

Algebra, Geometry and Number Theory

David Rufino

October 12, 2020

Contents

1	Introduction	5
2	Foundations	7
2.1	Set Theory	7
2.1.1	Relations	7
2.1.2	Functions	8
2.1.3	Partial Orders	9
2.1.4	Lattices	9
2.1.5	Galois Connections	13
2.2	Numbers	15
2.2.1	Integers	15
2.2.2	Arithmetic	17
2.2.3	Prime Factorization	18
2.3	Category Theory	18
2.3.1	Categories	18
2.3.2	Equivalence of categories	20
2.3.3	Properties of Morphisms	21
2.3.4	Directed Limits	24
2.3.5	Adjoint Functors	24
3	Algebra	29
3.1	Introduction	29
3.2	Magmas and Monoids	29
3.3	Groups	30
3.3.1	Cyclic Groups	33
3.3.2	Group Actions	34
3.4	Rings and Modules	35
3.4.1	Commutative Rings	35
3.4.2	Modules I	37
3.4.3	Operations on Ideals	38
3.4.4	Quotient Rings	41
3.4.5	Irreducible and Reduced rings	43
3.4.6	Algebra over a Commutative Ring	43
3.4.7	Modules II	43
3.4.8	Vector Spaces	46
3.4.8.1	Vector Space Hom	49
3.4.8.2	Dual Space	50
3.5	Localization	52
3.5.1	Rings	52
3.5.2	Modules	54
3.5.3	Ideals	55
3.5.4	Change of Rings	56
3.5.5	Localization at an element	59
3.5.6	Localization at a prime ideal	60
3.6	Polynomial Rings in One Variable	60
3.7	Polynomial Rings in Many Variables	62
3.8	Finiteness	63
3.9	Unique Factorization	63
3.10	Principal Ideal Domains	66
3.11	Matrix Rings	67
3.12	Polynomial ring over a field	68
3.12.1	Separable Polynomials	70
3.13	Cayley-Hamilton Theorem	71
3.14	Finite-type Algebras	72

3.15	Integral Algebras	72
3.16	Galois Theory	73
3.16.1	Algebraic Extensions	73
3.16.2	Galois Theory Summary	77
3.16.3	Algebraic Closure	78
3.16.4	Separability	78
3.16.5	Applications of Separability	80
3.16.6	Perfect Fields	81
3.16.7	Normal Extensions	81
3.16.8	Finite Fields	83
3.16.9	Galois Theory	84
3.17	Zariski's Lemma	86
3.18	Differentials	88
4	Topology and Differential Geometry	89
4.1	Topological Spaces	89
4.1.1	Continuous Maps	90
4.1.2	Irreducible Topological Spaces	90
4.2	Sheaves	92
4.3	Spaces of k -functions	95
4.4	Differentiable Manifolds	96
4.5	Locally Ringed Spaces	100
5	Algebraic Geometry	101
5.1	Algebraic Sets over a Field	101
5.1.1	Nullstellensatz	103
5.1.2	Morphisms of Algebraic Sets	105
5.1.3	Structure Sheaf for Algebraic Sets with $k = \bar{k}$	105
5.1.4	Rational points over finite fields and the Zeta Function	106
5.1.5	Cotangent Space	107
5.1.6	Tangent Space	108
5.2	Abstract Varieties and Schemes	108
5.2.1	Maximal Spectrum	109
5.2.2	Prime Spectrum	110
5.2.3	Abstract Structure Sheaf (Integral Case)	113
5.2.4	Abstract Structure Sheaf (General Case)	113

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.

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

$$yR^Tx \iff xRy$$

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

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

Definition 2.1.4 (Equivalence Relation)

Let R be a binary relation on (X, X) . It is said to be

- **reflexive** if xRx for all $x \in X$
- **symmetric** if $xRy \implies yRx$ for all $x, y \in X$
- **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 and \mathcal{F} a family of subsets of X . It is said to be a **partition** if

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

Proposition 2.1.1 (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 2.1.6 (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 2.1.7 (Function)

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

- $\text{dom}(f) = X$
- $\Gamma(f)$ 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 2.1.2 (Equality of Functions)

Two functions $f, g : X \rightarrow Y$ are equal if and only if $f(x) = g(x)$ for all $x \in X$.

Proposition 2.1.3 (Composition of Functions)

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ 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 2.1.8 (Injective, Surjective and Bijective)

Let $f : X \rightarrow Y$ be a function then we say

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

Definition 2.1.9 (Inverse Function)

Let $f : X \rightarrow Y$ and $g : Y \rightarrow X$ 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 2.1.4

Let $f : X \rightarrow Y$ 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 2.1.10 (Idempotent Function)

A function $p : X \rightarrow X$ is **idempotent** $p \circ p = p$.

Lemma 2.1.5 (Idempotent Criterion)

Let $p : X \rightarrow X$ be a function. Then $\text{Fix}(p) \subseteq \text{Im}(p)$ and these are equal if and only if p is idempotent.

2.1.3 Partial Orders

Definition 2.1.11 (Poset)

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

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

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

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

Example 2.1.12

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

Definition 2.1.13 (Top and Bottom)

Let (X, \leq) we say \top (resp. \perp) 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 2.1.14 (Monotone/Antitone Function)

Let (X, \leq) and (Y, \leq) be posets. A function $f : X \rightarrow Y$ 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 2.1.6

Let $f : X \rightarrow Y$ 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 2.1.15 (Closure operator)

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

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

Definition 2.1.16 (Kernel operator)

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

- **co-extensive** $\kappa(x) \leq x$
- **antitone** $x \leq y \implies \kappa(x) \leq \kappa(y)$
- **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 2.1.17 (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

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

Lemma 2.1.7 (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. \square

Lemma 2.1.8

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 \perp_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. \square

Definition 2.1.18 (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 $\inf S$.

Lemma 2.1.9 (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 2.1.10

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

Lemma 2.1.11 (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 $\inf T \leq \inf S$. \square

Remark 2.1.19

Note that $\emptyset^\uparrow = X$ and therefore $\sup \emptyset = \perp$ when it exists. Similarly $\inf \emptyset = \top$ when it exists.

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

Definition 2.1.20 (Lattice)

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

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

and

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

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

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

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

and

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

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

Trivially

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

Example 2.1.21 (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 $\perp = \emptyset$.

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

Lemma 2.1.12 (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 $S^{\uparrow\downarrow} \cap S^{\uparrow\uparrow}$. By Lemma 2.1.7 $S^{\uparrow\downarrow\uparrow} = S^\uparrow$ so they are equivalent. \square

Proposition 2.1.13 (Criteria to be a Complete Lattice)

Let (X, \leq) be a poset. Then the following are equivalent

1. X is a complete lattice
2. X admits arbitrary infimums (and in particular has $\top = \inf \emptyset$)
3. X admits arbitrary supremums (and in particular has $\perp = \sup \emptyset$)

In this case we have the relationships

$$\begin{aligned} \bigvee S &= \bigwedge S^\uparrow \\ \bigwedge S &= \bigvee S^\downarrow \end{aligned}$$

Proof. 1 \implies 2,3 is clear.

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

Lemma 2.1.14

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

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

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

Definition 2.1.22 (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 2.1.23 (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 2.1.15 (Equivalent Formulations of Complete Sub-lattice)

Let (X, \leq) be a complete lattice and (Y, \leq) a sub-poset. Then the following are equivalent

1. (Y, \leq) is a Moore family
2. (Y, \leq) is a complete lattice
3. Y is the image of some closure operator $c : X \rightarrow X$

In this case the closure operator is given by

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

For $S \subseteq Y$

$$\begin{aligned} \bigwedge_Y S &= \bigwedge_X S \\ \bigvee_Y S &= c\left(\bigvee_X S\right) \end{aligned}$$

and for $S \subseteq X$ we have

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

Proof. 1 \implies 2) By Lemma 2.1.14 $S \subseteq Y \implies \bigwedge_Y S = \bigwedge_X S$. By Proposition 2.1.13 then Y is a complete lattice.

2 \implies 3) Suppose that (Y, \leq) is a complete lattice then define the function $c : X \rightarrow X$ 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 Lemma 2.1.11 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 Lemma 2.1.14 we have $c(x) \in Y$ so that $\text{Im}(c) \subseteq Y$. 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 $Y \subseteq \text{Fix}(c) \subseteq \text{Im}(c) \subseteq Y$, whence $Y = \text{Im}(c) = \text{Fix}(c)$ and c is idempotent by Lemma 2.1.5. As c is extensive, monotone and idempotent it is by definition a closure operator.

3 \implies 1) In order for $Y := \text{Im}(c)$ 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

$$\begin{aligned} S \subseteq Y &\implies c(S^\downarrow) \subseteq S^\downarrow \\ T \subseteq X &\implies c(T^\uparrow) \subseteq T^\uparrow \end{aligned}$$

Therefore c maps the singleton set $S^\downarrow \cap S^{\downarrow\uparrow} = \{\bigwedge_X S\}$ to itself. In otherwords $\bigwedge_X S \in \text{Fix}(c) = \text{Im}(c) = Y$ 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 $c(x) = \bigwedge_{\Gamma_x} \Gamma_x$ as required.

Finally by Lemma 2.1.10 $\{\bigvee_X S\}^\uparrow = S^\uparrow$ for any $S \subseteq X$. Therefore, as $c(x) = \bigwedge_X \Gamma_x$ we find

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

as required. In particular when $S \subseteq Y$ we find by Proposition 2.1.15

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

□

Remark 2.1.24

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

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

Corollary 2.1.16 (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 $c : \mathcal{P}(E) \rightarrow \mathcal{F}$ given by

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

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

Proposition 2.1.17 (Alternative expression for join)

Let (X, \leq) be a complete lattice and $c : X \rightarrow X$ a closure operator with image Y . Then for any subset $S \subset X$

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

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

Proof. By Proposition 2.1.15 the expression for $c(\bigvee_X S)$ yields

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

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

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

as required. □

2.1.5 Galois Connections**Definition 2.1.25** (Galois Connection)

Let (X, \leq_X) and (Y, \leq_Y) be posets. A pair of functions

$$X \xrightleftharpoons[f_\star]{f^\star} Y$$

is called an **antitone Galois connection** if

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

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

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

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

Remark 2.1.26 (Duality Principle)

Note that this definition of antitone Galois connection is symmetric in X and Y , provided we swap f_\star and f^\star . So dual statements may be obtained easily.

Similarly a monotone Galois connection may be viewed as an antitone Galois connection by taking the dual ordering on Y .

Proposition 2.1.18 (Triangular Identities)

Consider an antitone (resp. monotone) Galois connection $X \xrightleftharpoons[f_\star]{f^\star} Y$ then the following **triangular identities** 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 $f^* \circ f_*$ and $f_* \circ f^*$ are closure operators. In the monotone case $f^* \circ f_*$ is a closure operator and $f_* \circ f^*$ is a kernel operator. Furthermore the following subsets are equal (the “closed elements”)

$$\begin{aligned} X^* &:= \text{Fix}(f^* \circ f_*) = \text{Im}(f^* \circ f_*) = \text{Im}(f^*) \\ Y^* &:= \text{Fix}(f_* \circ f^*) = \text{Im}(f_* \circ f^*) = \text{Im}(f_*) \end{aligned}$$

then this induces a dual isomorphism (resp. order isomorphism) on the “closed” sets

$$X^* \xrightleftharpoons[f_*]{f^*} Y^*$$

Proof. We deal only in the antitone case, as the monotone case follows by duality. For the first so-called triangular identity, note that $x \in X \implies x \leq f^*(f_*(x)) \implies f_*(x) \geq f_*(f^*(f_*(x)))$ by the antitone property of f_* . On the other hand $f_*(x) \in Y \implies f_*(x) \leq f_*(f^*(f_*(x)))$ be the extensive property of $f_* \circ f^*$. As a result they are equal. The second identity follows from duality.

The fact that $f^* \circ f_*$ and $f_* \circ f^*$ are closure operators follows immediately. Note that

$$\text{Im}(f^* \circ f_*) \subseteq \text{Im}(f^*) \subseteq \text{Fix}(f^* \circ f_*)$$

where the first inclusion is trivial and the second inclusion follows from the second triangular identity. However both sides are equal by Lemma 2.1.5 and the result follows. The expressions for Y^* follow from duality.

Finally note that $f_*(X^*) = (f_* \circ f^*)(Y) = Y^*$ and similarly $f^*(Y^*) = X^*$. Therefore the restriction to the closed sets is well-defined, and by the triangular identities the functions f^* and f_* are mutual inverses when restricted to these sets. \square

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 2.1.19 (Subordinated Closure Operator)

Let $X \xrightleftharpoons[f_*]{f^*} Y$ be a Galois connection and $c : X \rightarrow X$ be a closure operator with image X_c . Then

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

In this case

$$f_*(c(x)) = f_*(x)$$

Proof. Suppose $c(x) \leq (f^* \circ f_*)(x)$. Then define $x = f^*(y)$ and observe because c is extensive

$$f^*(y) \leq c(f^*(y)) \leq (f^* \circ f_* \circ f^*)(y) = f^*(y)$$

whence they are equal, and $X^* = \text{Im}(f^*) \subseteq \text{Fix}(c) = \text{Im}(c)$. Conversely suppose this holds then

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

Finally applying f_*

$$x \leq c(x) \leq (f^* \circ f_*)(x) \implies f_*(x) \leq f_*(c(x)) \leq f_*(x)$$

whence they are equal. \square

The following criterion is useful

Lemma 2.1.20 (Adjoint criterion)

Let (X, \leq_X) and (Y, \leq_Y) be posets. A pair of functions

$$X \xrightleftharpoons[f_*]{f^*} Y$$

constitutes an antitone Galois connection if and only if the following condition holds

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

Proof. Suppose we have an antitone Galois connection. Then applying f_* and f^* we have

$$x \leq f^*(y) \implies y \leq f_*(f^*(y)) \leq f_*(x)$$

and the reverse implication follows from duality. Conversely suppose this condition holds then observe that

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

and

$$x \leq x' \leq f^*(f_*(x')) \implies f_*(x') \leq f_*(x).$$

The rest follows from duality. \square

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

Example 2.1.27 (Canonical example of an antitone Galois connection)

Suppose there is a predicate

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

Define a connection

$$\mathcal{P}(X) \xrightleftharpoons[f_*]{f^*} \mathcal{P}(Y)$$

by

$$\begin{aligned} f_*(S) &= \{y \in Y \mid \psi(x, y) = 1 \quad \forall x \in S\} \\ f^*(T) &= \{x \in X \mid \psi(x, y) = 1 \quad \forall y \in T\} \end{aligned}$$

Then

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

Proposition 2.1.21 (Joins under Galois Correspondence)

Let (X, \leq_X) and (Y, \leq_Y) be complete lattices with an antitone Galois connection $X \xrightleftharpoons[f_*]{f^*} Y$. Then for $S \subseteq X$

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

Similarly for $T \subseteq Y$ we have

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

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

The second statement follows from duality. □

2.2 Numbers

Informally we consider the set of integers

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

and the subset of natural numbers

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

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

$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

and an involution

$$(-) : \mathbb{Z} \rightarrow \mathbb{Z}$$

satisfying

- $-0 = 0$
- $-(-x) = x$
- $x + 0 = 0 = 0 + x$
- $x + y = y + x$
- $(x + y) + z = x + (y + z)$
- $x + (-x) = 0 = (-x) + x$
- $-(x + y) = (-x) + (-y)$

- A subset \mathbb{N} such that
 - $0, 1 \in \mathbb{N}$
 - $x, y \in \mathbb{N} \implies x + y \in \mathbb{N}$
 - $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ and $\{0\} = \mathbb{N} \cap -\mathbb{N}$

which also satisfies the principle of induction

- Let $S \subseteq \mathbb{N}$ be a set such that
 - $0 \in S$
 - $x \in S \implies x + 1 \in S$
- then $S = \mathbb{N}$

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

Proposition 2.2.1 (Multiplication exists)

There exists a binary operation

$$\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

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*

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

such that

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

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 $|q - q'| = 0 \implies q = q' \implies r = r'$. \square

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 clearly $d\mathbb{Z} \subseteq S$. 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 $y \in d\mathbb{Z}$. \square

Definition 2.2.1 (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 2.2.7

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 2.2.8 (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 the previous Corollary 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 $d = \pm d'$ be the previous Lemma. Since they are positive and non-zero we have $d = d'$. □

Proposition 2.2.9

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 2.2.2

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 2.2.10

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 2.2.11 (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 Proposition 2.2.9 $(x', a') = 1$. 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 Lemma 2.2.10 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 Category Theory

2.3.1 Categories

Definition 2.3.1 (Category)

A (locally small) **category** \mathcal{C} consists of

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

- for every three objects a, b, c a **law of composition**

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

such that the following conditions hold

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

Example 2.3.2

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

Example 2.3.3 (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 $A \in \text{ob}(\mathcal{C})$ and $a \in A^n$. We consider only morphisms $f : A \rightarrow B$ such that $f(a_i) = b_i$.

Definition 2.3.4 (Initial object)

An **initial object** of a category \mathcal{C} is an object a such that for all objects b

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

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

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

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

Example 2.3.5

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

Definition 2.3.6 (Isomorphism)

A morphism $f : a \rightarrow b$ is an **isomorphism** if there exists $g : b \rightarrow a$ such that

$$g \circ f = 1_a$$

and

$$f \circ g = 1_b$$

Proposition 2.3.1 (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^a and $\eta_{a'}^{a'}$ respectively. Then by definition

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

and vice-versa. □

Definition 2.3.7 (Functor)

A **covariant functor** $F : \mathcal{C} \rightarrow \mathcal{D}$ consists of a mapping of objects

$$F : \text{ob}(\mathcal{C}) \rightarrow \text{ob}(\mathcal{D})$$

together with a mapping of morphisms

$$F(-) : \text{Mor}(a, b) \rightarrow \text{Mor}(F(a), F(b))$$

which satisfies

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

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

Definition 2.3.8 (Full and faithful)

A functor F is said to be

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

Definition 2.3.9 (Concrete Category)

A **concrete category** is a pair (\mathcal{C}, U) where \mathcal{C} and a “**forgetful functor**” $U : \mathcal{C} \rightarrow \mathbf{Set}$ which is faithful

Example 2.3.10 (Forgetful Functor)

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

Definition 2.3.11 (Mor functor)

For any objects $a, b, c \in \text{ob}(\mathcal{C})$, there is a canonical covariant functor

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

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

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

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

Definition 2.3.12 (Natural Transformation)

Let $F, G : \mathcal{C} \rightarrow \mathcal{D}$ be functors. A **natural transformation** $\eta : F \Rightarrow G$ consists of a family of morphisms

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

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

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

for all $f : c \rightarrow c'$.

Definition 2.3.13 (Natural isomorphism)

A natural transformation $\eta : F \Rightarrow G$ is a natural isomorphism if η_c is an isomorphism for all $c \in \mathcal{C}$.

2.3.2 Equivalence of categories

Definition 2.3.14 (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)

$$\mathcal{C} \xleftarrow[G]{F} \mathcal{D}$$

together with natural isomorphisms

$$\begin{aligned} \eta : \mathbf{1} &\Rightarrow GF \\ \epsilon : FG &\Rightarrow \mathbf{1} \end{aligned}$$

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

Definition 2.3.15

We say $F : \mathcal{C} \rightarrow \mathcal{D}$ 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 2.3.2

Let $F : \mathcal{C} \rightarrow \mathcal{D}, G : \mathcal{D} \rightarrow \mathcal{C}$ 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

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

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

Proof. Consider the sequence of maps

$$\text{Mor}(c, c') \xrightarrow{F(-)} \text{Mor}(F(c), F(c')) \xrightarrow{G(-)} \text{Mor}(GF(c), GF(c')) \xrightarrow{\text{Mor}(\eta_c, \eta_{c'}^{-1})} \text{Mor}(c, c')$$

Note that the composite of this map is given by

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

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

Proposition 2.3.3 (Equivalence is full and faithful)

Let $F : \mathcal{C} \rightarrow \mathcal{D}$ then the following are equivalent

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

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

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

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

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

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

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

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

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

Proposition 2.3.4 (Duality)

Let $(-)^* : \mathcal{C} \rightarrow \mathcal{C}$ be a (contravariant) functor such that there is a natural isomorphism

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

then $(-)^*$ 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 $(-)^*$ is full and faithful. \square

2.3.3 Properties of Morphisms

Definition 2.3.16 (Injective, Surjective and Bijective)

Let (\mathcal{C}, U) be a concrete category and $f : a \rightarrow c$ a morphism. Then we say

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

Remark 2.3.17

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 2.3.18 (Monomorphism)

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

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

for all $g_1, g_2 : c \rightarrow a$.

Definition 2.3.19 (Epimorphism)

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

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

for all $g_1, g_2 : b \rightarrow c$.

