \sum_{i=1}^{n}\sum_{k=1}^{n_i} \mu^\star(B \cap C_{ik}) + \mu^\star\left(B \cap \left(\bigcup_{i=1}^{\infty} A_i\right)^c\right)\end{aligned}$$

Letting $n \to \infty$ we find by subadditivity

$$\begin{aligned}\mu^\star(B) &\geq \sum_{i=1}^{\infty}\sum_{k=1}^{n_i} \mu^\star\left(B \cap C_{ik}\right) + \mu^\star\left(B \cap \left(\bigcup_{i=1}^{\infty} A_i\right)^c\right) \\ &\geq \mu^\star\left(B \cap \left(\bigcup_{i=1}^{\infty} A_i\right)\right) + \mu^\star\left(B \cap \left(\bigcup_{i=1}^{\infty} A_i\right)^c\right)\end{aligned}$$

However by subadditivity the reverse inequality holds and we deduce that these are all equal. This shows that $\bigcup_{i=1}^{\infty} A_i \in \widehat{\mathcal{F}}$ and $\widehat{\mathcal{F}}$ is closed under countable unions. Consider further the case A_i are disjoint and $B := \bigsqcup_{j=1}^{\infty} A_j$. Then we may assume that $n_i = 1$ and $C_{i1} = A_i$. Using the above relationship

$$\mu^\star\left(\bigsqcup_{j=1}^{\infty} A_j\right) = \sum_{i=1}^{\infty} \mu^\star\left(\left(\bigsqcup_{j=1}^{\infty} A_j\right) \cap A_i\right) = \sum_{i=1}^{\infty} \mu^\star\left(A_i\right).$$

This shows that $\mu^\star$ is countably additive.

□

Definition 5.8.27 (Complete Set Function)
*Let $(\Omega, \mathcal{F}, \mu)$ be a measure space. We say it is **complete** if for every null set N (such that $\mu(N) = 0$) and $N' \subseteq N$ we have $N' \in \mathcal{F}$.*

Proposition 5.8.28 (Completion of a Measure Space)
*Let $(\Omega, \mathcal{F}, \mu)$ be a measure space and define the **completion** by*

$$\begin{aligned}\overline{\mathcal{F}} &:= \{A \cup Z \mid A \in \mathcal{F},\, Z \subseteq N,\, \mu(N) = 0\} \\ \overline{\mu}(A \cup Z) &:= \mu(A)\end{aligned}$$

Then $(\Omega, \overline{\mathcal{F}}, \overline{\mu})$ is a well-defined complete measure space. Furthermore $\overline{\mathcal{F}}$ is the smallest complete σ-algebra containing $\mathcal{F}$, and $\overline{\mu}$ is the unique extension.

5.8.5 Borel Measure on $\mathbb{R}$

Proposition 5.8.29
Let $\mathcal{R}$ be the semi-ring of half-open intervals over $\mathbb{R}$ Then the set function

$$\mu : \mathcal{R} \to [0, \infty]$$

given by

$$\mu([a, b)) = b - a,$$

is countably additive and σ-finite.

Proof. Evidently μ is finitely additive, therefore by (5.8.25) it is sufficient to show that it is countably subadditive. Suppose that

$$\bigcup_{i=1}^{\infty} [a_i, b_i) = [a, b)$$

Let $\epsilon < b-a$. Then $[a, b-\epsilon]$ is compact by (...) and $U_i := (a_i - \frac{\delta}{2^i}, b_i)$ is open for every $\delta > 0$. By definition of compactness there is some finite integer n such that

$$[a, \tilde{b}] := [a, b-\epsilon] \subset \bigcup_{i=1}^{n} \left(a_i - \frac{\delta}{2^i}, b_i\right) =: (\tilde{a}_i, b_i)$$

By reordering we assume that $\tilde{a}_1 < \ldots < \tilde{a}_n$. As $[a, \tilde{b}]$ is an interval we must have $\tilde{a}_{i+1} < b_i$. Further we may assume that $b_i < b_{i+1}$ (otherwise we may omit the interval $(\tilde{a}_i, b_i)$). By construction we must also have $\tilde{a}_1 < a$ and $\tilde{b} < b_n$.

Consequently

$$b - a - \epsilon = \tilde{b} - a \leq b_n - \tilde{a}_1 = b_1 - \tilde{a}_1 + \sum_{i=1}^{n-1}(b_{i+1} - b_i) \leq \sum_{i=1}^{n}(b_i - \tilde{a}_i) \leq \sum_{i=1}^{n}(b_i - a_i) + \delta \leq \sum_{i=1}^{\infty}(b_i - a_i) + \delta$$

This shows

$$\mu([a,b)) = \mu\left(\bigcup_{i=1}^{\infty}[a_i, b_i)\right) \leq \sum_{i=1}^{\infty}\mu([a_i, b_i))$$

as required. □

Proposition 5.8.30
Let $D \subset \mathbb{R}$ be an additive subgroup containing $\mathbb{Q}$. Then $\mathcal{B}(\mathbb{R})$ is generated by any of the following families of intervals

1. $(a, b] \quad a < b \in D$
2. $(a, b) \quad a < b \in D$
3. $[a, b) \quad a < b \in D$
4. $(a, \infty) \quad a \in D$
5. $[a, \infty) \quad a \in D$
6. $(-\infty, a] \quad a \in D$
7. $(-\infty, a) \quad a \in D$

Further there is a unique measure

$$\mu : \mathcal{B}(\mathbb{R}) \to [0, \infty]$$

such that

$$\mu([b, a)) = b - a$$

Proof. Denote the corresponding σ-algebras by $\mathcal{F}_1, \ldots, \mathcal{F}_7$. Observe that by the Archimedean property

$$\begin{aligned}
(a, b) &= \bigcup_{n=1}^{\infty}\left(a, b - \frac{1}{n}\right] = \bigcup_{n=1}^{\infty}\left[a + \frac{1}{n}, b\right) \\
[a, b) &= \bigcap_{n=1}^{\infty}\left(a - \frac{1}{n}, b\right) \\
(a, b] &= \bigcap_{n=1}^{\infty}\left(a, b + \frac{1}{n}\right)
\end{aligned}$$

so that $\mathcal{F}_1 = \mathcal{F}_2 = \mathcal{F}_3$. We may argue similarly $\mathcal{F}_4 = \mathcal{F}_5 = \mathcal{F}_6 = \mathcal{F}_7$. Finally

$$(a, b) = (a, \infty) \cap (-\infty, b)$$

and

$$(a, \infty) = \bigcup_{n=1}^{\infty}(a, n)$$

to show these are equal. The measure μ exists by (5.8.29) and (5.8.26). □

Proposition 5.8.31 (Borel Measure on the Extended Real Line)
Let $\mathcal{B}(\mathbb{R}^\sharp)$ be the Borel Measure on the extended real line. Then $\mathcal{B}(\mathbb{R}^\sharp)$ consists of sets of the form

$$\{A \subset \mathbb{R}^\sharp \mid A \cap \mathbb{R} \in \mathcal{B}(\mathbb{R})\}$$

or equivalently

$$\{A \cup B \mid A \in \mathcal{B}(\mathbb{R}),\, B \subset \mathcal{P}(\{-\infty, \infty\})\}\,.$$

Furthermore it is generated by any of the following families

1. $(a, \infty]$
2. $[a, \infty]$
3. $[-\infty, a)$
4. $[-\infty, a]$

for $a \in D$ where $D \subset \mathbb{R}$ is an additive subgroup containing $\mathbb{Q}$.

Proof. If $U \subset \mathbb{R}$ is open, then it is also open in $\mathbb{R}^\sharp$. Therefore $\mathcal{B}(\mathbb{R}) \subset \mathcal{B}(\mathbb{R}^\sharp)$. Evidently $\mathbb{R}$, $\{\infty\}$, $\{-\infty\} \in \mathcal{B}(\mathbb{R}^\sharp)$ as they are open and closed respectively. This shows that the given family equals $\mathcal{B}(\mathbb{R}^\sharp)$.

Denote by $\mathcal{F}_1, \ldots, \mathcal{F}_4$ the σ-algebras generated by the respective families of rays. Note that $\mathcal{F}_1 = \mathcal{F}_4$ and $\mathcal{F}_2 = \mathcal{F}_3$ by taking complements. Further $\{\infty\} \in \mathcal{F}_1 \cap \mathcal{F}_2$ by taking intersections as $a \to \infty$ and similarly $\{-\infty\} \in \mathcal{F}_4 \cap \mathcal{F}_3$. This shows that they also contain either the open rays (a, ∞) or the semi-open rays $[a, \infty)$. Therefore they contain $\mathcal{B}(\mathbb{R})$ by (5.8.30). Then by the characterisation in the first part we see that this equals $\mathcal{B}(\mathbb{R}^\sharp)$. □

5.8.6 Product Measure

Definition 5.8.32 (Product of σ-algebra)
*Let $(\Omega_1, \mathcal{F}_1), \ldots, (\Omega_n, \mathcal{F}_n)$ be a family of measurable spaces. Then define the **product measurable space** $(\Omega_1 \times \ldots \times \Omega_n, \mathcal{F}_1 \otimes \ldots \otimes \mathcal{F}_n)$ to be given by*

$$\mathcal{F}_1 \otimes \ldots \otimes \mathcal{F}_n := \sigma\left(\mathcal{F}_1 \times \ldots \times \mathcal{F}_n\right)$$

and

$$\mathcal{F}_1 \times \ldots \times \mathcal{F}_n := \{A_1 \times \ldots \times A_n \mid A_i \in \mathcal{F}_i\}\,.$$

Definition 5.8.33 (Product Measure)
Let $(\Omega_i, \mathcal{F}_i, \mu_i)$ be a family of σ-finite measures for $i = 1 \ldots n$. Then we say a measure

$$\mu_1 \otimes \ldots \otimes \mu_n : \mathcal{F}_1 \otimes \ldots \otimes \mathcal{F}_n \to \mathbb{R}^\sharp$$

such that

$$\mu(A_1 \times \ldots \times A_n) = \mu_1(A_1) \cdot \ldots \cdot \mu_n(A_n)$$

*is called the **product measure space**.*

We defer proof of existence and uniqueness as it relies on theory of integration, but nevertheless prove the finitely additive case and then the case of $\mathbb{R}^n$ in the next section.

Lemma 5.8.34
Let $\mathcal{R}_1, \ldots, \mathcal{R}_n$ be semi-rings. Then the family

$$\mathcal{R}_1 \times \ldots \times \mathcal{R}_n = \{A_1 \times \ldots \times A_n \mid A_i \in \mathcal{R}_i\}$$

is a semi-ring.

Proof. We may reduce to the case of $n = 2$. Then observe that

$$(A_1 \times B_1) \setminus (A_2 \times B_2) = (A_1 \setminus A_2) \times (B_1 \setminus B_2) \sqcup (A_1 \cap A_2) \times (B_1 \setminus B_2) \sqcup (A_1 \setminus A_2) \times (B_1 \cap B_2)$$

□

Lemma 5.8.35
Let $\mathcal{R}$ be a semi-ring and $A_1, \ldots, A_n \in \mathcal{R}$ a family of subsets. Then there exists a family of disjoint subsets $\mathcal{S} := \{B_1, \ldots, B_N\} \subset \mathcal{R}$ such that $\mathcal{S} = \mathcal{S}_1 \cup \ldots \cup \mathcal{S}_n$ and

$$A_i = \bigsqcup_{B \in \mathcal{S}_i} B\,.$$

Proof. For a tuple $\epsilon := (\epsilon_1, \ldots, \epsilon_n)$ for which $\epsilon_i = \pm 1$ define the family of disjoint sets

$$A^\epsilon := A_1^{\epsilon_1} \cap \ldots \cap A_n^{\epsilon_n}$$

where $A_i^1 := A_i$ and $A_i^{-1} := A_i^c$. By (5.8.6) A^ϵ may be expressed as the disjoint union of some sets in $\mathcal{R}$, say $\mathcal{S}^\epsilon$. Then $\mathcal{S} = \bigcup_\epsilon \mathcal{S}^\epsilon$ consists of pairwise disjoint sets, where we consider tuples ϵ for each at least one entry is positive. Further

$$A_i = \bigsqcup_{\epsilon:\epsilon_i=1} A^\epsilon$$

therefore we may define $\mathcal{S}_i := \bigcup_{\epsilon:\epsilon_i=1} \mathcal{S}^\epsilon$. Note throughout we may omit ϵ for which $A^\epsilon = \emptyset$. □

Lemma 5.8.36
Let $\{(\Omega_i, \mathcal{R}_i, \mu_i)\}_{i=1\ldots n}$ be a collection of finitely additive set functions on semi-rings. The set function

$$\begin{aligned} \mu : \mathcal{R}_1 \times \ldots \times \mathcal{R}_n &\to \mathbb{R} \cup \{\infty\} \\ A_1 \times \ldots \times A_n &\to \mu_1(A_1) \ldots \mu_n(A_n) \end{aligned}$$

is finitely additive, and we write $\mu =: \mu_1 \times \ldots \times \mu_n$. Moreover if each μ_i is σ-finite then so is μ.

Proof. By induction it's enough to consider the case $n = 2$. Suppose that

$$\begin{aligned} A_i &= B_i \times C_i \quad i = 0, \ldots, n \\ A_0 &= \bigsqcup_{i=1}^n A_i \end{aligned}$$

for $B_i \in \Omega_1$ and $C_i \in \Omega_2$. By (5.8.35) we may write

$$\begin{aligned} B_i &:= \bigsqcup_{\widehat{B} \in \mathcal{S}_i} \widehat{B} \\ C_i &:= \bigsqcup_{\widehat{C} \in \mathcal{T}_i} \widehat{C} \end{aligned}$$

where $\mathcal{S}_i$ and $\mathcal{T}_i$ are finite subsets of $\mathcal{R}_1$ and $\mathcal{R}_2$ respectively. Evidently

$$B_i \times C_i = \bigsqcup_{(\widehat{B},\widehat{C}) \in \mathcal{S}_i \times \mathcal{T}_i} \widehat{B} \times \widehat{C}$$

and $\mathcal{S}_0 = \bigcup_{i=1}^n \mathcal{S}_i$ and $\mathcal{T}_0 := \bigcup_{i=1}^n \mathcal{T}_i$. As μ_1 and μ_2 are finitely additive then

$$\begin{aligned} \mu_1(B_i) &= \sum_{\widehat{B} \in \mathcal{S}_i} \mu_1\left(\widehat{B}\right) \\ \mu_2(C_i) &= \sum_{\widehat{C} \in \mathcal{T}_i} \mu_2\left(\widehat{C}\right) \\ \sum_{i=1}^n \mu(A_i) &= \sum_{i=1}^n \mu_1(B_i)\mu_2(C_i) = \sum_{i=1}^n \sum_{(\widehat{B},\widehat{C}) \in \mathcal{S}_i \times \mathcal{T}_i} \mu_1(\widehat{B})\mu_2(\widehat{C}) \\ \mu(A_0) &= \mu_1(B_0)\mu_2(C_0) = \sum_{(\widehat{B},\widehat{C}) \in \mathcal{S}_0 \times \mathcal{T}_0} \mu_1(\widehat{B})\mu_2(\widehat{C}) \end{aligned}$$

As the sets $B_i \times C_i$ are disjoint we may deduce that

$$\mathcal{S}_0 \times \mathcal{T}_0 = \bigsqcup_{i=1}^n \mathcal{S}_i \times \mathcal{T}_i$$

from which the result follows. □

5.8.7 Borel Measure on $\mathbb{R}^n$

Proposition 5.8.37
Let $\mathcal{R}$ be the semi-ring of half-open intervals over $\mathbb{R}^n$ Then the set function

$$\mu : \mathcal{R} \to [0, \infty]$$

given by

$$\mu([a_1, b_1) \times \ldots \times [a_n, b_n)) = \prod_{i=1}^n (b_i - a_i),$$

is countably additive and σ-finite.

Proof. By (5.8.36) μ is finitely additive. So by (5.8.25) it is sufficient to show that μ is countably subadditive. Suppose that

$$[\mathbf{a}_0, \mathbf{b}_0) = \bigcup_{i=1}^{\infty} [\mathbf{a}_i, \mathbf{b}_i)$$

Then for any positive constants $\boldsymbol{\epsilon}$, $\boldsymbol{\delta}_1, \boldsymbol{\delta}_2, \ldots$ we have

$$[\mathbf{a}_0, \mathbf{b}_0 - \boldsymbol{\epsilon}] \subset \bigcup_{i=1}^{\infty} (\mathbf{a}_i - \boldsymbol{\delta}_i, \mathbf{b}_i)$$

By the Heine-Borel theorem (5.7.7) closed intervals are compact, so we have

$$[\mathbf{a}_0, \mathbf{b}_0 - \boldsymbol{\epsilon}) \subset \bigcup_{i=1}^{N(\boldsymbol{\delta})} [\mathbf{a}_i - \boldsymbol{\delta}_i, \mathbf{b}_i)$$

Therefore by (5.8.9)

$$\begin{aligned}
\prod_{j=1}^{n} (b_{0j} - a_{0j} - \epsilon) &\leq \sum_{i=1}^{N(\boldsymbol{\delta})} \prod_{j=1}^{n} (b_{ij} - a_{ij} + \delta_{ij}) \\
&\leq \sum_{i=1}^{N(\boldsymbol{\delta})} \prod_{j=1}^{n} (b_{ij} - a_{ij}) \left(1 + \frac{\delta}{2^i}\right) \\
&\leq \sum_{i=1}^{N(\boldsymbol{\delta})} \prod_{j=1}^{n} (b_{ij} - a_{ij}) \sum_{i=1}^{N(\boldsymbol{\delta})} \left(1 + \frac{\delta}{2^i}\right) \\
&\leq (1+\delta) \sum_{i=1}^{\infty} \prod_{j=1}^{n} (b_{ij} - a_{ij})
\end{aligned}$$

where we have defined $\delta_{ij} := \frac{b_{ij} - a_{ij}}{n} \left(\frac{\delta}{2^i}\right)^{\frac{1}{n-1}}$ and used the inequality $(1+x)^n \leq 1 + nx^{n-1}$. As this holds for arbitrary $\delta > 0$ then it holds for $\delta = 0$. We may consider the sequence $\epsilon := \frac{1}{m}$ and letting $m \to \infty$ use (4.1.32) and (5.1.21) to deduce the case of $\epsilon = 0$. This shows that

$$\mu([\mathbf{a}_0, \mathbf{b}_0)) \leq \sum_{i=1}^{\infty} \mu([\mathbf{a}_i, \mathbf{b}_i))$$

i.e. μ is countably subadditive. □

Proposition 5.8.38 (Existence of Borel Measure)
Let $(\mathbb{R}^k, \mathcal{B}(\mathbb{R}^k))$ be the Borel measurable space. Then there exists a unique σ-finite measure

$$\mu : \mathcal{B}(\mathbb{R}^k) \to [0, \infty]$$

such that

$$\mu([\mathbf{a}, \mathbf{b})) = \prod_{i=1}^{k} (b_k - a_k)$$

Proof. This is a consequence of (5.8.26) and (5.8.37). □

5.8.8 Measurable Functions

Definition 5.8.39
*Let $(\Omega_1, \mathcal{F}_1)$ and $(\Omega_2, \mathcal{F}_2)$ be measurable spaces. A function $f : \Omega_1 \to \Omega_2$ is said to be **measurable** if*

$$E \in \mathcal{F}_2 \implies f^{-1}(E) \in \mathcal{F}_2$$

We may write $\mathcal{F}_1/\mathcal{F}_2$-measurable in order to make the σ-algebras explicit.

Similarly a function $f : \Omega \to X$ from a measurable space to a topological space is said to be measurable if it is $\mathcal{F}/\mathcal{B}(X)$ measurable.

Proposition 5.8.40
The following properties hold

a) *The composition of measurable functions is measurable*

b) *Suppose* $\mathcal{F}_2 = \sigma(\mathcal{C})$ *then a function* $f : \Omega_1 \to \Omega_2$ *is* $\mathcal{F}_1/\mathcal{F}_2$*-measurable iff*

$$E \in \mathcal{C} \implies f^{-1}(E) \in \mathcal{F}_1$$

c) *A function* $f : \Omega \to X$ *is measurable precisely when the inverse image of an open set (resp. closed set) is measurable.*

Corollary 5.8.41 (Criteria for measurablity of a real-valued function)
Let $(\Omega, \mathcal{F})$ *be a measurable space and* $f : \Omega \to \mathbb{R}^\sharp$ *a function. Then the following are equivalent*

a) f *is* $\mathcal{F}/\mathcal{B}(\mathbb{R}^\sharp)$*-measurable*

b) $f^{-1}((x, \infty]) \in \mathcal{F}$ *for all* $x \in D$

c) $f^{-1}([x, \infty]) \in \mathcal{F}$ *for all* $x \in D$

d) $f^{-1}([-\infty, x)) \in \mathcal{F}$ *for all* $x \in D$

e) $f^{-1}([-\infty, x]) \in \mathcal{F}$ *for all* $x \in D$

where $D \subset \mathbb{R}$ *is an additive subgroup containing* $\mathbb{Q}$.

Proof. We may combine (5.8.40).b) and (5.8.31). □

Proposition 5.8.42 (Measurable Space Isomorphism)
Let $(\Omega_1, \mathcal{F}_1)$ *and* $(\Omega_2, \mathcal{F}_2)$ *be measurable spaces and* $f : \Omega_1 \to \Omega_2$ *a bijective function. Then the following are equivalent*

a) f *and* f^{-1} *are measurable*

b) f *induces a bijection* $\mathcal{F}_1 \to \mathcal{F}_2$

c) f^{-1} *induces a bijection* $\mathcal{F}_2 \to \mathcal{F}_1$

In this case we say that $f : (\Omega_1, \mathcal{F}_1) \xrightarrow{\sim} (\Omega_2, \mathcal{F}_2)$ *is a* ***measurable space isomorphism****.*

Proposition 5.8.43 (Limits of Measurable Functions)
Let $f_n : (\Omega, \mathcal{F}) \to (\mathbb{R}^\sharp, \mathcal{B}(\mathbb{R}^\sharp))$ *be a sequence of measurable functions. Define the functions* $\sup f_n, \inf f_n, \limsup_n f_n, \liminf_n f_n$ *as follows*

$$\begin{aligned}
(\sup f_n)(x) &:= \sup_n f(x) \\
(\inf f_n)(x) &:= \inf_n f(x) \\
(\limsup_n f_n)(x) &:= \limsup_n f_n(x) \\
(\liminf_n f_n)(x) &:= \liminf_n f_n(x)
\end{aligned}$$

Then these functions are $\mathcal{F}/\mathcal{B}(\mathbb{R}^\sharp)$*-measurable.*

Proof. Observe that

$$(\inf_n f_n)^{-1}([x, \infty]) = \bigcap_{n=1}^{\infty} f_n^{-1}([x, \infty])$$

so $\inf f_n$ is measurable by (5.8.41). Further $\sup_n f_n = -\inf_n(-f_n)$. □

Proposition 5.8.44
Let $f, g : (\Omega, \mathcal{F}) \to \left(\mathbb{R}^\sharp, \mathcal{B}(\mathbb{R}^\sharp)\right)$ *be measurable functions. Then the following functions are measurable*

a) $f \pm g$

b) λf *is measurable for* $\lambda \in \mathbb{R}$

c) $f \cdot g$

d) $\max(f, g)$, $\min(f, g)$

Note when $f \pm g, fg$ *is not well-defined (e.g.* $\infty - \infty$ *or* $-\infty \times -\infty$*) then we choose an arbitrary, but fixed, sentinel value.*

Proof. We make use of (5.8.41) throughout.

a) Define $h(\omega) := f(\omega)+g(\omega)$ and let A be the set on which the sum is well-defined. Then it is evidently measurable and

$$\begin{aligned} h^{-1}\left((x,\infty]\right) &= \{\omega \in B_x^c \mid f(\omega)+g(\omega) > x\} \cup B_x \\ &= \{\omega \in A \mid f(\omega)+g(\omega) > x\} \cup B_x \\ &= \left(\bigcup_{r\in\mathbb{Q}} \{\omega \in A \mid f(\omega) > r\} \cap \{\omega \in A \mid g(\omega) > x-r\} \right) \cup B_x \end{aligned}$$

where $B_x = \emptyset$ or A^c according to if the sentinel value of $f+g$ is $\leq x$. For the final equality the reverse inclusion is immediate. Conversely suppose $f(\omega)+g(\omega) > x$ then by (5.1.28) there exists some $r \in \mathbb{Q}$ such that $f(\omega) > r > x - g(\omega)$. The case $f-g$ follows immediately from b).

b) Observe that

$$(\lambda f)^{-1}\left((x,\infty]\right) = \begin{cases} \left(\frac{x}{\lambda},\infty\right] & \lambda > 0 \\ \left[-\infty,\frac{x}{\lambda}\right) & \lambda < 0 \\ \Omega & \lambda = 0\,, x < 0 \\ \emptyset & \lambda = 0\,, x \geq 0 \end{cases}$$

c) First consider the case f^2 and observe

$$(f^2)^{-1}\left((x,\infty]\right) = \begin{cases} f^{-1}\left(\{-\infty,\infty\}\right) \cup f^{-1}\left((\sqrt{x},\infty]\right) \cup f^{-1}\left([-\infty,-\sqrt{x})\right) & x \geq 0 \\ \Omega & x < 0 \end{cases}$$

Then we may deduce the general case because

$$(fg)(\omega) = \begin{cases} \frac{(f(\omega)+g(\omega))^2-(f(\omega)-g(\omega))^2}{4} & f(\omega), g(\omega) \notin \{-\infty,\infty\} \\ \infty & (f(\omega),g(\omega)) \in \{(\infty,\infty),(-\infty,-\infty)\} \\ -\infty & (f(\omega),g(\omega)) \in \{(\infty,-\infty),(-\infty,\infty)\} \end{cases}$$

d) We may see this as a special case of (5.8.43)

□

5.8.9 Integration over a Measure

Definition 5.8.45

5.9 Differential Calculus on Banach Spaces

5.9.1 Total Derivatives

Definition 5.9.1
*Let $U \subset X$ be an open neighbourhood of 0 and $f : U \to Y$ a function. We say f is **sublinear** if*

$$\forall \epsilon > 0\, \exists \delta \text{ s.t. } \|h\| < \delta \implies h \in U \wedge \|f(h)\| < \epsilon \|h\|$$

Note sublinear functions are closed under linear combinations, and the property is unchanged under equivalent norms.