Definition 2.3.20 (Split-monic / Section)

A morphism $f : a \rightarrow b$ is **split-monic** if it has a left inverse, $g : b \rightarrow a$

$$g \circ f = 1_a$$

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

Definition 2.3.21 (Split-epic / Retraction)

A morphism $f : a \rightarrow b$ is **split-epic** if it has a right inverse, $g : b \rightarrow a$

$$f \circ g = 1_b$$

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

Proposition 2.3.5 (Split Monic \implies Monic)

For a general category \mathcal{C} we have

- $\text{split-monic} \implies \text{monic}$
- $\text{split-epic} \implies \text{epic}$

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 2.3.6 (Isomorphism Criteria)

Let $f : a \rightarrow b$ be a morphism. Then the following are equivalent

1. f is an **isomorphism**
2. f is both **split-epic** and **split-monic**
3. f is **split-epic** and **monic**
4. 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 Proposition 2.3.5.

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. \square

Proposition 2.3.7

For the category **Set** we have

- $\text{split-monic} \iff \text{monic} \iff \text{injective}$
- $\text{split-epic} \iff \text{epic} \iff \text{surjective}$
- $\text{isomorphism} \iff \text{bijective}$

Definition 2.3.22 (Preserves/Reflects)

Let \mathcal{P} be a property of morphisms and $F : \mathcal{C} \rightarrow \mathcal{D}$ be a functor then we say

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

Proposition 2.3.8

Let $F : \mathcal{C} \rightarrow \mathcal{D}$ 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. \square

Proposition 2.3.9

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 2.3.8 and so by 2.3.7 $U(f)$ is injective.

Suppose $U(f)$ injective, then by 2.3.7 $U(f)$ is monic. By 2.3.8 U reflects monics and so f is monic.

The other statements are similar. \square

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

Proposition 2.3.10

Let $f : a \rightarrow b$ be a morphism then

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

dually

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

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

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

A similar statement follows dually for f split-epic, and f monic. \square

Corollary 2.3.11 (Isomorphism Criteria)

Let $f : a \rightarrow b$ be a morphism then TFAE

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

Proof. This follows from combining Proposition 2.3.10 with Proposition 2.3.6. \square

Definition 2.3.23 (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

2.3.4 Directed Limits

Definition 2.3.24 (Directed Category)

We say a category I is **directed** if

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

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

Definition 2.3.25 (Direct limit)

Let I be a directed category and $F : I \rightarrow \mathcal{C}$ a functor (“diagram”). We write $A_i := F(i)$ and $\rho_{ij} : A_i \rightarrow A_j$ when $i \prec j$. Observe that

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

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

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

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

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

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

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

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

Proposition 2.3.12 (Direct limit of sets)

Let I be a directed category and $F : I \rightarrow \mathbf{Set}$ be a diagram of sets. Write $A = F(i)$ and $\rho_{ij} : A_i \rightarrow A_j$. 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 $\rho_{ik}(x) = \rho_{jk}(y)$.

2.3.5 Adjoint Functors

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

Definition 2.3.26 (Adjoint Pair)

Let $F : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$ be functors. We say that F is **left adjoint** to G if there is a bijection

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

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

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

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

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

Proposition 2.3.13 (Adjoint \implies unit, counit)

Let $F : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$ be adjoint functors with relationship

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

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

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

Furthermore we may recover the adjoint relationship via

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

Proof. We show that the transformations given are natural. Suppose $\alpha : c \rightarrow c'$ then

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

so 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 $\beta : d \rightarrow d'$

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

□

Given two natural transformations we may recover a corresponding adjoint

Proposition 2.3.14 (Adjoint from unit and counit)

Let $F : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$ 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

1. F is left adjoint to G with unit and counit η, ϵ
2. The so-called **triangular identities** are satisfied

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

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

More precisely the adjunction is given by

$$\begin{array}{ccc} \text{Mor}(F(c), d) & \xrightleftharpoons[\psi]{\phi} & \text{Mor}(c, G(d)) \\ f & \longrightarrow & G(f) \circ \eta_c \\ \epsilon_d \circ F(g) & \longleftarrow & g \end{array}$$

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

$$\psi\phi(g) = G(\epsilon_d \circ F(g)) \circ \eta_c = G(\epsilon_d) \circ \eta_{G(d)} \circ g \quad (2.6)$$

$$\phi\psi(f) = \epsilon_d \circ F(G(f) \circ \eta_c) = f \circ \epsilon_{F(c)} \circ F(\eta_c) \quad (2.7)$$

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

Further one may easily verify that 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 2.3.15 (Criteria for right adjoint to be full and faithful)

Let $F : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$ 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

$$\text{Mor}(d', d) \xrightarrow{\text{Mor}(\epsilon_{d'}, d)} \text{Mor}(F(G(d')), d) \xrightarrow{\psi_{G(d'), d}} \text{Mor}(G(d'), G(d))$$

which is natural in d and d' . Note that image of $\alpha \in \text{Mor}(d', d)$ 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 2.3.10 $\text{Mor}(\epsilon_{d'}, d)$ 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 Proposition 2.3.6. □

The following criteria will be useful

Proposition 2.3.16 (Alternative Characterization)

Let $F : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$ be functors. Suppose that we have natural transformations

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

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

Then η, ϵ induce an adjoint relationship between F and G as in Proposition 2.3.14.

Proof. Recall the proposed adjoint maps from Proposition 2.3.14, 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 Proposition 2.3.7 ψ has a left-inverse too. By Proposition 2.3.6 ψ is an isomorphism with inverse $\psi^{-1} = \phi$.

The case that ϕ is surjective is similar. □

Chapter 3

Algebra

3.1 Introduction

Follows largely Lang with some Bourbaki.

3.2 Magmas and Monoids

Definition 3.2.1 (Magma)

Let X be a set. A **law of composition** on $X \times X$ is a function

$$\cdot : X \times X \rightarrow X$$

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 3.2.1 (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 3.2.3 (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 3.2.2 (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 3.2.4 (Homomorphism)

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

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

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

$$\phi(e_X) = e_Y$$

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

3.3 Groups

Definition 3.3.1 (Group)

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

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

$$g + h$$

Definition 3.3.2 (Subgroup, Normal Subgroup)

A **subgroup** $H \leq G$ is a subset with the following properties

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

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

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

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

Proposition 3.3.1 (Subgroup is a group)

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

Example 3.3.3

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

Definition 3.3.4

Let (G, \cdot) and (H, \cdot) be groups. A function $\phi : G \rightarrow H$ 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

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

and the **kernel** to be

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

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

Proposition 3.3.2 (Raise to the n -th power)

Let $g \in G$ be a group element. Then there exist a unique group homomorphism

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

satisfying

$$g^1 = g$$

In other words such that

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

Proposition 3.3.3

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

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

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

Definition 3.3.5 (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 3.3.6 (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

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

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

Proposition 3.3.4 (Cosets)

Let H be a subgroup of G . The following is an equivalence relation on G

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

and the equivalence classes are precisely the sets of the form

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

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

$$G/H$$

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

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

Proof. It's trivial to show that \sim_H is an equivalence relation (precisely because H is a subgroup). Therefore by Proposition 2.1.1 the equivalence classes form a partition which we denote G/H .

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

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

Example 3.3.7

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

Corollary 3.3.5 (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 3.3.8

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

Proposition 3.3.6

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 $e = g^n = g^{qm+r} = (g^m)^q g^r = e^q g^r = g^r$. By minimality we have $r = 0$ and $m \mid n$ as required. \square

Proposition 3.3.7 (Quotient Group)

Let N be a normal subgroup G . Then the set of cosets

$$G/N$$

forms a group under the binary operation

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

with identity eN .

- There is a canonical surjective group homomorphism

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

$$g \rightarrow gN$$

with kernel N .

- Let $N \subseteq H$ be a subgroup then define the corresponding subgroup of G/N

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

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

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

such that

- $\text{Im}(\phi) = \text{Im}(\tilde{\phi})$
- $\ker(\tilde{\phi}) = \ker(\phi)/N$

Corollary 3.3.8 (Isomorphism Theorem)

Let $\phi : G \rightarrow H$ be a group homomorphism, then there is a canonical isomorphism

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

Proposition 3.3.9 (Correspondence Theorem)

Let $\pi : G \rightarrow G'$ be a surjective homomorphism with $\ker(\pi) = N$ then there is a bijective correspondence of subgroups

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

which preserves index, that is

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

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

3.3.1 Cyclic Groups

Definition 3.3.9

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 3.3.10

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

- Every subgroup is of the form $d\mathbb{Z}$ for $d \geq 0$ and is itself cyclic
- When $d > 0$, then $\mathbb{Z}/d\mathbb{Z}$ has a complete set of coset representatives

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

- In particular $[\mathbb{Z} : d\mathbb{Z}] = d$ when $d > 0$
- $d\mathbb{Z} \subseteq e\mathbb{Z} \iff e \mid d$ and in this case $[e\mathbb{Z} : d\mathbb{Z}] = \frac{d}{e}$

Proof. We prove each in turn

- By 2.2.6 every subgroup is of the form $d\mathbb{Z}$. Multiplication map $[d] : \mathbb{Z} \rightarrow d\mathbb{Z}$ shows it is itself cyclic.
- 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.
- This is clear from the previous step
- The first equivalence is clear. By 3.3.5

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

and the result follows. □

Proposition 3.3.11

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 $\mathbb{Z} \rightarrow G$ 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 3.3.10 (Euler Totient Function)

Define the function

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

Proposition 3.3.12 (Finite Cyclic Groups)

Consider a finite cyclic group G of order n . Then

- The order of g^r is $\frac{n}{(n, r)}$ where $0 < r \leq n$.
- There are $\phi(n)$ generators
- For every $d \mid n$ there is a unique subgroup of order n/d given by $\langle g^d \rangle$, which is cyclic.
- For $d \mid n$ there are precisely $\phi(d)$ elements of order d
- There are precisely d elements of order dividing d

Proof. We prove each in turn

- $(g^r)^s = e_G \iff g^{rs} = e_G \xrightarrow{3.3.6} n \mid rs \xrightarrow{2.2.11} \frac{n}{(n,r)} \mid s$. Therefore g^r has order $\frac{n}{(n,r)}$ as required.
- Note h is a generator iff $o(h) = n$. So g^r is a generator iff $(n, r) = 1$ by the previous step. As $G = \{g, g^2, \dots, g^n\}$ the result follows by definition of the totient function.
- Recall there is a canonical surjective morphism $\pi : \mathbb{Z} \rightarrow G$ with kernel $n\mathbb{Z}$ and $\pi(1) = g$. By 3.3.9 the subgroups H of G correspond bijectively to subgroups H' of \mathbb{Z} containing $n\mathbb{Z}$, preserving the index. By 3.3.10 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.
- 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 .
- 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 3.3.6. Therefore $G[d]$ consists of all the elements of order dividing d .

□

Corollary 3.3.13

Let n be a positive integer then

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

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 3.3.14 (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

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

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

Example 3.3.11

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 3.3.12 (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 3.3.13 (Faithful group action)

A group action G on S is faithful if

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

Definition 3.3.14 (Free group action)

A group action G on S is free if

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

Definition 3.3.15 (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 3.3.15 (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 3.3.16

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

Proposition 3.3.16 (Orbit-Stabilizer Theorem)

Let G be a group with an action on S . Given an element $s \in S$ there is a natural bijection

$$G/G_s \longrightarrow Gs$$

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

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

and when the action is free

$$\#G = \#Gs$$

3.4 Rings and Modules

3.4.1 Commutative Rings

Definition 3.4.1 (Ring)

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

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

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

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

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

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

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

Definition 3.4.2 (Subring)

A **subring** of a ring A is a subset B such that

- $0_A, 1_A \in B$
- $x \in B \implies -x \in B$

- $x, y \in B \implies x + y \in B$
- $x, y \in B \implies x \cdot y \in B$

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

Definition 3.4.3 (Multiplicative set)

A subset $S \subset A$ is said to be **multiplicative** if

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

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

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

Definition 3.4.4 (Integral Domain)

A commutative ring A is said to be an **integral domain** if it is not a zero-ring and it is cancellative, that is

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

Definition 3.4.5 (Reduced)

A commutative ring A is said to be **reduced** if

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

Definition 3.4.6 (Unit / Group of Units)

An element $0 \neq a$ of a ring A is called a **unit** if it has a two-sided multiplicative inverse.

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

Definition 3.4.7 (Field)

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

Note we have the implications

Proposition 3.4.1

Let A be a ring then we have the following implications

$$\text{field} \implies \text{integral domain} \implies \text{reduced}$$

Definition 3.4.8 (Ring homomorphism)

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

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

The **kernel** of ϕ is defined to be

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

Definition 3.4.9 (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 3.4.2 (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 3.4.3

Let $\phi : A \rightarrow B$ be a ring homomorphism, then

- The kernel $\ker(\phi)$ is a two-sided ideal of A
- The image $\phi(A)$ is a subring of B
- ϕ is injective if and only if $\ker(\phi) = \{0\}$

3.4.2 Modules I**Definition 3.4.10** (Module)

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

$$\cdot : A \times M \rightarrow M$$

which satisfies the **distributive** properties

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

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

Definition 3.4.11 (Submodule)

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

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

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

Definition 3.4.12 (Module homomorphism)

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

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

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

Definition 3.4.13 (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

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

Example 3.4.14 (Trivial Examples)

A ring A is a left A -module over itself, denoted A_s .

Definition 3.4.15 (Restriction of Scalars)

Let $\phi : A \rightarrow B$ 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 3.4.4 (Submodules constitute a lattice)

Let M be a left A -module then the collection $\text{SubMod}(M)$ 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**)

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

Moreover it is the image of the closure operator $\langle - \rangle : \mathcal{P}(M) \rightarrow \mathcal{P}(M)$ 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 Proposition 2.1.15 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. \square

Lemma 3.4.5

Let M be a module. Then

1. $\langle \bigcup_{i \in I} X_i \rangle = \sum_{i \in I} \langle X_i \rangle$
2. $\langle \bigcup_{i \in I} N_i \rangle = \sum_{i \in I} N_i$
3. $N_1 \subseteq N_2 \implies N_1 + N_2 = N_2$

Proof. 1. This follows from Proposition 2.1.17 applied to the closure operator $\langle - \rangle$

2. This follows by 1 because $N_i = \langle N_i \rangle$

3. This follows from 2 because $N_1 \cup N_2 = N_2$

\square

Definition 3.4.16 (External Direct Sum)

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

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

with the obvious module operations.

Definition 3.4.17 (Free Module)

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

3.4.3 Operations on Ideals

For this section we assume A is a commutative ring.

Proposition 3.4.6 (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

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

This induces a corresponding closure operator

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

given by

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

Proposition 3.4.7

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 3.4.18 (Product of ideals)

The product of two ideals $\mathfrak{a}\mathfrak{b}$ is

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

and is itself an ideal.

Definition 3.4.19 (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 3.4.20 (Principal Ideal)

A **principal ideal** is an ideal generated by a single element

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

Lemma 3.4.8

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

Definition 3.4.21 (Maximal Ideal)

An ideal $\mathfrak{m} \triangleleft A$ is **maximal** if it is both proper and not contained in another proper ideal.

Definition 3.4.22 (Prime Ideal)

An ideal $\mathfrak{p} \triangleleft A$ is **prime** if it is both proper and satisfies the following property

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

Definition 3.4.23 (Radical Ideal)

An ideal $\mathfrak{a} \triangleleft A$ is **radical** if it satisfies the following property

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

Proposition 3.4.9 (Maximal ideals exist)

Let A be a ring and $\mathfrak{a} \triangleleft A$ a proper ideal. Then it is contained in some maximal ideal \mathfrak{m} .

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

Proof. Simple application of Zorn's Lemma. □

Proposition 3.4.10 (Properties of prime ideals)

Let \mathfrak{p} be a prime ideal and $\mathfrak{a}, \mathfrak{b}$ be ideals then

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

Proof. 1 \implies 2) Follows because $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$

2 \implies 3) Follows because $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$

3 \implies 1) If $\mathfrak{a} \not\subseteq \mathfrak{p}$, then choose $a \in \mathfrak{a} \setminus \mathfrak{p}$. By hypothesis $\mathfrak{ab} \subseteq \mathfrak{p}$ and since \mathfrak{p} is prime $\mathfrak{b} \subseteq \mathfrak{p}$. □

Corollary 3.4.11 (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 Proposition 3.4.10. 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 3.4.12 (Generate prime ideals)

Let A be a ring, S a multiplicative set and $\mathfrak{b} \triangleleft A$ such that $\mathfrak{b} \cap S = \emptyset$ then

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

has a maximal element, which is prime.

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

Proposition 3.4.13

Let A be a ring. Then the set $\text{Rad}(A)$ of radical ideals forms a complete sub-lattice of the lattice of ideals $\mathcal{I}(A)$. This induces a closure operator

$$\sqrt{-} : \mathcal{I}(A) \rightarrow \text{Rad}(A)$$

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

- $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$
- $\mathfrak{a} \subseteq \mathfrak{b} \implies \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$
- $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$

Proof. The set of radical ideals is closed under arbitrary intersections (which are meets in the lattice $\mathcal{I}(A)$). Therefore by Proposition 2.1.15 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 $\text{Rad}(A)$, 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 $(ax)^n = a^n x^n \in \mathfrak{a}$. 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. \square

Proposition 3.4.14 (Prime Nullstellensatz)

The radical of an ideal satisfies

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

Proof. Suppose $x \in \sqrt{\mathfrak{a}}$ and $\mathfrak{p} \supseteq \mathfrak{a}$. Then $x^n \in \mathfrak{p} \implies x \in \mathfrak{p}$. Therefore $\sqrt{\mathfrak{a}} \subseteq \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}$. Conversely suppose $x \notin \sqrt{\mathfrak{a}}$ then $S := \{1, x, x^2, \dots\}$ is a proper multiplicative set such that $S \cap \mathfrak{a} = \emptyset$. By Lemma 3.4.12 there is a prime ideal \mathfrak{p} containing \mathfrak{a} which does not intersect S . Therefore $x \notin RHS$ as required. \square

Proposition 3.4.15 (Properties of Radical Ideals)

Let $\mathfrak{a}, \mathfrak{b}$ be ideals then

1. $\sqrt{\mathfrak{a}^k} = \sqrt{\mathfrak{a}}$ for $k > 0$
2. $\sqrt{\sum_i \mathfrak{a}_i} = \sqrt{\sum_i \sqrt{\mathfrak{a}_i}}$
3. $\sqrt{\mathfrak{a}} = A \iff \mathfrak{a} = A$
4. $\sum_i \mathfrak{a}_i = A \iff \sum_i \sqrt{\mathfrak{a}_i} = A$
5. $\sum_{i=1}^n \mathfrak{a}_i^{k_i} = A \iff \sum_{i=1}^n \mathfrak{a}_i = A \quad k_i > 0$.

Proof. 1. This may be shown by direct calculation or combining 3.4.14 and 3.4.10.

2. This follows by applying Proposition 2.1.17 to the closure operator $\sqrt{-}$.

3. $\sqrt{\mathfrak{a}} = A \iff 1 \in \sqrt{\mathfrak{a}} \iff 1 \in \mathfrak{a} \iff \mathfrak{a} = A$

4. This follows from combining 3 and 2

5. This follows from 4 and 1

\square

Definition 3.4.24 (Extended and contracted ideals)

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

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

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

Proposition 3.4.16 (Operations on ideals)

Let $\phi : A \rightarrow B$ a ring homomorphism and $\mathfrak{a} \triangleleft A$, $\mathfrak{b} \triangleleft B$ ideals then

1. $\mathfrak{b}^c \triangleleft A$ and $\mathfrak{a}^e \triangleleft B$
2. \mathfrak{b}^c proper if and only if \mathfrak{b} is proper
3. $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ and $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$
4. $\mathfrak{a}^{ece} = \mathfrak{a}^e$ and $\mathfrak{b}^{cec} = \mathfrak{b}^c$
5. $\mathfrak{b}^{ce} = \mathfrak{b} \iff \mathfrak{b}$ is an extended ideal $\iff \mathfrak{b} \subseteq \mathfrak{b}^{ce}$
6. $\mathfrak{a}^{ec} = \mathfrak{a} \iff \mathfrak{a}$ is a contracted ideal $\iff \mathfrak{a}^{ec} \subseteq \mathfrak{a}$
7. $\sqrt{\mathfrak{b}^c} = (\sqrt{\mathfrak{b}})^c$
8. $(\sqrt{\mathfrak{b}^c})^e \subseteq \sqrt{\mathfrak{b}}$ with equality when ϕ is surjective

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

Proof. We prove each in turn

1-3. Straightforward

4. 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.

5-6 These follow from 3 and 4

$$7 \quad x \in (\sqrt{\mathfrak{b}})^c \iff \phi(x) \in \sqrt{\mathfrak{b}} \iff \phi(x)^n \in \mathfrak{b} \iff \phi(x^n) \in \mathfrak{b} \iff x^n \in \mathfrak{b}^c \iff x \in \sqrt{\mathfrak{b}^c}$$

8 By 3 and 7 we find $(\sqrt{\mathfrak{b}^c})^e = (\sqrt{\mathfrak{b}})^{ce} \subseteq \sqrt{\mathfrak{b}}$. We will show that when ϕ is surjective every ideal is extended, in which case the equality follows from 5.

Suppose that ϕ is surjective. Then by 5 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 $y \in \mathfrak{b}^{ce}$. \square

Corollary 3.4.17

Let $\phi : A \rightarrow B$ be a ring homomorphism then there is a bijection between “contracted” and “extended ideals”

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

which restricts to proper ideals.

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

Proposition 3.4.18 (Inverse image of maximal / prime ideals)

Let $\phi : A \rightarrow B$ be a morphism then

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

3.4.4 Quotient Rings**Proposition 3.4.19** (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

$$\begin{aligned} \cdot : A/\mathfrak{a} \times A/\mathfrak{a} &\rightarrow A/\mathfrak{a} \\ (a + \mathfrak{a}) \cdot (b + \mathfrak{a}) &\rightarrow (a \cdot b + \mathfrak{a}) \end{aligned}$$

which makes $(A/\mathfrak{a}, +, \cdot)$ into a ring. Further there is a canonical surjective ring homomorphism

$$\pi : A \rightarrow A/\mathfrak{a}$$

with the following properties

- $\ker(\pi) = \mathfrak{a}$
- Every morphism $\phi : A \rightarrow B$ such that $\mathfrak{a} \subseteq \ker(\phi)$, factors uniquely through π .

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

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

For an ideal $\mathfrak{b} \supseteq \mathfrak{a}$ define the corresponding quotient ideal

$$\mathfrak{b}/\mathfrak{a} := \{b + \mathfrak{a} \mid b \in \mathfrak{b}\} = \pi(\mathfrak{b})$$

This induces a bijective, order-preserving correspondence of ideals

$$\{\mathfrak{b}' \triangleleft A/\mathfrak{a}\} \xleftrightarrow[\pi^{-1}(-)]{\pi(-)} \{\mathfrak{b} \triangleleft A \mid \mathfrak{a} \subseteq \mathfrak{b}\}$$

under which maximal ideals of A containing \mathfrak{a} correspond to maximal ideals of A/\mathfrak{a} .

Corollary 3.4.20 (Isomorphism Theorem)

Let $\phi : A \rightarrow B$ be a ring homomorphism. Then this induces a canonical isomorphism

$$A/\ker(\phi) \cong \phi(A) \subset B$$

Corollary 3.4.21 (Second Isomorphism Theorem)

Let $\mathfrak{b}, \mathfrak{a}$ be ideals then there is a unique morphism making the diagram commute

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

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

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

Proposition 3.4.22 (Criteria for Maximal, Prime and Reduced)

Let $\mathfrak{a} \triangleleft A$ then A/\mathfrak{a} is

- **maximal** if and only if A/\mathfrak{a} is a field
- **prime** if and only if A/\mathfrak{a} is an integral domain
- **radical** if and only if A/\mathfrak{a} is reduced

Corollary 3.4.23

Let $\mathfrak{a} \triangleleft A$ be a proper ideal, then the following implications hold

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

Proof. This follows by combining 3.4.1 and 3.4.22. □

Corollary 3.4.24

Let A be a non-zero ring. Then A is a field if and only if the only proper ideal is (0) .

Proof. Let $\mathfrak{a} = (0)$ then $A \rightarrow A/(0)$ is an isomorphism. Then it follows by a previous Proposition. □

Corollary 3.4.25

Let $\phi : k \rightarrow B$ 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 Proposition 3.4.13 these form an ideal.

Definition 3.4.25 (Nilradical)

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

$$\mathfrak{N}(A) := \sqrt{(0)} \stackrel{3.4.14}{=} \bigcap_{\mathfrak{p}} \mathfrak{p}$$

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

We also make the following definition

Definition 3.4.26 (Irreducible)

Let A be a ring. We say A is **irreducible** if $\mathfrak{N}(A)$ is prime.

Lemma 3.4.26 (Integral Domain \iff Reduced and Irreducible)

Let A be a ring. Then A is an integral domain if and only if it is reduced and irreducible

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

3.4.6 Algebra over a Commutative Ring

For what follows let A be a commutative ring.

Definition 3.4.27 (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 $i_B : A \rightarrow B$ 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 $\phi : B \rightarrow C$ such that $\phi \circ i_B = i_C$. This then constitutes a category **Alg_A**.

If k is a field an algebra over k is referred to as a k -algebra.

Definition 3.4.28 (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 3.4.29 (Algebra over commutative 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 3.4.30 (Algebra generated by a set)

Let B be an A -algebra. The collection of A -subalgebras forms a Moore family. Therefore by Proposition 2.1.15 there is a canonical closure operator

$$A[-] : \mathcal{P}(B) \rightarrow \text{SubAlg}_A(B)$$

which we denote by $A[S]$ for $S \subset B$. A more explicit characterization when S is finite is given in Section 3.7. More generally we have

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

3.4.7 Modules II

Definition 3.4.31 (Faithful Module)

We say an A -module M is **faithful** if

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

Definition 3.4.32 (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 $\{s_1, \dots, s_n\} \subseteq S$ we have

$$\sum_{i=1}^n a_i s_i = 0 \implies a_i = 0 \quad 1 \leq i \leq n$$

- a **basis** if it is both spanning and linearly independent

Definition 3.4.33 (Finite Module)

An A -module M is **finite** if there exists a finite spanning set.

Definition 3.4.34 (Free Module)

Let M be an A -module. We say that M is a **free module** over A if it has a basis.

Proposition 3.4.27 (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

$$\sum_{i \in I} a_i m_i \rightarrow (a_i)_{i \in I}$$

Definition 3.4.35 (Vector space)

If k is a field and V a k -module, then we say V is a **vector space** over k .

Definition 3.4.36 (Module homomorphism)

A **module homomorphism** $\phi : M \rightarrow N$ is an additive group homomorphism which commutes with the A action

$$\phi(am) = a\phi(m) \quad \forall a \in A, m \in M$$

Denote the A -module of morphisms

$$\text{Mor}_A(M, N)$$

and the A -algebra of endomorphisms

$$\text{End}_A(M) := \text{Mor}_A(M, M)$$

Proposition 3.4.28 (Kernel)

Let $\phi : M \rightarrow N$ 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 3.4.29 (Image)

Let $\phi : M \rightarrow N$ be an A -module homomorphism then the image

$$\text{Im}(\phi) = \{\phi(m) \mid m \in M\}$$

is an A -submodule of N .

Definition 3.4.37 (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 3.4.30 (Quotient Module Properties)

Let $N \subseteq M$ be an A -submodule then there is a canonical surjective morphism

$$\pi : M \rightarrow M/N$$

with the following properties

- $\pi(m) = m + N$
- $\ker(\pi) = N$
- Every homomorphism $\psi : M \rightarrow P$ such that $N \subseteq \ker(\psi)$, factors uniquely through π

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

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 3.4.31

Let $\psi : M \rightarrow P$ be an A -module homomorphism, then this induces an isomorphism

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

Definition 3.4.38 (Exact Sequence)

Let $N \xrightarrow{\phi} M \xrightarrow{\psi} P$ be a sequence of A -module homomorphisms. We say it is **exact** if

$$\text{Im}(\phi) = \ker(\psi)$$

It is equivalent to the following two conditions

- $\psi \circ \phi = 0$
- $\psi(m) = 0 \implies m = \phi(n)$ for some $n \in N$.

An exact sequence of the form

$$0 \rightarrow N \rightarrow M \rightarrow P \rightarrow 0$$

is said to be **short-exact**.

Remark 3.4.39

There are a few trivial observations

- $0 \rightarrow M \rightarrow N$ is exact if and only if the map $M \rightarrow N$ is injective
- $M \rightarrow N \rightarrow 0$ is exact if and only if the map $M \rightarrow N$ is surjective.

Proposition 3.4.32 (Isomorphism induced by short-exact sequence)

Let $N \subseteq M$ be a A -submodule then there is a canonical short-exact sequence

$$0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$$

Conversely suppose we have a short exact sequence

$$0 \rightarrow N \xrightarrow{i} M \xrightarrow{\pi} P \rightarrow 0$$

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 3.4.33 (Second Isomorphism Theorem)

Let $N \subseteq N' \subseteq M$ be a chain of modules then there is a short-exact sequence

$$0 \rightarrow N'/N \rightarrow M/N \rightarrow M/N' \rightarrow 0$$

which then induces an isomorphism

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

3.4.8 Vector Spaces

Definition 3.4.40 (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**

The theory is much simpler because all vector spaces are free modules.

Lemma 3.4.34

Let S be a linearly independent set. Then $S \cup \{x\}$ is linearly independent if and only if $x \notin \langle S \rangle$.

Proof. We only prove one direction. Suppose S is linearly independent and $S \cup \{x\}$ is linearly dependent. Then there exists a linear dependence with not all coefficients equal to zero

$$0 = \lambda x + \sum_i \lambda_i s_i \quad s_i \in S$$

As S is linearly independent we must have $\lambda \neq 0$ so

$$x = -\lambda^{-1} \left(\sum_i \lambda_i s_i \right) \in \langle S \rangle$$

as required. □

Theorem 3.4.35

Let Γ be a spanning set and S a linearly independent set such that $S \subseteq \Gamma$. Then there exists a basis \mathcal{B} such that $S \subseteq \mathcal{B} \subseteq \Gamma$.

Proof. Let \mathcal{I} be the set of subsets of Γ which contain S and are linearly independent. Then \mathcal{I} is non-empty and inductively ordered. Let \mathcal{B} be a maximal element of \mathcal{I} then we claim $\langle \mathcal{B} \rangle = V$ so \mathcal{B} is a basis.

Suppose not and choose $x \in V \setminus \langle \mathcal{B} \rangle$. Then by assumption

$$x = \sum_{i=1}^n \lambda_i \gamma_i$$

with all $\lambda_i \neq 0$ and $\gamma_i \in \Gamma$. If all $\gamma_i \in \langle \mathcal{B} \rangle$, then $x \in \langle \mathcal{B} \rangle$ a contradiction. Therefore at least one $\gamma_i \notin \mathcal{B}$ so by Lemma 3.4.34 $\mathcal{B} \cup \{\gamma_i\}$ is also a linearly independent subset of Γ , contradicting maximality. □

Corollary 3.4.36 (Vector Spaces are Free)

Every vector space has a basis.

Proof. Apply Theorem 3.4.35 with $S = \emptyset$ and $\Gamma = V$. □

Definition 3.4.41 (Finite dimensional)

We say that a vector space V is **finite-dimensional** if it is finite as a k -module.

Corollary 3.4.37 (Finite basis exists)

A finite-dimensional vector space has a finite basis.

Proof. Apply Theorem 3.4.35 with Γ any finite spanning set. □

Lemma 3.4.38 (Exchange Lemma)

Let V be a vector space over k with a finite linearly-independent set S and a spanning set Γ .

Then there exists a subset T of Γ of order $\#S$ such that

$$\Gamma' := (\Gamma \setminus T) \cup S$$

is a spanning set. In particular $\#S \leq \#\Gamma$.

Proof. TODO □

Proposition 3.4.39 (Dimension is well-defined)

If V is finite-dimensional then every basis is finite of the same order. We denote this order by $\dim_k V$.

Proof. By Corollary 3.4.37 there exists a finite basis \mathcal{B} . Let \mathcal{B}' be another basis. Then by Lemma 3.4.38 $\#\mathcal{B}' \leq \#\mathcal{B} < \infty$. Switching roles we find $\#\mathcal{B} \leq \#\mathcal{B}'$, whence $\#\mathcal{B} = \#\mathcal{B}'$ as required. □

Proposition 3.4.40

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

Proposition 3.4.41

Let V be a finite-dimensional vector space then

- S linearly independent $\implies \#S \leq \dim_k V$
- Γ spanning $\implies \#\Gamma \geq \dim_k V$

Proof. If S is linearly independent, it can be extended to a basis by Theorem 3.4.35 so the inequality follows from Proposition 3.4.39. The other statement is similar. \square

Proposition 3.4.42 (Basis criteria)

Let V be a finite-dimensional vector space. Let \mathcal{B} be a subset, then the following are equivalent

1. \mathcal{B} is a basis
2. \mathcal{B} is linearly-independent and $\#\mathcal{B} \geq \dim_k V$
3. \mathcal{B} is spanning and $\#\mathcal{B} \leq \dim_k V$.

Proof. Clearly $1 \implies 2, 3$ by definition

$2 \implies 3$) \mathcal{B} is contained in a basis \mathcal{B}' by Theorem 3.4.35. So using the inequality $\mathcal{B} = \mathcal{B}'$ is a basis.

$3 \implies 2$) is similar. \square

Corollary 3.4.43

Let $W_1 \subseteq W_2$ be two finite-dimensional vector subspaces then

$$\dim_k W_1 \leq \dim_k W_2$$

with equality if and only if $W_1 = W_2$.

Proof. Let \mathcal{B}_1 be a basis of W_1 . By Theorem 3.4.35 there is a basis \mathcal{B}_2 of W_2 containing \mathcal{B}_1 , whence the inequality follows.

If $\dim_k W_1 = \dim_k W_2$, then by counting we have $\mathcal{B}_1 = \mathcal{B}_2$ and $W_1 = W_2$ as required.

Conversely suppose $W_1 \subsetneq W_2$, then choose $w \in W_2 \setminus W_1$. As $w \notin \langle \mathcal{B}_1 \rangle$, Lemma 3.4.34 shows that $S_2 := \mathcal{B}_1 \cup \{w\}$ is a linearly independent subset of W_2 . Therefore $\dim_k W_1 = \#\mathcal{B}_1 \stackrel{3.4.41}{\leq} \#S_2 \leq \dim_k W_2$ as required. \square

Proposition 3.4.44 (Image of a basis)

Let $\phi: V \rightarrow W$ be a linear map

- If S is linearly-independent and ϕ is injective, then $\phi(S)$ is linearly-independent
- If Γ is spanning then (ϕ is surjective $\iff \phi(\Gamma)$ is spanning)
- 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. • Suppose $\sum_i \lambda_i \phi(s_i) = 0 \implies \phi(\sum_i \lambda_i s_i) = 0$. As ϕ is injective this implies $\sum_i \lambda_i s_i = 0 \implies \lambda_i = 0$.

- 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 $w = \sum_i \phi(\lambda_i \gamma_i)$. 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.
- Suppose ϕ is isomorphism, hence bijective, then it's surely injective on \mathcal{B} and by the previous two points $\phi(\mathcal{B})$ is a basis. Conversely if $\phi(\mathcal{B}) = \mathcal{B}'$ is a basis then by the previous point 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 therefore bijective. \square

Corollary 3.4.45 (Dimension is an invariant)

Dimension is preserved under isomorphism. More generally for $\phi: V \rightarrow W$ 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 3.4.46

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 $\{v_1, \dots, v_m\}$ be a basis of W , then there exists a basis $\{v_1, \dots, v_m, \dots, v_n\}$ of V containing the first by Theorem 3.4.35. We claim that

$$\{[v_{m+1}], \dots, [v_n]\}$$

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 3.4.47 (Injective Criteria)

Let $\phi : V \rightarrow W$ 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 3.4.42 (Rank)

Let $\phi : V \rightarrow W$ be a linear map then define

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

Proposition 3.4.48 (Surjective Criteria)

Let $\phi : V \rightarrow W$ be a linear map with W finite-dimensional then

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

Proof. This follows directly from Corollary 3.4.43. □

Proposition 3.4.49 (Isomorphism Theorem / Rank-Nullity)

Let $\phi : V \rightarrow W$ be a linear map then this induces an isomorphism

$$V / \ker(\phi) \longrightarrow \text{im}(\phi)$$

in particular when V is finite-dimensional

$$\dim_k V = \dim_k \ker(\phi) + \text{rank}_k(\phi)$$

Corollary 3.4.50 (Isomorphism Criteria)

Let V, W vector spaces with W finite-dimensional. A linear map $\phi : V \rightarrow W$ is an isomorphism if and only if any two of the following are satisfied

- $\dim_k \ker(\phi) = 0 \iff \phi \text{ injective}$
- $\dim_k V = \dim_k W$
- $\text{rank}_k(\phi) = \dim_k W \iff \phi \text{ surjective}$

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 3.4.51 (Endomorphism Isomorphism Criteria)

Let V be a finite-dimensional vector space and $\phi : V \rightarrow V$ then TFAE

- ϕ is injective
- ϕ is surjective
- ϕ is an isomorphism

Proof. Use the previous result with $W = V$ and note $\dim_k W = \dim_k V$ is automatically satisfied. □

Proposition 3.4.52 (Internal Direct Sum)

Let U_1, U_2 be two subspaces of V then TFAE

1. $U_1 \cap U_2 = \{0\}$ and $V = U_1 + U_2$
2. 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 3.4.53

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 3.4.54 (Dimension formula for direct sums)

Suppose $V = U_1 \oplus U_2$, \mathcal{B}_1 is a basis for U_1 and \mathcal{B}_2 is a basis for U_2 . Then $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$ and $\mathcal{B}_1 \cup \mathcal{B}_2$ is a basis for V . In particular

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

3.4.8.1 Vector Space Hom**Definition 3.4.43**

Let V, W be two k -vector spaces. Define the k -vector space

$$\text{Hom}_k(V, W) := \text{Mor}(V, W)$$

with the obvious module operations

$$(\phi + \psi)(v) = \phi(v) + \psi(v)$$

$$(\lambda\phi)(v) = \lambda\phi(v)$$

For every V this yields a covariant functor

$$\text{Hom}_k(V, -) : \mathbf{Vect}_k \rightarrow \mathbf{Vect}_k$$

and a contravariant functor

$$\text{Hom}_k(-, W) : \mathbf{Vect}_k \rightarrow \mathbf{Vect}_k$$

Proposition 3.4.55 (Basis for Hom-Set)

Let V, W be finite-dimensional vector spaces. Then

$$\dim_k \text{Hom}_k(V, W) = \dim_k V \times \dim_k W$$

More precisely if $\{v_1, \dots, v_n\}$ is a basis for V and $\{w_1, \dots, w_m\}$ is a basis for W , then $\{F_{ij}\}_{i=1\dots n, j=1\dots m}$ is a basis for $\text{Hom}_k(V, W)$ where

$$F_{ij} \left(\sum_{p=1}^n \lambda_p v_p \right) := \lambda_i w_j$$

3.4.8.2 Dual Space

Definition 3.4.44 (Dual Space)

Let V be a k -vector space and define the **dual space** to be

$$V^* := \text{Hom}_k(V, k)$$

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

$$(-)^* : \mathbf{Vect}_k \rightarrow \mathbf{Vect}_k$$

Proposition 3.4.56 (Double Dual)

There is a natural transformation $\eta : \mathbf{1} \Rightarrow (-)^{**}$ given by

$$\eta_V : V \rightarrow V^{**} \quad (3.1)$$

$$v \rightarrow (\theta \mapsto \theta(v)) \quad (3.2)$$

which is injective. When V is finite-dimensional then it is an isomorphism.

Proof. It's clearly linear. Suppose the image of v is 0, by definition $\theta(v) = 0$ for all $\theta \in V^*$. Suppose v is non-zero, then $\{v\}$ is linearly independent and so may be extended to a basis $\mathcal{B} = \{v_i\}_{i \in I}$ with $v_{i_0} = v$. Define

$$\theta\left(\sum_i \lambda_i v_i\right) = \lambda_{i_0}$$

clearly $\theta(v) \neq 0$ a contradiction. Therefore $\ker(\psi) = \{0\}$ and ψ is injective. We show in Proposition 3.4.58 that $\dim_k V^* = \dim_k V$ whence $\dim_k V^{**} = \dim_k V$. By Corollary 3.4.50 it's an isomorphism. \square

Corollary 3.4.57

The contravariant functor $(-)^* : \mathbf{FdVect}_k \rightarrow \mathbf{FdVect}_k$ is an equivalence of categories and therefore full and faithful.

Proof. Use the dual isomorphism η together with Proposition 2.3.4 and 2.3.3. \square

Proposition 3.4.58 (Dual Basis)

Let V be a finite-dimensional k -vector space, then $\dim_k V = \dim_k V^*$. In particular if v_1, \dots, v_n be a basis for V then there are elements $v_1^*, \dots, v_n^* \in V^*$ such that

$$v_i^*(v_j) = \delta_{ij} \quad (3.3)$$

and these form a basis for V^* . Each v_i^* is uniquely defined by this condition. Similarly given any basis $v_1^*, \dots, v_n^* \in V^*$ then there exists a basis v_1, \dots, v_n such that (3.3) holds.

Proof. Note that k as a k -vector space has basis $\{1\}$. So apply Proposition 3.4.55 to obtain the required dual basis. For the reverse direction suppose v_1^*, \dots, v_n^* be a basis of V^* . By the same token there is a basis $v_1^{**}, \dots, v_n^{**} \in V^{**}$ such that

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

Let v_1, \dots, v_n be the unique inverse image under the dual isomorphism $V \rightarrow V^{**}$ from Proposition 3.4.56. These clearly satisfy (3.3) and furthermore by 3.4.44 is a basis for V as required. \square

Definition 3.4.45 (Annihilator)

Let V be a vector space and $U \subseteq V$ a subspace. Define the **annihilator** of U by

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

This is a linear subspace of V^* .