Definition 5.9.2 (Total Derivative)
Let $U \subset X$ be an open subset of a Banach space, Y a Banach space and $x \in U$. We say that a map $f : U \to Y$ is differentiable at x if there exists a continuous linear map $Df(x) \in L(X,Y)$ such that

$$f(x+h) - f(x) - Df(x)(h) \text{ is sublinear}$$

*This determines the **total derivative***

$$Df : U \to L(X,Y)$$

*If this is also continuous we say f is **continuously differentiable** or C^1. If in addition Df is C^1 we say f is C^2 and write*

$$D^2 f := D(Df) : U \to L(X, L(X,Y))$$

The following result shows that the total derivative is necessarily unique.

Proposition 5.9.3
Let $\alpha : X \to Y$ be a linear map which is also sublinear. Then $\alpha = 0$.

Proof. Consider $x \in X$ then for every $\epsilon > 0$ there exists δ such that $\|h\| < \delta \implies \|\alpha(h)\| < \epsilon \|h\|$. Define $\lambda := \frac{\delta}{2\|x\|}$. Then evidently $\|\alpha(\lambda x)\| < \epsilon \|\lambda x\|$ whence $\|\alpha(x)\| < \epsilon \|x\|$. As this holds for every ϵ we see $\|\alpha(x)\| = 0$ and $\alpha(x) = 0$. □

Proposition 5.9.4
Let $f : U \to Y$ be a differentiable map and $\alpha : Y \to Z$ a linear map. Then

$$D(\alpha \circ f)(x) = \alpha \circ Df(x)$$

Proposition 5.9.5
Let $U \subset K$ an open set and $f : U \to Y$ a function. Then the following are equivalent

a) *f is (continuously) differentiable in the sense of (5.9.2)*

b) *f is (continuously) differentiable in the sense of (5.5.1)*

Furthermore we may identify the derivatives as follows

$$Df(t)(\lambda) = f'(t)\lambda$$

Proposition 5.9.6 (Chain Rule)
Let $U \subset X$ and $V \subset Y$ be open sets and $f : U \to Y$ and $g : V \to Z$ (continuously) differentiable functions. Then $g \circ f$ is (continuously) differentiable and

$$(D(g \circ f))(x) = (Dg)(f(x)) \circ (Df)(x)$$

In the case $X = K$ we have

$$(g \circ f)'(t) = (Dg)(f(t))(f'(t))$$

Proposition 5.9.7 (Product Rule I)
Let $U \subset X$ and $V \subset Y$ open sets, $f : U \to X'$, $g : V \to Y'$ differentiable maps and $\psi : X' \times Y' \to Z$ a continuous bilinear map. Then

$$D(f \times_\psi g)(x, y)(h, k) = \psi(Df(x)(h), g(y)) + \psi(f(x), Dg(y)(k))$$

Corollary 5.9.8 (Product Rule II)
Let $U \subset X$ be an open set, and $f : U \to K$ and $g : U \to Y$ differentiable maps. Then

$$D(f \cdot g)(x)(h) = Df(x)(h)g(x) + f(x)Dg(x)(h)$$

If f, g are C^1 then so is $f \cdot g$.

5.9.2 Taylor's Theorem

Proposition 5.9.9 (Mean Value Theorem)
Let $U \subset X$ be an open subset and $f : U \to Y$ a C^1 map. Suppose that $h \in B(x; r) \subset U$. Then

$$f(x + h) = f(x) + \int_0^1 Df(x + th)(h)dt$$

Proof. Let $G(t) := f(x + th)$ be defined as a function on $[0, 1] \to Y$. Then by (5.9.6) $G'(t) = Df(x + th)(h)$ is continuous, because evidently $t \to x + th$ is continuously differentiable with scalar derivative h. The result follows by applying (5.8.20) to $G(t)$. □

Lemma 5.9.10 (Integration by Parts)
Let $U : [0, 1] \to K$ and $V : [0, 1] \to X$ be C^1 functions. Then

$$\int_0^1 U'(t)V(t)dt = U(1)V(1) - U(0)V(0) - \int_0^1 U(t)V'(t)dt$$

Proof. Let $H(t) := U(t)V(t)$ then by (5.9.8) $H'(t) = U'(t)V(t) + U(t)V'(t)$ is continuous. The result then follows from (5.8.20). □

Corollary 5.9.11 (Integration by Parts II)
Let $G : [0,1] \to X$ be a C^1 function. Then

$$\int_0^1 G(t)dt = G(0) + \int_0^1 (1-t)G'(t)dt$$

Proposition 5.9.12 (Taylor's Theorem)
Let $U \subset X$ be an open set and $f : U \to Y$ a C^2 map. Suppose $x \in U$ and $h \in B(x;r) \subset U$. Then

$$f(x+h) = f(x) + Df(x)(h) + \int_0^1 (1-t)D^2 f(x+th)(h,h)dt$$

Proof. Let $G(t) = Df(x+th)(h) : [0,1] \to Y$ then

$$G(t) = \mathrm{ev}_h \circ Df \circ (x+th)$$

By (5.9.4)

$$D(\mathrm{ev}_h \circ Df)(x) = \mathrm{ev}_h \circ D^2 f(x)$$

whence by (5.9.6) $G(t)$ is C^1 with scalar derivative

$$G'(t) = (\mathrm{ev}_h \circ D^2 f(x+th))(h) = D^2 f(x+th)(h,h)$$

Recall by the Mean Value Theorem (5.9.9) and Integration by Parts (5.9.11)

$$\begin{aligned} f(x+h) &= f(x) + \int_0^1 G(t)dt \\ &= f(x) + G(0) + \int_0^1 (1-t)G'(t)dt \end{aligned}$$

which is the required result. □

5.9.3 Jacobian Matrix

Proposition 5.9.13 (Partial derivatives)
Let $X_1, \ldots, X_n, Y$ be Banach spaces and $U \subset X := X_1 \times \ldots \times X_n$ an open subset. Consider a continuous map

$$f : U \to Y$$

The following are equivalent

a) *The map f is continuously differentiable (with respect to the sup norm on the product)*

b) *For every $x \in U$ and every basic open neighbourhood $x \in U_1 \times \ldots \times U_n$*

i) *The map*

$$\begin{aligned} f_i : U_i &\to Y \\ x &\to f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n) \end{aligned}$$

is differentiable with derivative $(D_i f)(x_1, \ldots, x_n)$ for all $i = 1 \ldots n$

ii) *The map*

$$D_i f : U_1 \times \ldots \times U_n \to L(X_i, Y)$$

is continuous for all $i = 1 \ldots n$.

Furthermore in this case

$$Df(x)(h) = \sum_{i=1}^n (D_i f)(x)(h_i)$$

Proof. *a)* $\implies$ *b)* Consider $h_i \in X_i$ such that $x_i + h_i \in U_i$. Then we may define $h := (0, \ldots, h_i, \ldots, 0)$ and evidently $\|h\| = \|h_i\|$. We claim that the given map is differentiable with derivative $(D_i f)(x)(h_i) := f'(x)(0, \ldots, h_i, \ldots, 0)$. For

$$\|f_i(x_i + h_i) - f_i(x_i) - (D_i f)(x)(h_i)\| = \|f(x+h) - f(x) - f'(x)(h)\|$$

is sublinear. Furthermore

$$\begin{aligned}\|(D_i f)(x)\| &= \sup\{\|(D_i f)(x)(h_i)\| \mid h_i \in X_i \ \|h_i\| = 1\} \\ &= \sup\{\|f'(x)(0,\ldots,h_i,\ldots,0)\| \mid h_i \in X_i \ \|h_i\| = 1\} \\ &\leq \sup\{\|f'(x)(h)\| \mid h \in X \ \|h\| = 1\} \\ &= \|f'(x)\| < \infty\end{aligned}$$

whence $(D_i f)$ is continuous.

b) $\implies$ *a)* We consider the case $n = 2$. Observe

$$\begin{aligned}f(x_1+h_1,x_2+h_2) - f(x_1,x_2) &= f(x_1+h_1,x_2+h_2) - f(x_1+h_1,x_2) + f(x_1+h_1,x_2) - f(x_1,x_2) \\ &= \int_0^1 D_2 f(x_1+h_1,x_2+th_2)(h_2)dt + \int_0^1 D_1 f(x_1+th_1,y)(h_1)dt \\ &= D_2 f(x_1,x_2)(h_2) + D_1 f(x_1,x_2)(h_1) \\ &+ \int_0^1 [D_2 f(x_1+h_1,x_2+th_2)(h_2) - D_2 f(x_1,x_2)(h_2)]\,dt \\ &+ \int_0^1 [D_1 f(x_1+th_1,x_2)(h_1) - D_1 f(x_1,x_2)(h_1)]\,dt\end{aligned}$$

Then

$$\begin{aligned}\left\|\int_0^1 [D_2 f(x_1+h_1,x_2+th_2)(h_2) - D_2 f(x_1,x_2)(h_2)]\,dt\right\| &\leq \int_0^1 \|D_2 f(x_1+h_1,x_2+th_2)(h_2) - D_2 f(x_1,x_2)(h_2)\|\,dt \\ &\leq \int_0^1 \|D_2 f(x_1+h_1,x_2+th_2) - D_2 f(x_1,x_2)\|\,\|h_2\|\,dt \\ &\leq \int_0^1 \|D_2 f\|\,\|(h_1,th_2)\|\,\|h_2\|\,dt \\ &\leq \|D_2 f\|\,\|h\|^2\end{aligned}$$

and similarly for the second integral. Therefore

$$Df(x_1,x_2) = D_1 f(x_1,x_2)(h_1) + D_2 f(x_1,x_2)(h_2)$$

as required. □

Proposition 5.9.14
Let $U \subset X$ be an open set and

$$f : U \to Y_1 \times \ldots \times Y_m$$

Then f is differentiable (resp. C^1) iff $\pi_i \circ f$ is differentiable (resp. C^1) for $i = 1 \ldots m$.

Proposition 5.9.15 (Jacobian Matrix)
Let X, Y be finite-dimensional Banach spaces with bases $\{x_1,\ldots,x_n\},\{y_1,\ldots,y_m\}$ such that $U \subset X$ is open and $f : U \to Y$ a map. Then the following are equivalent

a) *f is C^1*

b) *For every $x \in U_1 \oplus \ldots \oplus U_n \subset U$ s.t. $U_j \subset \langle x_j \rangle$ the map $D_j(y_i^\vee \circ f)(x)$ exists and is continuous*

Furthermore if this is the case define the Jacobian Matrix

$$\frac{\partial f_i}{\partial x_j}(x) := D_j(y_i^\vee \circ f)(x)(x_j)$$

Then the linear map $Df(x)$ has the following matrix representation

$$[Df(x)] = \left(\frac{\partial f_i}{\partial x_j}\right)$$

*which we refer to as the **Jacobian Matrix**.*

Proof. a) $\implies$ *b)* Define $Y_i := \langle y_i \rangle$ then $Y_i \cong K$ is a continuous linear isomorphism, as every norm is equivalent. Consequently by (5.9.14) we have $y_i^\vee \circ f$ is C^1. Define $X_j := \langle x_j \rangle$ then by (5.9.13) $D_j(y_i^\vee \circ f)(x)$ exists and is continuous. By the same result and by (5.9.4)

$$y_i^\vee \circ Df(x)(x_j) = D(y_i^\vee \circ f)(x)\,(x_j) = D_j(y_i^\vee \circ f)(x)(x_j) = \frac{\partial f_i}{\partial x_j}(x)$$

whence

$$y_i^\vee \circ Df(x) = \sum_{j=1}^{m} \frac{\partial f_i}{\partial x_j}(x) x_j^\vee$$

and so the matrix representation follows from (3.4.108).

b) $\implies$ *a)* By (5.9.13) $y_i^\vee \circ f$ is C^1, whence by (5.9.14) so is f. □

5.9.4 Second Derivative

Definition 5.9.16
*For a map $\alpha : X \times X \to Y$ we say that $\alpha(v, w)$ is **sublinear** if for all $\epsilon > 0$ there exists $\delta > 0$ such that*

$$\|(v, w)\| < \delta \implies \|\alpha(v, w)\| < \epsilon \|v\| \|w\|$$

where the norm on $X \times X$ is the product norm.

As before we have the following uniqueness property

Lemma 5.9.17
Let $\alpha : X \times X \to Y$ be a bilinear map which is also sublinear. Then $\alpha = 0$.

Proposition 5.9.18 (Second derivative is symmetric)
Let $f : U \to Y$ be a C^2 map. Then for all $x \in U$ we have $D^2 f(x)$ is the unique bilinear map $X \times X \to Y$ such that

$$f(x + v + w) - f(x + w) - f(x + v) + f(x) - D^2 f(x)(v, w) \text{ is sublinear}$$

Furthermore it is symmetric.

Proof. Uniqueness follows from (5.9.17) and from this it immediately follows that $D^2 f(x)$ is symmetric. Therefore we only need to show the required property. Let $v, w \in X$ be such that $x + tv + sw \in U$ for all $0 \leq s, t \leq 1$. Then define

$$g(x) := f(x + v) - f(x)$$

By (...) applied to g and Df we find

$$\begin{aligned} g(x + w) - g(x) &= \int_0^1 [Df(x + v + tw)(w) - Df(x + tw)(w)]\, dt \\ &= \int_0^1 \int_0^1 D^2 f(x + sv + tw)(v) ds(w) dt \\ &= D^2 f(x)(v, w) + \int_0^1 \int_0^1 \left[D^2 f(x + sv + tw)(v) - D^2 f(x)(v)\right] ds(w) dt \end{aligned}$$

Let $\psi(v, w)$ denote the integral then

$$\begin{aligned} \|\psi(v, w)\| &\leq \int_0^1 \int_0^1 \left\|D^2 f(x + sv + tw)(v) - D^2 f(x)(v)\right\| ds \|w\| dt \\ &\leq \int_0^1 \int_0^1 \left\|D^2 f(x + sv + tw) - D^2 f(x)\right\| ds dt \cdot \|v\| \|w\| \\ &\leq \sup_{0 \leq s,t \leq 1} \left\|D^2 f(x + sv + tw) - D^2 f(x)\right\| \|v\| \|w\| \end{aligned}$$

where the estimate is finite by continuity of $D^2 f$ and the Boundedness Theorem (5.7.8). Note that $\|sv + tw\| \leq \|v\| + \|w\| \leq 2\|(v, w)\|$. Therefore we may use the continuity of $D^2 f$ to show that ψ is sublinear as required. □

Proposition 5.9.19 (Symmetry of partial derivatives)
Let $X = X_1 \times \ldots \times X_n$, $f : U \to Y$ be a C^2 map and $x \in U$. Then

$$D^2 f(x)((0, \ldots, h_i, \ldots, 0), (0, \ldots, h_j, \ldots, 0) = D_i D_j f(x)(h_j, h_i)$$

In particular

$$D_i D_j f(x)(h_j, h_i) = D_j D_i f(x)(h_i, h_j)$$

Proof. The first equation follows from (5.9.13) and the second from (5.9.18). □

5.9.5 Differential Forms

Definition 5.9.20
Let X, Y be Banach spaces and $U \subset X$ an open subset. A differential p-form is a mapping

$$\omega : U \to L_a^p(X, Y)$$

*where $L_a^p(X, Y)$ is the subspace of **alternating linear maps** (3.4.119) which are also continuous (5.4.41). Observe that $L_a^1(X, Y) = L(X, Y)$ and we maintain the convention that $L_a^0(X, Y) = Y$.*

We define $\Omega_p^{(n)}(U; Y)$ to be the K-vector space of differential p-forms which are C^n.

Example 5.9.21
Consider a C^n function $f : U \to Y$. Then f is a C^n 0-form and Df is a C^{n-1} 1-form.

5.10 Complex Analysis

5.10.1 Cauchy-Riemann Equations

Proposition 5.10.1 (Isometry between $\mathbb{C}$ and $\mathbb{R}^2$)
The canonical map $\chi : \mathbb{C} \to \mathbb{R}^2$ is a Banach space isometry (using the square norm $\|\cdot\|_2$). Furthermore define

$$\begin{aligned} \mathrm{Re}(z) &:= \pi_1 \chi(z) \\ \mathrm{Im}(z) &:= \pi_2 \chi(z) \end{aligned}$$

then

$$z = \mathrm{Re}(z) \cdot 1 + \mathrm{Im}(z) \cdot i$$

where $\mathbb{C}$ is viewed as an $\mathbb{R}$ vector space. One may also verify that complex multiplication may be represented in matrix form

$$\chi(z \cdot w) = \begin{pmatrix} \mathrm{Re}(z) & -\mathrm{Im}(z) \\ \mathrm{Im}(z) & \mathrm{Re}(z) \end{pmatrix} \chi(w)^T$$

Proposition 5.10.2 (Cauchy-Riemann Equations)
Let $U \subset \mathbb{C}$ and $f : U \to \mathbb{C}$ a function. There exists unique functions $u, v : \chi(U) \to \mathbb{R}$ such that

$$f(x + yi) = u(x, y) + v(x, y)i$$

Further the following are equivalent

a) *$f(z)$ is continuously differentiable (as a complex function)*

b) *u, v are C^1 and satisfy the relations*

$$\begin{aligned} \frac{\partial u}{\partial x}(x, y) &= \frac{\partial v}{\partial y}(x, y) \\ \frac{\partial u}{\partial y}(x, y) &= -\frac{\partial v}{\partial x}(x, y) \end{aligned}$$

Proof. We may define $F : \chi(U) \to \mathbb{R}^2$ by $F = \chi \circ f \circ \chi^{-1}$ and $u = \pi_1 \circ F$ and $v = \pi_2 \circ F$.

a) $\implies$ *b)* Fix $z = x + yi \in U$ and $f'(z) = a + bi$. Then for sufficiently small $w = h + ki$

$$f(z + w) - f(z) - f'(z)w$$

is sublinear in w. By assumption F is C^1 and has Jacobian matrix (...) at (x, y) equal to

$$J(x, y) := \begin{pmatrix} \frac{\partial u}{\partial x}(x, y) & \frac{\partial u}{\partial y}(x, y) \\ \frac{\partial v}{\partial x}(x, y) & \frac{\partial v}{\partial y}(x, y) \end{pmatrix}$$

and $Df(x, y)(h, k) = J(x, y) \begin{pmatrix} h \\ k \end{pmatrix}^T$. However by conjugating the above equation by χ we find that

$$F(x + h, y + k) - F(x, y) - \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} h \\ k \end{pmatrix}^T$$

is sublinear (and using the fact χ is an isometry). Therefore the result then follows from the uniqueness of the total derivative $Df(x,y)$.

b) $\implies$ *a)* Conversely if the conditions hold then we may define $f'(z) := \frac{\partial u}{\partial x}(\chi(z)) + \frac{\partial v}{\partial x}(\chi(z))i$ which is evidently continuous. Then by using matrix representation of complex multiplication (5.10.1) we find

$$\chi\left[f(z+w) - f(z) - f'(z)w\right] = F(\chi(z+w)) - F(\chi(z)) - J'(\chi(z))\chi(w)^T$$

where

$$J'(x,y) \quad = \quad \begin{pmatrix} \frac{\partial u}{\partial x}(x,y) & -\frac{\partial v}{\partial x}(x,y) \\ \frac{\partial v}{\partial x}(x,y) & \frac{\partial u}{\partial x}(x,y) \end{pmatrix}$$

The conditions mean precisely that $J'(x,y) = J(x,y)$. As χ is an isometry we find that $f(z+w) - f(z) - f'(z)w$ is sublinear in w as required. □

5.10.2 Exponential and Trigonometric Functions

Proposition 5.10.3 (Exponential Function)
The K be a complete valued field. Then the series

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

has infinite radius of convergence. Furthermore it satisfies the following properties

a) e^z *is infinitely differentiable with derivative* e^z

b) $e^{z+w} = e^z e^w$

c) $e^z e^{-z} = 1$

In the case $K = \mathbb{R}$ then we also have the following property

d) e^x *is positive, strictly increasing and bijective* : $(-\infty, \infty) \to (0, \infty)$

Proof. We have

$$\left|\frac{a_{n+1}z^{n+1}}{a_n z^n}\right| = \frac{z}{n+1} \to 0$$

so the series converges unconditionally. Therefore by (5.6.2) it has infinite radius of convergence and is infinitely differentiable. Observe formally the product of power series is given by

$$\begin{aligned} e^z e^w &= \left(\sum_{n=0}^{\infty} \frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty} \frac{w^n}{n!}\right) \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \frac{z^k w^{n-k}}{k!(n-k)!}\right) \\ &= \sum_{n=0}^{\infty} \frac{(z+w)^n}{n!} \\ &= e^{z+w} \end{aligned}$$

which by (5.4.33) converge to the same value.

Evidently $x \geq 0 \implies e^x \geq 1 + x$. Then $x > y \geq 0 \implies e^x = e^{(x-y)+y} = e^{x-y}e^y \geq (1+x-y)e^y > 1 \cdot e^y$. Similarly suppose $x < y \leq 0$ then $-y > -x \geq 0 \implies e^{-y} > e^{-x} \implies e^x < e^y$. Finally $x \leq 0 \implies e^{-x} \geq 1 - x \implies e^x \leq \frac{1}{1+x}$. This shows that e^x is strictly increasing and therefore injective on $(0, \infty)$. Further using $e^x e^{-x} = 1$ we see it is a positive function and $x \leq 0 \implies e^x \leq 1$.