Proposition 3.4.59 (Dimension formula for annihilators)

There is a canonical isomorphism by restriction

$$V^*/U^\circ \longrightarrow U^*$$

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 3.4.49 and 3.4.58. \square

Corollary 3.4.60 (Dual rank = rank)

Let $\phi : V \rightarrow W$ be a linear map and $\phi^* : W^* \rightarrow V^*$ then

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

In the finite-dimensional case, the last is equal and

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

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

Consider the finite-dimensional case. By 3.4.59

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

By rank-nullity applied to ϕ^* and $\dim_k W = \dim_k W^*$ we deduce

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

By 3.4.59 and rank-nullity applied to ϕ

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

Finally by 3.4.43 $\operatorname{im}(\phi^*) = \ker(\phi)^\circ$.

□

From this it follows that taking duals reflects and preserve isomorphisms

Corollary 3.4.61 $((-))^*$ reflects isomorphisms)

Let $\phi : V \rightarrow W$ be a linear map of finite-dimensional spaces then

- ϕ is injective if and only if ϕ^* is surjective
- ϕ is surjective if and only if ϕ^* is injective
- ϕ is iso if and only if ϕ^* is iso

Proof. Note by 3.4.60 we have $\operatorname{rank}_k(\phi) = \operatorname{rank}_k(\phi^*)$ and by 3.4.58 $\dim_k V^* = \dim_k V$.

$$\phi \text{ is surjective} \iff \operatorname{rank}_k(\phi) = \dim_k W = \operatorname{rank}_k(\phi^*) \xrightarrow{3.4.49} \dim_k \ker(\phi^*) = 0 \iff \ker(\phi^*) = \{0\}$$

$$\phi \text{ is injective} \iff \dim_k \ker(\phi) = 0 \xrightarrow{3.4.49} \operatorname{rank}_k(\phi) = \dim_k V \iff \dim_k V^* = \operatorname{rank}_k(\phi^*) \iff \phi^* \text{ is surjective.}$$

The last point may be deduced from the first two, or the fact that $((-))^*$ is full and faithful 3.4.57 and category-theoretic result 2.3.8. □

Definition 3.4.46 (Bilinear maps)

Let V, W be vector spaces a bilinear map ψ is a map

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

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

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

Proposition 3.4.62 (Dual maps)

Let V and W be vector spaces, then there is a natural bijection

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

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 $\psi_L = \psi_R^* \circ \eta_V$ where η_V is the dual isomorphism. Therefore ψ_L is an isomorphism if and only if ψ_R^* is an isomorphism, and by 3.4.61 if and only if ψ_R is an isomorphism. Since η_V is surjective we have $\text{rank}_k(\psi_L) = \text{rank}_k(\psi_R^*) = \text{rank}_k(\psi_R)$, by 3.4.60. \square

3.5 Localization

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

Recall the definition of multiplicative set. Some rather canonical examples are as follows

Example 3.5.1

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

Example 3.5.2

If $\mathfrak{p} \triangleleft A$ is a prime ideal, then $A \setminus \mathfrak{p}$ is a saturated multiplicative set. More generally, we show later that S is a saturated multiplicative set if and only if it's of the form

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

for some family of prime ideals.

3.5.1 Rings

Definition 3.5.3 (Localization of a ring)

Let A be a ring and S a multiplicative set. Define the set

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

under the equivalence relation

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

then this is a ring in the obvious way

Definition 3.5.4 (Localization of an ideal)

Let A be a ring and S a multiplicative set and $\mathfrak{a} \triangleleft A$ 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 3.5.1

The set $S^{-1}A$ is a ring under the obvious ring operations. It is non-zero precisely when S is proper. There is a canonical homomorphism

$$\begin{aligned} i_S : A &\rightarrow S^{-1}A \\ a &\rightarrow \left[\frac{a}{1} \right] \end{aligned}$$

- $i_S(a) = 0 \iff sa = 0$ for some $s \in S$
- $S^{-1}A$ is the zero-ring if and only if $0 \in S$ if and only if there exists $s, t \in S$ such that $st = 0$.
- $i_S(s)$ is invertible for all $s \in S$
- i_S is injective if and only if S has no zero-divisors
- This is an isomorphism if and only if $S \subseteq A^*$ already consists only of invertible elements (e.g. $S = \{1\}$).

Proof. • This follows by the definitions

- $1/1 = 0/0 \iff s = 0$ for some $s \in S$ by the definitions
- $\frac{s}{1} \frac{1}{s} = \frac{s}{s} = \frac{1}{1}$

- This follows from the first part.
- If $S \subseteq A^*$ then it contains no zero-divisors and i_S is injective. Further it's clear that $\frac{a}{s} = \frac{as^{-1}}{1}$ so that the map is surjective. Similarly if the map is bijective S does not contain zero-divisors and $\frac{1}{s}$ is in the image. Therefore there is a such that $tas = 1$ for some t , which implies s is invertible.

□

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

Proposition 3.5.2 (Universal Property)

Let $\phi : A \rightarrow B$ be a ring homomorphism and S a multiplicative set. Then

- There is a unique morphism $\tilde{\phi}$ making the diagram commute

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

if and only if $\phi(S) \subseteq B^*$. In this case it's given by

$$\tilde{\phi}\left(\frac{a}{s}\right) = \phi(a)\phi(s)^{-1}$$

- $\ker(\tilde{\phi}) = S^{-1}\ker(\phi)$

Proof. • If $\tilde{\phi}$ exists then $1 = \tilde{\phi}(1) = \tilde{\phi}\left(\frac{s}{1}\frac{1}{s}\right) = \tilde{\phi}\left(\frac{s}{1}\right)\tilde{\phi}\left(\frac{1}{s}\right) = \phi(s)\tilde{\phi}\left(\frac{1}{s}\right)$. Which shows that $\phi(S) \subseteq B^*$ and $\phi(s)^{-1} = \tilde{\phi}\left(\frac{1}{s}\right)$.

Conversely suppose $\phi(S) \subseteq B^*$ 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

$$\begin{aligned} \tilde{\phi}\left(\frac{a}{s} + \frac{b}{t}\right) &= \tilde{\phi}\left(\frac{at + bs}{st}\right) \\ &= \phi(at + bs)\phi(st)^{-1} \\ &= \phi(a)\phi(t)\phi(s)^{-1}\phi(t)^{-1} + \phi(b)\phi(s)\phi(s)^{-1}\phi(t)^{-1} \\ &= \phi(a)\phi(s)^{-1} + \phi(b)\phi(t)^{-1} \\ &= \tilde{\phi}\left(\frac{a}{s}\right) + \tilde{\phi}\left(\frac{b}{t}\right) \end{aligned}$$

- Suppose $\tilde{\phi}\left(\frac{a}{s}\right) = 0$ then clearly $a \in \ker(\phi) \implies \frac{a}{s} \in S^{-1}\ker(\phi)$. The converse is clear.

□

In the case that A is an integral domain then generally everything becomes a lot simpler.

Example 3.5.5 (Field of fractions)

Let A be an integral domain then $A \setminus 0 = A^*$ and we define the field of fractions

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

Proposition 3.5.3 (Field of fractions contains all localization)

Let A be an integral domain, and $\text{Frac}(A)$ the field of fractions. Define another model for $S^{-1}A$ as follows

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

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

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

□

Proposition 3.5.4 (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

$$\varinjlim_i S_i^{-1} A \rightarrow S^{-1} A$$

induced by the canonical maps

$$S_i^{-1} A \rightarrow S^{-1} A$$

Proof. The canonical maps $i_{S_i, S}$ induce a unique morphism

$$\begin{aligned} \varinjlim_i S_i^{-1} A &\longrightarrow S^{-1} A \\ [a_i/s_i] &\longrightarrow a_i/s_i \end{aligned}$$

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. \square

3.5.2 Modules**Definition 3.5.6** (Localization of a module)

Let A be a ring with S multiplicative set and M an A -module. Then we define

$$S^{-1} M = \left\{ \frac{m}{s} \mid m \in M \right\}$$

under the obvious equivalence relation. This is then an $S^{-1} A$ -module in the obvious way.

Definition 3.5.7 (Localization of a sub-module)

Let M be an A -module and $N \subseteq M$ a sub- A -module then define

$$S^{-1} N = \left\{ \frac{n}{s} \mid n \in M, s \in S \right\} \subseteq S^{-1} M$$

Proposition 3.5.5

$S^{-1}(-)$ constitutes a functor $A - \mathbf{Mod} \rightarrow S^{-1} A - \mathbf{Mod}$. More precisely there is a unique morphism ψ making the following diagram commute as A -module morphisms

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

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

It is an exact functor; for an exact sequence

$$N \rightarrow M \rightarrow P$$

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

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

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

Proposition 3.5.6 (Localization commutes with quotients)

There is a commutative diagram of A -module morphisms

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \xrightarrow{i} & M & \xrightarrow{\pi} & M/N \longrightarrow 0 \\ & & \downarrow i_S & & \downarrow i_S & & \downarrow \\ 0 & \longrightarrow & S^{-1} N & \longrightarrow & S^{-1} M & \xrightarrow{S^{-1}(\pi)} & S^{-1}(M/N) \longrightarrow 0 \end{array}$$

with exact rows and the bottom row consists of $S^{-1} A$ -module morphisms. This induces an isomorphism of $S^{-1} A$ -modules.

$$S^{-1} M / S^{-1} N \cong S^{-1}(M/N)$$

Proposition 3.5.7

Suppose $N \subseteq N' \subseteq M$ then there is a canonical short-exact sequence of $S^{-1}A$ -modules

$$0 \rightarrow S^{-1}(N'/N) \rightarrow S^{-1}(M/N) \rightarrow S^{-1}(M/N') \rightarrow 0$$

which induces an isomorphism

$$S^{-1}(M/N)/S^{-1}(N'/N) \cong S^{-1}(M/N')$$

3.5.3 Ideals

Recall the notion of extended and contracted ideals in Definition 3.4.24.

Definition 3.5.8 (Localization of an ideal)

Let A be a ring, S a multiplicative set and \mathfrak{a} an ideal. Then define

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

an ideal of $S^{-1}A$.

Proposition 3.5.8 (Extension and Contraction)

Let A be a ring with multiplicative set S and canonical morphism $i_S : A \rightarrow S^{-1}A$.

1. $\mathfrak{a}^e = \left\{ \frac{a}{s} \mid a \in \mathfrak{a}, s \in S \right\} = S^{-1}\mathfrak{a}$
2. $\mathfrak{b}^c = \left\{ a \mid \frac{a}{1} \in \mathfrak{b} \right\}$
3. 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

$$as \in \mathfrak{a} \wedge s \in S \implies a \in \mathfrak{a}$$

4. \mathfrak{b} proper $\iff \mathfrak{b}^c$ proper $\iff \mathfrak{b}^c \cap S = \emptyset$
5. \mathfrak{a}^e proper $\iff \mathfrak{a} \cap S = \emptyset$
6. Every ideal $\mathfrak{b} \triangleleft S^{-1}A$ is extended (equiv. $\mathfrak{b} = \mathfrak{b}^{ce} = S^{-1}\mathfrak{b}^c$).
7. 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. .

1. $S^{-1}\mathfrak{a}$ 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.
2. This is clear
3. 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 Proposition 3.4.16 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.

4. This first equivalence is true in general, see Proposition 3.4.16. Clearly $\mathfrak{b}^c = A \implies \mathfrak{b}^c \cap S \neq \emptyset$. Similarly if $S \cap \mathfrak{b}^c \neq \emptyset$ then $s \in \mathfrak{b}^c \implies \frac{s}{1} \in \mathfrak{b} \implies 1 \in \mathfrak{b} \implies 1 \in \mathfrak{b}^c$.
5. By 4. \mathfrak{a}^e is proper if and only if \mathfrak{a}^{ec} is proper. By 3. we see $1 \in \mathfrak{a}^{ec}$ if and only if $S \cap \mathfrak{a} \neq \emptyset$ and the result follows.
6. By Proposition 3.4.16 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.

7. If $\mathfrak{p} \cap S = \emptyset$ then by primality it automatically satisfies the conditions in 3. and is therefore contracted. Conversely if a prime ideal \mathfrak{p} is contracted then $\mathfrak{p} = \mathfrak{q}^c$. It is by definition proper so by 4. it satisfies $\mathfrak{p} \cap S = \emptyset$ as required.

Suppose $\frac{a}{s} \frac{b}{t} \in \mathfrak{p}^e$ then $\frac{ab}{st} = \frac{x}{u}$ for $x \in \mathfrak{p} \implies v(abu - xst) = 0 \implies uvab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Therefore $\frac{a}{s} \in \mathfrak{p}^e$ or $\frac{b}{t} \in \mathfrak{p}^e$ as required.

Generically \mathfrak{q}^c is a contracted prime ideal and we've already shown in 4. that $\mathfrak{q}^c \cap S = \emptyset$.

□

Corollary 3.5.9 (Ideal Structure Localization)

Let A be a ring and S a multiplicative set then there is a bijection of proper ideals

$$\{\mathfrak{a} \triangleleft A \mid \mathfrak{a} \text{ contracted}\} \longleftrightarrow \{\mathfrak{b} \triangleleft S^{-1}A\}$$

which restricts to a bijection of prime ideals

$$\{\mathfrak{p} \triangleleft A \mid \mathfrak{p} \cap S = \emptyset\} \longleftrightarrow \{\mathfrak{q} \triangleleft S^{-1}A\}$$

Proof. From Proposition 3.5.8 every ideal of $S^{-1}A$ is extended. Therefore the bijection of proper ideals follows from Corollary 3.4.17. For prime ideals each direction is well-defined by 3.5.8 7. □

3.5.4 Change of Rings

For what follows it is useful to have the concept of saturation of a multiplicatively closed set. Essentially taking the saturation \bar{S} of S doesn't change the ring $S^{-1}A$.

Proposition 3.5.10 (Saturation)

Let A be a ring and S a multiplicatively closed set. Then the following sets are equal

- $(i_S)^{-1}((S^{-1}A)^*)$
- $\{t \mid at \in S \text{ for some } a \in A\}$
- $\bigcap_{T \supseteq S: T \text{ saturated}} T$

which we denote by \bar{S} . We have the following properties

- \bar{S} is saturated.
- S is saturated if and only if $S = \bar{S}$
- $\bar{\bar{S}} = \bar{S}$.

Proof. TODO

□

We also give another characterization of saturated multiplicatively closed subsets

Proposition 3.5.11

Let A be a ring and S a multiplicatively closed subset. Then

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

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

Conversely suppose $a \notin \bar{S}$. Consider the principal ideal (a) then $(a) \cap S = \emptyset$ (because $ab \in S \implies a \in \bar{S}$ by Proposition 3.5.10). Therefore by Lemma 3.4.12 there is a prime ideal \mathfrak{p} containing a which does not intersect S . Therefore $a \notin T$. We have shown that $a \notin \bar{S} \implies a \notin T$, contrapositively $T \subseteq \bar{S}$ as required. □

Proposition 3.5.12 (Change of Rings)

Let $\phi : A \rightarrow B$ be a ring homomorphism, S, T corresponding multiplicative subsets. Then

- There exists a unique morphism $\tilde{\phi}$ making the diagram commute

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

if and only if $\phi(S) \subseteq \overline{T}$. In this case it's given by

$$\tilde{\phi}\left(\frac{a}{s}\right) = \frac{\phi(a)b'}{\phi(s)b'}$$

where $b' \in B$ is any b' such that $\phi(s)b' \in T$.

- If in addition $T \subseteq \phi(\overline{S})$ then 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 the previous Proposition the morphism exists making the diagram commute.

Note that

$$\tilde{\phi}\left(\frac{a}{s}\right) = \tilde{\phi}(i_S(a)i_S(s)^{-1}) = \tilde{\phi}(i_S(a))\tilde{\phi}(i_S(s))^{-1}$$

so it is uniquely defined by the commutativity condition. Note that given $s \in S$ by (...) there exists $b' \in B$ such that $\phi(s)b' \in T$. In this case it's clear that $i_T(\phi(s))^{-1} = \frac{b'}{\phi(s)b'}$ from which the explicit form results.

- Suppose $T \subseteq \phi(\overline{S})$ and 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 3.5.13

Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be a sequence of homomorphisms and S, T, U be multiplicative sets such that $\phi(S) \subseteq \overline{T}$ and $\psi(T) \subseteq \overline{U}$, then in the notation of the previous Proposition

$$\tilde{\psi} \circ \tilde{\phi} = \widetilde{\psi \circ \phi}$$

Proof. This follows from the uniqueness condition in the previous Proposition. □

Corollary 3.5.14 (Localization Maps)

Let A be a ring and S, T two multiplicative sets. Then TFAE

- There exists $i_{ST} : S^{-1}A \rightarrow T^{-1}A$ such that $i_{ST} \circ i_S = i_T$
- $S \subseteq \overline{T}$

In this case i_{ST} is the unique such map. We have the transitivity relationships

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

$$i_{SS} = \mathbf{1}_{S^{-1}A}$$

and furthermore i_{ST} is an isomorphism if and only if $\overline{S} = \overline{T}$. In particular $i_{S\overline{S}}$ is an isomorphism.

Proof. This largely follows from the previous Proposition when considering the map $\phi = 1_A$. The transitivity and reflexive relationships follow from the uniqueness condition. □

Corollary 3.5.15 (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

$$\begin{array}{ccc}
A & \xrightarrow{\pi} & A/\mathfrak{a} \\
\downarrow i_S & & \downarrow i_{\pi(S)} \\
S^{-1}A & & \\
\downarrow \pi & & \\
S^{-1}A/S^{-1}\mathfrak{a} & \xrightarrow{\sim} & \pi(S)^{-1}(A/\mathfrak{a})
\end{array}$$

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

$$\begin{array}{ccc}
\mathfrak{b} & \xrightarrow{\pi} & \mathfrak{b}/\mathfrak{a} \\
\downarrow i_S & & \downarrow i_{\pi(S)} \\
S^{-1}\mathfrak{b} & & \\
\downarrow \pi & & \\
S^{-1}\mathfrak{b}/S^{-1}\mathfrak{a} & \xrightarrow{\sim} & \pi(S)^{-1}(\mathfrak{b}/\mathfrak{a})
\end{array}$$

and the bottom arrow is still an isomorphism of $S^{-1}A/S^{-1}\mathfrak{a}$ -modules.

Corollary 3.5.16 (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

$$\begin{array}{ccc}
A & \xrightarrow{\pi} & A/\mathfrak{a} \\
\downarrow i_S & & \downarrow \\
S^{-1}A & \xrightarrow{\pi} & S^{-1}A/S^{-1}\mathfrak{a}
\end{array}$$

given by

$$a + \mathfrak{a} \rightarrow \frac{a}{1} + S^{-1}\mathfrak{a}$$

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

$$\begin{array}{ccc}
\mathfrak{b} & \xrightarrow{\pi} & \mathfrak{b}/\mathfrak{a} \\
\downarrow i_S & & \downarrow \\
S^{-1}\mathfrak{b} & \xrightarrow{\pi} & S^{-1}\mathfrak{b}/S^{-1}\mathfrak{a}
\end{array}$$

which is an A/\mathfrak{a} -module morphism, and is an isomorphism when the condition (...) holds.

Proof. □

Proposition 3.5.17 (Transitivity)

Let $S \subset T$ be multiplicative subsets of A and let

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

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

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

3.5.5 Localization at an element

Definition 3.5.9 (Localization at an element)

Let A be a ring and $f \in A$. Then define

$$S_f = \{1, f, \dots, f^n, \dots\}$$

and

$$A_f := (\overline{S_f})^{-1} A$$

where we have canonical map

$$i_f : A \rightarrow A_f$$

given by $i_f = i_{\overline{S_f}}$.

Proposition 3.5.18 (Transition maps for localization at an element)

Let A be a ring and $f, g \in A$ then

$$\overline{S_f} \subseteq \overline{S_g} \iff f \mid g^N \text{ some } N > 0$$

in this case define $i_{fg} = i_{\overline{S_f} \overline{S_g}}$ to be the unique morphism such that $i_{fg} \circ i_f = i_g$. In addition if $h \in A$ and $\overline{S_g} \subseteq \overline{S_h}$ we have a commutative diagram

$$\begin{array}{ccccc} & & A & & \\ & i_f \swarrow & \downarrow i_g & \searrow i_h & \\ A_f & \xrightarrow{i_{fg}} & A_g & \xrightarrow{i_{gh}} & A_h \\ & \searrow i_{fh} & & \nearrow i_{gh} & \end{array}$$

Furthermore $\overline{S_1} = A^*$ and i_1 is an isomorphism.

Proposition 3.5.19 (Transitivity of localizing at elements)

Let A be a ring and $f, g \in A$ such that $\overline{S_f} \subseteq \overline{S_g}$. Then $i_f(\overline{S_g}) = \overline{S_{g/1}}$ as multiplicatively closed subsets of A_f . Therefore there is a canonical isomorphism

$$(A_f)_{g/1} \longrightarrow A_g$$

Furthermore $\overline{S_g} \subseteq \overline{S_h} \iff \overline{S_{g/1}} \subseteq \overline{S_{h/1}}$ and there is a commutative diagram

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

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

Proof. Firstly let $S'_g := \overline{i_f(\overline{S_g})}$, which is a saturated multiplicatively closed set containing $g/1$, whence $S_{g/1} \subseteq S'_g$ and $\overline{S_{g/1}} \subseteq S'_g$ by Proposition 3.5.10. Suppose $h \in S'_g$ then $ah = b/1$ for $b \in \overline{S_g}$ whence $a'h = g^N/1$ and $h \in \overline{S_{g/1}}$. Therefore $i_f(\overline{S_g}) = \overline{S_{g/1}}$ as required.

Suppose we have $\overline{S_f} \subseteq \overline{S_g}$ and $\overline{S_f} \subseteq \overline{S_h}$. We claim that $\overline{S_g} \subseteq \overline{S_h} \iff \overline{S_{g/1}} \subseteq \overline{S_{h/1}}$. Note the former implies $g \mid h^N \implies g/1 \mid (h/1)^N$ which implies the latter. Conversely suppose $g/1 \mid h^N/1$ then $ag/f^r = h^N/1 \implies f^s(ag - f^r h^N) = 0$. But similarly $f \mid h^M$ so we find $g \mid h^N$ for some suitably large N and $\overline{S_g} \subseteq \overline{S_h}$.

The required isomorphisms and commutative diagrams follow from Proposition 3.5.17. \square

3.5.6 Localization at a prime ideal

Definition 3.5.10 (Localization at a prime ideal)

Let A be a ring and $\mathfrak{p} \triangleleft A$ a prime ideal. Then $A \setminus \mathfrak{p}$ is a saturated multiplicatively closed subset, and we define

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} A$$

For an ideal $\mathfrak{a} \triangleleft A$ write the extended ideal

$$\mathfrak{a}^e = S^{-1} \mathfrak{a} =: \mathfrak{a} A_{\mathfrak{p}}$$

Proposition 3.5.20

Let A be a ring and \mathfrak{p} a prime ideal. Consider the localization $A \rightarrow A_{\mathfrak{p}}$. Then there is a bijection between prime ideals contained in \mathfrak{p} and prime ideals of $A_{\mathfrak{p}}$

$$\begin{aligned} \{\mathfrak{q} \triangleleft A \mid \mathfrak{q} \subseteq \mathfrak{p}\} &\longleftrightarrow \{\mathfrak{q} \triangleleft A_{\mathfrak{p}}\} \\ \mathfrak{q} &\longrightarrow \mathfrak{q} A_{\mathfrak{p}} \end{aligned}$$

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 Corollary 3.5.9. \square

Proposition 3.5.21 (Localization at prime is direct limit of localization at an element)

Let A be a ring and \mathfrak{p} a prime ideal then

$$S_{\mathfrak{p}} := A \setminus \mathfrak{p} = \bigcup_{f \in A \setminus \mathfrak{p}} \overline{S_f}$$

Therefore there are canonical morphisms (for $f \notin \mathfrak{p}$)

$$i_{\overline{S_f} S_{\mathfrak{p}}} : A_f \longrightarrow A_{\mathfrak{p}}$$

Furthermore the family of multiplicatively closed sets $\{\overline{S_f}\}_{f \notin \mathfrak{p}}$ (resp. rings $\{A_f\}_{f \notin \mathfrak{p}}$) form a directed system. Therefore we have a canonical morphism

$$\varinjlim_{f \notin \mathfrak{p}} A_f \longrightarrow A_{\mathfrak{p}}$$

which is an isomorphism.

Proof. As $A \setminus \mathfrak{p}$ is a saturated multiplicatively closed set we have $f \in A \setminus \mathfrak{p} \iff S_f \subseteq A \setminus \mathfrak{p} \iff \overline{S_f} \subseteq A \setminus \mathfrak{p}$.

The family of multiplicatively closed subsets is a directed system because $\overline{S_f} \subseteq \overline{S_{fg}} \implies f \in \overline{S_{fg}} \implies S_f \subseteq \overline{S_{fg}} \implies \overline{S_f} \subseteq \overline{S_{fg}}$.

The rest follows from Proposition 3.5.4. \square

3.6 Polynomial Rings in One Variable

Definition 3.6.1

Let A be a ring. The polynomial ring $A[X]$ is an A -algebra consisting of formal sums

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

such that only finitely many a_i are non-zero. Define degree in the obvious way

$$\deg(f) = \inf\{n \mid m > n \implies a_m = 0\} < \infty$$

and the leading coefficient to be $c(f) := a_{\deg(f)}$. By convention $\deg(0) = -\infty$. We say f is monic if the leading coefficient is 1.

Addition is defined in the obvious way and multiplication is defined by

$$f(X)g(X) = \sum_{d=0}^{\infty} \left(\sum_{i+j=d} a_i b_j \right) X^d$$

It's associative because

$$f(X)g(X)h(X) = \sum_{d=0}^{\infty} \left(\sum_{i+j+k=d} a_i b_j c_k \right) X^d$$

Lemma 3.6.1

If A is an integral domain then for elements $f, g \in A[X]$

$$\deg(fg) = \deg(f) + \deg(g)$$

$$c(fg) = c(f)c(g)$$

Further $A[X]$ is an integral domain.

Proposition 3.6.2 (Nilpotent and Invertible Polynomials)

Let A be a ring then

1. $\mathfrak{N}(A[X]) = \mathfrak{N}(A)[X] \subset A[X]$
2. $A[X]^* = A^* + X\mathfrak{N}(A)[X]$

Proof. Suppose $a \in \mathfrak{N}(A)$ then clearly aX^i is nilpotent. Therefore $\mathfrak{N}(A)[X] \subseteq \mathfrak{N}(A[X])$ since the nilradical is an ideal. Conversely suppose $f \in A[X]$ is nilpotent, i.e. $f^n = 0$. For any prime ideal $\mathfrak{p} \triangleleft A$ we find that $\bar{f}^n = 0$ as an element of $(A/\mathfrak{p})[X]$. As A/\mathfrak{p} is an integral domain we have by the previous Lemma $\bar{f} = 0$. As \mathfrak{p} is arbitrary and $\mathfrak{N}(A) = \bigcap \mathfrak{p}$ we see that $f \in \mathfrak{N}(A)[X]$ as required.

Suppose $f \in A[X]^*$ 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 $A[X]^* \subseteq A^* + X\mathfrak{N}(A)[X]$. Conversely it's a general fact that $B^* + \mathfrak{N}(B) \subseteq B^*$, for if

$$f = a + g$$

with $g^r = 0$ and $a \in B^*$ then one may check that

$$f^{-1} = (a^{-1} - a^{-2}g + a^{-3}g^2 - \dots + (-1)^{r-1}a^{-r}g^{r-1})$$

□

It satisfies the following universal property

Proposition 3.6.3 (Evaluation at a point)

Consider an A -algebra B and $b \in B$. Then there exists a unique A -algebra homomorphism

$$\text{ev}_b : A[X] \rightarrow B$$

such that $\text{ev}_b(X) = b$. We write $p(b) = \text{ev}_b(p)$. 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 $\phi : B \rightarrow C$ such that $\phi(b) = c$ we have

$$\phi \circ \text{ev}_b = \text{ev}_c$$

Remark 3.6.2

In categorical jargon $A[X]$ is an initial object in the category of pointed A -algebras.

Proposition 3.6.4 (Evaluation commutes with algebra homomorphism)

Let $\phi : B \rightarrow C$ be a homomorphism of A -algebras and $p \in A[X]$ then

$$\phi(p(b)) = p(\phi(b))$$

Definition 3.6.3 (Conjugate polynomial)

Let $\phi : A \rightarrow B$ 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

$$A[X] \rightarrow B[X]$$

and has the property that

$$f^\phi(\phi(a)) = \phi(f(a))$$

Proposition 3.6.5 (Division Algorithm I)

Let A be an integral domain and $f(X) \in A[X]$ a polynomial and $g(X) \in A[X]$ a non-zero monic polynomial. Then there exists $q(X)$ and $r(X)$ such that

$$f(X) = q(X)g(X) + r(X)$$

and $\deg(r) < \deg(g)$. In particular when $\deg(g) = 1$ then $r \in A$.

Proof. If $\deg(f) < \deg(g)$ then $q = 0$ and $r = f$. Otherwise assume $n = \deg(f) \geq \deg(g) = m$ and proceed by induction on n . Note that since g is monic then we have $f - c(f)gX^{n-m}$ has degree $n - 1$, so by induction

$$f - c(f)gX^{n-m} = q'g + r$$

with $\deg(r) < \deg(g)$. Therefore

$$f = (q' + c(f)X^{n-m})g + r$$

as required. □

3.7 Polynomial Rings in Many Variables

Definition 3.7.1

Let A be a ring then the polynomial ring $A[X_1, \dots, X_n]$ consists of formal sums of monomials

$$f(X_1, \dots, X_n) = \sum_{v \in \mathbb{N}^n} f_v X_1^{v_1} \dots X_n^{v_n}$$

where $f_v \in A$ and only finitely many coefficients are non-zero. Addition is defined in the obvious way. Multiplication is defined as

$$\left(\sum_v f_v X^v \right) \left(\sum_w g_w X^w \right) := \sum_z \left(\sum_{v,w: v+w=z} f_v g_w \right) X^z$$

We may canonically regard A , $A[X_i]$ and $A[X_1, \dots, X_i]$ as subrings in the obvious way.

Define to be the maximal degree in X_n to be

$$\deg(f, n) := \operatorname{argmax}_{v_n} \{n \mid f_{v_1, \dots, v_n} \neq 0 \text{ some } v_1, \dots, v_{n-1} \in \mathbb{N}\}$$

Remark 3.7.2

It may be useful for certain induction arguments to write

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

when $n = 0$.

Proposition 3.7.1 (Universal Property)

$A[X_1, \dots, X_n]$ satisfies the following universal property. Given any A -algebra B and points (b_1, \dots, b_n) there exists morphism

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

such that

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

given by

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

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

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

Lemma 3.7.2 (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

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

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

Proof. Define $g_i = \sum_{v:v_n=i} f_v X_1^{v_1} \dots X_{n-1}^{v_{n-1}}$ □

Proposition 3.7.3 (Division Algorithm II)

Let $f \in A[X_1, \dots, X_n]$ and $g \in A[X_n]$ a monic polynomial. Then there exist polynomials $q, r \in A[X_1, \dots, X_n]$ such that

$$f = qg + r$$

such that $\deg(r, n) < \deg(g)$. In particular if $\deg(g) = 1$ then $r \in A[X_1, \dots, X_{n-1}]$ for $n > 1$ and $r \in A$ for $n = 1$.

Proof. Consider $F = \psi^{-1}(f)$ and $G = \psi^{-1}(g)$. Then $\deg(F) = \deg(f; n)$ and $\deg(G) = \deg(g)$. Therefore by the Division Algorithm 3.6.5 in $A[X_1, \dots, X_{n-1}][X_n]$ we have

$$F = QG + R$$

with $\deg(R) < \deg(F)$. Define $q = \psi(Q)$ and $r = \psi(R)$. Then we have

$$f = qg + r$$

with $\deg(r, n) < \deg(g)$ as required. □

3.8 Finiteness

Definition 3.8.1 (Noetherian)

We say an A -module M is Noetherian if every submodule is finitely generated as an A -module

We say a ring A is Noetherian if every ideal is finitely generated as an A -module (i.e. A is Noetherian as an A -module)

The following is useful

Proposition 3.8.1 (Ascending chain condition (ACC))

Let M be an A -module. The following are equivalent

- M is Noetherian
- Every ascending chain of submodules eventually terminates

Proof. □

Proposition 3.8.2 (Restriction of Scalars preserves finiteness)

Let $\phi: A \rightarrow B$ be a finite A -algebra and M a finite B -module. Then $[M]_\phi$ is a finite A -module.

Proof. We suppose that M is generated by m_1, \dots, m_n , and B is generated by b_1, \dots, b_m . Then we claim that the elements $b_i m_j$ generate $[M]_\phi$. □

3.9 Unique Factorization

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

Definition 3.9.1 (Associates)

We say two non-zero elements x and y are **associates** if $x = uy$ for some $u \in A^*$. We write $x \sim y$.

Lemma 3.9.1

The associate relation $x \sim y$ is an equivalence relation on $A \setminus \{0\}$.

Definition 3.9.2 (Irreducible element)

We say $0 \neq x$ is **irreducible** if $x = ab \implies a$ a unit or b a unit.

Definition 3.9.3 (Prime element)

We say $0 \neq p$ is prime if $p \mid ab \implies p \mid a$ or $p \mid b$.

Example 3.9.4

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

Lemma 3.9.2

Suppose A is an integral domain. Then $x \mid y \wedge y \mid x \iff x \sim y$.

Proof. We have $y = ax = aby \implies y(1 - ab) = 0$. Since A is an integral domain $1 = ab$, i.e. a is a unit as required. The converse is clear. □

Example 3.9.5

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 2.2.11).

The concept of associates is important to unique factorization, because we may only hope to have unique factorization upto multiplication by a unit.

Lemma 3.9.3

If $x \sim y$ are associates then x is irreducible iff y is

Proof. Suppose $x \sim y$ and x irreducible. If $y = ab$ then $x = abu \implies a$ a unit and bu a unit $\implies b$ a unit. Therefore y is irreducible as required. \square

Example 3.9.6

The units of \mathbb{Z} are $\{-1, 1\}$. Therefore n is irreducible (i.e. prime) iff $-n$ is.

Lemma 3.9.4 (Criterion for primality)

p is prime if and only if (p) is a prime ideal

Proof. Note $x \mid y \iff y \in (x)$. So in particular if p is prime then $xy \in (p) \implies p \mid xy \implies p \mid x$ or $p \mid y \implies x \in (p)$ or $y \in (p)$, whence (p) is prime.

Conversely if (p) is prime, then $p \mid xy \implies xy \in (p) \implies x \in (p)$ or $y \in p \implies p \mid x$ or $p \mid y$, so that p is prime. \square

Lemma 3.9.5 (Criterion for irreducibility)

Let A be an integral domain. Then f is irreducible if and only if (f) is maximal amongst principal ideals.

Proof. Suppose f is irreducible and $(f) \subseteq (g)$. Then $f = ag$ with either a a unit or g a unit. If a is a unit then $(f) = (g)$, and if g is a unit $(g) = A$. So the result follows.

Conversely TODO \square

Proposition 3.9.6 (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 Lemma 3.9.2 $p \sim a$ (resp. b) as required. \square

Definition 3.9.7 (Unique Factorization Domain (UFD) or Factorial Ring)

We say an integral domain A is factorial (or a UFD) if every element $0 \neq a$ may be represented as

$$a = u \prod_{i=1}^n p_i$$

for u a unit and p_i irreducible, and moreover this is unique in the sense that given another factorization

$$a = u' \prod_{i=1}^m p'_i$$

we have $n = m$ and $p_i \sim p'_{\psi(i)}$, for ψ a permutation on $\{1, \dots, n\}$.

Definition 3.9.8 (Atomic Ring)

*We say that A is **atomic** if it has a (not necessarily unique) decomposition into irreducible elements.*

Proposition 3.9.7

A Noetherian ring is atomic.

In fact we need only the weaker condition that any ascending chain of principal ideals terminates (ACCP).

Proof. \square

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

Proposition 3.9.8 (Atomic + AP \iff UFD)

The following are equivalent

- A is a UFD
- A is integral, atomic and (p irreducible $\implies p$ prime)

NB a ring satisfying irreducible \implies prime is referred to as an AP-domain.

Proof. Suppose A is a UFD. Then by definition it is atomic. Suppose p is an irreducible element and $p \mid ab$, then by uniqueness it must appear in the irreducible factorization of either a or b , so we are done.

Conversely suppose A is integral and atomic. We wish to show uniqueness of factorization, that is if

$$\prod_{i=1}^n p_i \sim \prod_{j=1}^m p'_j$$

then $n = m$ and $p_i \sim p'_{\sigma(i)}$ for some permutation σ . 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 $p_1 \mid \text{RHS}$, 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. \square

Furthermore it may be convenient in applications to count the multiplicities

Proposition 3.9.9 (Factorization with multiplicities)

Let A be a unique factorization domain, then for every element $0 \neq a \in A$ there is a factorization of the form

$$a = u \prod_{i=1}^n p_i^{r_i}$$

where $r_i > 0$ and none of the p_i are associate to each other. Furthermore this is essentially unique in the sense that given another such factorization we have $n = n'$, $r_i = r'_{\sigma(i)}$ and $p_i \sim p'_{\sigma(i)}$ for some permutation $\sigma \in S_n$.

Proof. Given a factorization into irreducible elements

$$a = u \prod_{i=1}^n p_i$$

Consider a representative set of irreducibles q_1, \dots, 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 $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$. Let $r_j = \#\pi^{-1}(j)$. Then we have that the set of irreducibles $\{p_1, \dots, p_n\}$ 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 $\sigma : I \rightarrow J$ such that $p_i \sim p'_{\sigma(i)}$, and $\tau : J \rightarrow I$ such that $p'_j \sim p_{\tau(j)}$. Which means that $p_i \sim p_{\tau(\sigma(i))}$ and $p'_j \sim p_{\sigma(\tau(j))}$. 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 $r_i = r'_{\sigma(i)}$. \square

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

Definition 3.9.9

Let A be a ring we say \mathcal{P} is a **representative set of irreducible elements** if

- No two elements $p, q \in \mathcal{P}$ are associate
- Every irreducible element $p \in A$ is associate to one in \mathcal{P}

Example 3.9.10

For \mathbb{Z} the positive primes are a canonical set of irreducible elements.

Corollary 3.9.10 (Canonical Factorization)

Let A be a UFD and let \mathcal{P} be a set of representative irreducible elements, then we may define a valuation function

$$v_{(-)}(-) : \mathcal{P} \times A \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$$

such that for all $0 \neq a \in A$ we have

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

This factorization is totally unique, and so v_p is additive in the sense that for a fixed irreducible $p \in \mathcal{P}$

$$v_p(ab) = v_p(a) + v_p(b)$$

Lemma 3.9.11 (Divisibility)

Suppose A is a UFD with a canonical factorization function v_p . Then $f \mid g$ iff $v_p(f) \leq v_p(g) \forall p$ iff $(g) \subseteq (f)$

3.10 Principal Ideal Domains

Definition 3.10.1

An integral domain A is a principal ideal domain (PID) if every ideal \mathfrak{a} is principal.

Proposition 3.10.1

Let A be a PID. An element $a \in A$ is irreducible if and only if (a) is maximal.

Proof. This follows from the definition of a PID and Lemma 3.9.5. □

Proposition 3.10.2

A PID is a Noetherian UFD.

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

Proof. Suppose we have an ascending chain of ideals

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots \subset \mathfrak{a}_n \dots$$

Clearly the union is again an ideal, which is also principal of the form (a) . We must have $a \in \mathfrak{a}_n$ for some n , whence it terminates after n . Therefore A is Noetherian by Proposition 3.8.1 and atomic by Proposition 3.9.7. By Proposition 3.9.8 it's enough to show that an irreducible element is prime.

Note that from previous results, and by hypothesis, we have

$$p \text{ irreducible} \xLeftrightarrow{3.10.1} (p) \text{ maximal} \xRightarrow{3.4.23} (p) \text{ prime} \xLeftrightarrow{3.9.4} p \text{ is prime}$$

Finally $p \text{ prime} \implies p \text{ irreducible}$ by Proposition 3.9.6 to complete the equivalences.

Every prime ideal is principal of the form (p) and we've already shown it's maximal. □

Proposition 3.10.3

\mathbb{Z} is a PID.

In particular an integer m is irreducible \iff it is prime and every prime ideal is maximal.

Proof. This follows from the well-ordering principle. Let \mathfrak{a} be an ideal with minimal positive element d . We claim $\mathfrak{a} = (d)$. By the division algorithm (or apply well-ordering principle to the coset $x + (d)$), for every $x \in \mathfrak{a}$ there is $0 \leq r < d$ and $q \in \mathbb{Z}$ such that

$$x = qd + r.$$

Clearly $r \in \mathfrak{a}$, whence by minimality $r = 0$ as required. □

Example 3.10.2

Let k be a field, then the ring of polynomials $k[X]$ is a PID, as shown in later.

Lemma 3.10.4 (Co-prime elements in a PID)

Let A be a PID, then x, y are coprime if and only if they have no non-invertible common divisors.

Proof. First suppose $(x, y) = A$, then $ax + by = 1$ and any common divisor d must divide 1 and therefore be invertible.

Conversely suppose $(x, y) \neq (1)$, since A is a PID it must equal (d) for some non-invertible d which is then a common divisor. □

3.11 Matrix Rings

Definition 3.11.1

Let A be a non-zero commutative ring. Define the set of matrices

$$\text{Mat}_{m,n}(A) = \{(E_{ij})_{i=1\dots n, j=1\dots m}\}$$

There is the standard multiplication operator

$$\text{Mat}_{m,n}(A) \times \text{Mat}_{n,p}(A) \rightarrow \text{Mat}_{m,p}(A)$$

If $\phi : A \rightarrow B$ is a ring homomorphism, then there is a pointwise map

$$\begin{aligned} \text{Mat}_{m,n}(A) &\rightarrow \text{Mat}_{m,n}(B) \\ E &\rightarrow E^\phi \end{aligned}$$

Matrices are concrete realisations of linear maps of finite free A -modules, as demonstrated in the next two Propositions.