As e^x is unbounded the intermediate value theorem (5.7.10) shows it achieves every value in $[1, \infty)$. Using $e^x e^{-x} = 1$ we see it also achieves every value in $(0, \infty)$. Therefore it is a bijection $(-\infty, \infty) \to (0, \infty)$ as required. □

Proposition 5.10.4 (Trigonometric Functions)
The power series

$$\sin(z) = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \dots$$

$$\cos(z) = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \dots$$

have infinite radius of convergence in $\mathbb{C}$. Furthermore

a) $\sin(0) = 0$ *and* $\cos(0) = 1$

b) $e^{iz} = \cos(z) + i\sin(z)$

c) $\sin(z) = \frac{e^{iz} - e^{-iz}}{2i}$ *and* $\cos(z) = \frac{e^{iz} + e^{-iz}}{2}$. $\sin(-z) = -\sin(z)$ *and* $\cos(-z) = \cos(z)$

d) $\sin'(z) = \cos(z)$ *and* $\cos'(z) = -\sin(z)$ *are infinitely differentiable*

e) $\sin^2(z) + \cos^2(z) = 1$

f) $\sin(w + z) = \sin(w)\cos(z) + \cos(w)\sin(z)$

g) $\cos(w + z) = \cos(w)\cos(z) - \sin(w)\sin(z)$

Proof. It is simpler to define $\sin(z)$ and $\cos(z)$ by c). The power series expansion then follows from (5.4.26).

a) Immediate from the series expansion

b) Immediate from c)

c) Already shown

d) Immediate from c) and the chain rule (5.9.6).

e) Use b) and $e^{iz}e^{-iz} = 1$

$f) - g)$ Using b) we find

$$\begin{aligned} \cos(z+w) + i\sin(z+w) &= e^{i(z+w)} = e^{iz}e^{iw} \\ &= (\cos(z) + i\sin(z))\,(\cos(w) + i\sin(w)) \\ &= (\cos(z)\cos(w) - \sin(z)\sin(w)) + i\,(\sin(z)\cos(w) + \cos(z)\sin(w)) \end{aligned}$$

and the result follows from equating real and imaginary parts

□

Proposition 5.10.5 (cos and sin are periodic)
There is a unique positive real number $\pi \in \mathbb{R}$ *such that the real roots of* $\sin(x)$ *are precisely*

$$\{n\pi \mid n \in \mathbb{Z}\}$$

Furthermore we have the period formulae

a) $\sin(x) = \cos(x - \frac{\pi}{2}) = \cos(\frac{\pi}{2} - x)$

b) $\cos(x) = \sin(\frac{\pi}{2} - x) = -\sin(x - \frac{\pi}{2})$

c) $\sin(x) = -\sin(x + \pi)$ *and* $\sin(x + 2\pi) = \sin(x)$

d) $\cos(x) = -\cos(x + \pi)$ *and* $\cos(x + 2\pi) = \cos(x)$

and the real roots of $\cos(x)$ *are precisely*

$$\left\{\left(n + \frac{1}{2}\right)\pi \mid n \in \mathbb{Z}\right\}$$

Proof. By (5.10.4).e) we know that $0 \leq \sin^2(x) \leq 1$ which means $-1 \leq \sin(x) \leq 1$, and similarly for $\cos(x)$. We first prove that $\cos(x)$ has a positive root. Suppose not then by the intermediate value theorem (5.7.10) we must have $\cos(x) > 0$ for all x. Then by the Mean-Value Theorem (5.7.12) $\sin(x)$ must be strictly increasing and therefore positive for all $x > 0$. We claim that for $x \geq a > 0$

$$\cos(x) \leq \cos(a) + \cos'(a)(x - a) = \cos(a) - \sin(a)(x - a)$$

For define $g(x) := \cos(a) - \sin(a)(x - a) - \cos(x)$ then $g(a) = \cos(a) > 0$ and $g'(x) = \sin(x) - \sin(a) > 0$. By the Mean-Value Theorem $g(x)$ is increasing and the claim is proven. However it is evident that this implies $\cos(x)$ is unbounded below contradicting $-1 \leq \cos(x)$. Therefore $\cos(x)$ has a strictly positive root.

Define this to be

$$\frac{\pi}{2} := \inf\{x \in \mathbb{R}^+ \mid \cos(x) = 0\}$$

By (5.1.18) there exists a sequence x_n such that $\cos(x_n) = 0$ and $x_n \downarrow \frac{\pi}{2}$. By continuity and (5.3.5) we have $\cos(\frac{\pi}{2}) = 0$, and evidently $\pi \neq 0$. We must have $\cos(x)$ positive on the interval $[0, \frac{\pi}{2}]$, for otherwise by the intermediate value theorem we would have a smaller root. This shows that $\sin(x)$ is increasing on the interval $[0, \pi/2]$. By (5.10.4) we have $\sin^2(\frac{\pi}{2}) = 1$ and therefore $\sin(\frac{\pi}{2}) = 1$.

The period formula $a)$ then follows from the addition formula (5.10.4).g)

$$\cos\left(\frac{\pi}{2} - x\right) = \cos\left(x - \frac{\pi}{2}\right) = \cos(x)\cos\left(-\frac{\pi}{2}\right) - \sin(x)\sin\left(-\frac{\pi}{2}\right) = \sin(x)$$

and $b)$ follows directly from $a)$. Then $c), d)$ follow from combining $a), b)$. In particular $\sin(n\pi) = 0$. We claim that π is the smallest positive root of $\sin(x)$. For suppose $0 < x < \pi$ satisfies $\sin(x) = 0$ then by $a)$ we have $\cos(\left|x - \frac{\pi}{2}\right|) = 0$ and $0 \leq \left|x - \frac{\pi}{2}\right| < \frac{\pi}{2}$ which contradicts the choice of π. Suppose $\sin(y) = 0$ with $y > 0$. Then consider

$$n := \max\{m \in \mathbb{N} \mid y - m\pi \geq 0\}$$

Then $\sin(y - n\pi) = 0$ by $c)$. By choice of m we have $0 \leq y - n\pi < \pi$. As π is the smallest positive root we have $y - n\pi = 0$. By symmetry then the roots of $\sin(x)$ are precisely $\{n\pi\}$. Evidently any such π is unique because $\pi' = n\pi = nm\pi'$ whence $n = m = 1$. Using $a)$ yields the precise set of roots of $\cos(x)$. □

Proposition 5.10.6
There is a continuous, strictly decreasing function

$$\arccos : [-1, 1] \to [0, \pi]$$

such that

$$\cos(\arccos(x)) = x$$

Proof. By (5.10.5) $\sin(x)$ is positive on the interval $(0, \pi)$ (by the intermediate value theorem). By the Mean Value Theorem then $\cos(x)$ is strictly decreasing on this interval. Furthermore $\cos(0) = 1$ and $\cos(\pi) = -\cos(\pi - \pi) = -1$. By the intermediate value theorem then $\cos : [0, \pi] \to [-1, 1]$ is surjective and injective. Therefore the map arccos is well-defined and it is continuous by (5.7.13). □

Proposition 5.10.7 (Polar Coordinates)
There is a unique function

$$\theta : \mathbb{R}^2 \setminus \{(0, 0)\} \to [0, 2\pi)$$

such that

$$r(x, y)\cos(\theta(x, y)) = x \text{ and } r(x, y)\sin(\theta(x, y)) = y$$

where $r(x, y) := \sqrt{x^2 + y^2}$. *Explicitly it is given by*

$$\theta(x, y) \quad := \quad \begin{cases} \arccos\left(\frac{x}{r(x,y)}\right) & y \geq 0 \\ 2\pi - \arccos\left(\frac{x}{r(x,y)}\right) & y < 0 \end{cases}$$

and it is continuous on $\mathbb{R}^2 \setminus \{(x, 0) \mid x > 0\}$, *and* $\theta(x, 0-) = 2\pi + \theta(x, 0+)$ *when* $x > 0$.

Proof. Observe that $0 \leq \frac{x}{\sqrt{x^2+y^2}} \leq 1$ and so $r(x, y)\cos(\theta(x, y)) = x$. Further $\sin^2(\theta(x, y)) = 1 - \cos^2(\theta(x, y)) = \frac{y^2}{x^2+y^2}$, and so $r(x, y)\sin(\theta(x, y)) = \pm y$. When $y \geq 0$ we have $\theta(x, y) \in [0, \pi] \implies \sin(\theta(x, y)) \geq 0$. Similarly from the case $y \leq 0$ we find $r(x, y)\sin(\theta(x, y)) = y$ as required. □

Proposition 5.10.8
Let $r, r' > 0$ *and* $\theta, \theta' \in \mathbb{R}$. *Then*

$$(r\cos(\theta), r\sin(\theta)) = (r'\cos(\theta'), r'\sin(\theta'))$$

if and only if

$$r = r' \text{ and } \theta = \theta' + 2n\pi$$

Proof. We may use (5.10.4) to show that

$$r^2 = (r\cos(\theta))^2 + (r\sin(\theta))^2 = (r'\cos(\theta'))^2 + (r'\sin(\theta'))^2 = (r')^2$$

which means $r = r'$. Similarly we may use the addition formula to find

$$\sin(\theta - \theta') = \sin(\theta)\cos(\theta') - \cos(\theta')\sin(\theta) = 0$$

which means $\theta = \theta' + n\pi$ by (5.10.5). Using the fact $\cos(\theta + n\pi) = (-1)^n\cos(\theta)$ and $\sin(\theta + n\pi) = (-1)^n\sin(\theta)$ we may deduce that n is even (since $\sin(\theta) = \cos(\theta) = 0$ is impossible). □

5.10.3 Polar Coordinates of a Path

We would like to show that any path $\gamma : [a,b] \to \mathbb{C} \setminus \{0\}$ has a *continuous* parameterisation $(r(t), \theta(t))$ in polar coordinates, and that this is essentially unique.

Definition 5.10.9
*Suppose X is a Hausdorff space. A continuous surjective map $p : \widetilde{X} \to X$ is a **covering map** if every $x \in X$ has a neighbourhood U_x such that*

a) $p^{-1}(U_x) = \bigsqcup_{i \in I_x} V_{x,i}$

b) $p|_{V_{x,i}} : V_{x,i} \to U_x$ *is a homeomorphism for all* $i \in I_x$

We may show that $\widetilde{X}$ is necessarily Hausdorff.

Proposition 5.10.10 (Punctured Plane Covering Map)
The map

$$\begin{aligned} \mathbb{R}_{>0} \times \mathbb{R} &\to \mathbb{R}^2 \setminus \{(0,0)\} \\ (r, \theta) &\to (r\cos(\theta), r\sin(\theta)) \end{aligned}$$

is a covering map.

Proof. Define

$$\begin{aligned} U_1 &:= \mathbb{R}^2 \setminus \{(x,0) \mid x \geq 0\} \\ U_2 &:= \mathbb{R}^2 \setminus \{(x,0) \mid x \leq 0\} \end{aligned}$$

We claim that

$$\begin{aligned} p^{-1}(U_1) &= \bigsqcup_n \mathbb{R}_{>0} \times (2n\pi, (2n+2)\pi) \\ p^{-1}(U_2) &= \bigsqcup_n \mathbb{R}_{>0} \times ((2n-1)\pi, (2n+1)\pi) \end{aligned}$$

Denote the open sets by $V_{i,n}$ for $i = 1, 2$. Then the maps

$$p|_{V_{i,n}} \to U_i$$

are injective by (5.10.8). We may define explicit continuous inverses by

$$\begin{aligned} U_1 &\to V_{1,n} \\ (x,y) &\to \left(\sqrt{x^2+y^2}, \theta(x,y) + 2n\pi\right) \\ U_2 &\to V_{2,n} \\ (x,y) &\to \left(\sqrt{x^2+y^2}, -\theta(-x,y) + 2(n-1)\pi\right) \end{aligned}$$

□

Proposition 5.10.11 (Path lifting)
Let $p : \widetilde{X} \to X$ be a convering map and $\gamma : [a,b] \to X$ a continuous path. Consider any $\widetilde{x}_0 \in \widetilde{X}$ such that $p(\widetilde{x}_0) = \gamma(a)$. Then there exists a unique lifting $\widetilde{\gamma} : [a,b] \to \widetilde{X}$ such that $p \circ \widetilde{\gamma} = \gamma$ and $\widetilde{\gamma}(a) = \widetilde{x}_0$.

Proof. We first prove uniqueness. Consider two liftings $\widetilde{\gamma}_1, \widetilde{\gamma}_2 : [a,b] \to \widetilde{X}$ and define

$$X := \{t \in [a,b] \mid \widetilde{\gamma}_1(t) = \widetilde{\gamma}_2(t)\}$$

Fix $t \in X$ and let U be a neighbourhood of $\gamma(t)$ such that $p^{-1}(U) = \bigsqcup_{i \in I} V_i$. Suppose $\widetilde{\gamma}_1(t) = \widetilde{\gamma}_2(t) \in V_i$. By continuity there exists a neighbourhood W of t such that $\widetilde{\gamma}_1(W) \subseteq V_i$ and $\widetilde{\gamma}_2(W) \subseteq V_i$. By definition of X this means $W \subseteq X$. Therefore X is open. By (4.1.67) X is also closed. By (5.7.9) then X is either empty or $[a,b]$. However we have $a \in X$ and the liftings must be equal.

Define

$$L := \{x \in [a,b] \mid \exists\, \widetilde{\gamma} : [a,x] \to \widetilde{X} \text{ s.t. } p \circ \widetilde{\gamma} = \gamma \text{ and } \widetilde{\gamma}(a) = \widetilde{x}_0\}$$

To show that L is closed consider a sequence $x_n \in L$ such that $x_n \to x \in [a,b]$. Choose $\gamma(x) \in U$ such that $p^{-1}(U) = \sqcup_i V_i$ and $p|_{V_i}$ is a homeomorphism. For some ϵ we have $(x-\epsilon, x+\epsilon) \cap [a,b] \subset \gamma^{-1}(U)$, and for some N, $x_N \in (x-\epsilon, x+\epsilon) \cap [a,b]$. In particular there is a lift

$$\widetilde{\gamma}' : [a, x_N] \to \widetilde{X}$$

. and $\widetilde{\gamma}'(x_N) \in V_i$ for some i. If $x_N \geq x$ then we are done, otherwise assume $x_N < x$ and define the lift

$$\widetilde{\gamma}(t) \quad := \quad \begin{cases} \widetilde{\gamma}'(t) & t \leq x_N \\ (p|_{V_i})^{-1}(\gamma(t)) & x_N \leq t \leq x \end{cases}$$

Therefore $x \in L$, and L is closed. By (5.7.9) we conclude $L = [a, b]$ and we are done. □

Proposition 5.10.12 (Almost uniqueness of polar coordinates)
Let $p : \mathbb{R}_{>0} \times \mathbb{R} \to \mathbb{R}^2 \setminus \{(0,0)\}$ be the covering map of the punctured plane (5.10.10) and $\gamma : [a, b] \to \mathbb{R}^2 \setminus \{(0,0)\}$ a continuous path. Suppose (r_1, θ_1) and (r_2, θ_2) are liftings. Then

$$r_1(t) = r_2(t)$$

$$\theta_1(t) = \theta_2(t) + 2n\pi$$

for some $n \in \mathbb{Z}$.

Proof. By (5.10.8) we have $\theta_2(a) - \theta_1(a) = 2n\pi$. Then $(r_2(t), \theta_2(t) - 2n\pi)$ is also a lifting and so by uniqueness equals $(r_1(t), \theta_1(t))$ as required. □

Definition 5.10.13 (Winding Number)
*Let $\gamma : [a, b] \to \mathbb{C} \setminus \{0\}$ be a continuous path. We define the **angle traversed** by the path γ to be*

$$\theta(b) - \theta(a)$$

*where $(r(t), \theta(t))$ is any lifting of γ. Note when γ is a closed path then this equals $2n\pi$ for a unique integer n. We call this the **winding number** of the closed path γ, which we denote by $W(\gamma; 0)$. In general we define*

$$W(\gamma; z_0) := W(\gamma - z_0; 0)$$

for any $z_0 \notin \gamma([a, b])$.

5.10.4 Path Integrals

Definition 5.10.14
*A **curve** is a continuous path $\gamma : [a, b] \to \mathbb{C}$, for which there exists a partition*

$$a = x_0 < x_1 < \ldots < x_{n+1} = b$$

such that

a) *γ is C^1 on (x_i, x_{i+1}) for $i = 0 \ldots n - 1$*

b) *γ is left and right differentiable at x_i and*

$$\lim_{h \downarrow 0} \frac{\gamma(x_i + h) - \gamma(x_i)}{h} = \lim_{h \downarrow 0} \gamma'(x_i + h)$$

$$\lim_{h \uparrow 0} \frac{\gamma(x_i + h) - \gamma(x_i)}{h} = \lim_{h \uparrow 0} \gamma'(x_i + h)$$

We say γ is closed if in addition $\gamma(b) = \gamma(a)$.

Definition 5.10.15 (Path Integral)
Let $\gamma : [a, b] \to \mathbb{C}$ be a curve supported on $\{x_0, \ldots, x_{n+1}\}$. Define the integral

$$\int_\gamma f(z)dz := \sum_{i=0}^{n} \int_{x_i}^{x_{i+1}} f(\gamma(t))\gamma'(t)dt$$

Proposition 5.10.16 (Path Integral of a function with primitive)
Let $f : U \to \mathbb{C}$ be a continuous function and $g : U \to \mathbb{C}$ a differentiable function such that $g'(z) = f(z)$. Then for any curve $\gamma : [a, b] \to U$ we have

$$\int_\gamma f(z)dz = g(b) - g(a)$$

In particular the integral over a closed curve is zero.

Proposition 5.10.17
Let $\gamma : [0,1] \to \mathbb{C}$ the path given by $\gamma(t) := Re^{2\pi it}$. Then evidently $W(\gamma, 0) = 1$. Further

$$\int_\gamma z^n dz = \begin{cases} 2\pi i & n = -1 \\ 0 & n \neq -1 \end{cases}$$

Proof. When $n \neq -1$ then z^n has primitive $\frac{z^{n+1}}{n+1}$ and we are done by the previous result. In the case $n = -1$ we may calculate explicitly

$$\int_\gamma z^{-1} dz \quad = \quad \int_0^1 \frac{\gamma'(t)}{\gamma(t)} dt = 2\pi i$$

□

Chapter 6

Algebraic Geometry

We first consider the development of algebraic varieties over a field k in order to motivate the more general theory of Schemes. We do not assume that k is algebraically closed which makes the development of "classical algebraic geometry" slightly more complex than for example [Har13, Chapter I]. However this approach yields more interesting applications sooner (in particular the definition of the Zeta Function) and provides deeper motivation for some of the constructions in Scheme Theory.

6.1 Affine Varieties

In order to generalise the usual notions to non-algebraically closed field, and develop a "coordinate-free" approach, we introduce the following concept

Definition 6.1.1 (K-Rational Maximal Ideal)
*Let A be a f.g. k-algebra and $\mathfrak{m}$ a maximal ideal. Recall (3.29.18) 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 (3.4.56). 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 6.1.2 (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 (3.29.18).

Every maximal ideal is $\bar{k}$-rational by the Weak Nullstellensatz (3.29.19). We may consider $K = k(x_1, \dots, x_n)$ which is finite by (3.18.56). □

Definition 6.1.3 (K-Radical)
Let A be a finitely generated k-algebra, K/k an algebraic extension and $\mathfrak{a} \lhd A$ an ideal. Define the K-radical by

$$\sqrt{\mathfrak{a}}^K := \bigcap_{\substack{\mathfrak{a} \subseteq \mathfrak{m} \\ \text{K}-\text{rational}}} \mathfrak{m}$$

Then $\sqrt{-}^K$ is a closure operator (apply (2.1.42) to the family of intersections of K-rational maximal ideals). 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 6.1.4 (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

1. *V_K and I_k are order-reversing*
2. *$S \subseteq I_k(V_K(S))$*
3. *$Y \subseteq V_K(I_k(Y))$*

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

$$V_K(I_k(Y)) = \overline{Y}$$

Furthermore

$$I_k(Y) = I_k(\overline{Y})$$

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 is straightforward.

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. The last statement follows by applying I_k and using 4.. □

For a fixed ideal $\mathfrak{a} \triangleleft k[X_1, \ldots, X_n]$ we may vary the field K to obtain families of solutions in different fields.

Definition 6.1.5 (Algebraic Set and L-valued points)
*Let $\mathfrak{a} \triangleleft k[X_1, \ldots, X_n]$ be a **radical** ideal. For every (not-necessarily algebraic) field extension L/k define the L-valued points to be*

$$V(\mathfrak{a})(L) := V_L(\mathfrak{a})$$

Definition 6.1.6 (Affine Variety)
*Let $\mathfrak{a} \triangleleft k[X_1, \ldots, X_n]$ be a **radical** ideal. The family $X(-) := V(\mathfrak{a})(-)$ is called an **affine variety** to which we associate the **coordinate ring** $k[X] := k[X_1, \ldots, X_n]/\mathfrak{a}$, 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 $X(L)$.*

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

$$X(i_{jk}) : X(K_j) \to X(X_k)$$

Definition 6.1.7 (Residue Field)
*Let $X = V(\mathfrak{a})$ be an affine variety. For a point $(x) \in X(L)$ define the **residue field** to be*

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

and the degree of x to be

$$\deg(x) := [k(x) : k]$$

Furthermore we define

$$M_{X,x} := I_k(\{(x)\})$$

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 (6.1.2) $\mathfrak{m}_{X,x}$ is K-rational.

Remark 6.1.8
$\mathbb{A}^n_k := V((0))$ is an affine variety and $\mathbb{A}^n_k(L) = L^n$.

Proposition 6.1.9 (Rational Points are Algebra Homomorphisms)
Let $X = V(\mathfrak{a})$ be an affine variety and K/k a field extension. Then there is a bijection

$$\{(x) \in X(K)\} \longleftrightarrow \mathrm{AlgHom}_k(k[X], K)$$

Proof. Given $(x) \in X(K)$ then the evaluation map $\mathrm{ev}_x : k[X_1, \ldots, X_n] \to K/k$ contains $\mathfrak{a}$ by definition and therefore (3.10.3) yields a unique map $\phi_x : k[X] \to K/k$ such that $\phi_x(\overline{X}_i) = x_i$.

Similarly given an algebra homomorphism $\phi : k[X] \to K$ we may define $(x) = (\phi(\overline{X}_1), \ldots, \phi(\overline{X}_n))$. Then by uniqueness these are mutual inverses. □

For completeness we also consider affine subvarieties in the same way as before

Proposition 6.1.10 (Affine subvarieties)
*Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n_k$ be an affine variety and $A := k[X]$ the coordinate ring. For any ideal $\mathfrak{b} \triangleleft A$ and field extension K/k define the **zero-locus** by*

$$V_K(\mathfrak{b}) := \big\{(x) \in X(K) \mid f(x) = 0 \quad \forall f \in \mathfrak{b}\big\}$$

Similarly for a subset $Y \subset X(K)$ define

$$I_k(Y) := \big\{f \in k[X] \mid f(x) = 0 \quad \forall x \in Y\big\}$$

Suppose $\pi : k[X_1, \ldots, X_n] \to k[X]$ is the quotient map. Then we have the following properties

$$\begin{aligned} V_K(\mathfrak{b}) &= V_K(\pi^{-1}(\mathfrak{b})) \cap X(K) \\ I_k(Y \cap X(K)) &= \pi(I_k(Y)) \quad Y \subset \mathbb{A}_k^n(K) \\ I_k(V_K(\mathfrak{b})) &= \pi(I_k(V_K(\pi^{-1}(\mathfrak{b})))) \end{aligned}$$

The pair (V_K, I_k) satisfies the same properties as (...). The image of V_K forms the closed sets of a topology on $X(K)$ which coincides with the subspace topology from $\mathbb{A}_k^n(K)$.

We may now generalize the Weak Nullstellensatz to arbitrary affine varieties and non-algebraically closed fields K/k.

Proposition 6.1.11 (Galois Quotient)
Let $X = V(\mathfrak{a})$ be an affine variety and K/k a normal algebraic field extension. There is a well-defined group action

$$\begin{aligned} \mathrm{Aut}(K/k) \times X(K) &\to X(K) \\ (\sigma, (x_1, \ldots, x_n)) &\to (\sigma(x_1), \ldots, \sigma(x_n)) \end{aligned}$$

Denote the set of Galois Orbits by $X_0(K)$ then the quotient map

$$\pi : X(K) \to X_0(K)$$

is precisely the Kolmogorov Quotient (4.1.29) and therefore a quasi-homeomorphism.