Proposition 3.11.1 (Matrix by vector multiplication)

There is a canonical bijection of A -modules

$$\begin{aligned} \text{Mat}_{m \times n}(A) &\longrightarrow \text{Hom}_A(A^n, A^m) \\ E &\longrightarrow \widehat{E} : (v_j)_{j=1\dots n} \rightarrow \left(\sum_{j=1}^n E_{ij} v_j \right)_{i=1\dots m} \end{aligned}$$

under which matrix multiplication corresponds to composition of functions, that is

$$\widehat{E} \circ \widehat{F} = \widehat{EF}$$

Corollary 3.11.2 (Algebra of matrices)

The set of square matrices $\text{Mat}_{n,n}(A)$ forms an A -algebra under multiplication, with the structural morphism given by

$$a \longrightarrow aI_n$$

Similarly

Proposition 3.11.3 (Matrix representation of a morphism)

Let M, N be two finite free A -modules with bases $\mathcal{B}, \mathcal{B}'$ of order p and q respectively. Let $\phi \in \text{Mor}_A(M, N)$, then there is a unique matrix $[\phi]_{\mathcal{B}'}^{\mathcal{B}} \in \text{Mat}_{q \times p}(A)$ such that

$$\phi(m)_{\mathcal{B}'} = [\phi]_{\mathcal{B}'}^{\mathcal{B}} m_{\mathcal{B}}.$$

Explicitly it is characterized by the relationship

$$\phi(m_i) = \sum_{j=1}^q [\phi]_{ji} n_j \quad i = 1 \dots p$$

where $\mathcal{B} = \{m_1, \dots, m_p\}$ and $\mathcal{B}' = \{n_1, \dots, n_q\}$.

In addition if L is a finite free A -module with basis \mathcal{B}'' and $\psi \in \text{Mor}_A(N, L)$, then

$$[\psi \circ \phi]_{\mathcal{B}''}^{\mathcal{B}} = [\psi]_{\mathcal{B}''}^{\mathcal{B}'} [\phi]_{\mathcal{B}'}^{\mathcal{B}}$$

In particular we induce an A -module isomorphism

$$\begin{aligned} \text{End}_A(M, N) &\longrightarrow \text{Mat}_{n \times m}(A) \\ \phi &\longrightarrow [\phi]_{\mathcal{B}'}^{\mathcal{B}} \end{aligned}$$

for every pair of bases (which is an A -algebra isomorphism when $N = M$) and

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

is the identity matrix.

Corollary 3.11.4

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

Corollary 3.11.5 (Change of basis)

Let M be a finite free A -module and $\mathcal{B}, \mathcal{B}'$ bases then

$$[1_M]_{\mathcal{B}'} = \left([1_M]_{\mathcal{B}}\right)^{-1}$$

and

$$[\phi]_{\mathcal{B}'}^{\mathcal{B}'} = P[\phi]_{\mathcal{B}}^{\mathcal{B}} P^{-1}$$

where

$$P := [1_M]_{\mathcal{B}'}^{\mathcal{B}}$$

is invertible.

We may define determinants as follows

Definition 3.11.2 (Determinant of a Matrix)

Let A be a ring, then define the determinant of a square matrix $E \in \text{Mat}_{n \times n}(A)$ as follows

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

Proposition 3.11.6

The determinant satisfies a number of properties

- $\det(EF) = \det(E) \det(F)$
- $\det(I_n) = 1$
- $\det(PEP^{-1}) = \det(E)$

Proof. TODO

□

Proposition 3.11.7

Let $\phi : A \rightarrow B$ be a ring homomorphism and $E \in \text{Mat}_{n,n}(A)$, then

$$\det(E^\phi) = \phi(\det(E))$$

Definition 3.11.3

Let M be a finite free A -module and $\phi \in \text{End}_A(M)$, then define

$$\det(\phi) := \det([\phi]_{\mathcal{B}})$$

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

Proposition 3.11.8 (Adjoint Matrix)

Let $E \in \text{Mat}_n(A)$ then there exists an adjoint matrix E^{ad} such that

$$EE^{\text{ad}} = E^{\text{ad}}E = \det(E)I_n$$

Explicitly

$$E_{ij}^{\text{ad}} = (-1)^{i+j} \det(E_{(ji)})$$

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

Corollary 3.11.9 (Existence of an Inverse)

Let $E \in \text{Mat}_n(A)$ then E is invertible if and only if $\det(E) \neq 0$.

3.12 Polynomial ring over a field

Consider polynomials over a field k .

Proposition 3.12.1

Degree is multiplicative in the sense $0 \neq f, g$ we have

$$\deg(fg) = \deg(f) + \deg(g)$$

In particular $f \mid g \implies \deg(f) \leq \deg(g)$.

Proposition 3.12.2

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

Proposition 3.12.3 (Associate polynomials)

The following are equivalent for $0 \neq f, g$

- $f \sim g$
- $f = \lambda g$ for $\lambda \neq 0$
- $f \mid g$ and $g \mid f$

Proposition 3.12.4

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

Proof. **TODO** □

Proposition 3.12.5 (Division Algorithm over a field)

For k a field consider the polynomial ring $k[X]$. For every pair of polynomials $f(X), g(X)$ there exists unique polynomials $q(X)$ and $r(X)$ such that

$$f(X) = q(X)g(X) + r(X)$$

and $\deg(r) < \deg(g)$.

Proof. Apply Proposition 3.6.5 to $g/c(g)$, and multiply by $c(g)$ again. □

Proposition 3.12.6 (Polynomial ring is a PID)

Let k be a field, then $k[X]$ is a PID, and therefore a Noetherian UFD.

Proof. Let $(0) \neq \mathfrak{a}$ be an ideal and let $f \in \mathfrak{a}$ be a polynomial of minimal degree. We may assume it is monic. Any $g \in \mathfrak{a}$ may be represented as $f = qg + r$ by the division algorithm. Clearly $r \in \mathfrak{a}$, therefore by minimality $r = 0$, whence $g \in (f)$. □

Proposition 3.12.7 (Unique Factorization of Polynomials)

For the ring $k[X]$ the set of irreducible monic polynomials constitutes a representative set (Definition 3.9.9). Therefore we have a unique factorization

$$f = c(f) \prod_{p \text{ irreducible monic}} p^{v_p(f)}$$

such that

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

Proof. Proposition 3.12.4 shows that the irreducible monic polynomials constitute a representative set. Therefore the result follows from Corollary 3.9.10. Let u be the unit appearing in the factorization, it must be an element of k . Compare leading coefficients to see that $u = c(f)$. □

Lemma 3.12.8 (Roots and Multiplicity)

For $f \in k[X]$ a non-constant polynomial and $\alpha \in k$ we have

$$f(\alpha) = 0 \iff (X - \alpha) \mid f \iff v_{(X-\alpha)}(f) > 0$$

In this case $r := v_{(X-\alpha)}(f)$ is the multiplicity of the root α , and observe

$$f(X) = c(f)(X - \alpha)^r g(X)$$

with $g(\alpha) \neq 0$ (equivalently $v_{(X-\alpha)}(g) = 0$).

Proof. The right to left implication is obvious. Conversely by the division algorithm we may write

$$f(X) = f(\alpha) + (X - \alpha)Q(X)$$

Then if $f(\alpha) = 0$ we clearly have $v_{(X-\alpha)}(f) > 0$. Finally we may construct

$$g(X) = \prod_{p \neq (X-\alpha)} p^{v_p(f)}$$

It's clear that for every p appearing in the product $p(\alpha) \neq 0$ because otherwise we would have $(X - \alpha) \mid p$ and by irreducibility $(X - \alpha) = p$. Therefore $g(\alpha) \neq 0$ as required. □

Definition 3.12.1 (Splitting Polynomial)

Let K/k be a field extension and $f \in k[X]$. We say a polynomial f splits completely in K if the irreducible factorization of f^i in $K[X]$ is

$$f^i(X) = c(f^i) \prod_{i=1}^n (X - \alpha_i)^{r_i}$$

where α_i are the distinct roots of $f(X)$ in K and $r_i := v_{(X-\alpha_i)}(f^i)$ are the multiplicities. Equivalently f splits in K if

$$p \in K[X] \text{ irreducible} \wedge \deg(p) > 1 \implies v_p(f^i) = 0 \quad (3.4)$$

Observe that the number of roots counting multiplicities is $\deg(f)$

$$\deg(f) = \sum_{i=1}^n v_{(X-\alpha_i)}(f^i)$$

Corollary 3.12.9

A polynomial f has at most $\deg(f)$ roots

3.12.1 Separable Polynomials

We are interested in characterizing polynomials $f \in k[X]$ which do not have multiple roots in any extension field K/k . These are exactly the separable polynomials, and it useful to consider the formal derivative $f'(X)$ as follows

Proposition 3.12.10 (Criteria for Multiple Roots)

Let $f(X) \in k[X]$ be a polynomial and either $\text{char}(k) = 0$ or $r < \text{char}(k)$. Then $\alpha \in k$ is a root of multiplicity r precisely when

$$f(\alpha) = f^{(1)}(\alpha) = \dots = f^{(r-1)}(\alpha) = 0$$

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 Lemma 3.12.8

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

with $g(\alpha) \neq 0$ and r the multiplicity of the root. If $r = 1$, then $f^{(1)}(\alpha) = g(\alpha) \neq 0$ as required. If $r > 1$, then $f^{(1)}(X)$ has α as a root of multiplicity $r - 1$, so it follows by induction.

The second statement is simply the case $r = 1$. □

Definition 3.12.2 (Separable Polynomial)

A polynomial $f \in k[X]$ is separable if f and f' are coprime.

Proposition 3.12.11 (Separable Polynomial)

A separable polynomial $f \in k[X]$ has no multiple roots in any extension field K/k

Proof. Since $(f, f') = 1$ we have $af + bf' = 1$. Clearly f and f' have no common roots, and therefore f has no multiple roots by Proposition 3.12.10. □

Proposition 3.12.12

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 Lemma 3.10.4 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 Lemma 3.10.4. □

We can provide a partial converse to Proposition 3.12.11 by working in a large enough extension field

Proposition 3.12.13 (Separability)

Let K/k be a field extension and $f \in k[X]$ a polynomial which splits completely in K . Then TFAE

1. f is separable
2. f has no multiple roots in K
3. f has $\deg(f)$ distinct roots in K

Proof. Using the formula

$$\deg(f) = \sum_{i=1}^n v_{(X-\alpha_i)}(f)$$

we see easily that $3 \iff 2$. The previous Proposition shows that $1 \implies 2$.

Conversely suppose f is not separable, then by Lemma 3.10.4 f and f' must have a non-trivial common divisor h . Using 3.9.11 and (3.4) we see that h splits in K . Any root of h is a common root of f and f' in K , which by Proposition 3.12.10 is a multiple root of f in K . □

3.13 Cayley-Hamilton Theorem

Definition 3.13.1 (Characteristic Polynomial of a Matrix)

For a matrix $E \in \text{Mat}_n(A)$ define the characteristic polynomial by

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

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

Definition 3.13.2 (Characteristic Polynomial of an endomorphism of a free module)

Let M be a finite free A -module. Define the characteristic polynomial of $\phi \in \text{End}_A(M)$ by

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

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

Adapted from Atiyah-Macdonald (...) but more explicit theorems

Theorem 3.13.1 (Cayley-Hamilton)

Let M be a finitely generated A -module and $\phi \in \text{End}_A(M)$ then there exists a monic polynomial $P(X) \in A[X]$ such that

$$P(\phi) = 0$$

When M is a finite free A -module then P may be taken to be the characteristic polynomial $P_\phi(X)$.

Proof. First since $\text{End}_A(M)$ is an A -algebra there is a canonical evaluation morphism

$$\text{ev}_\phi : A[X] \rightarrow \text{End}_A(M)$$

and the meaning of $P(\phi)$ is simply $\text{ev}_\phi(P)$.

Let $\{m_1, \dots, m_n\}$ be a generating set, then by definition

$$\phi(m_i) = \sum_j E_{ij} m_j$$

for some $E \in \text{Mat}_n(A)$. Consider the matrix

$$B(X) = XI_n - E \in \text{Mat}_n(A[X])$$

Then we may define $B(\phi) := B(X)^{\text{ev}_\phi} \in \text{Mat}_n(\text{End}_A(M))$ pointwise, so given by

$$B(\phi)_{ij} = \delta_{ij}\phi - E_{ij}1_M.$$

By definition

$$\sum_j B(\phi)_{ij} m_j = \phi(m_i) - \sum_j E_{ij} m_j = 0$$

Formally we have a group action

$$\text{Mat}_n(\text{End}_A(M)) \times M^n \rightarrow M^n$$

$$F \cdot (x_1, \dots, x_n)^T \rightarrow \left(\sum_{ij} F_{ij}(x_j) \right)_i$$

such that $(EF)v = E(Fv)$ (check).

And we have shown that

$$B(\phi)(m_1, \dots, m_n)^T = \mathbf{0}$$

Using Proposition 3.11.8, premultiply by the adjoint to show that

$$\det(B(\phi))I_n(m_1, \dots, m_n)^T = \mathbf{0}$$

and $\det(B(\phi)) \in \text{End}_A(M)$ annihilates m_1, \dots, m_n and therefore M .

Finally we claim that $P(X) := \det(B(X)) \in A[X]$ is a suitable monic polynomial. We see that

$$P(\phi) := \text{ev}_\phi(\det(B(X))) \stackrel{3.11.7}{=} \det(B(X)^{\text{ev}_\phi}) = \det(B(\phi)) = 0$$

When M is a finite free A -module then we may choose $\{m_1, \dots, m_n\}$ to be a basis, and then the matrix E equals $[\phi]^T$ as required. □

3.14 Finite-type Algebras

Definition 3.14.1 (Finite algebra)

An A -algebra B is finite if it is finite as an A -module.

Definition 3.14.2 (Finitely generated algebra)

An A -algebra B is finitely generated (or of finite type) if there exists an integer $n \in \mathbb{N}$ and a surjection of A -algebras

$$A[X_1, \dots, X_n] \rightarrow B$$

the images of X_i are the generators.

3.15 Integral Algebras

Definition 3.15.1 (Integral Element)

Let $\phi : A \rightarrow B$ be a ring homomorphism and $\alpha \in B$. Then we say α is integral over A if $m^\phi(\alpha) = 0$ for some monic polynomial $m(X) \in A[X]$.

Definition 3.15.2 (Ring Extensions)

Let $\phi : A \rightarrow B$ be a ring homomorphism. Then B is

- finite over A if it is finite as an A -module
- finite-type over A if it is finitely generated as an A -algebra
- integral over A if every element is 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.

Proposition 3.15.1

Let $\phi : A \rightarrow B$ be a ring map and $b \in B$. Then the following are equivalent

1. b is integral over A
2. $\phi(A)[b]$ is a finitely generated A -module
3. $\phi(A)[b]$ is contained in a subring C of B which is finitely generated as an A -module.
4. There exists a $\phi(A)[b]$ -module M which is faithful and finitely generated as a $\phi(A)$ -module.

Proof. Note C is a faithful module, so only non-trivial step is $4 \implies 1$. This is the usual “determinant trick”. We apply Theorem 3.13.1 by considering $\psi_b \in \text{End}_{\phi(A)}(M)$ to be multiplication by b . Then we have some monic polynomial $P(X) \in \phi(A)[X]$ such that $P(\psi_b) = 0$, whence $P(b)m = 0$ for all $m \in M$. Since M is faithful, then we have $P(b) = 0$ as required. \square

Corollary 3.15.2

Let b_i be elements of B integral over A then $A[x_1, \dots, x_n]$ is a finite A -module.

Proof. Apply the previous Proposition inductively by considering $A_r = A[x_1, \dots, x_r] = A_{r-1}[x_r]$. \square

Proposition 3.15.3 (Finite-type + integral \implies finite)

Let B be integral over A and $B = A[a_1, \dots, a_n]$ is finitely generated as an A -algebra then B is finitely generated as an A -module.

Proof. Consider a tower

$$A \subset A[b_1] \subset \dots \subset A[b_1, \dots, b_n] = B$$

We proceed inductively on n . Namely we assume that $A[b_1, \dots, b_i]$ is a finite A -module. Then a-fortiori $A[b_1, \dots, b_{i+1}]$ is integral over $A[b_1, \dots, b_i]$. Therefore by the previous Proposition it is a finite $A[b_1, \dots, b_i]$ -module and therefore a finite A -module (by Proposition 3.8.2) \square

Proposition 3.15.4 (Integral preserves Krull Dimension 0)

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

Proof. \square

3.16 Galois Theory

3.16.1 Algebraic Extensions

Definition 3.16.1 (Field Extension)

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.

We typically denote the structural morphism by $i_{kK} : k \rightarrow K$, and it is automatically injective (...). We may write (K, i_{kK}) if we need to stress the relevance of the structural morphism to the argument.

These objects form a category \mathbf{Field}_k in the obvious way. The morphisms may be called k -embeddings and we denote them by

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

and the set of automorphisms by

$$\mathrm{Aut}(K/k).$$

Observe every extension K/k may be viewed as a k -vector space so we define the degree of an extension field to be the vector space dimension

$$[K : k] := \dim_k K$$

Definition 3.16.2 (Finite field extension)

A field extension K/k is finite if $[K : k] < \infty$

Definition 3.16.3 (Tower of Field Extensions)

We may also consider a “tower” of extensions

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

with embeddings $i_{K_i K_{i+1}} : K_i \rightarrow K_{i+1}$, 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

$$\sigma_i : K_i \rightarrow M$$

they would commute with these embeddings. In particular we may abuse notation by defining $\sigma_i|_{K_j} = \sigma_i \circ i_{K_{i-1} K_i} \circ \dots \circ i_{K_j K_{j+1}}$.

Proposition 3.16.1

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 $\{l_i k_j\}_{i,j}$. In particular

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

Corollary 3.16.2

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

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

Definition 3.16.4 (Evaluation homomorphism)

Let L/k be a field extension and $\alpha \in K$. There is a canonical homomorphism

$$\mathrm{ev}_\alpha : k[X] \rightarrow K$$

$$\sum_{i=0}^n a_i X^i \rightarrow \sum_{i=0}^n i_{kK}(a_i) \alpha^i$$

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

Proposition 3.16.3 (Morphisms commute with evaluation)

Let $\sigma : K/k \rightarrow L/k$ 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 Proposition 3.6.4, The last statement is obvious, modulo the fact σ is injective (...). \square

Definition 3.16.5 (Subalgebra generated by a set)

Let K/k be a field extension and $S \subset K$ a finite subset. Recall $k[S]$ is the smallest sub-algebra containing S . When $S = \{\alpha_1, \dots, \alpha_n\}$ is finite then

$$k[\alpha_1, \dots, \alpha_n] = \text{im}(\text{ev}_\alpha) = \{p(\alpha_1, \dots, \alpha_n) \mid p \in k[X_1, \dots, X_n]\}$$

from the characterization from Proposition 3.7.1. In general then

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

Lemma 3.16.4 (Trivial result)

For $S, T \subset K/k$ finite

- $S \subset T \implies k[S] \subseteq k[T]$
- $k[S][T] = k[S \cup T]$

Proof. The first is obvious. For the second we wish to show

$$k[S][t] = k[S \cup \{t\}]$$

This essentially follows from Lemma 3.7.2. By induction it's true in general. □

Definition 3.16.6 (Subfield generated by a set)

Let K/k be a field extension and $S \subset K$ a subset. When $S = \{\alpha_1, \dots, \alpha_n\}$ is finite define

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

Clearly this is independent of the ordering on S . And in general

$$k(S) := \bigcup_{S' \subset S \text{ finite}} k(S')$$

It is the smallest subfield of K containing S .

Lemma 3.16.5 (Trivial result)

For $S, T \subset K/k$ finite

- $S \subset T \implies k(S) \subseteq k(T)$
- $k(S)(T) = k(S \cup T)$

Lemma 3.16.6

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

Proof. This follows from the characterization of $k(S)$ and $k[S]$ when S is finite. The infinite case then follows easily. □

Lemma 3.16.7 (Image of f.g. field extension)

Let K/k be a field extension and S a subset. If $\sigma : K/k \rightarrow L/k$ is a morphism then

$$\sigma(k(S)) = k(\sigma(S))$$

Proposition 3.16.8 (Uniqueness of morphisms on a generating set)

Let K/k be a field extension and $S \subset K$ a finite set. If $\sigma, \sigma' : k(S)/k \rightarrow L/k$ are morphisms of field extensions such that $\sigma|_S = \sigma'|_S$. Then $\sigma = \sigma'$.

Definition 3.16.7 (Simple Extension)

A field extension K/k is simple if $K = k(\{\alpha\}) =: k(\alpha)$ for some $\alpha \in K$.

Definition 3.16.8 (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)

We say an extension K/k is algebraic if every element $\alpha \in K$ is algebraic.

Proposition 3.16.9 (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 Proposition 3.4.41. Therefore there is a non-zero polynomial with α as a root. □

Proposition 3.16.10 (Endomorphisms are automorphisms)

Let $\sigma \in \text{Mor}_k(K, K)$ be an endomorphism of an algebraic extension. Then it is an isomorphism.

Proof. As field morphisms are injective (...) 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 Corollary 3.12.9 T is finite. Further by Proposition 3.16.3 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. \square

Proposition 3.16.11 (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 $(m_{\alpha,k}) = \ker(\text{ev}_\alpha)$.

Proof. Let $\mathfrak{a} = \ker(\text{ev}_\alpha)$. 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 Proposition 3.12.3 $m_{\alpha,k} = \lambda p$. In particular $\deg(m_{\alpha,k}(X)) = \deg(p(X))$ so $\deg(q(X)) = 0$ and $q(X)$ is a unit 3.12.2. Therefore by definition $m_{\alpha,k}(X)$ is irreducible.

Dividing by the leading coefficient we may assume that this polynomial is monic. Suppose $m'(X)$ is another such irreducible monic polynomial. Then $m_\alpha \mid m'$. Since m_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 $m' = m_\alpha$. \square

Definition 3.16.9 (Conjugate elements)

Two elements $\alpha, \beta \in K$ are said to be conjugate if they have the same minimal polynomial.

NB it's necessary and sufficient that $m_{\alpha,k}(\beta) = 0$.

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 3.16.12 (Construct simple extension)

Let $f \in k[X]$ be an irreducible polynomial. Then (f) is maximal and $K := k[X]/(f)$ is a field extension with canonical structural morphism. Define $\alpha := X + (f)$

- $f(\alpha) = 0$
- $K = k(\alpha)$ is a simple field extension and $k(\alpha) = k[\alpha]$
- $m_\alpha = f/c(f)$ and $\deg(m_\alpha) = \deg(f) =: n$
- K is a finite-dimensional k -vector space with basis

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

Example 3.16.10

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 $i : k \rightarrow k[X]$ and canonical surjective homomorphism

$$\pi : k[X] \rightarrow k[X]/(f)$$

and $\alpha = X + (f) = \pi(X)$. As $k[X]$ is a PID, f irreducible implies (f) maximal by Lemma 3.10.1 so K is a field by Proposition 3.4.22. 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 $\pi(p(X)) \stackrel{3.16.3}{=} p(\pi(X)) = p(\alpha)$. By Proposition 3.16.5 we see $K = k[\alpha]$. Since K is a field then $K = k[\alpha] = k(\alpha)$ is simple by Lemma 3.16.6.

Similarly $f(\alpha) = f(\pi(X)) \stackrel{3.16.3}{=} \pi(f(X)) = 0$, so α is a root of f . By Proposition 3.12.3 $f/c(f)$ is irreducible and by uniqueness in Proposition 3.16.11 we have $m_\alpha = f/c(f)$.

Given $\beta = p(\alpha)$, the division algorithm (...) yields

$$p(X) = q(X)f(X) + r(X)$$

with $\deg(r) < \deg(f) = n$. Therefore $\beta = r(\alpha)$ and the given set is spanning. A non-trivial linear dependence yields a non-zero polynomial $g(X)$ such that $g(\alpha) = 0$ and $\deg(g) < \deg(f)$. But by definition of the minimal polynomial $m_\alpha \mid g$ a contradiction by comparing degrees. Therefore the given set is linearly independent and hence a basis. \square

Conversely any simple algebraic extension is obtained in this way, as follows

Proposition 3.16.13 (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 $X + (m_\alpha) \rightarrow \alpha$. 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 Proposition 3.16.11, Definition 3.16.5 and Corollary 3.4.20 there is a canonical isomorphism $k[X]/(m_\alpha) \rightarrow k[\alpha]$ of k -algebras induced by the evaluation homomorphism $\text{ev}_\alpha : k[X] \rightarrow K$. Proposition 3.16.12 shows that the image of this isomorphism, $k[\alpha]$, is a field, whence $k[\alpha] = k(\alpha)$ by Lemma 3.16.6. Since a k -algebra isomorphism is a fortiori a k -vector space isomorphism it maps a basis to a basis. The result follows from Proposition 3.16.12 as the basis thus defined is the image of the basis in the proposition under the specified isomorphism. \square

Definition 3.16.11 (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 3.16.14 (Finitely generated by algebraic \implies finite and algebraic)

Let $K = k(\alpha_1, \dots, \alpha_n)/k$ be a field extension such that α_i is algebraic. Then K/k is a finite algebraic extension. Furthermore

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

In particular a finitely-generated algebraic extension is finite.

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

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

such that $K_i = K_{i-1}(\alpha_i)$ is a simple algebraic extension. By Proposition 3.16.13 K_i/K_{i-1} is finite. Therefore by Corollary 3.16.2 K/k is finite. By Proposition 3.16.9 it's also algebraic. For the second statement we may proceed inductively. Note we have

$$k[\alpha_1, \dots, \alpha_{i+1}] \stackrel{3.16.4}{=} k[\alpha_1, \dots, \alpha_i][\alpha_{i+1}] = k(\alpha_1, \dots, \alpha_i)[\alpha_{i+1}] \stackrel{3.16.13}{=} k(\alpha_1, \dots, \alpha_i)(\alpha_{i+1}) \stackrel{3.16.5}{=} k(\alpha_1, \dots, \alpha_{i+1})$$

The second equality is simply the inductive hypothesis. \square

Corollary 3.16.15

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. \square

The following is useful for reducing to cases of finite extensions where counting arguments work.

Lemma 3.16.16 (Reduce to finite extensions)

Let K/k be a field extension and $E \subset K$ 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
- $m_{\alpha,E} = m_{\alpha,E_0}$

Furthermore α is algebraic over k and $m_{\alpha,E_0} \mid m_{\alpha,k}^{i_{kK}}$.

Proof. Suppose

$$m_{\alpha,E}(X) = a_0 + a_1X + \dots + a_nX^n$$

Then define $E_0 = k(a_0, \dots, a_n)$. By Proposition 3.16.14 E_0/k is finite. Clearly α is algebraic over E_0 as it is a root of $m_{\alpha,E}$. By Proposition 3.16.11 $m_{\alpha,E_0} \mid m_{\alpha,E}$ as elements of $E_0[X]$ and $m_{\alpha,E} \mid m_{\alpha,E_0}$. Therefore $m_{\alpha,E_0} = m_{\alpha,E}$.

By Proposition 3.16.13 $E_0(\alpha)/E$ is finite, therefore $E_0(\alpha)/k$ is finite. By Proposition 3.16.9 $E_0(\alpha)/k$ is algebraic, whence α is algebraic over k . The last statement follows from Proposition 3.16.11 again. \square

Corollary 3.16.17

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

Proof. One direction is obvious. The converse follows from the previous result. \square

We may prove the first lifting theorem

Proposition 3.16.18 (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 $\sigma : k(\alpha)/k \rightarrow L/k$.

More precisely there is a bijective mapping

$$\text{Mor}_k(k(\alpha), L) \longrightarrow \{\beta \in L \mid m_{\alpha,k}(\beta) = 0\}$$

where

$$\sigma \rightarrow \sigma(\alpha)$$

and $\sigma(k(\alpha)) = k(\sigma(\alpha))$. In particular if $m_{\alpha,k}$ is separable and splits completely in L then there are precisely $\deg(m_{\alpha,k}) \stackrel{3.16.13}{=} [k(\alpha) : k]$ such extensions.

Proof. Observe $m_{\alpha,k}(\sigma(\alpha)) \stackrel{3.16.3}{=} \sigma(m_{\alpha,k}(\alpha)) = 0$. Therefore the mapping is well-defined. By Proposition 3.16.8 it is injective. We claim it is also surjective. By Proposition 3.16.13 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 Proposition 3.16.11. The final statement follows from Corollary 3.12.13 \square

3.16.2 Galois Theory Summary

Definition 3.16.12 (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
- 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 Proposition 3.12.13).

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

To summarize the main results

1. The group of automorphism of a normal extension K/k acts transitively on the roots of a given irreducible polynomial.
2. For K/k finite we have $\# \text{Aut}(K/k) \leq [K : k]$ with equality if and only if K/k is Galois.
3. An algebraic extension K/k is automatically separable whenever either $\text{char}(k) = 0$ or k is finite.
4. When K/k is finite and Galois then we have an order-reversing bijection between subfields and subgroups

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

We follow the approach in Lang72 and rephrase the concepts of “Normal” and “Separable” in terms of morphisms into an algebraic closure, i.e. the set $\text{Mor}_k(K, \bar{k})$. The first requires some work to set up the algebraic closure \bar{k} .

3.16.3 Algebraic Closure

Proposition 3.16.19 (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

If M is an extension field of k , then we say it is algebraically closed over k .

Definition 3.16.13 (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 3.16.20 (Existence of Algebraic Closure)

Given a field k there exists an algebraic closure \bar{k}/k

Proposition 3.16.21 (Generic Lifting Theorem)

Let K/k be a field extension. Suppose L/K is an algebraic extension and $\sigma : K \rightarrow M$ a k -embedding into an algebraically closed field. Then there exists an extension $\tilde{\sigma} : L \rightarrow M$. In other words there is a surjection

$$\text{Mor}_k(i_{KL}, M) : \text{Mor}_k(L, M) \rightarrow \text{Mor}_k(K, M)$$

Proof. Broadly speaking consider the poset of extensions to subfields of L ordered under consistency and take a maximal element by Zorn's Lemma. Apply Proposition 3.16.18 to show that this maximal element must be an extension to L .

If $[L : K] < \infty$, then we may simply proceed by induction on dimension. □

Corollary 3.16.22 (Unique up to isomorphism)

An algebraic closure \bar{k} of k is unique up to (non-unique) isomorphism.

Remark 3.16.14

Note if K/k is an algebraic extension then the Proposition shows that we may consider construct an embedding $K \rightarrow \bar{k}$ commuting with $k \rightarrow \bar{k}$.

In general given a tower of algebraic extensions

$$K = k_n / \dots / k_0 = k$$

we will assume the existence of compatible embeddings $i_{k_i} : k_i \rightarrow \bar{k}$ such that $i_{k_{i+1}} \circ i_{k_i, k_{i+1}} = i_{k_i}$.

Corollary 3.16.23 (Extension to algebraic closure II)

Let K/k be an algebraic extension and $i_K : K \rightarrow \bar{k}$ a k -embedding. Then every $\sigma : K \rightarrow \bar{k}$ lifts to $\sigma : \bar{k} \rightarrow \bar{k}$. i.e. there is a canonical surjection by restriction

$$\begin{aligned} \text{Mor}_k(i_K, \bar{k}) : \text{Aut}(\bar{k}/k) &\longrightarrow \text{Mor}_k(K, \bar{k}) \\ \sigma &\longrightarrow \sigma \circ i_K \end{aligned}$$

When i is inclusion then this is simply the restriction to K .

Proof. Given $\sigma \in \text{Mor}_k(K, \bar{k})$ there exists an extension $\tilde{\sigma} \in \text{Mor}_k(\bar{k}, \bar{k})$ by Proposition 3.16.21 with $L = M = \bar{k}$. This is automatically an automorphism by Proposition 3.16.10 as required. □

3.16.4 Separability

We follow Lang and not only characterize separability but define a “separability degree” which equals the extension degree if and only if it's separable. The proofs are somewhat technical, especially in light of the fact most base fields will be perfect.

Definition 3.16.15 (Separable element)

We say $\alpha \in K/k$ is separable over k if $m_{\alpha, k}(X)$ is a separable polynomial.

We say K/k is separable if every $\alpha \in K$ is separable.

Lemma 3.16.24

$\alpha \in K/k$ 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 $E \subset K$.

Proof. One direction is obvious. Conversely suppose $f(\alpha) = 0$ with f separable. Then $m_{\alpha,k} \mid f$ so the result follows from Proposition 3.12.12. \square

The main results of this section are the following

Proposition 3.16.25 (Separability Degree)

Let K/k be a finite extension and define the separability degree $[K : k]_s$ as

$$[K : k]_s = \# \text{Mor}_k(K, \bar{k})$$

1. It is independent of the choice of embedding into \bar{k}
2. It is multiplicative in the sense that

$$[K : k]_s = [K : F]_s [F : k]_s$$

3. $[K : k]_s \leq [K : k]$ with equality if and only if K/k is separable

Proposition 3.16.26

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 Lemma 3.16.24.

Conversely the finite case follows from Proposition 3.16.25 by multiplicativity. We delay the proof of the general case until later in the section, as we don't need it for subsequent results. \square

Proposition 3.16.27

An algebraic extension $K = k(\alpha_1, \dots, \alpha_n)/k$ is separable iff α_i are.

Proposition 3.16.28 (Equivalent definition of separability)

An algebraic extension K/k . TFAE

1. K/k is separable
2. E/k is separable for every finite sub-extension
3. $[E : k]_s = [E : k]$ for every finite sub-extension

NB 3) is Lang's definition of separability which makes it a lot easier to prove certain results.

First we prove a key lemma regarding simple extension

Lemma 3.16.29 (Separability degree of simple extension)

If $k(\alpha)/k$ is a simple extension then

$$[k(\alpha) : k]_s = \#\{\text{roots of } m_\alpha \text{ in } \bar{k}\} \leq \deg(m_\alpha) = [k(\alpha) : k]$$

Furthermore equality holds iff α is separable over k .

Proof. The first equality follows from 3.16.18, the final equality from Proposition 3.16.13. The inequality follows from Corollary 3.12.9. The final statement follows from Corollary 3.12.13. \square

Proof. Proof of 3.16.25

Note that any two algebraic closures $(\bar{k}/k, i_k)$ and $(\bar{k}'/k, i_k)$ are k -isomorphic by (...). Since $\text{Mor}(K, -)$ is a covariant functor (2.3.11) this implies $\text{Mor}(K, \bar{k})$ is isomorphic to $\text{Mor}(K, \bar{k}')$ as a set by 2.3.8. Therefore $[K : k]_s$ is well-defined and independent of the embedding of k in an algebraic closure.

For a tower $K/F/k$ consider the restriction map

$$\psi := \text{Mor}_k(i_{FK}, \bar{k}) : \text{Mor}_k(K, \bar{k}) \rightarrow \text{Mor}_k(F, \bar{k})$$

It is surjective by Proposition 3.16.21. Consider $\sigma \in \text{Mor}_k(F, \bar{k})$ and the fibre $\psi^{-1}(\sigma) = \text{Mor}_F(K, (\bar{k}/F, \sigma))$. 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_F . As $\text{Mor}_k(K, \bar{k})$ 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

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

with $K_i = K_{i-1}(\alpha_i)$. By Lemma 3.16.29 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 Lemma 3.16.24 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. \square

Proof. Proof of 3.16.27

Let $K = k(\alpha_1, \dots, \alpha_n)$. Then we may construct a tower of finite (simple) extensions

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

with $K_i = k(\alpha_1, \dots, \alpha_i)$ and $K_i = K_{i-1}(\alpha_i)$. By Lemma 3.16.24 α_i is separable over K_{i-1} . Therefore $[K_i : K_{i-1}]_s = [K_i : K_{i-1}]$ by Lemma 3.16.29 and $[K : k]_s = [K : k]$ by multiplicativity. Proposition 3.16.25 shows that K/k is separable. \square

Proof. Proof of 3.16.26 general case

Assume K/E and E/k are separable. Take $\alpha \in K$. Then Lemma 3.16.16 shows the existence of a finite sub-extension E_0/k of E such that $m_{\alpha, E} = m_{\alpha, E_0}$. Therefore α is separable over E_0 . By Lemma 3.16.29 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 Proposition 3.16.25 $[E_0 : k]_s = [E_0 : k]$. 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. \square

Proof. Proof of 3.16.28 $1 \implies 2$ is trivial and $2 \iff 3$ follows from Proposition 3.16.25. We need only show $2 \implies 1$.

Consider $\alpha \in K$. Then by Lemma 3.16.16 there exists a finite sub-extension E/k such that α is algebraic over E . Therefore $E(\alpha)/k$ is finite, and by assumption $E(\alpha)/k$ separable as required. \square

3.16.5 Applications of Separability

Definition 3.16.16 (Bounds on $\text{Aut}(K/k)$)

Let K/k be an algebraic extension and $i_K : K \rightarrow \bar{k}$ a fixed k -embedding. Then there is a natural injection

$$\begin{aligned} \text{Mor}_k(K, i_K) : \text{Aut}(K/k) &\rightarrow \text{Mor}_k(K, \bar{k}) \\ \sigma &\rightarrow i_K \circ \sigma \end{aligned}$$

In particular in the finite case

$$\# \text{Aut}(K/k) \leq [K : k]_s \leq [K : k] < \infty$$

If i_K is inclusion, then we may regard $\text{Aut}(K/k)$ as a subset of $\text{Mor}_k(K, \bar{k})$

Corollary 3.16.30 (Conjugate elements)

We say $\alpha, \beta \in \bar{k}$ are conjugate if they have the same minimal polynomial.

This is the case if and only if there is an element $\sigma \in \text{Aut}(\bar{k}/k)$ such that $\sigma(\alpha) = \beta$.

Proof. By Proposition 3.16.18 there is an isomorphism $k(\alpha) \rightarrow k(\beta)$. Corollary 3.16.23 gives the required automorphism. The converse is easy. \square

As an application of the concept of separability degree we prove

Proposition 3.16.31 (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^* is cyclic.

Consider the set $\text{Mor}_k(K, \bar{k}) = \{\sigma_1, \dots, \sigma_n\}$ which by Proposition 3.16.28 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 $\# \text{Mor}_k(k(\alpha + c\beta), \bar{k}) \geq n$ 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 Corollary 3.4.43).

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 . \square

3.16.6 Perfect Fields

For large classes of base fields all algebraic extensions are separable :

Proposition 3.16.32 (Perfect field)

Let k be a field. Then TFAE

- Every irreducible polynomial in $k[X]$ is separable
- Every algebraic extension K/k is separable
- \bar{k} is separable

In this case we say k is perfect.

Proposition 3.16.33 (Criteria for perfectness)

k is perfect if and only if one of the following holds

- k has characteristic 0
- k has characteristic p and every element is a p -th power

In particular finite fields are perfect.

3.16.7 Normal Extensions

We characterize normal extensions in terms of morphisms $\text{Mor}_k(K, \bar{k})$.

Proposition 3.16.34 (Normal Criteria)

Let K/k be an algebraic extension and \bar{k} a given algebraic closure, then the following are equivalent

NOR1 For any two k -embeddings $\sigma, \tau \in \text{Mor}_k(K, \bar{k})$ we have $\sigma(K) = \tau(K)$.

NOR2 K is the splitting field of some family of polynomials $f_i \in k[X]$.

NOR3 K/k is normal (i.e. every minimal polynomial in $k[X]$ splits completely in K)

Proof. Clearly $3 \implies 2$, for K is the splitting field of all the minimal polynomials of elements in K .

We show $2 \implies 1$. Define $T_j = \{\alpha \in K \mid f_j(\alpha) = 0\}$ and $T'_j = \{\alpha \in \bar{k} \mid f_j(\alpha) = 0\}$. These are finite and by hypothesis $K = k(\cup_j T_j)$. Assume wlog that the f_j are irreducible.

It's clear that any σ induces an injection $T_j \rightarrow T'_j$ preserving multiplicity, which by counting is a bijection. In particular $\sigma(\cup_j T_j) = \cup_j T'_j$. By Lemma 3.16.7 we have $\sigma(K) = k(\cup_j T'_j)$. In particular any two embeddings σ, τ have the same image.

Finally we show $1 \implies 3$. Suppose $f(X)$ is an irreducible polynomial with roots $\alpha'_1, \dots, \alpha'_n \in \bar{k}$ and $\alpha_1 \in K$ such that $i_K(\alpha_1) = \alpha'_1$. By Corollary 3.16.30 there is a morphism $\phi \in \text{Aut}(\bar{k}/k)$ such that $\phi(\alpha_1) = \alpha_j$. By hypothesis i_K and the composite map $\phi \circ i_K$ must have the same image, K . Therefore $\alpha_j \in K$ as required. \square

We provide some more straightforward criteria based on a specific embedding $K \subset \bar{k}$.

Proposition 3.16.35 (Normal Criteria II)

Let K/k be an algebraic extension and $i_K : K \rightarrow \bar{k}$ a given k -embedding then the following are equivalent

1. K/k is normal
2. Every $\sigma \in \text{Mor}_k(K, \bar{k})$ has image $i_K(K)$
3. The embedding $\text{Mor}_k(K, i_K) : \text{Aut}(K/k) \rightarrow \text{Mor}_k(K, \bar{k})$ (3.16.16) is a bijection

When K/k is finite it's necessary and sufficient that $\# \text{Aut}(K/k) = [K : k]_s$

Proof. $1 \iff 2$). This is clear by NOR1.