Proof. Given $F \in \mathfrak{a}$ we have $\sigma(F(x)) = F(\sigma(x))$. This shows that $(x) \in X(K) \implies \sigma((x)) \in X(K)$. Further it's clear that $\sigma(\tau((x))) = (\sigma \circ \tau)((x))$ so the group action is well-defined.

We need to show that $x, y \in X(K)$ are topologically indistinguishable precisely when they are Galois conjugate. Suppose $x = \sigma(y)$. Let $V(\mathfrak{b})$ be any closed set containing x. Then evidently $(y) \in V(\mathfrak{b})$, so $(y) \in \overline{(x)}$. Symmetrically we may deduce $\overline{(x)} = \overline{(y)}$ so they are topologically indistinguishable. Conversely given $(x), (y) \in X(K)$ topologically indistinguishable, then by definition $(x) \in V(\mathfrak{m}_{X,x})$ and $(y) \in V(\mathfrak{m}_{X,x})$, so $\mathfrak{m}_{X,x} \subset \mathfrak{m}_{X,y}$. By maximality $\mathfrak{m}_{X,x} = \mathfrak{m}_{X,y}$. This means there exists an isomorphism $k(x) \cong k(y) \subset K$ which lifts to an element of $\mathrm{Aut}(K/k)$ by (3.18.80). □

Proposition 6.1.12 (Generalized Weak Nullstellensatz)
Let X be an affine variety and K/k a normal algebraic field extension. Then the correspondence (...) induces a bijection between K-rational maximal ideals and Galois orbits of points

$$\begin{aligned} \{\mathfrak{m} \lhd k[X] \mid K\text{−rational}\} &\longleftrightarrow X_0(K) \\ \mathfrak{m} &\longrightarrow [V_K(\mathfrak{m})] \\ \mathfrak{m}_{X,x} &\longleftarrow [(x)] \end{aligned}$$

In particular there is a bijection

$$\mathrm{Specm}(k[X]) \longleftrightarrow X_0(\bar{k})$$

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 (3.18.80)).

Further from (6.1.5) we know $\mathfrak{m}_{X,x} = \mathfrak{m}_x/\mathfrak{a}$ is K-rational. Therefore the right-to-left map is well-defined. By (6.1.2) 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 6.1.13 (Correspondence between Zero-Loci and K-Radical Ideals)
Let X be an affine variety over k and K/k an algebraic field extension. Then we have the following formula

$$I_k(V_K(\mathfrak{a})) = \sqrt{\mathfrak{a}}^K$$

Therefore there is a a dual isomorphism

$$\mathrm{Rad}(k[X]; K) \underset{V_K}{\overset{I_k}{\leftrightarrows}} \mathrm{Zar}_k(X(K))$$

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 $I_k(V_{\bar{k}}(\mathfrak{a})) = \sqrt{\mathfrak{a}}^J$.

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 (6.1.12) 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 6.1.14 (Rabinowitsch Trick)
Let $\mathfrak{a} \triangleleft A$ 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 (3.8.4) $\bar{f}$ is nilpotent in $(A/\mathfrak{a})$ whence $f \in \sqrt{\mathfrak{a}}$. □

Proposition 6.1.15 (Strong Nullstellensatz)
Let X be an affine variety and $\mathfrak{a} \triangleleft k[X]$. 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. and there is a dual isomorphism

$$\mathrm{Rad}(k[X]) \longleftrightarrow \mathrm{Zar}_k(X(\bar{k}))$$

Proof. Note we've already shown the first equality (6.1.13).

First we consider the case $X = \mathbb{A}^n_k$ and $k[X] = k[X_1, \ldots, X_n]$. Let $\mathfrak{a} \triangleleft k[X]$ 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 the Weak Nullstellensatz (3.29.20) 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 $\mathfrak{b} \triangleleft k[X]$ is proper. Using Propositions (6.1.10) and (3.4.50) 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 6.1.16
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

$$\bigcap_{\mathfrak{m}} \mathfrak{m} = 0$$

6.1.1 Topological Properties

Proposition 6.1.17 (Principal Open Sets)
Let $X = V(\mathfrak{a})$ be an affine variety over k and K/k a field extension. For every $f \in k[X]$ the sets

$$D(f) := X(K) \setminus V_K((f)) = \{(x) \in X(K) \mid f(x) \neq 0\}$$

form a base for the Zariski topology $\mathrm{Zar}_k(X(K))$.

Proof. Let $U = X(K) \setminus V(\mathfrak{a})$ be an open set. For every $(x) \in U$ there by definition exists $f \in \mathfrak{a}$ such that $f(x) \neq 0$. Therefore $D(f)$ is a neighbourhood of (x) in the Zariski topology. □

The topological notion of irreducibility is important, and may be reduced to a purely algebraic statement on the coordinate ring.

Proposition 6.1.18 (Criterion for Irreducibility)
Let X be an affine variety (e.g. $\mathbb{A}^n_k$), K/k an algebraic field extension and $Y = V(\mathfrak{b})$ an affine subvariety corresponding to a K-radical ideal $\mathfrak{b} \lhd k[X]$. Then the following are equivalent

a) *$Y(K)$ is an irreducible subset of $\mathrm{Zar}_k(X(K))$*

b) *$Y_0(K)$ is an irreducible subset of $\mathrm{Zar}_k(X_0(K))$*

c) *$\mathfrak{b}$ is prime*

d) *$k[Y]$ 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 6.1.19 (Closed sets $\longleftrightarrow$ radical ideals)
Let $X = V(\mathfrak{a})$ be an affine variety. Recall (6.1.15) there is a dual lattice isomorphism between radical ideals and "Zariski"-closed subsets of $X(\bar{k})$ (and indeed $X_0(\bar{k})$).

$$\mathrm{Rad}(k[X]) \underset{V_{\bar{k}}(-)}{\overset{I_k(-)}{\leftrightarrows}} \mathrm{Zar}_k(X(\bar{k}))$$

Under this isomorphism we have

- *maximal ideals correspond to $\mathrm{Aut}(\bar{k}/k)$-orbits of $X(\bar{k})$ (or elements of $X_0(\bar{k})$))*
- *prime ideals of $k[X]$ correspond to irreducible subsets of $X(\bar{k})$ (and therefore of $X_0(\bar{k})$)*
- *minimal prime ideals of $k[X]$ correspond to irreducible components of $X(\bar{k})$ (and therefore of $X_0(\bar{k})$))*

Recall that prime ideals are precisely the meet-prime radical ideals and irreducible subsets are precisely the join-prime closed subsets (see (4.1.37)). 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 (6.1.12) and prime ideals in (6.1.18). Then as irreducible components are precisely maximal irreducible subsets the final statement follows from the dual order isomorphism. □

Definition 6.1.20 (Irreducible Affine Variety)
*We say an affine variety $X = V(\mathfrak{a})$ is **integral** or **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 (6.1.19), or equivalently irreducible (3.4.64), since it is assumed to be reduced.

Proposition 6.1.21 (Decomposition into Irreducible Components)
Let $X = V(\mathfrak{a})$ be an affine variety 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 (3.13.6) $k[X]$ is a Noetherian ring, so by (6.1.19) $X(\bar{k})$ is Noetherian. The result then follows from (4.1.51) □

Proposition 6.1.22 (Subspace Topology)
Let $X = V(\mathfrak{a})$ an affine variety and $Y = V(\mathfrak{b})$ an affine subvariety. Then there is a commutative diagram

$$\begin{array}{ccc} \left\{\mathfrak{c} \in \operatorname{Rad}(k[X]) \mid \mathfrak{b} \subseteq \mathfrak{c}\right\} & \underset{I}{\overset{V}{\rightleftarrows}} & \left\{Z \in \operatorname{Zar}_k(X(\bar{k})) \mid Z \subseteq Y(\bar{k})\right\} \\ {\scriptstyle \pi^{-1}}\uparrow\downarrow{\scriptstyle \pi} & & \| \\ \operatorname{Rad}(k[X]/\mathfrak{b}) & \underset{I}{\overset{V}{\rightleftarrows}} & \operatorname{Zar}_k(Y(\bar{k})) \end{array}$$

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 (3.4.55). The horizontal maps are dual isomorphisms by (6.1.19). The equality then follows from (6.1.10). □

6.1.2 Dimension

Definition 6.1.23 (Dimension)
Let $X = V(\mathfrak{a})$ be an affine variety. Then we define the dimension to be

$$\dim X := \dim X(\bar{k}) = \dim X_0(\bar{k})$$

where this is the Krull Dimension (4.1.56) of the $\bar{k}$-rational points with the k-Zariski topology. This is the supremum of dimension over all irreducible components by (4.1.58).

*We say X is of **pure dimension** n if all irreducible components have the same dimension n. Note an irreducible variety is always of pure dimension.*

*We say X is an **affine curve** if it is of pure dimension* 1.

Proposition 6.1.24 (Dimension of subspace)
Let $X = V(\mathfrak{a})$ be an affine variety and $Y = V(\mathfrak{b})$ an affine subvariety 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 integral then $\operatorname{codim}(Y, X) = \dim k[X]_{\mathfrak{p}}$.

Proof. *a)* follows from (6.1.22).

b) follows similarly by observing that the definition of ideal height (3.25.1) is dual to the topological definition of codimension (4.1.56). The last statement follows from (3.25.5). □

Corollary 6.1.25
Let $X = V(\mathfrak{a})$ is an affine variety then $\dim X = \dim k[X]$. *In particular* $\dim \mathbb{A}^n_k = n$.

Proof. The first statement is a consequence of (6.1.24) in the case $\mathfrak{b} = (0)$. The dimension for $\mathbb{A}^n_k$ then follows (3.29.21). □

As we showed in Section 3.29.3 the lattice of irreducible subsets is particularly well behaved.

Proposition 6.1.26 (Biequidimensional Algebraic Sets)
Let $X = V(\mathfrak{a})$ be an affine variety. 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

$$\dim k[X] = \dim \mathfrak{b} + \operatorname{ht}(\mathfrak{b})$$

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 (3.29.28).

The codimension formula follows from (4.1.61) and the algebraic version from (6.1.24). □

In the irreducible case we recover the "classical" field-theoretic version of dimension

Proposition 6.1.27 (Dimension of Function Field)
Let $X = V(\mathfrak{p})$ be an irreducible affine variety. 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 (3.29.21). □

Proposition 6.1.28 (Criteria for dimension 0)
Let $X = V(\mathfrak{a})$ an affine variety 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

$$\operatorname{ht}(\mathfrak{b}) = \operatorname{codim}(Y, X) = \dim X$$

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 $c) \implies a)$.

$a) \iff b)$ 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 codimension formula □

Proposition 6.1.29
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

$$\dim X = n - 1$$

6.1.3 Regular Function and Morphisms of Affine Algebraic Sets

Proposition 6.1.30 (Regular Function)
*Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ be an affine variety then we say an element $f \in k[X]$ is by definition a **regular function**. For every field extension K/k then this determines a function*

$$f_K : X(K) \to K$$

Furthermore $f = g \iff f_{\bar{k}} = g_{\bar{k}}$. Therefore there is an isomorphism of k-algebras (which we frequently identify)

$$k[X] \xrightarrow{\sim} \{f : X(\bar{k}) \to \bar{k} \mid \text{ regular } \} \xrightarrow{\sim} \{f : X_0(\bar{k}) \to \bar{k} \mid \text{ regular } \}$$

*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. The evaluation homomorphism

$$k[X_1, \ldots, X_n] \to \mathrm{Fun}_k(X(K), K)$$

by definition has kernel containing $\mathfrak{a}$ and so by definition induces a well-defined homomorphism

$$k[X] \to \mathrm{Fun}_k(X(K), K)$$

When $K = \bar{k}$ this is injective for suppose $f = \overline{F}$ maps to 0 then by definition $F \in I_k V_{\bar{k}}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ by the Strong Nullstellensatz (6.1.15). We assumed $\mathfrak{a}$ is radical so $F \in \mathfrak{a}$ and $f = 0$ as required. □

Definition 6.1.31 (Regular Morphism)
*Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ and $Y = V(\mathfrak{b}) \subset \mathbb{A}_k^m$ be affine varieties. A **regular morphism** $\phi : X \to Y$ is defined to be a tuple $(\phi_1, \ldots, \phi_m)$ of elements of $k[X]$ which satisfy the following property*

$$G \in \mathfrak{b} \implies G(\phi_1, \ldots, \phi_m) = 0$$

In particular for any extension K/k, ϕ determines a well-defined map

$$\begin{aligned} \phi_K : X(K) &\to Y(K) \\ (x) &\to (\phi_1(x), \ldots, \phi_m(x)) \end{aligned}$$

and if K/k is normal algebraic a well-defined map

$$X_0(K) \to Y_0(K)\,.$$

Proposition 6.1.32 (Morphisms $\leftrightarrow$ Polynomials on $\bar{k}$-rational points)
Let $X = V(\mathfrak{a})$ and $Y = V(\mathfrak{b})$ be affine varieties. For two regular morphisms $\phi, \psi : X \to Y$ to be equal it is necessary and sufficient that $\phi_{\bar{k}} = \psi_{\bar{k}}$. Therefore we may also see there is a bijection

$$\{\phi : X \to Y \mid \textit{ regular }\} \longleftrightarrow \{\phi_{\bar{k}} : X(\bar{k}) \to Y(\bar{k}) \mid \textit{ determined by a regular map }\}$$

Proof. The condition is clearly necessary. For the reverse implication we may reduce to the case $\phi, \psi \in k[X]$. If $\phi_{\bar{k}} = \psi_{\bar{k}}$ then by assumption $(\phi - \psi) \in \bigcap_{x \in X(\bar{k})} \mathfrak{m}_{X,x} = \bigcap_{\mathfrak{m}} \mathfrak{m} = (0)$ (6.1.16). □

Proposition 6.1.33 (Regular Morphisms are Reversed Algebra Homomorphisms)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n$ and $Y = V(\mathfrak{b}) \subset \mathbb{A}^m$ be affine varieties. There is a bijection

$$\begin{aligned} \mathrm{AlgHom}_k(k[Y], k[X]) &\leftrightarrow \{\phi : X \to Y\} \\ \phi_\star &\to (\phi_\star(\overline{Y}_1), \ldots, \phi_\star(\overline{Y}_m)) \\ \overline{G} \to G(\phi_1, \ldots, \phi_m) &\leftarrow \phi \end{aligned}$$

For K/k a field extension, $f \in k[Y]$ and $(x) \in X(K)$ we have the following relation

$$\phi_\star(f)(x) = f(\phi_K(x)) \quad x \in X(K)$$

Proof. A regular map $\phi = (\phi_1, \ldots, \phi_m)$ by definition induces the given algebra homomorphism $\phi_\star : k[Y] := k[Y_1, \ldots, Y_m]/\mathfrak{b} \to k[X]$. Further

$$\phi_\star(\overline{Y}_j) = Y_j(\phi_1, \ldots, \phi_m) = \phi_j$$

whence $(\phi_\star(\overline{Y}_1), \ldots, \phi_\star(\overline{Y}_m)) = \phi$. Similarly given an algebra homomorphism $\phi_\star$ then

$$G(\phi_\star(\overline{Y}_1), \ldots, \phi_\star(\overline{Y}_m)) = \phi_\star(G(\overline{Y}_1, \ldots, \overline{Y}_m)) = \phi_\star(\overline{G})$$

which shows that the maps are mutual inverses. By definition

$$\phi_\star(f)(x) = \phi_\star(\overline{F})(x) = F(\phi_1, \ldots, \phi_m)(x) = F(\phi_1(x), \ldots, \phi_m(x)) = f(\phi(x))$$

for all $x \in X(K)$. □

Definition 6.1.34 (Composition of Regular Morphisms)
Let $\phi : X \to Y$ and $\psi : Y \to Z$ be regular morphisms. We define $\psi \circ \phi$ to be the unique regular morphism associated to the k-algebra homomorphism $\phi_\star \circ \psi_\star$ (6.1.33). We may easily show that it satisfies

$$(\psi \circ \phi)_K = \psi_K \circ \phi_K$$

for every field extension K/k, and so corresponds to the usual notion of composition of functions.

Proposition 6.1.35 (Affine Varieties form a Category)
The collection of affine varieties together with regular morphisms form a category $\mathbf{AffVar}_k$ *. Furthermore there is an equivalence of categories*

$$\mathbf{AffVar}_k \xrightarrow{\sim} \mathbf{ReducedFgAlg}_k^{op}$$

Proof. By using the correspondence with k-algebra homomorphisms (6.1.33) we may show that the law of composition for regular morphisms also satisfy the axioms of a category. We have therefore shown that the assignment $X \to k[X]$ is full and faithful functor. To show it is essentially surjective consider a reduced finitely-generated k-algebra A. Then by definition $A \cong k[X_1, \dots, X_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$. As A is reduced we see $\mathfrak{a}$ is radical and therefore A is the coordinate ring of the affine variety $X = V(\mathfrak{a})$ and by definition $k[X] \cong A$. □

Definition 6.1.36
Let $\phi : X \to Y$ *be a regular morphism of affine varieties. Then we say it is*

- ***finite*** *if* $\phi_\star : k[Y] \to k[X]$ *is module-finite (equivalently integral)*
- ***dominant*** *if* $\phi(X(\bar{k}))$ *is dense in* $Y(\bar{k})$

Proposition 6.1.37 (Criteria for dominant morphisms)
A regular morphism $\phi : X \to Y$ *is dominant if and only if* $\phi_\star : k[Y] \to k[X]$ *is injective. In particular when both* X *and* Y *are irreducible then this induces a field extension*

$$k(Y) \hookrightarrow k(X)$$

Proof. Recall $\phi(X)$ is dense precisely when the closure $\overline{\phi(X(\bar{k}))} = Y(\bar{k})$. Then

$$\begin{aligned} \ker(\phi_\star) = I_k(\phi(X(\bar{k}))) \quad &\implies \quad V_{\bar{k}}(\ker(\phi_\star)) = V_{\bar{k}}(I_k(\phi(X(\bar{k})))) = \overline{\phi(X(\bar{k}))} \\ &\implies \quad \sqrt{\ker(f_\star)} = I_k(\overline{\phi(X(\bar{k}))}) \end{aligned}$$

by (...). If $\ker(\phi_\star) = 0$ then clearly $\overline{f(X(\bar{k}))} = Y$. Conversely if this holds then

$$\sqrt{\ker(\phi_\star)} = I_k(Y(\bar{k})) = I_k(V_{\bar{k}}(0)) = \sqrt{(0)} = (0)$$

as $k[Y]$ is reduced, whence $\ker(\phi_\star) = 0$. □

6.1.4 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. We show shortly that this is equivalent to the earlier definition in the case of "global sections", i.e. $U = X(\bar{k})$.

Definition 6.1.38 (Sheaf of Regular Functions)
Let $X = V(\mathfrak{a})$ *be an affine variety and* $U \subset X(\bar{k})$ *an open set. We say a function* $\sigma : U \to \bar{k}$ *is* ***regular*** *at* $x \in X$ *if there exists* $g, h \in k[X]$ *and an open neighbourhood* V *of* x *such that*

$$\sigma(y) = \frac{g(y)}{h(y)} \quad \forall y \in V$$

We say σ *is regular on* U *if it is regular at all* $x \in U$*. Then we may define the* ***structure sheaf***

$$\mathcal{O}_X(U) := \{\sigma : U \to \bar{k} \mid \sigma \text{ regular } \}$$

The elements are referred to as ***sections*** *over* U*.*

We will see that in the case of affine varieties the sheaf of regular functions can be characterized purely by the coordinate ring over particular open sets.

Definition 6.1.39 (Principal Open Set)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}_n^k$ *be an affine variety 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 6.1.40 (Coordinate ring is reduced)
Let $X = V(\mathfrak{a})$ be an affine variety. 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 6.1.41
The principal open sets form a basis for the Zariski topology, closed under finite intersection.

Furthermore $D(g) \subset D(f) \iff f \mid g^N$ some $N > 0$

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 (6.1.30), namely that the sections which are regular everywhere are precisely the regular functions.

Proposition 6.1.42 (Sections are localisation of coordinate ring)
Let $X = V(\mathfrak{a})$ be an affine variety and $f \in k[X]$. There is a canonical isomorphism

$$\begin{array}{rcl} i_f : k[X]_f & \xrightarrow{\sim} & \mathcal{O}_X(D(f)) \\ \dfrac{g}{f^n} & \longrightarrow & \dfrac{g(-)}{f(-)^n} \end{array}$$

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.

6.1.5 Local Rings

Definition 6.1.43 (Local Ring)
*Let $X = V(\mathfrak{a})$ be an affine variety and $W \subset X(\bar{k})$ be an irreducible subvariety. Then we define the **local ring** at W to be*

$$\mathcal{O}_{X,W} := \varinjlim_{U \cap W \neq \emptyset} \mathcal{O}_X(U)$$

It is a local ring with unique maximal ideal

$$\mathfrak{m}_{X,W} = \{(U,\sigma) \mid \sigma(x) = 0 \; \forall x \in W\}.$$

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 $(\mathcal{O}_{X,x}, \mathfrak{m}_{X,x})$.

Proof. First of all the family of open sets such that $U \cap W \neq \emptyset$ is directed by reverse inclusion precisely because W is irreducible, see (4.1.36).

Any section $\sigma \in \mathcal{O}_X(U)$ is continuous with respect to the cofinite topology on k. Therefore $D(\sigma) := \sigma^{-1}(k \setminus \{0\}) \subset U$ is an open set and $\sigma \notin \mathfrak{m}_{X,W} \implies D(\sigma) \cap W \neq \emptyset$. Then evidently $[(D(\sigma), \sigma^{-1})]$ is a multiplicative inverse for (U,σ) and by (...) $\mathcal{O}_{X,W}$ is a local ring with unique maximal ideal $\mathfrak{m}_{X,W}$. □

Proposition 6.1.44 (Local Ring is Localization of Coordinate Ring)
Let $X = V(\mathfrak{a})$ be an affine variety and $W \subset X(\bar{k})$ an irreducible subset with $\mathfrak{p} := I(W)$. Then we have an isomorphism

$$\begin{array}{ccc} k[X]_{\mathfrak{p}} & \xrightarrow{\sim} & \mathcal{O}_{X,W} \\ \dfrac{f}{g} & \to & \left[\left(D(g), \dfrac{f}{g}\right)\right] \end{array}$$

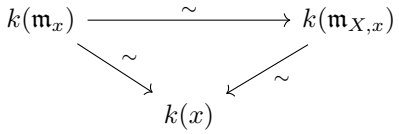
under which $\mathfrak{p}k[X]_{\mathfrak{p}}$ is mapped to $\mathfrak{m}_{X,W}$. This induces an isomorphism

$$k(\mathfrak{p}) = k[X]_{\mathfrak{p}}/\mathfrak{p}k[X]_{\mathfrak{p}} \xrightarrow{\sim} k(\mathfrak{m}_{X,W})$$

We have the following dimension formula

$$\dim \mathcal{O}_{X,W} = \operatorname{codim}(W, X) = \operatorname{ht}(\mathfrak{p})$$

In particular $k(\mathfrak{m}_{X,x})$ is finitely generated as a field and we have a commutative diagram



and the dimension formula holds

$$\dim \mathcal{O}_{X,x} = \operatorname{codim}(\{x\}, X) = \sup_{\alpha : x \in X_\alpha} \dim(X_\alpha)$$

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 (6.1.42), 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 (6.1.24). □

Proposition 6.1.45 (Dimension of Local Ring)
Let $X = V(\mathfrak{a})$ be an affine variety and $W \subset X(\bar{k})$ an irreducible subset. Then

$$\dim \mathcal{O}_{X,W} = \dim X - \dim W$$

In particular

$$\dim \mathcal{O}_{X,x} = \sup_{\alpha} \{\dim X_\alpha \mid x \in X_\alpha \text{ where } X_\alpha \text{ is an irreducible component of } X\}$$

Proof. The first statement follows from (6.1.44) and (6.1.26), the second from (6.1.28). □

Proposition 6.1.46
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 (6.1.44) 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 (6.1.19).

As $\mathcal{O}_{X,x}$ is reduced, it is an integral domain iff it has a unique minimal prime ideal (3.4.64). □

6.1.6 Generic Points

When considering irreducible subsets $W \subset X$ there is another way of looking at these in terms of "generic points".

Definition 6.1.47 (Generic Point)
Let $X = V(\mathfrak{a})$ be an affine variety and $(\xi) \in X(\Omega)$ for some extension field Ω/k. Then we may define the irreducible subset of $X(\bar{k})$

$$W_\xi := V_{\bar{k}}(\mathfrak{p}_\xi) = \Big\{(x) \in X(\bar{k}) \mid \forall f \in k[X]\,(f(\xi) = 0 \implies f(x) = 0)\Big\}$$

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.

6.1.7 Tangent Space and Non-Singular Points

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 6.1.48
*Let $X = V(\mathfrak{a})$ be an affine variety 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 $k(\mathfrak{m}_{X,x})$-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 6.1.49 (Concrete interpretation of Tangent Space)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ be an affine variety and $(x) \in X(\bar{k})$. Then there are natural $k(x)$-module isomorphisms

$$\begin{array}{ccccc} T_x X & \xrightarrow{\sim} & \mathrm{Der}_k\,(k[X], k(x)) & \xrightarrow{\sim} & \Big\{v \in k(x)^n \mid \sum_{i=1}^n v_i \dfrac{\partial F}{\partial X_i}(x) = 0 \quad \forall F \in \mathfrak{a}\Big\} \\ D & & \to & & (D(\overline{X_1}), \ldots, D(\overline{X_n})) \end{array}$$

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

$$\begin{pmatrix} \frac{\partial F_1}{\partial X_1}(x) & \dots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_m}{\partial X_1}(x) & \dots & \frac{\partial F_m}{\partial X_n}(x) \end{pmatrix} : k(x)^n \to k(x)^m$$

In particular

$$\dim_{k(x)} T_x X = n - \operatorname{rk}\left(\frac{\partial F_i}{\partial X_j}(x)\right)$$

Proof. Recall by (6.1.44) and (6.1.47) that $\mathcal{O}_{X,x} \cong k[X]_{\mathfrak{m}_x}$ and $k(\mathfrak{m}_{X,x}) \cong k(x)$ so we have isomorphisms

$$\operatorname{Der}_k(\mathcal{O}_{X,x}, k(\mathfrak{m}_{X,x})) \cong \operatorname{Der}_k(k[X]_{\mathfrak{m}_x}, k(x)) \overset{(3.24.9)}{\cong} \operatorname{Der}_k(k[X], k(x))$$

and the remaining isomorphism is from (3.29.34) □

Proposition 6.1.50
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n_k$ be an affine variety and $(x) \in X(\bar{k})$. There is a canonical $k(\mathfrak{m}_{X,x})$-module homomorphism

$$T_x X \quad \longrightarrow \quad (T^\star_x X)^\vee$$

Under the condition that $k(\mathfrak{m}_{X,x})/k$ is separable (e.g. k is perfect) then this map is an isomorphism. In particular $\dim T_x X = \dim T^\star_x X$ *by (3.4.103).*

Proof. This follows directly from (3.29.41) 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 6.1.51 (Non-Singular Point)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n_k$ be an affine variety, X_α an irreducible component and $(x) \in X_\alpha$. Then we have the following inequality

$$\dim_{k(x)} T_x X \geq \dim \operatorname{Der}(k(X_\alpha))) \tag{6.1}$$

Furthermore equality holds a non-empty dense open subset of each irreducible component X_α.

When $k(X_\alpha)/k$ is separably generated (e.g. k perfect) then $\dim \operatorname{Der}(k(X_\alpha)) = \operatorname{trdeg}(k(X_\alpha)) = \dim X_\alpha$.

Proof. Let $\Omega := k(X_\alpha) = \operatorname{Frac}(k[X_\alpha])$, $(\xi) := (\overline{X}_1, \dots, \overline{X}_n) \in \Omega^n$ 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

$$\operatorname{Der}(\Omega) \overset{(3.24.9)}{=} \operatorname{Der}(k[X_\alpha], \Omega) \overset{(3.29.34)}{\cong} \ker\left(\frac{\partial F_i}{\partial X_j}(\xi)\right)$$

There is a k-algebra homomorphism $k[\xi] \to k[x]$ and so by the determinant criteria of rank (3.4.170) we see

$$\operatorname{rk}\left(\frac{\partial F_i}{\partial X_j}(x)\right) \leq \operatorname{rk}\left(\frac{\partial F_i}{\partial X_j}(\xi)\right)$$

and therefore the inequality follows from (6.1.49). 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 (6.1.40).

When $k(X_\alpha)/k$ is separably generated then $\dim \operatorname{Der}(\Omega) = \operatorname{trdeg}(\Omega/k) = \dim X_\alpha$ by (3.29.37). □

Definition 6.1.52 (Non-Singular Point)
Let $X = V(\mathfrak{a})$ be an affine variety and $(x) \in X(\bar{k})$. Then we say (x) is a ***non-singular point*** *if*

a) *There is precisely one irreducible component, X_α, containing (x) (i.e. $\mathcal{O}_{X,x}$ is an integral domain)*

b) $\dim T_x X = \dim \operatorname{Der}(k(X_\alpha))$

We say X is non-singular if all points are non-singular.

Definition 6.1.53 (Regular Point)
*Let $X = V(\mathfrak{a})$ be an affine variety and $(x) \in X(\bar{k})$. Then we say that (x) is **regular** if*

a) *There is precisely one irreducible component, X_α, containing x (i.e. $\mathcal{O}_{X,x}$ is an integral domain)*

b) *$\mathcal{O}_{X,x}$ is a regular local ring (i.e. $\dim T_x^\star X = \dim X$)*

*We say X is **regular** if all its $\bar{k}$-rational points are regular.*

Fortunately these concepts are typically equivalent.

Proposition 6.1.54 (Regular = Non-Singular)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ an affine variety with k perfect. Then

$$\dim T_x^\star X = \dim T_x X$$

and the following are equivalent

a) *(x) is regular*

b) *(x) is non-singular*

c) *$\dim T_x X = \dim X$ and $\mathcal{O}_{X,x}$ is an integral domain*

When X is an affine curve this is equivalent to $\mathcal{O}_{X,x}$ being a discrete valuation ring.

Proof. Recall by (6.1.45) that $\dim \mathcal{O}_{X,x} = \dim X$ and by definition $T_x^\star X = \mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2$. Further by definition (x) is regular iff $\dim T_x^\star X = \dim \mathcal{O}_{X,x}$. Finally by (6.1.50) $\dim T_x^\star X = \dim T_x X$ so we see $a) \iff c)$.

Similarly $b) \iff c)$ is essentially by definition. □

Example 6.1.55 (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.

6.1.8 Zeta Function over Finite Fields

For this section let $k = \mathbb{F}_p$ with algebraic closure $\overline{k}$. Then for every $n \geq 1$ by (...) $\overline{k}$ has a unique subfield k_n of degree n, and order p^n. Furthermore we have the following properties

a) $k_m \subseteq k_n \iff [k_m : k] \mid [k_n : k] \iff m \mid n$

b) $[k_n : k_m] = n/m$

c) k_n/k_m is Galois with the group of automorphisms generated by ϕ^m for all integers $m \mid n$, and the Galois group has order n/m.

d) every finite subextension is of this form

Lemma 6.1.56
Let $x_1, \ldots, x_N \in \overline{k}$. Then

$$k(x_1, \ldots, x_N) = k_n$$

where

$$n := \operatorname{lcm}_i [k(x_i) : k]$$

Proof. By definition $[k(x_i) : k] \mid n$ whence $k(x_i) \subseteq k_n$ by the previous observations, and therefore $k(x_1, \ldots, x_N) \subseteq k_n$.

Similarly as $k(x_i) \subset k(x_1, \ldots, x_N)$ we have $[k(x_i) : k] \mid [k(x_1, \ldots, x_N) : k]$. Then by definition $r \mid [k(x_1, \ldots, x_N) : k]$ which shows $k_n \subset k(x_1, \ldots, x_N)$. □

The following result shows that the number of rational points over a finite field may be characterized by algebraic properties of the coordinate ring $k[X]$. This is essentially because maximal ideals correspond to Galois orbits of rational points and we may count rational points by summing over Galois orbits.

Proposition 6.1.57 (Counting Rational Points)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^N$ be an affine variety. Then for all integers $n \geq 1$ we have the following relation

$$\#X(k_n) = \sum_{d|n} d \times \#\{\mathfrak{m} \mid \dim_k k(\mathfrak{m}) = d\}$$

Proof. For $(x) \in X(\bar{k})$, then by the previous discussion

$$(x) \in X(k_n) \iff k(x) \subseteq k_n \iff \dim_k k(x) \mid n$$

This shows that

$$\begin{aligned} \#X(k_n) &= \sum_{d|n} \#\{(x) \in X(k_n) \mid \dim_k k(x) = d\} \\ &= \sum_{d|n} \#\{(x) \in X(k_d) \mid \dim_k k(x) = d\} \end{aligned} \tag{6.2}$$

By (6.1.12) we have a bijection

$$X(k_d)/\operatorname{Gal}(k_d/k) \xrightarrow{\sim} \{\mathfrak{m} \mid \dim_k k(\mathfrak{m}) \mid d\}$$

As we have an isomorphism $k(x) \cong k(\mathfrak{m}_x)$ this restricts to a bijection

$$\{(x) \in X(k_d) \mid \dim_k k(x) = d\}/\operatorname{Gal}(k_d/k) \xrightarrow{\sim} \{\mathfrak{m} \mid \dim_k k(\mathfrak{m}) = d\}$$

We claim that the action of $\operatorname{Gal}(k_d/k) = \langle \phi \rangle$ is free. For suppose $(x) \in X(k_d)$ such that $\dim_k k(x) = d$ and $\phi^r(x_i) = x_i$ for $i = 1 \dots N$ and $0 < r \leq d$. Then by (3.18.115) we have $x_i \in k_r$ whence $\dim_k k(x) \leq r$. This shows we must have $r = d$ and in particular only the identity automorphism fixes (x).

Therefore we see that

$$\#\{(x) \in X(k_d) \mid \dim_k k(x) = d\} = \#\operatorname{Gal}(k_d/k) \times \#\{\mathfrak{m} \mid \dim_k k(\mathfrak{m}) = d\}$$

From (3.18.118) we recall $\operatorname{Gal}(k_d/k)$ is cyclic of order d so we may combine this with (6.2) to obtain the required result.

□

Proposition 6.1.58 (Zeta function of an affine variety over a finite field)
Formally as elements of the power series ring $\mathbb{Q}[[T]]$ we have

$$Z(X,T) := \prod_{\mathfrak{m} \in \operatorname{Specm}(k[X])} (1 - T^{\deg(\mathfrak{m})})^{-1} = \exp\left(\sum_{m=1}^{\infty} \frac{\#X(k_m)}{m} T^m \right)$$

Proof. Define

$$b_d := \#\{\mathfrak{m} \mid \dim_k k(\mathfrak{m}) = d\}$$

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 6.1.59
For $X(k) = k^n$ we have $\#X(k_m) = p^{mn}$. Then

$$Z(X,T) = \exp\left(\sum_{n=1}^{\infty} \frac{p^{mn}T^m}{m}\right) = \exp(-\log(1-p^nT)) = \frac{1}{1-p^nT}$$

6.1.9 Base Change

In the context of affine varieties **base change** refers to extending the coefficient ring k to some larger extension K/k (denoted $X \to X_K$). In the category of affine varieties, base change is only well-defined when the tensor product $k[X] \otimes_k K$ is reduced, which corresponds to the notion of "**geometrically reduced algebras**", see Section 3.31.2. We use results from this section to determine when the base change is well-defined.

We are also interested in when X_K is an **integral** (or **irreducible**) variety, and in particular when it is integral for all field extensions K/k.

For applications one may want to restrict to the category of "geometrically integral affine varieties".

Definition 6.1.60 (Properties of Base Change)
*Let $X = V(\mathfrak{a})$ be an affine variety and K/k is a field extension. We say that X_K is **reduced** (resp. **integral**) if the tensor product $k[X] \otimes_k K$ is reduced (resp. integral)*

*We say that X is **geometrically reduced** (resp. **geometrically integral**) if X_K is reduced (resp. integral) for every field extension K/k.*

When X_K is reduced then it is an affine variety.

Proposition 6.1.61 (Reduced Base Change is Well-Defined)
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n_k$ be an affine variety and K/k is a field extension. Suppose one of the following conditions holds

a) *$k[X]$ is geometrically reduced (equivalently if $k[X] \otimes_k k^{1/p}$ is reduced (3.31.23))*

b) *K/k is geometrically reduced (for example when K/k is separable algebraic (3.31.17))*

*Then X_K is **reduced** and the extended ideal $\mathfrak{a}^e = \mathfrak{a} \otimes_k K \lhd K[X_1, \dots, X_n]$ is radical.*

*In this case define the **base change** $X_K := V(\mathfrak{a}^e) \subset \mathbb{A}^n_K$ with coordinate ring $K[X_K] \cong k[X] \otimes_k K$. Then X_K is integral $\iff$ $X_K(\overline{K})$ is irreducible.*

For any field extension L/K there is a commutative diagram

$$\begin{array}{ccc} \mathrm{AlgHom}_k(k[X], L) & \xrightarrow{\sim} & X(L) \\ \downarrow \sim & & \vdots \downarrow \\ \mathrm{AlgHom}_K(K[X_K], L) & \xrightarrow{\sim} & X_K(L) \end{array}$$

where the horizontal arrows are given by (6.1.33) and the vertical arrow by (3.5.37). Consequently there is a bijection

$$X(K) \xrightarrow{\sim} X_K(K) = (X_K)_0(K)$$

Proof. Observe that $\mathfrak{a}^e$ is radical iff $K[X_1, \dots, X_n]/\mathfrak{a}^e \overset{(3.5.41)}{\cong} k[X] \otimes_k K$ is reduced. Then $k[X] \otimes_k K$ is reduced either by definition in case *a*) or by (3.31.19) in case *b*). □

Proposition 6.1.62 (Criteria to be Geometrically Reduced)
Let $X = V(\mathfrak{a})$ be an affine variety. Then the following are equivalent

a) *X is geometrically reduced*

b) *$X_{\bar{k}}$ is reduced*

c) *$X_{k^{1/p}}$ is reduced*

When X is irreducible then this is equivalent to

d) $k(X)/k$ geometrically reduced

e) $k(X)/k$ separably generated

In particular we see that for k perfect every affine variety is geometrically reduced.

Proof. For the equivalence of $a) - c)$ this is simply (3.31.23).

When X is irreducible then $k[X]$ is integral (6.1.18) so $k(X) = \mathrm{Frac}(k[X])$ is well-defined. Then by (3.31.20) $k[X]$ is geometrically reduced iff $k(X)$ is. Then the equivalence follows because $k(X)$ is finitely generated and (3.31.26). □

Proposition 6.1.63 (Criteria to be Geometrically Integral)
Let $X = V(\mathfrak{a})$ be a geometrically reduced affine variety (e.g. k perfect). Then the following are equivalent

a) *X is geometrically integral*

b) *$X_{\bar{k}}$ is integral*

c) *$X_{k'}$ is integral for every finite separable extension k'/k*

d) *X is integral and $k(X)/k$ is geometrically integral*

e) *k is relatively separably closed in $k(X)$*

f) *k is relatively algebraically closed in $k(X)$*

Proof. This is simply a translation of (3.31.41). □

6.1.10 Locally Ringed Space

The canonical approach of patching together affine varieties (analogously to differentiable manifolds) is to embed in the category of locally ringed spaces. For technical reasons this construction only works when considering the set of Galois orbits $X_0(\bar{k})$.

Proposition 6.1.64
Let $X = V(\mathfrak{a})$ be an affine variety and $\pi : X(\bar{k}) \to X_0(\bar{k})$ the Galois quotient (6.1.11). Define $\mathcal{O}_{X_0} := \pi_\star \mathcal{O}_X$. Then $(X_0(\bar{k}), \mathcal{O}_{X_0})$ is a locally ringed space. More precisely for every $x \in X(\bar{k})$

$$\mathcal{O}_{X_0,[x]} = \mathcal{O}_{X,x}$$

Proof. π induces a bijection

$$\{V_0 \subset X_0 \mid [x] \in V_0\} \longleftrightarrow \{V \subset X \mid x \in V\}$$

therefore

$$(\pi_\star \mathcal{O}_X)_{[x]} = \varinjlim_{[x] \in V_0} \mathcal{O}_X(\pi^{-1}(V_0)) = \varinjlim_{x \in V} \mathcal{O}_X(V) = \mathcal{O}_{X,x}$$

□

Proposition 6.1.65
Let $X \subset \mathbb{A}^n_k$ and $Y \subset \mathbb{A}^m_k$ be affine varieties. Then there are bijection

$$\{\phi : X \to Y \ \text{ regular }\} \overset{(6.1.33)}{\longleftrightarrow} \{\phi_\star : k[Y] \to k[X]\} \longleftrightarrow \{(\phi_{\bar{k},0}, \phi^\sharp) : (X_0(\bar{k}), \mathcal{O}_{X_0}) \to (Y_0(\bar{k}), \mathcal{O}_{Y_0})\}$$

determined by

$$\begin{aligned} \phi^\sharp : \mathcal{O}_{Y_0}(U) = \mathcal{O}_Y(\pi^{-1}(U)) &\to \mathcal{O}_{X_0}(\phi^{-1}_{\bar{k},0}(U)) = \mathcal{O}_X(\phi^{-1}_{\bar{k}}(\pi^{-1}(U))) \\ \sigma &\to \sigma \circ \phi_{\bar{k}} \end{aligned}$$

and $\phi^\sharp_{Y_0} = \phi_\star$ after suitable identification $\mathcal{O}_{X_0}(X_0) \cong k[X]$ and $\mathcal{O}_{Y_0}(Y_0) \cong k[Y]$.

Proof. Recall that ϕ determines a unique k-algebra homomorphism $\phi_\star : k[Y] \to k[X]$. Then $\phi_{\bar{k}}$ is continuous because $\phi^{-1}(D(g)) = D(\phi_\star(g))$. If σ is determined by some family of rational sections $\{(U_i, \frac{g_i}{h_i})\}$ then it's clear $\sigma \circ \phi$ is determined by $\{(\phi^{-1}(U_i), \frac{\phi_\star(g_i)}{\phi_\star(h_i)})\}$. By (6.1.32) the map is injective.

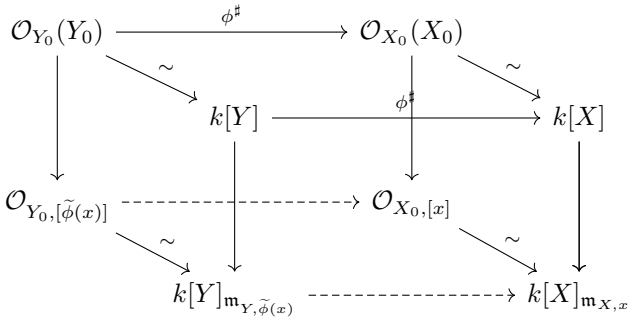
We may demonstrate that the morphism of sheaves $\phi^\sharp$ is uniquely determined by its value on global sections, $\phi^\sharp_Y$. For

$$\phi^\sharp(\sigma)|_{U_i} = \phi^\sharp(\sigma|_{U_i}) = \phi^\sharp_{U_i}\left(\frac{g_i}{h_i}\right) = \frac{\phi^\sharp_{U_i}(g_i)}{\phi^\sharp_{U_i}(h_i)} = \frac{\phi^\sharp_Y(g_i)|_{U_i}}{\phi^\sharp_Y(h_i)|_{U_i}}$$

Therefore we may show the given map is surjective if for every pair $(\widetilde{\phi}, \phi^\sharp)$ we have $\widetilde{\phi} = \phi_{\bar{k}}$ where

$$\phi := (\phi^\sharp_Y(y_1), \dots, \phi^\sharp_Y(y_m))$$

using the identifications $\mathcal{O}_{X_0}(X_0) \cong k[X]$ and $\mathcal{O}_{Y_0}(Y_0) \cong k[Y]$. Consider $[(x)] \in X_0(\bar{k})$ and the commutative diagram



where the isomorphisms follow from (6.1.42) and the dashed arrows are local homomorphisms. Chasing the ideal $\mathfrak{m}_{X,x}k[X]_{\mathfrak{m}_{X,x}}$ shows that $(\phi^\sharp)^{-1}(\mathfrak{m}_{X,x}) = \mathfrak{m}_{Y,\widetilde{\phi}(x)}$. Recall by (6.1.33) that $\phi^\sharp(g)(x) = g(\phi(x))$. Therefore by definition $\left(\phi^\sharp\right)^{-1}(\mathfrak{m}_{X,x}) \subseteq \mathfrak{m}_{Y,\phi(x)}$ whence by maximality $\mathfrak{m}_{Y,\widetilde{\phi}(x)} = \mathfrak{m}_{Y,\phi(x)}$. By the Weak Nullstellensatz (6.1.12) we see that $\phi(x) = \widetilde{\phi}(x)$ as required. □

6.1.11 Valuation Rings on the Function Field

Proposition 6.1.66
Let K/k be a field extension and R a valuation ring of K/k. Then there exists a valuation ring $R' \subset R$ such that $k(\mathfrak{m}_{R'})/k$ is algebraic.

Proof. By (3.23.8) the identity map $1 : k \to \overline{k}$ extends to a ring homomorphism $S \to \bar{k}$ where $(S, \mathfrak{m}_S)$ is a valuation ring of $k(\mathfrak{m}_R)/k$. Considering the quotient map $\pi : R \to k(\mathfrak{m}_R)$ let $R' := \pi^{-1}(S)$. The restriction map

$$\pi' : R' \to S \to k(\mathfrak{m}_S)$$

is surjective, and so the kernel $\mathfrak{m}_{R'} := \ker(\pi')$ is a maximal ideal of R' and $k(\mathfrak{m}_{R'}) \cong k(\mathfrak{m}_S)$. Observe that by $R' \subseteq R$ and $\mathfrak{m}_R \subseteq \mathfrak{m}_{R'}$. If $x \notin R$ then $x^{-1} \in \mathfrak{m}_R \implies x^{-1} \in R$ by (3.23.2). If $x \in R \setminus R'$ then $\pi(x) \notin S \implies \pi(x^{-1}) \in S \implies x^{-1} \in R'$. Therefore we conclude that R' is a valuation ring with maximal ideal $\mathfrak{m}_{R'}$ and algebraic residue field as required. □

The following result was proven in the case of a finitely generated k-algebra (3.29.21), where equality holds. In general only the inequality holds by considering for example the case $\dim K = 0$. The proof below is taken from [Rey11].

Lemma 6.1.67
Let R be a subring of a finitely generated field extension K/k. Then $\dim R \leq \operatorname{trdeg}(K/k)$.

Proof. Consider a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n \subset R$$

Choose $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_{i-1}$ and define $A := k[x_1, \ldots, x_n] \subset R$ with $K' := \operatorname{Frac}(A) \subset K$. Then there is a chain of prime ideals of A

$$\mathfrak{p}_0 \cap A \subsetneq \ldots \subsetneq \mathfrak{p}_n \cap A$$

whence $n \leq \dim A \overset{(3.29.21)}{=} \operatorname{trdeg}(K'/k) \overset{(3.18.136)}{\leq} \operatorname{trdeg}(K/k)$. Taking supremum over n we reach the required result. □

Lemma 6.1.68
Let $R \subseteq S$ be proper valuation rings of K with $\dim R < \infty$. *Then* $\dim S \leq \dim R$, *with equality iff $R = S$.*

Proof. Firstly we claim that $\mathfrak{m}_S \subseteq \mathfrak{m}_R$. For $x \in \mathfrak{m}_S \implies x^{-1} \notin S \implies x^{-1} \notin R \implies x \in \mathfrak{m}_R$.

Secondly if $R \subsetneq S$ then $\mathfrak{m}_S \subsetneq \mathfrak{m}_R$. For given $x \in S \setminus R$ we have $x^{-1} \in \mathfrak{m}_R \implies x^{-1} \in S \implies x^{-1} \in S^\star \implies x^{-1} \notin \mathfrak{m}_S$.

Let $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ be a chain of prime ideals in S. As these are contained in $\mathfrak{m}_S$, they are also contained in $\mathfrak{m}_R$ and therefore R. Therefore this constitutes a chain of prime ideals in R from which we deduce the inequality. Further if $R \subsetneq S$ then we may always extend the chain by at least one prime ideal, namely $\mathfrak{m}_R$. □

Proposition 6.1.69
Let $X = V(\mathfrak{a}) \subset \mathbb{A}^n_k$ be an irreducible affine variety. Suppose $k[X] \subset R \subset k(X)$ be a valuation ring. Then there exists a point $(x) \in X(\bar{k})$ such that R dominates $k[X]_{\mathfrak{m}_x} \cong \mathcal{O}_{X,x}$. Further $\dim R \leq \dim k[X]$ *with equality iff $\mathcal{O}_{X,x} = R$.*

Proof. By (6.1.66) we may assume that $k(\mathfrak{m}_R)/k$ is algebraic. Choose any embedding $k(\mathfrak{m}_R)/k \hookrightarrow \bar{k}/k$ (3.18.72). Then there is a composite k-algebra homomorphism

$$k[X] \hookrightarrow R \to k(\mathfrak{m}_R) \hookrightarrow \bar{k}$$

Let x_i be the image of X_i under this homomorphism. The the image $k[x_1, \dots, x_n]$ is a (finite) field extension of k by (3.18.56). Then under this map the image of f is $f(x_1, \dots, x_n)$, so the kernel is precisely $M_{X,x} = \mathfrak{m}_R \cap k[X]$. Suppose that $f \notin M_{X,x}$ then $f \notin \mathfrak{m}_R \implies f^{-1} \in R$. In particular we conclude that $\mathcal{O}_{X,x} \subset R$. Further $\mathfrak{m}_{X,x} = M_{X,x}\mathcal{O}_{X,x} \subseteq \mathfrak{m}_R k[X] \subseteq \mathfrak{m}_R$, so R dominates $\mathcal{O}_{X,x}$ by (3.23.3).

The final statement follows from (6.1.68) and $\dim k[X] = \dim \mathcal{O}_{X,x}$ (6.1.45). □

6.1.12 Affine Curves

Definition 6.1.70
*An **affine curve** is an affine variety of pure dimension* 1.

For example an irreducible polynomial $F(X, Y)$ yields an affine curve and is known as a plane curve. The singular points are precisely the common roots of

$$F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}$$

in $\bar{k}^2$. If there are no such roots then the affine curve is non-singular.

Proposition 6.1.71 (Characterisation Regular Point on a curve)
Let $X = V(\mathfrak{a})$ be an affine curve and $(x) \in X(\bar{k})$. Then the following are equivalent

a) *(x) is regular*

b) *$\mathcal{O}_{X,x}$ is a discrete valuation ring*

c) *$\mathcal{O}_{X,x}$ is an integrally closed domain*

When k is perfect then this is equivalent to (x) being a non-singular point.

Proof. Note that in each case (x) lies on a unique irreducible component and $\mathcal{O}_{X,x}$ is an integral domain using the equivalence (6.1.46) (and definition of regular).

$a) - c)$ then follows directly from (3.28.2) and the fact $\dim \mathcal{O}_{X,x} = \dim X = 1$ (6.1.45). The final statement follows from (6.1.54). □

Proposition 6.1.72
Let $X = V(\mathfrak{a})$ be a regular and irreducible affine curve. Then there exists a bijection

$$X(\bar{k})/\operatorname{Aut}(\bar{k}/k) \longleftrightarrow \{k[X] \subset R \subsetneq k(X) \mid R \text{ valuation ring}\}$$

By (6.1.71) all such local rings are discrete valuation rings, and by (...) $\operatorname{trdeg}_k(k(X)) = 1$.

Proof. The map $(x) \to \mathcal{O}_{X,x}$ is well-defined by (6.1.71). If $\mathcal{O}_{X,x} = \mathcal{O}_{Y,y}$ then $\mathcal{O}^\star_{X,x} = \mathcal{O}^\star_{Y,y} \implies \mathfrak{m}_{X,x} = \mathfrak{m}_{X,y} \implies M_{X,x} = M_{X,y} \implies (x) \sim (y)$ by the Weak Nullstellensatz (6.1.12) so the map is injective.

To show surjectivity, observe by (6.1.69) there exists $(x) \in X(\bar{k})$ such that $\mathcal{O}_{X,x} \subseteq R$. Furthermore by repeated application of (6.1.68) we see

$$0 < \dim R \leq \dim \mathcal{O}_{X,x} = \dim k[X] = 1$$

This forces $\dim R = \dim \mathcal{O}_{X,x} = 1$ and so $R = \mathcal{O}_{X,x}$ by the same result. □

6.2 Projective Varieties

Definition 6.2.1 (Projective Space)
Let K be a field extension define

$$\mathbb{P}^n(K) := K^{n+1} \setminus \{(0, \dots, 0)\}/\sim$$

where

$$(x_0, \dots, x_n) \sim (x'_0, \dots, x'_n) \iff x_i = \lambda x'_i \text{ some } \lambda \in K^\star$$

and write $[x_0 : \dots : x_n]$ for the corresponding equivalence class in $\mathbb{P}^n(K)$.

Proposition 6.2.2 (Projective Space is Functorial)
Let $\phi : K \to L$ be an injective ring homomorphism Then there is a well-defined injective map

$$\begin{aligned} \mathbb{P}^n(K) &\to \mathbb{P}^n(L) \\ [x_0 : \ldots : x_n] &\to [\phi(x_0) : \ldots : \phi(x_n)] \end{aligned}$$

Proof. Evidently the map is well-defined. Suppose that

$$(\phi(x_0) : \ldots : \phi(x_n)) \sim (\phi(x_0') : \ldots : \phi(x_n'))$$

Then for some i we have $x_i \neq 0$ and $\phi(x_i) = \lambda\phi(x_i')$ and $\lambda \in L^\star$. Therefore $\phi(x_i') \neq 0 \implies x_i' \neq 0$ and $\lambda = \phi(x_i/x') =: \phi(\mu)$. Similarly $\phi(x_j) = \phi(\mu)\phi(x_j') \implies \phi(x_j - \mu x_j') = 0 \implies x_j = \mu x_j'$. □

Proposition 6.2.3 (Zero Loci in Projective Space)
Let $A = k[X_0, \ldots, X_n]$ be the graded polynomial ring in $(n+1)$-variables over a field k. For a homogenous ideal $\mathfrak{a} \subset k[X_0, \ldots, X_n]$ and field extension K/k define the ***zero-locus***

$$V_+(\mathfrak{a})(K) := \{[x_0 : \ldots : x_n] \in \mathbb{P}^n(K) \mid F(x_0, \ldots, x_n) = 0 \quad \forall F \in \mathfrak{a}\}$$

Similarly for a subset $Y \subset \mathbb{P}^n(K)$ define

$$I_+(Y) := \{F \in k[X_0, \ldots, X_n] \mid F_d(x_0, \ldots, x_n) = 0 \quad \forall d \geq 0, [x_0 : \ldots : x_n] \in Y\}$$

Then

a) *$I_+(Y)$ is a homogenous radical ideal and $\sqrt{\langle S \rangle} \subseteq I_+(V_+(S)(K))$*

b) *I_+ and V_+ are order-reversing*

c) *$S \subseteq I_+(V_+(S)(K))$ and $Y \subseteq V_+(I_+(Y))(K)$*

d) *$V_+ \circ I_+ \circ V = V_+$ and $I_+ \circ V_+ \circ I_+ = I_+$*

e) *$V_+(S) = V_+(\sqrt{\langle S \rangle})$ and $V_+(\mathfrak{a}) = V_+(\sqrt{\mathfrak{a}})$*

f) *$\bigcap_i V_+(S_i) = V_+\left(\bigcup_i S_i\right)$ and $\bigcap_i V_+(\mathfrak{a}_i) = V_+(\sum_i \mathfrak{a}_i)$*

g) *$\bigcap_i I_+(W_i) = I_+(\bigcup W_i)$*

h) *$V_+(\mathfrak{a}) \cup V_+(\mathfrak{b}) = V_+(\mathfrak{a} \cap \mathfrak{b})$*

i) *$V_+((0)) = \mathbb{P}^n(K)$*

The sets of the form $V_+(\mathfrak{a})(K)$ determine the ***Zariski Topology*** *on $\mathbb{P}^n(K)$. We denote the topological space by $\mathbb{P}^n_k(K)$. The topological closure satisfies the following identities*

$$V_+(I_+(X)) = \overline{X}$$

and

$$I_+(X) = I_+(\overline{X})$$

There is a form of the Weak Nullstellensatz

$$V_+(\mathfrak{a})(\bar{k}) = \emptyset \iff A_+ \subset \sqrt{\mathfrak{a}} \iff \mathfrak{a} \text{ is "irrelevant"}$$

and a form of the Strong Nullstellensatz namely

$$\mathfrak{a} \text{ essential} \implies I_+(V_+(\mathfrak{a})(\bar{k})) = \sqrt{\mathfrak{a}}$$

Further there is a dual isomorphism

$$\left\{\mathfrak{a} \lhd A \mid \mathfrak{a} \text{ radical homogenous and } A_+ \not\subset \mathfrak{a}\right\} \underset{V_+}{\overset{I_+}{\leftrightarrows}} \left\{Z \in \mathbb{P}^n_k(\bar{k}) \mid Z \neq \emptyset\right\}$$

Proof. Let $V_K(S) := \{(x) \in K^{n+1} \mid f(x) = 0 \quad \forall s \in S\}$ denote the affine zero-locus. Then $V_+(S)(K) = \pi(V_K(S) \backslash \{\mathbf{0}\})$, where $\mathbf{0} = (0, \ldots, 0)$ is the origin in K^{n+1}.

a) Homogeneity follows from definition. The relation is straightforward.

b) Follows by definition

c) The pair I, V form a Galois connection by Example 2.1.53 and the relations follow formally by (2.1.49).

d) Follows formally by (2.1.51)

e) Follows from (2.1.52) by considering the closure operators $\sqrt{\langle - \rangle}$ and $\langle - \rangle$.

f) The first equality follows from (2.1.54). The second equality follows from (3.4.28).

g) This follows from (2.1.54).

h) Then using the affine case we may deduce

$$V_+(\mathfrak{a} \cap \mathfrak{b}) = \pi(V(\mathfrak{a} \cap \mathfrak{b}) \setminus \mathbf{0}) = \pi(V(\mathfrak{a}) \cup V(\mathfrak{b}) \setminus \mathbf{0}) = \pi(V(\mathfrak{a}) \setminus \mathbf{0}) \cup \pi(V(\mathfrak{b}) \setminus \mathbf{0}) = V_+(\mathfrak{a}) \cup V_+(\mathfrak{b})$$

i) Trivial

- **Weak Nullstellensatz** Observe that using the affine case $V_{\bar{k}}(A_+) = \{\mathbf{0}\}$ and $I_{\bar{k}}(\mathbf{0}) = A_+$. Therefore

$$V_+(\mathfrak{a})(\bar{k}) = \emptyset \iff V_{\bar{k}}(\mathfrak{a}) \subset \{\mathbf{0}\} \iff A_+ \subset \sqrt{\mathfrak{a}} \overset{(3.12.7)}{\iff} \mathfrak{a} \text{ irrelevant}$$

- **Strong Nullstellensatz** Assume $\mathfrak{a}$ is an essential homogenous ideal then $Y := V(\mathfrak{a}) \setminus \{\mathbf{0}\}$ is non-empty and $\overline{Y} = V(\mathfrak{a})$. Because $\mathfrak{a}$ is homogenous then Y is a cone- $x \in Y \implies \lambda x \in Y$ for $\lambda \in \bar{k}^\star$. We claim that $V_+(\mathfrak{a}) = \pi(Y)$ and $I(Y) = I_+(\pi(Y))$. Suppose $F \in I(Y)$ then $F(\lambda x) = 0$ for all $\lambda \in \bar{k}^\star$ and $x \in Y$. As $\bar{k}$ is infinite we deduce that $F_d \in I(Y)$ whence $F \in I_+(\pi(Y))$. The remaining claims are clear. Therefore we may deduce from (6.1.4) and (6.1.15)

$$I_+V_+(\mathfrak{a}) = I_+(\pi(Y)) = I(Y) = I(\overline{Y}) = I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$$

- **Topological Closure** By (2.1.51) $V_+ \circ I_+$ is a closure operator with image precisely the closed sets. Therefore by (2.1.40) $V_+ \circ I_+$ is the topological closure (4.1.18). Finally $I_+(\overline{X}) = I_+(V_+(I_+(X))) = I_+(X)$ using d).

The dual isomorphism follows from the Strong Nullstellensatz □

Definition 6.2.4 (Projective Variety)
For a homogenous radical ideal $\mathfrak{a} \lhd k[X_0, \ldots, X_n]$ we say the family

$$X(K) := V_+(\mathfrak{a})(K) \subset \mathbb{P}^n_k(K)$$

*is a **projective variety** and write it as $X(K) := V_K(\mathfrak{a})$. We say X is **irreducible** if $X(\bar{k})$ is irreducible in the subspace topology. We also define the **homogenous coordinate ring***

$$k[X] := k[X_0, \ldots, X_n]/\mathfrak{a}$$

*which is naturally a positive graded ring by (3.11.11). Define the **irrelevant ideal***

$$k[X]_+ := \bigoplus_{d>0} k[X]_d$$

We may generalise (6.2.3) as follows.

Proposition 6.2.5 (Zero Loci in Projective Varieties)
*Let $X = V_+(\mathfrak{a}) \subset \mathbb{P}^n_k$ be a projective variety and $A = k[X]$ the coordinate ring. For any homogenous ideal $\mathfrak{b} \lhd A$ and field extension K/k define the **zero-locus** by*

$$V_+(\mathfrak{b})(K) := \{[x_0 : \ldots : x_n] \in X(K) \mid f(x_0, \ldots, x_n) = 0 \quad \forall f \in \mathfrak{b}\}$$

Similarly for a subset $Y \subset X(K)$ define

$$I_+(Y) := \{f \in k[X] \mid f_d(x) = 0 \quad \forall d \geq 0, x \in Y\}$$

Suppose $\pi : k[X_0, \ldots, X_n] \to k[X]$ is the quotient map. Then we have the following properties

$$\begin{aligned} V_+(\mathfrak{b})(K) &= V_+(\pi^{-1}(\mathfrak{b}))(K) \cap X(K) \\ I_+(Y \cap X(K)) &= \pi(I_+(Y)) \quad Y \subset \mathbb{P}^n_k(K) \\ I_+(V_+(\mathfrak{b})(K)) &= \pi(I_+(V_+(\pi^{-1}(\mathfrak{b})))) \end{aligned}$$

The pair $(V_+(-)(K), I_+)$ satisfies the same properties as (6.2.3). The image of $V_+(-)(K)$ forms the closed sets of a topology on $X(K)$ which coincides with the subspace topology from $\mathbb{P}^n_k(K)$. Further the Weak and Strong Nullstellensatz also hold

$$V_+(\mathfrak{b})(\bar{k}) = \emptyset \iff k[X]_+ \subset \sqrt{\mathfrak{b}} \iff \mathfrak{b} \text{ is irrelevant}$$

and

$$\mathfrak{b} \text{ essential} \implies I_+(V_+(\mathfrak{b})(\bar{k})) = \sqrt{\mathfrak{b}}$$

Proposition 6.2.6 (Principal Open Sets)
Let $X \subset \mathbb{P}^n_k$ be a projective variety. The Zariski topology on $X(K)$ has a base consisting of subsets of the form

$$D_+(f)(K) := X(K) \setminus V_+((f)) = \{(x) \in X(K) \mid f_d(x) \neq 0 \text{ some } d > 0\}$$

where $f \in k[X]$ is a homogenous form. Note that $(x) = (y) \implies (f_d(x) = 0 \iff f_d(y) = 0)$ so the second form is well-defined.

Proof. A generic open set $U = X(K) \setminus V_+(\mathfrak{b})(K)$ where $\mathfrak{b}$ is a homogenous ideal of $k[X]$. Given $(x) \in U$ there is some $f \in \mathfrak{b}$ and $d > 0$ such that $f_d(x) \neq 0$. Therefore $D_+(f_d) \subset U$ is an open neighbourhood of (x). □

Proposition 6.2.7
Let $X = V_+(\mathfrak{b})$ be a projective variety and $f, g \in k[X]$ essential homogenous forms. Then

$$D_+(g) \subset D_+(f) \iff f \mid g^N \text{ some } N > 0$$

Proof.

$$D_+(g) \subset D_+(f) \iff V_+((f)) \subset V_+((g)) \iff \sqrt{(g)} \subset \sqrt{(f)} \iff f \mid g^N$$

□

Proposition 6.2.8 (Irreducible Subsets)
Let $X = V_+(\mathfrak{a}) \subset \mathbb{P}^n_k$ be a projective variety and $\mathfrak{b} \triangleleft k[X]$ a homogenous radical ideal. Then a closed subset $V_+(\mathfrak{b}) \subset X$ is irreducible iff $\mathfrak{b}$ is prime.

In particular $\mathbb{P}^n_k(\bar{k})$ is irreducible.

Proof. Let $Y := V_+(\mathfrak{b})$. Suppose that Y is not irreducible then $Y \subseteq V_+(\mathfrak{c}) \cup V_+(\mathfrak{d})$ is a non-trivial decomposition into closed subsets for $\mathfrak{c}, \mathfrak{d}$ essential homogenous radical ideals for which $Y \not\subseteq V_+(\mathfrak{c}) \implies \mathfrak{c} \not\subseteq \mathfrak{b}$ and similarly $\mathfrak{d} \not\subseteq \mathfrak{b}$ (see (4.1.37)). Choose $f \in \mathfrak{c} \setminus \mathfrak{b}$ and $g \in \mathfrak{d} \setminus \mathfrak{b}$. Then fg is zero on Y whence $fg \in \mathfrak{b}$. This shows that $\mathfrak{b}$ is not prime.

Conversely suppose $Y \subset V_+(\mathfrak{c}) \cup V_+(\mathfrak{d}) = V_+(\mathfrak{c} \cap \mathfrak{d})$ then by (6.2.3) $\mathfrak{c}\mathfrak{d} \subset \mathfrak{c} \cap \mathfrak{d} \subset \mathfrak{b}$. By (3.4.38) we have $\mathfrak{c} \subset \mathfrak{b}$ or $\mathfrak{d} \subset \mathfrak{b}$, whence $Y \subset V_+(\mathfrak{c})$ or $Y \subset V_+(\mathfrak{d})$. Therefore we conclude that Y is irreducible by (4.1.37).

Therefore $\mathbb{P}^n_k(\bar{k})$ is irreducible by the special case both $\mathfrak{a}$ and $\mathfrak{b}$ being the zero ideals. □

Proposition 6.2.9 (Dual Isomorphism between Closed Sets and Homogenous Ideals)
Let $X = V_+(\mathfrak{a}) \subset \mathbb{P}^n_k$ be a projective variety and $A = k[X]$ the coordinate ring. Then there is a dual isomorphism

$$\{\mathfrak{b} \triangleleft A \mid \mathfrak{b} \text{ radical homogenous and } A_+ \not\subseteq \mathfrak{b}\} \underset{V_+}{\overset{I_+}{\rightleftarrows}} \{Z \subset X(\bar{k}) \text{ closed } \mid Z \neq \emptyset\}$$

under which

- *irreducible sets correspond to prime ideals*
- *irreducible components (of $V_+(\mathfrak{b})$) correspond to minimal prime ideals (of $\mathfrak{b}$)*

Proposition 6.2.10 (Decomposition into Irreducible Components)
Let $X = V_+(\mathfrak{a})$ be a projective variety then the topological space $X(\bar{k})$ is Noetherian. Furthermore every closed subset Z has finitely many irreducible components Z_i and the decomposition

$$Z = Z_1 \cup \ldots \cup Z_n$$

is the unique incomparable decomposition into irreducible closed subsets.

If $Z = V_+(\mathfrak{b})$ then the irreducible components correspond to precisely the minimal prime ideals over $\mathfrak{b}$.

Proof. $X(\bar{k})$ is Noetherian by using the order isomorphism in (6.2.9) and the fact $k[X]$ is Noetherian. The result then follows from (4.1.51). □

6.2.1 Affine Patches

References :

- Algebraic Curves [Ful08, Chap. 4.3]
- Algebraic Geometry [Har13, Chap. I §2]

For every $i = 0 \dots n$ the subset of $\mathbb{P}^n_k(K)$ consisting of points of the form

$$\{[x_0 : \dots : x_{i-1} : 1 : x_{i+1} : \dots x_n] \mid x_j \in K\}$$

may be naturally identified with $\mathbb{A}^n_k(K)$. The purpose of this section is to make this notion precise.

Lemma 6.2.11
There is an isomorphism of rings

$$\begin{aligned} \theta_i^\sharp : k[X_0, \dots, X_n]_{(X_i)} &\longleftrightarrow k[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n] \\ \frac{X_j}{X_i} &\longleftrightarrow x_j \end{aligned}$$

Proof. The algebra homomorphism $\theta_i^\sharp$ exists by (3.8.5) and (3.6.6), restricting to the subring $k[X_0, \dots, X_n]_{(X_i)}$. The inverse algebra homomorphism exists by (3.8.5), sending $x_j \to \frac{X_j}{X_i}$. We may verify directly that these are mutually inverse. □

Lemma 6.2.12 ((De-)Homogenisation)
Fix n and $0 \le i \le n$. For $G \in k[X_0, \dots, X_n]$ homogenous and $F \in k[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$ define

$$\begin{aligned} G^a &:= G(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \\ F^h &:= X_i^{\deg(F)} F\left(\frac{X_0}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_n}{X_i}\right) \\ &= \sum_{j=0}^{\deg F} X_i^{\deg(F)-j} F_j\left(X_0, \dots, X_{i-1}, X_{i+1}, \dots, X_n\right) \end{aligned}$$

Then

a) $(FF')^h = F^h F'^h$ *and* $(GG')^a = G^a G'^a$

b) $F^{ha} = F$ *and* $X_i^k G^{ah} = G$ *where* $k := v_{X_i}(G)$ *is the smallest power of* X_i *appearing in* G.

c) *For* $\mathfrak{b} \lhd k[X_0, \dots, X_n]$ *a homogenous ideal the set* $\mathfrak{b}^a := \{G^a \mid G \in \mathfrak{b}\}$ *is an ideal.*

For $\mathfrak{a} \lhd k[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$ *define the homogenous ideal*

$$\mathfrak{a}^h := \langle \{F^h \mid F \in \mathfrak{a}\} \rangle$$

Then we also have the identities

d) $\mathfrak{b} \subset \mathfrak{b}^{ah}$ *with equality when* $\mathfrak{b}$ *is radical and* $\mathfrak{b} \subset \mathfrak{p}$ *minimal* $\implies X_i \notin \mathfrak{p}$

e) $\mathfrak{a} = \mathfrak{a}^{ha}$

f) $\mathfrak{b}$ *prime and* $X_i \notin \mathfrak{b} \implies \mathfrak{b}^a$ *prime.*

g) $\mathfrak{a}$ *prime* $\implies \mathfrak{a}^h$ *prime*

h) $\mathfrak{a}$ *radical* $\implies \mathfrak{a}^h$ *radical*

Proof. Mostly tedious verification

a) Using the notation of (6.2.11) we see that $F^h = X_i^{\deg(F)}(\theta_i^\sharp)^{-1}(F)$ so evidentally $(FF')^h = F^h F'^h$ because $\deg(FF') = \deg(F) + \deg(F')$.

   The second relation follows immediately from (6.2.11).

b) The first identity is clear. We may write

$$G = \sum_{j=0}^{\deg(G)-v_{X_i}(G)} X_i^{\deg(G)-j} G_j(X_0,\ldots,X_{i-1},X_{i+1},\ldots,X_n)$$

where $\deg(G_j) = j$ and $v_{X_i}(G)$ is the smallest power of X_i appearing in G. So

$$\begin{aligned} G^a &= \sum_{j=0}^{\deg(G)-v_{X_i}(G)} G_j(x_0,\ldots,x_{i-1},x_{i+1},\ldots,x_n) \\ G^{ah} &= \sum_{j=0}^{\deg(G)-v_{X_i}(G)} X_i^{\deg(G)-v_{X_i}(G)-j} G_j(X_0,\ldots,X_{i-1},X_{i+1},\ldots,X_n) \end{aligned}$$

whence $G = X_i^{v_{X_i}(G)} G^{ah}$.

c) This is evident because $(-)^a$ is a ring homomorphism.

d) The first part is evident from *b*). Suppose $G \in \mathfrak{b}^{ah}$ then

$$G = \sum_{j=1}^{r} \lambda_j G_j^{ah} \implies X_i^k G = \sum_{j=1}^{r} \lambda_j X_i^{k_j} G_j$$

for $G_j \in \mathfrak{b}$. Then $X_i^k G \in \mathfrak{b} \implies G \in \mathfrak{b}$ as we assumed $X_i \notin \mathfrak{b}$.

e) Trivially $F \in \mathfrak{a} \implies F^h \in \mathfrak{a}^h \implies F^{ha} = F \in \mathfrak{a}^{ha}$. Conversely any $G \in \mathfrak{a}^h$ is of the form

$$G = \sum_j \lambda_j F_j^h \implies G^a = \sum_j \lambda_j^a F_j^{ha} = \sum_j \lambda_j^a F_j \in \mathfrak{a}^{ha}$$

for some $\lambda_i \in k[X_0,\ldots,X_n]$.

f) Suppose $FF' \in \mathfrak{b}^a \implies F^h F'^h \in \mathfrak{b}^{ah} = \mathfrak{b} \implies F^h \in \mathfrak{b}$ or $F'^h \in \mathfrak{b} \implies F \in \mathfrak{b}^a$ or $F' \in \mathfrak{b}^a$.

g) Suppose $GG' \in \mathfrak{a}^h$ then $GG' = \sum_j \lambda_j F_j^h$ for $F_j \in \mathfrak{a}$. Then $G^a G'^a = \sum_j \lambda_j^a F_j^{ha} = \sum_j \lambda_j^a F_j \in \mathfrak{a}$. Therefore say $G^a \in \mathfrak{a} \implies G^{ah} \in \mathfrak{a}^h \implies G = X_i^k G^{ah} \in \mathfrak{a}^h$.

h) Suppose $G^n \in \mathfrak{a}^h$, then $(G^a)^n \in \mathfrak{a}^{ha} = \mathfrak{a}$ whence $G^a \in \mathfrak{a}$ and $G^{ah} \in \mathfrak{a}^h \implies G \in \mathfrak{a}^h$

□

Proposition 6.2.13 (Projective Space has Affine Covering)
Consider subsets $D_+(X_i)(K) = U_i(K) \subset \mathbb{P}_k^n(K)$ of the form

$$D_+(X_i)(K) = U_i(K) := \{[x_0 : \ldots : x_{i-1} : 1 : x_i : \ldots : x_n] \mid x_i \in K\} \quad i = 0 \ldots n$$

These are open in the Zariski topology. Furthermore under the subspace topology U_i is homeomorphic to $\mathbb{A}_k^n(K)$, with an explicit homeomorphism given by

$$\begin{aligned} \theta_i : \mathbb{A}_k^n(K) &\to U_i \\ (x_0,\ldots,x_{i-1},x_{i+1},\ldots,x_n) &\to [x_0 : \ldots : 1 : \ldots : x_n] \end{aligned}$$

For $F \in k[x_0,\ldots,x_{i-1},x_{i+1},\ldots,x_n]$ and $(x) \in U_i$ we have

$$F(x) = 0 \iff F^h(\theta_i(x)) = 0$$

and similarly for $G \in k[X_0,\ldots,X_n]$ we have

$$G(\theta_i(x)) = 0 \iff G^a(x) = 0$$

Further we have

a) $\theta_i(V^{\text{aff}}(\mathfrak{a})) = V_+(\mathfrak{a}^h) \cap U_i$ *for* $\mathfrak{a} \lhd k[x_0,\ldots,x_{i-1},x_{i+1},\ldots,x_n]$

b) $\theta_i(V^{\text{aff}}(\mathfrak{b}^a)) = V_+(\mathfrak{b}) \cap U_i = V_+(\mathfrak{b}^{ah}) \cap U_i$ *for* $\mathfrak{b} \lhd k[X_0,\ldots,X_n]$ *homogenous*

c) $I^{\mathrm{aff}}(Y)^h = I_+(\theta_i(Y))$ *for* $Y \subset U_i$

Proof. This follows largely from (6.2.12). The relations show that $\theta_i(D(F)) = D_+(F^h)$ and $\theta_i^{-1}(D_+(G)) = D(G^a)$, so that θ_i is a homeomorphism as required.

a) $x \in \theta_i(V^{\mathrm{aff}}(\mathfrak{a})) \implies x \in U_i$ and $F(\theta_i^{-1}(x)) = 0 \quad \forall F \in \mathfrak{a} \implies x \in U_i$ and $F^h(x) = 0 \quad \forall F \in \mathfrak{a} \implies G(x) = 0 \quad \forall G \in \mathfrak{a}^h \implies x \in V_+(\mathfrak{a}^h) \cap U_i$. Conversely $x \in V_+(\mathfrak{a}^h) \cap U_i \implies G(x) = 0 \quad \forall G \in \mathfrak{a}^h \implies F(\theta_i^{-1}(x)) = 0 \quad \forall F \in \mathfrak{a}^{ha} = \mathfrak{a} \implies x \in \theta_i(V^{\mathrm{aff}}(\mathfrak{a}))$

b) $\theta_i(V^{\mathrm{aff}}(\mathfrak{b}^a)) = V_+(\mathfrak{b}^{ah}) \cap U_i$. It remains to show that $V_+(\mathfrak{b}) \cap U_i = V_+(\mathfrak{b}^{ah}) \cap U_i$. As (6.2.12) $\mathfrak{b} \subset \mathfrak{b}^{ah}$ then $V_+(\mathfrak{b}^{ah}) \cap U_i \subset V_+(\mathfrak{b}) \cap U_i$. Conversely if $x \in V_+(\mathfrak{b}) \cap U_i$ then $G(x) = 0 \implies x_i^k G^{ah}(x) = 0 \implies G^{ah}(x) = 0$ because $x_i \neq 0$. This shows $x \in V_+(\mathfrak{b}^{ah}) \cap U_i$

c) Suppose $G \in I^a(Y)^h$ then $G = \sum_j \lambda_j F_j^h$ for $F_j \in I^{\mathrm{aff}}(Y)$ and $\lambda_j \in k[X_0, \ldots, X_n]$. Then $F_j(x) = 0 \implies F_j^h(\theta_i(x)) = 0 \implies G(\theta_i(x)) = 0$. Therefore we conclude $G \in I_+(\theta_i(Y))$. Conversely if $G \in I_+(\theta_i(Y))$ then $G^a(x) = 0$ for all $x \in Y$ and $G^a \in I^{\mathrm{aff}}(Y) \implies G^{ah} \in I^{\mathrm{aff}}(Y)^h \implies G = X_i^k G^{ah} \in I^{\mathrm{aff}}(Y)^h$.

□

Lemma 6.2.14
Let $X = V_+(\mathfrak{b})$ *be a projective variety. Then* $X \cap U_i \neq \emptyset \iff X_i \notin \mathfrak{b} \iff \overline{X_i} \neq 0$.

Proof. Observe $X \cap U_i = \emptyset \iff X \subset V_+(X_i) \iff X_i \in I_+(X) = \mathfrak{b}$. □

Corollary 6.2.15
Let $X = V_+(\mathfrak{b}) \subset \mathbb{P}_k^n$ *be a projective variety and for each affine patch* $U_i \subset \mathbb{P}_k^n$ *consider the affine variety* $X^a := V^{\mathrm{aff}}(\mathfrak{b}^a) \subset \mathbb{A}_k^n$. *Then there is a natural homeomorphism*

$$\theta_i : X^a(K) \xrightarrow{\sim} D_+(\overline{X_i}) = X(K) \cap U_i(K)$$

for all normal algebraic extensions K/k.

Proposition 6.2.16
Identify $\mathbb{A}_k^n(\bar{k})$ *with* $U_i \subset \mathbb{P}_k^n(\bar{k})$. *Let* $Y \subset U_i$ *be a subset. Then we have the following expression for topological closure*

$$\begin{aligned} \overline{Y} &= V_+(I^{\mathrm{aff}}(Y)^h) \\ \overline{Y} \cap U_i &= \mathrm{cl}_{U_i}(Y) \end{aligned}$$

We call $\overline{Y}$ *the* ***projective closure*** *of* Y.

Proof. By (6.2.13).c) $I_+(Y) = I^{\mathrm{aff}}(Y)^h \implies \overline{Y} \overset{(6.2.5)}{=} V_+I_+(Y) = V_+(I^{\mathrm{aff}}(Y)^h)$.

Then $\mathrm{cl}_{U_i}(Y) = \overline{Y} \cap U_i$ by (4.1.20) (or more directly $\overset{(6.1.4)}{=} V_+(I_+(Y)) \overset{(6.2.13).a)}{=} V_+(I^{\mathrm{aff}}(Y)^h) \cap U_i = \overline{Y} \cap U_i$). □

Proposition 6.2.17
Identify $\mathbb{A}_k^n(\bar{k})$ *with* $U_i \subset \mathbb{P}_k^n(\bar{k})$. *There is an order isomorphism*

$$\begin{array}{ccc} \{Y \subset U_i \mid Y \text{ closed non-empty}\} & \longleftrightarrow & \{Z \subset \mathbb{P}_k^n(\bar{k}) \mid Z \text{ closed and every irreducible component meets } U_i\} \\ Y & \to & \overline{Y} \\ Z \cap U_i & \leftarrow & Z \end{array}$$

which restricts to irreducible subsets. In terms of ideals

$$\begin{array}{ccc} \{\mathfrak{a} \lhd k[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n] \text{ proper, radical}\} & \longleftrightarrow & \{\mathfrak{b} \lhd k[X_0, \ldots, X_n] \mid \mathfrak{b} \text{ is essential, radical and every minimal prime does not contain } X_i\} \\ \mathfrak{a} & \to & \mathfrak{a}^h \\ \mathfrak{b}^a & \leftarrow & \mathfrak{b} \end{array}$$

which restricts to prime ideals.

Proof. The first correspondence follows from (4.1.54). Further for $\mathfrak{a}$ radical

$$I_+(\overline{Y}) = I_+(V_+(\mathfrak{a}^h)) = \sqrt{\mathfrak{a}^h} = \mathfrak{a}^h = I(Y)^h$$

and for $\mathfrak{p}$ prime and $X_i \notin \mathfrak{p}$ then $\mathfrak{p}^a$ prime and

$$I^{\mathrm{aff}}(V_+(\mathfrak{p}) \cap U_i) = I^{\mathrm{aff}}(V^{\mathrm{aff}}(\mathfrak{p}^a)) = \mathfrak{p}^a$$

In the general case $\mathfrak{b} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$ and $X_i \notin \mathfrak{p}_j$ for all j, then

$$I^{\text{aff}}(V_+(\mathfrak{b}) \cap U_i) = I^{\text{aff}}((V_+(\mathfrak{p}_1) \cap U_i) \cup \ldots \cup (V_+(\mathfrak{p}_n) \cap U_i)) = \bigcap_{i=1}^{n} I^{\text{aff}}(V_+(\mathfrak{p}_i) \cap U_i) = \bigcap_{i=1}^{n} \mathfrak{p}_i^a = \mathfrak{b}^a$$

which demonstrates the correspondence of ideals commutes with the first correspondence □

6.2.2 Galois Orbits

Proposition 6.2.18
Let $X = V_+(\mathfrak{a}) \subset \mathbb{P}_k^n$ be a projective variety and K/k a normal algebraic extension (e.g. $\bar{k}$). Then there is a well-defined group action

$$\begin{aligned} \text{Aut}\,(K/k) \times X(K) &\to X(K) \\ (\sigma, [x_0 : \ldots : x_n]) &\to [\sigma(x_0) : \ldots : \sigma(x_n)] \end{aligned}$$

which commutes with the affine patches

$$\sigma(\theta_i(x)) = \theta_i(\sigma(x)) \quad \forall x \in U_i(K) \cap X(K)$$

Write $X_0(K)$ for the set of equivalence classes under this action. The projection map

$$\pi : X(K) \to X_0(K)$$

is the Kolmogorov Quotient (4.1.29).

Proof. First consider the case $X = \mathbb{P}_k^n$. If $[x_0 : \ldots : x_n] \sim [x_0' : \ldots : x_n']$ then $x_i = \lambda_i x_i'$ for $\lambda_i \in K^\star$. Then $\sigma(x_i) = \sigma(\lambda_i)\sigma(x_i')$ so $[\sigma(x_0) : \ldots : \sigma(x_{n+1})] \sim [\sigma(x_0') : \ldots : \sigma(x_n')]$ and the action is well-defined. For $x \in X(K)$ write $\sigma(x)$. Then $\tau(\sigma(x)) = (\tau \circ \sigma)(x)$ so it is a group action.

For the general case if $F(x) = 0$ for $F \in k[X_0, \ldots, X_n]$ then $F(\sigma(x)) = 0$. Therefore $x \in V(\mathfrak{a})(K) \implies \sigma(x) \in V(\mathfrak{a})(K)$ and the action is well-defined on $X(K)$.

We need to show that two points $x, y \in X(K)$ are conjugate by $\text{Aut}(K/k)$ iff they are topologically indistinguishable. Suppose $x = \sigma(y)$ and $x \in V(\mathfrak{b})$. Then evidentally $y \in V(\mathfrak{b})$. Conversely if they are topologically indistinguishable then we may suppose $x, y \in U_i$. Then $\theta_i(x), \theta_i(y)$ are also indistinguishable, so by (6.1.11) they are Galois conjugate, and so $\theta_i(x) = \theta_i(\sigma(y))$. As θ_i is bijective we deduce $x = \sigma(y)$ as required. □

Proposition 6.2.19
Let $X = V_+(\mathfrak{a}) \subset \mathbb{P}_k^n$ be a projective variety and $L/K/k$ a tower of normal extensions. Then there is an injective map

$$\begin{array}{ccc} X(K) & \xhookrightarrow{i_{KL}} & X(L) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ X_0(K) & \xhookrightarrow{i_0} & X_0(L) \end{array}$$

Proof. In order for i_0 to be well-defined, we require that $\pi(x) = \pi(y) \implies \pi(i_{KL}(x)) = \pi(i_{KL}(y))$. Recall $\pi(x) = \pi(y) \implies x = \sigma(y)$ for some $\sigma \in \text{Aut}(K/k)$. Then $i_{KL} \circ \sigma \in \text{Mor}_k(K, L)$ and by (3.18.80) there exists $\widehat{\sigma} \in \text{Aut}(L/k)$ such that $\widehat{\sigma}|_K := \widehat{\sigma} \circ i_{KL} = i_{KL} \circ \sigma$. Therefore $\widehat{\sigma}(i_{KL}(x)) = i_{KL}(y) \implies \pi(i_{KL}(x)) = \pi(i_{KL}(y))$.

To show i_0 is injective we need to show the converse, which follows from (3.18.82). □

6.2.3 Structure Sheaf

Definition 6.2.20 (Structure Sheaf)
Let $X = V_+(\mathfrak{a}) \subset \mathbb{P}_k^n$ be a projective variety and $U \subset X(\bar{k})$ an open subset. We say a function

$$f : U \to \bar{k}$$

*is **regular** if for all $(x) \in U$ there is a neighbourhood V of (x) such that*

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

*for $g, h \in k[X]$ homogenous elements with $\delta(g) = \delta(h)$. We therefore define the **structure sheaf** as follows*

$$\mathcal{O}_X(U) := \{ f : U \to \bar{k} \mid f \text{ regular} \}$$

The pair $(X, \mathcal{O}_X)$ is a locally ringed space.

Proposition 6.2.21 (Structure Sheaf of Regular Functions)
Let $X = V_+(\mathfrak{a}) \subset \mathbb{P}^n_k$ be a projective variety, $U \subset X(\bar{k})$ open and $f : U \to \bar{k}$ a function. Consider the affine patches

$$\theta_i : X^a(\bar{k}) \xrightarrow{\sim} D_+(\overline{X_i}) = X(\bar{k}) \cap U_i \quad i = 0 \dots n$$

where $X^a = V^{\mathrm{aff}}(\mathfrak{a}^a)$ as in (6.2.15). Then the following are equivalent

a) *f is regular in the sense of (6.2.20)*

b) *$f \circ \theta_i : \theta_i^{-1}(U) \to \bar{k}$ is regular in the sense of (6.1.38) whenever $U \cap U_i \neq \emptyset$*

In other words for each $i = 1 \dots n$ there is an isomorphism of locally ringed spaces

$$(\theta_i, \theta_i^\sharp) : (X^a(\bar{k}), \mathcal{O}_{X^a}) \quad \xrightarrow{\sim} \quad (D_+(\overline{X_i}), \mathcal{O}_X|_{D_+(\overline{X_i})})$$

where $\theta_i^\sharp(f) := f \circ \theta_i$.

Proof. *a)* $\implies$ *b)* Suppose $\hat{x} \in \theta_i^{-1}(U_i)$ and $x := \theta(\hat{x})$. There exists an open nbhd V of x such that $f(y) = \frac{g(y)}{h(y)}$ for all $y \in V$. By definition $g = G + \mathfrak{a}$ and $h = H + \mathfrak{a}$ for $G, H \in k[X_0, \dots, X_n]$ homogenous polynomials of the same degree, for which H doesn't vanish on V. Then $\widehat{V} := \theta_i^{-1}(V)$ is a open nbhd of $\hat{x}$. For all $\hat{y} \in \widehat{V}$ we have

$$(f \circ \theta_i)(\hat{y}) = f(\theta_i(\hat{y})) = \frac{G(\hat{y})}{H(\hat{y})} = \frac{G^a(y)}{H^a(y)}$$

As this holds for every $\hat{x} \in \theta_i^{-1}(U)$ we see $f \circ \theta_i$ is regular by definition.

b) $\implies$ *a)* Given $x \in U$ then as U_i covers X there exists some i such that $x \in U \cap U_i$. For any such i we have by definition an open nbhd $\widehat{V}$ of $\theta_i^{-1}(x)$ and $G, H \in k[x_0, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$ for which

$$(f \circ \theta_i)(\hat{y}) = \frac{G(\hat{y})}{H(\hat{y})} \quad \forall \hat{y} \in \widehat{V}$$

As θ_i is a homeomorphism, $V := \theta_i(\widehat{V_i})$ is an open nbhd of x. By (6.2.13) we have for $y := \theta_i(\hat{y})$

$$f(y) = \frac{G^h(y)}{H^h(y)}$$

which holds for all $y \in V$. As x was arbitrary f is by definition regular.

As θ is a homeomorphism then θ_i^{-1} is continuous and $\left(\theta^\sharp_{i,W}\right)^{-1}$ is well-defined for every $W \subset \widehat{U_i}$. This shows that $(\theta, \theta_i^\sharp)$ is an isomorphism of ringed spaces. Suppose $\sigma \in \mathcal{O}_{\widehat{U_i}}(W)$, $\hat{x} \in W$ and $\sigma_{\hat{x}} \in \mathfrak{m}_{\widehat{U}_i, \hat{x}}$. Then by definition $\sigma(\hat{x}) = 0$, and $\theta_i^\sharp(\sigma)(x) = 0 \implies \theta_i^\sharp(\sigma)_x \in \mathfrak{m}_{X,x} \implies \theta^\sharp_{i,\hat{x}}(\sigma_{\hat{x}}) \in \mathfrak{m}_{X,x}$. Therefore $(\theta, \theta_i^\sharp)$ is an isomorphism of locally ringed spaces. □

We may generalise the dehomogenisation

Proposition 6.2.22 (Structure Sheaf on Basic Affines)
Let $X = V_+(\mathfrak{p})$ be an irreducible projective variety and suppose $X \cap U_i \neq \emptyset$. Then there is an isomorphism of k-algebras

$$\begin{array}{ccc} \mathcal{O}_X(D_+(\overline{X_i})) & \xrightarrow[\sim]{(6.2.21)} & \mathcal{O}_{X \cap U_i}(X \cap U_i) \\ \uparrow & & \sim \uparrow (6.1.42) \\ k[X]_{(\overline{X_i})} & \xrightarrow{\sim} & k[X \cap U_i] \\ \frac{\overline{X_0}}{\overline{X_i}} & \longleftrightarrow & \overline{x_i} \end{array}$$

and the dashed arrow is defined in the obvious way (and is therefore an isomorphism).

Proof. By (6.2.14) $X_i \notin \mathfrak{p}$. We first demonstrate the bottom map is well-defined and an isomorphism. Consider the following commutative diagram

$$\begin{array}{ccccc} & & k[X_0, \dots, X_n]_{(X_i)} & \xrightarrow[\sim]{\theta_i^\sharp} & k[U_i] \\ & \swarrow & \downarrow \pi_1 & & \downarrow \pi_2 \\ k[X_0, \dots, X_n]_{(X_i)}/\mathfrak{p}_{(X_i)} & \xrightarrow[(3.11.16)]{\sim} & k[X]_{(\overline{X_i})} & \dashrightarrow^{\sim} & k[X \cap U_i] \end{array}$$

where the isomorphism $\theta_i^\sharp$ is defined in (6.2.11).

It follows from (3.4.55) that π_1 is uniquely defined and has kernel $\mathfrak{p}_{(X_i)}$ which equals $\mathfrak{p}_{X_i} \cap k[X_0, \ldots, X_n]_{(X_i)}$ by (3.11.14). Therefore we may regard π_1 as a quotient map.

We also claim that the diagonal map $\pi_2 \circ \theta_i^\sharp$ has kernel $\mathfrak{p}_{(X_i)}$. It is enough by (3.6.6).b) and the preceding comment to show that the composite map $\pi_2 \circ (-)^a : k[X_0, \ldots, X_n] \to k[X \cap U_i]$ has kernel $\mathfrak{p}$. However this follows from (6.2.12) for $F \in \ker(\pi_2 \circ (-)^a) \implies F^a \in \mathfrak{p}^a \implies F^a = G^a \implies F^{ah} = G^{ah} \in \mathfrak{p}^{ah} = \mathfrak{p} \implies F^{ah} \in \mathfrak{p} \implies X_i^k F \in \mathfrak{p} \implies F \in \mathfrak{p}$.

The required map exists by (3.4.55), as π_1 is a quotient map. Further it is injective, surjective and therefore an isomorphism

The map $k[X]_{(\overline{X_i})} \to \mathcal{O}_X(D_+(\overline{X_i}))$ is defined in the obvious way. It is clear the diagram commutes and so this map is an isomorphism. □

6.2.4 Local Ring

Definition 6.2.23 (Local Ring)
*Let $X = V(\mathfrak{a}) \subset \mathbb{P}_k^n$ be a projective variety and $W \subset X(\bar{k})$ an irreducible subset. Then we define the **local ring** at W to be (see (4.2.5) and (4.3.1))*

$$\mathcal{O}_{X,W} := \varinjlim_{U \cap W \neq \emptyset} \mathcal{O}_X(U)$$

It is a local ring with unique maximal ideal

$$\mathfrak{m}_{X,W} := \{(V, \sigma) \mid \sigma(x) = 0 \, \forall x \in W \cap V\}$$

*Define the **residue field***

$$k(W) := \mathcal{O}_{X,W}/\mathfrak{m}_{X,W}$$

In the case $W = \{x\}$ we write $\mathcal{O}_{X,x}$, $\mathfrak{m}_{X,x}$ and $k(\mathfrak{m}_{X,x})$.

The local ring is preserved if we reduce to an affine patch, or indeed any open subset.

Proposition 6.2.24
Let $X = V_+(\mathfrak{b})$ be a projective variety and $W \subset X(\bar{k})$ be an irreducible subset. Suppose $U \subset X$ is an open subset for which $U \cap W \neq \emptyset$. Then there is a local isomorphism of k-algebras

$$\mathcal{O}_{U,U\cap W} \xrightarrow{\sim} \mathcal{O}_{X,W}$$

and therefore an isomorphism

$$k(U \cap W)/k \xrightarrow{\sim} k(W)/k$$

In particular

$$\operatorname{trdeg}_k(k(U \cap W)) = \operatorname{trdeg}_k(k(W))$$

Proof. The isomorphism of sheaves exists by (4.2.15), and it is evidentally a local homomorphism. □

Proposition 6.2.25
Let $X = V_+(\mathfrak{b}) \subset \mathbb{P}_k^n$ be a projective variety and $W = V_+(\mathfrak{p})$ an irreducible subset. Then there is an isomorphism

$$\begin{array}{ccc} k[X]_{(\mathfrak{p}/\mathfrak{b})} & \xrightarrow{\sim} & \mathcal{O}_{X,W} \\ \dfrac{\overline{F}}{\overline{G}} & \to & \left[\left(D(\overline{G}), \dfrac{F(-)}{G(-)}\right)\right] \end{array}$$

More precisely for any affine patch U_i such that $U_i \cap W \neq \emptyset$ there is a commutative diagram

$$\begin{array}{ccccc} k[U_i]_{\mathfrak{p}^a} & \xrightarrow[(3.6.34)]{\sim} & k[U_i \cap X]_{\mathfrak{p}^a/\mathfrak{b}^a} & \xrightarrow[(6.1.44)]{\sim} & \mathcal{O}_{U_i\cap X, U_i \cap W} \\ \sim\downarrow & & & & \wr\downarrow{\scriptstyle (6.2.24)} \\ k[X_0, \ldots, X_n]_{(\mathfrak{p})} & \xrightarrow[(3.11.17)]{\sim} & k[X]_{(\mathfrak{p}/\mathfrak{b})} & \dashrightarrow^{\sim} & \mathcal{O}_{X,W} \end{array}$$

Proof. We construct the left vertical map, and then the dashed arrow is uniquely defined.

As $U_i \cap W \neq \emptyset$ then $W \not\subset V(X_i) \implies X_i \notin \mathfrak{p}$. So by (6.2.12).d) $\mathfrak{p}^{ah} = \mathfrak{p}$. To complete the diagram we consider the mutually inverse maps

$$\begin{aligned} k[U_i] = k[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]_{\mathfrak{p}^a} &\to k[X_0, \dots, X_n]_{(\mathfrak{p})} \\ \frac{F}{F'} &\to \frac{F\left(\frac{X_0}{X_i}, \dots, \frac{X_n}{X_i}\right)}{F'\left(\frac{X_0}{X_i}, \dots, \frac{X_n}{X_i}\right)} \\ \frac{G^a}{G'^a} &\leftarrow \frac{G}{G'} \end{aligned}$$

Note $F'^h \in \mathfrak{p} \implies F' = F'^{ha} \in \mathfrak{p}^a$. Therefore $F' \notin \mathfrak{p}^a \implies F'^h = X_i^{\deg(F)} F'\left(\frac{X_0}{X_1}, \dots, \frac{X_n}{X_i}\right) \notin \mathfrak{p} \implies F'\left(\frac{X_0}{X_1}, \dots, \frac{X_n}{X_i}\right) \notin \mathfrak{p}$. Similarly $G'^a \in \mathfrak{p}^a \implies G'^{ah} \in \mathfrak{p}^{ah} = \mathfrak{p} \implies G' = X_i^k G'^{ah} \in \mathfrak{p}$, so $G' \notin \mathfrak{p} \implies G'^a \notin \mathfrak{p}^a$. Finally

$$\frac{G^a\left(\frac{X_0}{X_i}, \dots, \frac{X_n}{X_i}\right)}{G^a\left(\frac{X_0}{X_i} \dots, \frac{X_n}{X_i}\right)} = \frac{X_i^{-\deg(G)} G}{X_i^{-\deg(G')} G'} = \frac{G}{G'}$$

so the maps are mutually inverse. □

Definition 6.2.26
Let X be an irreducible projective variety. Then define the field of rational functions to be

$$k(X) := k[X]_{(0)} = \mathrm{Frac}(k[X])_0$$

6.2.5 Dimension

Definition 6.2.27
Let $X = V(\mathfrak{a})$ be a projective variety. Then we define the dimension $\dim X$ to be the Krull Dimension of $X(\bar{k})$ as a topological space (4.1.56).

Proposition 6.2.28
Let $X = V(\mathfrak{p})$ be an irreducible projective variety. Then $X(\bar{k})$ is biequidimensional and

$$\dim X = \mathrm{trdeg}(k(X)/k) = \dim X \cap U_i$$

where U_i is any affine patch such that $X \cap U_i \neq \emptyset$.

Proof. Recall by (6.2.17) $X \cap U_i$ is an irreducible affine variety for every affine patch U_i. By (6.2.24) and (6.1.27)

$$\mathrm{trdeg}(k(X)/k) = \mathrm{trdeg}(k(X \cap U_i)/k) = \dim X \cap U_i$$

In particular $\dim X \cap U_i$ is independent of the patch U_i chosen. By the correspondence in (6.2.17) and the corresponding result for affine varieties (6.1.26) we deduce that X is biequidimensional and $\dim X = \dim X \cap U_i = \mathrm{trdeg}(k(X)/k)$. □

Corollary 6.2.29
$\dim \mathbb{P}^n_k = n$

Corollary 6.2.30
Let X be a projective variety. Then it is quasi-biequidimensional. Moreover every closed subset $W \subset X$ satisfies the codimension formula

$$\dim X = \dim W + \mathrm{codim}(W, X)$$

Proof. The codimension formula is from (4.1.61). □

Proposition 6.2.31
Let $X = V(\mathfrak{p})$ be an irreducible projective variety then $\dim k[X] = \dim X + 1$.

Proof. We have $\overline{X_i} \neq 0$ for some i as X is non-empty. Therefore

$$\dim k[X] \overset{(3.29.24)}{=} \dim k[X]_{\overline{X_i}} \overset{(3.12.8)}{=} \dim k[X]_{(\overline{X_i})}[T, T^{-1}] \overset{(3.9.3)}{=} \dim k[X]_{(\overline{X_i})}[T]_T \overset{(3.29.24)}{=} \dim k[X]_{(\overline{X_i})}[T] \overset{(3.29.22)}{=} \dim k[X]_{(\overline{X_i})} + 1$$

By (6.2.22) $\dim k[X]_{(\overline{X_i})} = \dim k[X \cap U_i] = \dim X \cap U_i$.

Finally this equals $\dim X$ either by (6.2.28) or (4.1.62). □

6.2.6 Tangent Space

Definition 6.2.32
*Let $X = V_+(\mathfrak{b})$ be a projective variety and $(x) \in X(\bar{k})$. Define the **tangent space***

$$T_x X := \mathrm{Der}\left(\mathcal{O}_{X,x}, k(\mathfrak{m}_{X,x})\right)$$

*and the **cotangent space***

$$T_x^\star X := \mathrm{Hom}\left(\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2, k(\mathfrak{m}_{X,x})\right)$$

Definition 6.2.33 (Regular / Non-Singular)
Let $X = V_+(\mathfrak{b})$ be a projective variety and $(x) \in X(\bar{k})$.

*We say (x) is **regular** (resp. **non-singular**) if both*

a) *(x) lies on a unique irreducible component X_α, and*

b) *$\dim \mathcal{O}_{X,x} = \dim T_x^\star X$ (resp. $\dim T_x X$)*

*We say X is **regular** (resp. **non-singular**) if all the $\bar{k}$-rational points are regular (resp. non-singular).*

Proposition 6.2.34
Let $X = V_+(\mathfrak{b})$ be a projective variety and $(x) \in X(\bar{k})$ such that $k(\mathfrak{m}_{X,x})/k$ is separable *(e.g. k perfect). Then there is a canonical isomorphism*

$$T_x X \xrightarrow{\sim} T_x^\star X$$

*In particular when (x) lies on a single irreducible component (i.e. $\mathcal{O}_{X,x}$ is an integral domain) we have **regular** $\iff$ **non-singular**.*

6.2.7 Valuation Rings

Lemma 6.2.35
Let R be a valuation ring for K. Suppose $x_0, \ldots, x_n \in K^\star$, then there exists $\lambda \in K^\star$ such that $\lambda x_0, \ldots, \lambda x_n \in R$ and $\lambda x_i \in R^\star$ for at least one $i = 1 \ldots n$.

Proposition 6.2.36
Let $X = V(\mathfrak{p}) \subset \mathbb{P}_k^n$ be an irreducible projective variety. Let $k \subset R \subset k(X)$ be a valuation ring. Then there exists a point $(x) \in X(\bar{k})$ such that $\mathcal{O}_{X,x} \cong k[X]_{(\mathfrak{p}_x)} \subset R$.

Proof. By (...) we may assume that $k(\mathfrak{m}_R)/k$ is algebraic and therefore we have k-algebra homomorphisms

$$\pi : R \to k(\mathfrak{m}_R) \hookrightarrow \bar{k}$$

We may assume wlog that $X \cap U_0 \neq \emptyset$ and therefore $X_0 \notin \mathfrak{p}$ where $X_0, \ldots, X_n$ are the homogenous coordinates . So we may consider $t_i := \frac{\overline{X}_i}{\overline{X}_0} \in k(X) := \mathrm{Frac}(k[X])_0$ for $i = 0 \ldots n$. By (6.2.35) there exists $\lambda \in k(X)^\star$ such that $\lambda t_0, \ldots, \lambda t_n \in R$ and $\lambda t_k \in R^\star$.

Given $F \in \mathfrak{p}$ homogenous of degree d then considering $k(X) \subset \mathrm{Frac}(k[X])$ we have

$$\begin{aligned} F(\lambda t_0, \ldots, \lambda t_n) &= \lambda^d F(t_0, \ldots, t_n) \\ &= \lambda^d \overline{X}_0^{-d} F(\overline{X}_0, \ldots, \overline{X_0}) \\ &= \lambda^d \overline{X}_0^{-d} \overline{F} \\ &= 0 \end{aligned}$$

Therefore we may deduce

$$\begin{aligned} F(\pi(\lambda t_0), \ldots, \pi(\lambda t_n)) &= \pi\left(F\left(\lambda t_0, \ldots, \lambda t_n\right)\right) \\ &= \pi(0) \\ &= 0 \end{aligned}$$

As F was arbitrary and $\pi(\lambda t_k) \neq 0$, $(x) := [\pi(\lambda t_0) : \ldots : \pi(\lambda t_n)]$ lies in $X(\bar{k})$.

Consider $g, h \in k[X]$ homogenous of the same degree with $h \notin \mathfrak{p}_x$. We claim that $g/h \in R$. For there exists $G, H \in k[X_0, \ldots, X_n]$ homogenous such that

$$\begin{aligned} g &= G(\overline{X_0}, \ldots, \overline{X_n}) \\ &= \lambda^{-d} G(\lambda t_0, \ldots, \lambda t_n) \\ h &= H(\overline{X_0}, \ldots, \overline{X_n}) \\ &= \lambda^{-d} H(\lambda t_0, \ldots, \lambda t_n) \\ \frac{g}{h} &= \frac{G(\lambda t_0, \ldots, \lambda t_n)}{H(\lambda t_0, \ldots, \lambda t_n)} \end{aligned}$$

Evidentally $G(\lambda t_0, \dots, \lambda t_n) \in R$ since R is a k-algebra. Further by assumption

$$\begin{aligned} 0 &\neq h(\pi(\lambda t_0), \dots \pi(\lambda t_n)) \\ &= H(\pi(\lambda t_0), \dots, \pi(\lambda t_n)) \\ &= \pi(H(\lambda t_0, \dots, \lambda t_n)) \end{aligned}$$

which means $H(\lambda t_0, \dots, \lambda t_n) \notin \mathfrak{m}_R \implies H(\lambda t_0, \dots, \lambda t_n) \in R^\star$. Using the expression above for $\frac{g}{h}$ shows it lies in R as required. □

6.2.8 Projective Curves

Definition 6.2.37
*A **projective curve** is a projective variety of pure dimension one.*

Proposition 6.2.38 (Characterisation Regular Point on a curve)
Let $X = V_+(\mathfrak{b})$ be a projective curve and $(x) \in X(\bar{k})$. Then the following are equivalent

a) *(x) is regular*

b) *$\mathcal{O}_{X,x}$ is a discrete valuation ring*

c) *$\mathcal{O}_{X,x}$ is an integrally closed domain*

when k is perfect this is equivalent to (x) being non-singular.

Proof. Follows exactly the same lines as (6.1.71). □

Proposition 6.2.39
Let $X = V_+(\mathfrak{p})$ be an irreducible, regular projective curve. Then there is a bijection

$$X(\bar{k})/\operatorname{Aut}(\bar{k}/k) \longleftrightarrow \left\{ k \subset R \subsetneq k(X) \mid R \text{ valuation ring} \right\}$$

Further the corresponding valuation rings are all discrete valuation rings

Proof. Using (6.2.36) this follows exactly the same lines as the affine case (6.1.72). □

6.3 Affine Schemes

We observed that for X an affine variety 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.

6.3.1 Maximal Spectrum

We observed that for X an affine variety that $k[X]$ is a finitely generated reduced k-algebra. It's possible to reverse the construction in some sense

Definition 6.3.1 (Maximal Spectrum)
Let A be a ring. Define

$$\operatorname{Specm}(A) := \{[\mathfrak{m}] \mid \mathfrak{m} \lhd A\}$$

For $S \subseteq A$ define

$$V(S) := \{[\mathfrak{m}] \mid S \subseteq \mathfrak{m}\}$$

and for $Y \subseteq \operatorname{Specm}(A)$ define

$$I(Y) = \bigcap_{[\mathfrak{m}] \in Y} \mathfrak{m}$$

Proposition 6.3.2 (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 (6.1.4). The relation $IV(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ results from the Strong Nullstellensatz, or from the definition of a Jacobson ring. □

Proposition 6.3.3 (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 6.3.4
Let $X = V(\mathfrak{a})$ *be an affine variety with coordinate ring* $k[X]$*. If* $k = \bar{k}$ *then there is a commutative diagram*

$$\begin{array}{ccc} \text{Specm}(k[X]) & \underset{I}{\overset{V}{\leftrightarrows}} & k[X] \\ \updownarrow \simeq & & \downarrow = \\ X & \underset{I}{\overset{V}{\leftrightarrows}} & k[X] \end{array}$$

where the left arrow is the bijection described in (3.29.20) and is in fact a homeomorphism. For general k *we still have a commutative diagram*

$$\begin{array}{ccc} \text{Specm}(k[X]) & \underset{I}{\overset{V}{\leftrightarrows}} & k[X] \\ \updownarrow \simeq & & \downarrow = \\ X(\bar{k})/G_k & \underset{I_{\bar{k}}}{\overset{V_{\bar{k}}}{\leftrightarrows}} & k[X] \end{array}$$

6.3.2 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 6.3.5 (Prime Spectrum)
Let A be a ring, then define the prime spectrum of A to be the set

$$\operatorname{Spec}(A) = \{[\mathfrak{p}] \mid \mathfrak{p} \lhd A\}$$

For $\mathfrak{a} \lhd A$ 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 6.3.6 (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 (6.3.2), except for the relation $IV(\mathfrak{a}) = \mathfrak{a}$ which is precisely (3.4.46).

Last bit TODO □

The Zariski topology differs to the maximal case because not all points are closed. More precisely

Proposition 6.3.7 (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

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}) = \{\mathfrak{q} \mid \mathfrak{q} \supseteq \mathfrak{p}\} \tag{6.3}$$

Proof. Equation (6.3) follows from the definitions and the fact $V(\mathfrak{p}) = VI(\{\mathfrak{p}\}) = \overline{\{\mathfrak{p}\}}$ from the final result in (6.3.6).

Then by **??** $\{\mathfrak{p}\}$ is closed if and only $\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}}$ if and only if $\mathfrak{p}$ is maximal (see (3.4.59), (3.4.36)). □

Similarly to (6.1.18) we may characterize irreducible subsets of $\mathrm{Spec}(A)$ as the zero-locus of prime ideals

Proposition 6.3.8 (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 (6.1.18). □

Corollary 6.3.9
$\mathrm{Spec}(A)$ *(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 (6.3.8) □

We may summarize in a correspondence much as in the classical case

Corollary 6.3.10 (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*

$$\{Y \subset X \text{ closed }\} \underset{I}{\overset{V}{\rightleftarrows}} \{\mathfrak{a} \lhd A \text{ radical }\}$$

under which

- *Prime ideals correspond to irreducible closed subsets*
- *Minimal prime ideals correspond to irreducible components*
- *Maximal ideals correspond to closed points*

Proof. The correspondence follows directly from (6.3.6). The first statement follows from (6.3.8) □

There is another way of viewing the non-closed points :

Proposition 6.3.11 (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 (6.3.8). 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 6.3.12 (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 6.3.13 (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 (4.1.6) 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 (6.3.10)) $D(g) \subseteq D(f) \iff V((f)) \subseteq V((g)) \iff \sqrt{(g)} \subseteq \sqrt{(f)} \iff g \in \sqrt{(f)} \iff f \mid g^N$.

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 6.3.14 (Functoriality)
Let $\phi : A \to B$ be homomorphism then there is a natural map

$$\operatorname{Spec}(\phi) : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$$

$$\mathfrak{p} \to \phi^{-1}(\mathfrak{p})$$

and satisfies

$$\operatorname{Spec}(\phi)^{-1}(D(f)) = D(\phi(f))$$

It is continuous with respect to the Zariski topology. If any one of the following conditions holds

- *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 (3.4.53). 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 (3.4.53).

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 (3.22.11) $\bar{A}$ is a field and $\phi^{-1}(\mathfrak{m})$ is maximal by (3.4.58) 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 (3.22.11). □

Proposition 6.3.15
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. □

6.3.3 Abstract Structure Sheaf (Integral Case)

Note in the case of an affine variety X with coordinate ring $k[X]$ we associated to it a natural structure sheaf $\mathcal{O}_X$ (6.1.38) 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 6.3.16
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 (6.3.13) 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 (3.4.46) 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. □

6.3.4 Abstract Structure Sheaf (General Case)

For this section we generalize the structure sheaf construction to a general ring A, and let $X = \text{Spec}(A)$. We will also consider the case A a Jacobson ring and $X = \text{Specm}(A)$. The main result is the following

Proposition 6.3.17 (Structure Sheaf)
Let A be a ring and $X = \text{Spec}(A)$. Recall from (6.3.13) 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

$$\begin{aligned} \text{Mor}(\mathcal{O}_X, \mathcal{G}) &\to \text{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}}) \\ \phi &\longrightarrow \phi|_{\mathcal{B}} \circ \eta_A \end{aligned}$$

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

$$\begin{array}{ccccccc} \mathcal{O}_{\operatorname{Spec}(A_f)}(\operatorname{Spec}(A_f)) & \xleftrightarrow{\eta_{A_f,1}} & (A_f)_1 & \xleftrightarrow{\sim} & A_f & \xleftrightarrow{\eta_{A,f}} & \mathcal{O}_X(D(f)) \\ \downarrow & & \downarrow{\scriptstyle i_{1(g/1)}} & & \downarrow{\scriptstyle i_{fg}} & & \downarrow \\ \mathcal{O}_{\operatorname{Spec}(A_f)}(D(g/1)) & \xleftrightarrow{\eta_{A_f,g/1}} & (A_f)_{g/1} & \xleftrightarrow{\sim} & A_g & \xleftrightarrow{\eta_{A,g}} & \mathcal{O}_X(D(g)) \\ \downarrow & & \downarrow{\scriptstyle i_{(g/1)(h/1)}} & & \downarrow{\scriptstyle i_{gh}} & & \downarrow \\ \mathcal{O}_{\operatorname{Spec}(A_f)}(D(h/1)) & \xleftrightarrow{\eta_{A_f,h/1}} & (A_f)_{h/1} & \xleftrightarrow{\sim} & A_h & \xleftrightarrow{\eta_{A,h}} & \mathcal{O}_X(D(h)) \end{array}$$

where the inner diagram is from (3.6.29), 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 $\mathcal{G}$)

$$\begin{aligned} \operatorname{Mor}(\mathcal{O}_X, \mathcal{G}) &\longrightarrow \operatorname{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}}) \\ \alpha &\to \alpha|_{\mathcal{B}} \circ \eta_A \end{aligned}$$

This shows the existence of the required isomorphism and its universal property. Furthermore the isomorphism of stalks is also the content of Propositions (4.2.11) and (3.6.33).

We claim there is an isomorphism of $\mathcal{B}$-presheaves

$$\widetilde{i_f}_\star(\mathcal{O}'_{\operatorname{Spec}(A_f)}) \longrightarrow \mathcal{O}'_X|_{D(f)} \tag{6.4}$$

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 (6.3.18)

$$1 = \sum_i g_i f_i^N$$

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

$$(f_i f_j)^M (f_j^N a_i - f_i^N a_j) = 0 \tag{6.5}$$

for sufficiently large M. By (6.3.18) 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 (6.5)

$$f_i^{N+M} a = f_i^{N+M} \sum_j g_j f_j^M a_j = a_i f_i^M \sum_j g_j f_j^{N+M} = a_i f_i^M$$

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 (6.4)) and reflect it back to get the stated isomorphism. □

We used the following Lemma

Lemma 6.3.18 (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] Nicolas Bourbaki. *Algebra: Chapters 4-7*. Springer-Verlag, 1989.

[Bou98a] N. Bourbaki. *Commutative Algebra: Chapters 1-7*. Number v. 1 in Elements de mathematique. English. Springer, 1998.

[Bou98b] Nicolas Bourbaki. *Algebra I: Chapters 1-3*. Springer, 1998.

[Car67] Henri Cartan. *Differential Calculus*. 1967.

[Die11] Jean Dieudonné. *Foundations of modern analysis*. Read Books Ltd, 2011.

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

[Ful08] William Fulton. Algebraic curves. 2008.

[Gro64] Alexander Grothendieck. éléments de géométrie algébrique : IV. étude locale des schémas et des morphismes de schémas, Première partie. *Publications Mathématiques de l'IHÉS*, 20:5–259, 1964.

[Hal17] P.R. Halmos. *Naive Set Theory*. Dover Books on Mathematics. Dover Publications, 2017.

[Har13] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2013.

[Hei17] Katharina Heinrich. Some remarks on biequidimensionality of topological spaces and noetherian schemes. *Journal of Commutative Algebra*, 9(1):49–63, 2017.

[Kap74] Irving Kaplansky. *Commutative Rings*. The University of Chicago Press, 1974.

[Kel71] John L Kelley. *General Topology*. Springer, 1971.

[Lan11] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2011.

[Lan12] Serge Lang. *Real and functional analysis*, volume 142. Springer Science & Business Media, 2012.

[Lan19] Serge Lang. *Introduction to Algebraic Geometry*. Dover Books on Mathematics. Dover Publications, 2019.

[Liu06] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2006.

[Mat70] H. Matsumura. *Commutative Algebra*. Mathematics lecture note series. Benjamin, 1970.

[Mil17] James Milne. Algebraic geometry. http://www.jmilne.org/math/xnotes/AG.pdf, 2017.

[Mum99] David Mumford. *The red book of varieties and schemes : includes the Michigan Lectures (1974) on Curves and their Jacobians*. Springer, New York, 1999.

[Nag75] M. Nagata. *Local Rings*. R.E. Krieger Publishing Company, 1975.

[Rey11] Manny Reyes. Krull dimension less or equal than transcendence degree? https://mathoverflow.net/q/79974, 2011.

[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.

[Sha00] R.Y. Sharp. *Steps in Commutative Algebra*. London Mathematical Society Student Texts. Cambridge University Press, 2000.

[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.

[Wil70] Stephen Willard. *General Topology.* Dover Publications, 1970.

[ZS76] Oscar Zariski and Pierre Samuel. *Commutative Algebra II.* Graduate Texts in Mathematics. Springer New York, 1976.