$2 \implies 3$). Given $\sigma \in \text{Mor}_k(K, \bar{k})$, by hypothesis it has image $i_K(K)$, so we may define $\tau(x) = i_K^{-1}(\sigma(x))$ and $\tau \in \text{Aut}(K/k)$.

$3 \implies 2$). Conversely given $\sigma \in \text{Mor}_k(K, \bar{k})$, by hypothesis $\sigma = i_K \circ \tau$, and so has image $i_K(K)$.

For the final statement if K/k is finite, then we've shown in Proposition 3.16.25 that $[K : k]_s < \infty$. So the embedding $\text{Mor}_k(K, i_K)$ is bijective if and only if $\# \text{Aut}(K/k) = \# \text{Mor}_K(K, \bar{k}) = [K : k]_s$ as required. \square

Corollary 3.16.36 (Galois Criteria)

Let K/k be a finite extension. Then

$$\# \text{Aut}(K/k) \leq [K : k]_s \leq [K : k]$$

with equalities if and only if K/k is Galois.

Proof. We've seen the inequalities (Definition 3.16.16)

$$\# \text{Aut}(K/k) \leq [K : k]_s \leq [K : k] < \infty$$

with equality if and only if K/k is both normal (Proposition 3.16.35) and separable (Proposition 3.16.25) □

Corollary 3.16.37 (Subfield is Normal)

Let K/k be a normal extension and $F \subset K$ a subfield, then K/F is normal.

Proof. We assume the tower F/k has compatible embeddings into \bar{k} , then we have

$$\text{Mor}_F(K, \bar{k}) \subset \text{Mor}_k(K, \bar{k})$$

and the result follows from NOR1 . □

Proposition 3.16.38 (Automorphisms of Normal Extension)

Let K/k be a normal extension with compatible embeddings in \bar{k} . There is a canonical isomorphism of groups

$$\begin{aligned} \text{Aut}(\bar{k}/k) / \text{Aut}(\bar{k}/K) &\rightarrow \text{Aut}(K/k). \\ \sigma &\rightarrow i_K^{-1} \circ \sigma \circ i_K \end{aligned}$$

When $K \subset \bar{k}$ then this map is simply restriction to K .

Proof. By NOR1 $(\sigma \circ i_K)(K) = i_K(K)$ so that the group homomorphism, so that $\hat{\sigma} := i_K^{-1} \circ \sigma \circ i_K$ is well-defined. Furthermore $\hat{\sigma}$ fixes k because

$$\hat{\sigma} \circ i_{kK} = i_K^{-1} \circ \sigma \circ i_k = i_K^{-1} \circ i_k = i_K^{-1} \circ i_K \circ i_{kK} = i_{kK}$$

Therefore there is a well-defined group homomorphism

$$\text{Aut}(\bar{k}/k) \rightarrow \text{Aut}(K/k)$$

It is surjective, for given any $\hat{\sigma} \in \text{Aut}(K/k)$ there is by Corollary 3.16.23 $\sigma \in \text{Aut}(\bar{k}/k)$ such that $i_K \circ \hat{\sigma} = \sigma \circ i_K$. Clearly the image of σ under this homomorphism is $\hat{\sigma}$ as required. Note that $i_K^{-1} \circ \sigma \circ i_K = \text{id} \iff \sigma \circ i_K = i_K \iff \sigma$ fixes K , so the kernel of the homomorphism is precisely $\text{Aut}(\bar{k}/K)$. Therefore the isomorphism follows from Proposition 3.3.8. □

In fact we can replace \bar{k} with a normal overfield and obtain results corresponding to Corollary 3.16.23 and Proposition 3.16.35 respectively. Due to the explicit embeddings in \bar{k} the arguments become slightly awkward.

Corollary 3.16.39 (Extension to normal overfield)

Let L/k be a normal extension such that $K \subset L$ then there is a canonical surjective monoid morphism

$$\text{Aut}(L/k) \rightarrow \text{Mor}_k(K, L)$$

by restriction. The kernel is $\text{Aut}(L/K)$.

Proof. Assume an embedding $i_L : L \rightarrow \bar{k}$.

Consider $\sigma \in \text{Mor}_k(K, L)$, then by Corollary 3.16.23 there exists an extension $\tilde{\sigma} \in \text{Aut}(\bar{k}/k)$ such that $i_L \circ \sigma = \tilde{\sigma} \circ i_K$. As in the previous Proposition there exists $\hat{\sigma} \in \text{Aut}(L/k)$ such that $\tilde{\sigma} \circ i_L = i_L \circ \hat{\sigma}$. Therefore $i_L \circ \sigma = i_L \circ \hat{\sigma}|_K$ which implies $\sigma = \hat{\sigma}|_K$ as required, since i_L is injective. □

Corollary 3.16.40 (Automorphisms of Normal subextension)

Let L/k be a normal extension and $K \subset L$, then the following are equivalent

1. K/k is normal
2. $\text{Mor}_k(K, L) = \text{Aut}(K/k)$, i.e. every k -embedding $\sigma : K \rightarrow L$ has $\sigma(K) = K$.
3. For every $\sigma \in \text{Aut}(L/k)$ we have $\sigma(K) = K$

In this case $\text{Aut}(L/K) \triangleleft \text{Aut}(L/k)$ is normal and we have a canonical group isomorphism

$$\text{Aut}(L/k) / \text{Aut}(L/K) \rightarrow \text{Aut}(K/k)$$

Proof. Fix an embedding $i_L : L \rightarrow \bar{k}$.

- 1 \implies 2). Given $\sigma \in \text{Mor}_k(K, L)$ then as K is normal we have $(i_L \circ \sigma)(K) = (i_L)(K)$, which means $\sigma(K) = K$ since $i_L : K \rightarrow i_L(K)$ is a bijection.
- 2 \implies 1). Given any $\sigma \in \text{Mor}_k(K, \bar{k})$, this extends to $\tilde{\sigma} \in \text{Mor}_k(L, \bar{k})$ by Proposition 3.16.21. Since L is normal $\tilde{\sigma}(L) = i_L(L)$, we see $\hat{\sigma} := i_L^{-1} \circ \tilde{\sigma} \in \text{Aut}(L/k)$. By hypothesis $\hat{\sigma}(K) = K$, therefore $\sigma(K) = \tilde{\sigma}(K) = i_L(\hat{\sigma}(K)) = i_L(K)$. Since σ was arbitrary this shows K is normal.
- 2 \implies 3). This is clear, because $\sigma(K) = \sigma|_K(K) = K$.
- 3 \implies 2). Given $\sigma \in \text{Mor}_k(K, L)$ by Corollary 3.16.39 we can extend to $\hat{\sigma}$ in $\text{Aut}(L/k)$. By hypothesis $\sigma(K) = \hat{\sigma}(K) = K$ as required.

By Corollary 3.16.39 the canonical restriction map $\text{Aut}(L/k) \rightarrow \text{Aut}(K/k)$ is surjective, so the isomorphism follows from Proposition 3.3.8. \square

The following is straight-forward

Corollary 3.16.41 (Conjugate Elements)

Let K/k be a normal extension and two elements $\alpha, \beta \in K$ be two conjugate elements. Then there exists $\sigma \in \text{Aut}(K/k)$ such that $\sigma(\alpha) = \beta$.

Proof. By Proposition 3.16.18 there is an isomorphism $k(\alpha) \rightarrow k(\beta)$. Corollary 3.16.39 gives the required extension. \square

3.16.8 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 3.16.42 (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^* is cyclic.
- K/\mathbb{F}_p is simple

Proof. Since K/\mathbb{F}_p is a finite-dimensional vector space it must have order p^n .

The group of units has order $p^n - 1$, so by Lagrange's theorem every non-zero element satisfies $X^{p^n-1} - 1 = 0$, so therefore every element satisfies $X^{p^n} - X = 0$. Since this polynomial can have at most p^n roots (3.12.9) 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 Corollary 3.12.9. Therefore the fact K^* is cyclic follows from Proposition 3.3.14. \square

Proposition 3.16.43 (Frobenius morphism)

Given any field K/\mathbb{F}_p the Frobenius map

$$\phi : x \rightarrow x^p$$

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 Proposition 3.16.10. \square

Further we can show existence and uniqueness of finite fields.

Proposition 3.16.44 (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 Proposition 3.12.13 $f(X)$ 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 Theorem 3.3.5, 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 $\alpha \in \mathbb{F}_{p^n}$. \square

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 Proposition 3.16.33 that every finite field $\mathbb{F}_q := \mathbb{F}_{p^n}$ is perfect and therefore every algebraic extension is separable. In fact we may show that every finite extension is Galois.

Proposition 3.16.45

The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle$$

cyclic of order n generated by the Frobenius automorphism.

Proof. Let $G = \text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. 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 $\mathbb{F}_{p^n}^*$ implies $\phi^n = 1$. Therefore $d \mid n$ by 3.3.5 applied to G . By definition $\phi^d = e$, so every $\alpha \in \mathbb{F}_{p^n}$ satisfies the polynomial $X^{p^d} - X = 0$. This has at most p^d roots (3.12.9) so we must have $d \geq n$, and therefore $d = n$. Clearly ϕ generates a cyclic subgroup of order n . However by Corollary 3.16.36 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. \square

Proposition 3.16.46 (Subfields of \mathbb{F}_{p^n})

Consider the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. Then it has a unique subfield of order p^m if and only if $m \mid n$. In this case $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois and

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \phi^m \rangle$$

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 $H = \text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$. Note ϕ^m has order n/m . Furthermore from Proposition 3.16.44 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 Corollary 3.16.36 $\#H \leq [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$, whence we have equality and so the extension is Galois and $H = \langle \phi^m \rangle$. \square

The following is quite straightforward but also fundamental.

Corollary 3.16.47 (Finite fields are fixed points of Frobenius)

Let $\alpha \in \overline{\mathbb{F}_p}$ then

$$\deg(\alpha) \mid d \iff \alpha \in \mathbb{F}_{p^d} \iff \phi^d(\alpha) = \alpha$$

where ϕ is the Frobenius automorphism.

Proof. Recall by Definition 3.16.11 that $\deg(\alpha) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$. Then $\alpha \in \mathbb{F}_{p^d} \iff \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^d}$. The first equivalence then follows from the tower law and uniqueness of subfields.

Define $K = \mathbb{F}_p(\alpha)$ and $G = \text{Gal}(K/\mathbb{F}_p)$. Then by Proposition 3.16.45 $G = \langle \phi \rangle$ is cyclic of order $m = \deg(\alpha)$.

In particular Lagrange's theorem shows $\phi^m = e$. Then $m = \deg(\alpha) \mid d \implies \phi^d = e$ and in particular $\phi^d(\alpha) = \alpha$.

Conversely suppose $\phi^d(\alpha) = \alpha$. As α generates K we see $\phi^d = e$ (by 3.16.8), and by 3.3.6 we have $\deg(\alpha) = m = o(\phi) \mid d$. \square

3.16.9 Galois Theory

We've seen that for K/k a finite extension

$$\# \text{Aut}(K/k) \leq [K : k]_s \leq [K : k]$$

with equality if and only if K/k is Galois, by Corollary 3.16.36.

Remark 3.16.17

If k is perfect then \bar{k}/k is Galois.

The main result of Galois Theory is

Proposition 3.16.48

Let K/k be a finite Galois extension then there is an order-reversing bijection between subgroups and subfields

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

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 3.16.49

If K/k is Galois and $F \subset K$ then K/F is Galois.

Proof. This follows from Corollary 3.16.37 and Proposition 3.16.26. □

We need to show that $\phi \circ \psi = \text{id}$ and $\psi \circ \phi = \text{id}$. The first is marginally easier, and follows purely from the definition of Galois without making any finiteness assumptions.

Proposition 3.16.50 (Fixed field of Galois group)

If K/k is Galois and $F \subset K$ then

$$K^{\text{Gal}(K/F)} = F$$

or in other words $\phi \circ \psi = \text{id}$, and in particular ϕ is injective.

Proof. Clearly $F \subseteq K^{\text{Gal}(K/F)}$. 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 Corollary 3.16.41 there is an element $\sigma \in \text{Gal}(K/F)$ such that $\sigma(\alpha) = \beta$. In other words $\alpha \notin K^{\text{Gal}(K/F)}$, which shows the reverse inclusion. □

Proposition 3.16.51

Let K/k be a field extension and $H \subseteq \text{Aut}(K/k)$ a finite subgroup then K/K^H is finite Galois with

$$H = \text{Gal}(K/K^H)$$

and order equal to $[K : K^H]$. In particular for a finite Galois Extension K/k we have $\psi \circ \phi = \text{id}$.

Proof. Firstly observe that trivially $H \subseteq \text{Aut}(K/K^H)$. If we know that $[K : K^H] < \infty$, then by Corollary 3.16.36 we have

$$\#H \leq \# \text{Aut}(K/K^H) \leq [K : K^H]_s \leq [K : K^H]$$

We can prove equality everywhere if we show that $[K : K^H] \leq \#H$, which is shown either by Lemma 3.16.52 or Lemma 3.16.53. Note equality also shows that K/K^H is finite Galois by the same result. □

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 3.16.52 (Bound degree of fixed field I)

Let K/k be a field extension and $H \subset \text{Aut}(K/k)$ a finite subgroup. Then $[K : K^H] \leq \#H$

Proof. Let $H = \{\sigma_1, \dots, \sigma_n\}$ with $\sigma_1 = \text{id}$ and $\alpha_1, \dots, \alpha_m$ a K^H -basis for K .

Consider the vector space K^n and the elements $\hat{\alpha}_j = (\sigma_1(\alpha_j), \dots, \sigma_n(\alpha_j))$ for $j = 1 \dots m$. It's enough to show that these are linearly independent over K , as that implies $m \leq n$ by Proposition 3.4.41.

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 $\alpha_1, \dots, \alpha_m$ by considering the first component ($\sigma_1 = \text{id}$). 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. \square

Lemma 3.16.53 (Bound degree of fixed field II)

Let K/k be a field extension and H a finite subgroup of $\text{Aut}(K/k)$. 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 Proposition 3.12.13. 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 Proposition 3.12.12.

If K/k is finite, then a-fortiori K/K^H is finite, so we may apply the Primitive Element Theorem 3.16.31 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 $K^H \subsetneq K^H(\alpha) \subsetneq K^H(\alpha, \beta)$ is a finite separable extension of K^H , whence it must be simple by the Primitive Element Theorem 3.16.31, contradicting maximality. Finally the degree of $[K : K^H]$ is the degree of α , which we've seen is bounded above by $\#H$. \square

Now we may demonstrate straightforward criteria for subfield to be normal

Proposition 3.16.54

Let K/k be a finite Galois extension and $F \subset K$ a subfield.

Then F/k is Galois if and only if $\text{Gal}(K/F) \triangleleft \text{Gal}(K/k)$ is normal. In this case we have a canonical isomorphism

$$\text{Gal}(K/k)/\text{Gal}(K/F) \rightarrow \text{Gal}(F/k)$$

Proof. Recall from Corollary 3.16.40 we have F/k is normal iff $\sigma(F) = F$ for all $\sigma \in \text{Gal}(K/k)$. We also observe that

$$\text{Gal}(K/\sigma(F)) = \sigma \text{Gal}(K/F) \sigma^{-1}$$

By the correspondence theorem 3.16.48 $\text{Gal}(K/F) = \text{Gal}(K/F') \iff F = F'$. Therefore

$$\begin{aligned} F/k \text{ normal} &\iff \sigma(F) = F \quad \forall \sigma \in \text{Gal}(K/k) \\ &\iff \text{Gal}(K/\sigma(F)) = \text{Gal}(K/F) \quad \forall \sigma \in \text{Gal}(K/k) \\ &\iff \sigma \text{Gal}(K/F) \sigma^{-1} = \text{Gal}(K/F) \quad \forall \sigma \in \text{Gal}(K/k) \\ &\iff \text{Gal}(K/F) \triangleleft \text{Gal}(K/k) \end{aligned}$$

Finally the natural restriction homomorphism

$$\text{Gal}(K/k) \rightarrow \text{Gal}(F/k)$$

is surjective by Corollary 3.16.39 and has kernel precisely $\text{Gal}(K/F)$. Therefore the result follows from the Group Isomorphism Theorem 3.3.8. \square

3.17 Zariski's Lemma

Definition 3.17.1 (k -algebra)

A k -algebra A is simply a commutative algebra over a field, k .

Definition 3.17.2 (Residue field)

Let \mathfrak{m} be a maximal ideal of the k -algebra A . Define the residue field by

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

It is a field extension $k(\mathfrak{m})/k$. If it is finite/algebraic over k we write

$$\deg(\mathfrak{m}) := \dim_k k(\mathfrak{m})$$

Essentially when A is finitely generated then the residue field is finite.

Theorem 3.17.1 (Zariski's Lemma)

Let A be a finitely generated k -algebra which is a field over k . Then A/k is an algebraic, and hence finite, field extension.

Proof. TODO.. □

Proposition 3.17.2 (Weak Nullstellensatz I)

There is a bijective map

$$\begin{aligned} \bar{k}^n / \text{Aut}(\bar{k}/k) &\longrightarrow \{ \mathfrak{m} \triangleleft k[X_1, \dots, X_n] \text{ maximal} \} \\ x &\longrightarrow \mathfrak{m}_x := \ker(\text{ev}_x) \end{aligned}$$

When $x \in k^n$ then

$$\mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n)$$

Proof. Consider $x \in \bar{k}^n$. Then $1 \notin \mathfrak{m}_x$ so it's proper. To show that \mathfrak{m}_x is maximal consider the isomorphism of k -algebras

$$k \rightarrow k[X_1, \dots, X_n]/\mathfrak{m}_x \xrightarrow{\sim} k[x_1, \dots, x_n] \subset \bar{k}$$

By Proposition 3.16.14 the image is a field. Therefore by Proposition 3.4.22 \mathfrak{m}_x is maximal. As $\mathfrak{m}_{\sigma(x)} = \mathfrak{m}_x$ then this is well-defined. If $\mathfrak{m}_x = \mathfrak{m}_y$ then there is a field isomorphism $\sigma : k(x_1, \dots, x_n) \rightarrow k(y_1, \dots, y_n) \subset \bar{k}$ s.t. $\sigma(x_i) = y_i$ obtained by composing the two isomorphisms just given. By Corollary 3.16.23 this extends to $\sigma \in \text{Aut}(\bar{k}/k)$. This shows the map is injective.

Suppose we are given a maximal ideal $\mathfrak{m} \triangleleft k[X_1, \dots, X_n]$. Then $K := k[X_1, \dots, X_n]/\mathfrak{m}$ is a field (3.4.22) and f.g. as a k -algebra, therefore algebraic over k by Zariski's Lemma. By Theorem 3.16.21 there is a k -embedding $K \rightarrow \bar{k}$. Consider the map

$$k \rightarrow k[X_1, \dots, X_n] \xrightarrow{\pi} K \xrightarrow{i_K} \bar{k}$$

Define $x_i = i_K(\pi(X_i))$. Then by universal property $\text{ev}_x(f) = i_K(\pi(f))$. When $f \in \mathfrak{m}$ then $\text{ev}_x(f) = 0$, in other words $\mathfrak{m} \subseteq \mathfrak{m}_x$ and these are equal by maximality. This shows that the map is surjective.

For any $f \in k[X_1, \dots, X_n]$ and $x \in k^n$, apply the division algorithm with $q = (X_n - x_n)$ to find

$$f(X_1, \dots, X_n) = g_n(X_1, \dots, X_n)(X_n - x_n) + r(X_1, \dots, X_{n-1})$$

Applying the same result recursively to r to find

$$f(X_1, \dots, X_n) = \sum_{i=1}^n g_i(X_1, \dots, X_i)(X_i - x_i) + r_0$$

with $r_0 = f(x)$. This shows that $f \in \mathfrak{m}_x \iff f(x) = 0 \iff f \in (X_1 - x_1, \dots, X_n - x_n)$ as required. □

Corollary 3.17.3 (Weak Nullstellensatz II)

Let $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$. Then \mathfrak{a} is proper if and only if there exists $x \in \bar{k}^n$ such that $f(x) = 0 \quad \forall f \in \mathfrak{a}$.

Proof. If \mathfrak{a} is proper then it's contained in a maximal ideal which by the previous result is of the form \mathfrak{m}_x as required. The converse is straightforward. □

Definition 3.17.3 (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 3.4.14 and 3.4.23

$$\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}}^J$$

Proposition 3.17.4 (Jacobson Ring)

Let A be a ring the following are equivalent

1. For any ideal \mathfrak{a} , $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}}^J$
2. For any radical ideal $\mathfrak{a} = \sqrt{\mathfrak{a}}^J$
3. For any prime ideal $\mathfrak{p} = \sqrt{\mathfrak{p}}^J$

We say such a ring is a Jacobson ring.

Proof. 1 \implies 2). This clear because in this case $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

2 \implies 3). This is clear because a prime ideal is radical.

3 \implies 1). By 3.4.14

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

as required □

We prove later that the Weak Nullstellensatz implies the following result

Proposition 3.17.5 (Strong Nullstellensatz)

$k[X_1, \dots, X_n]$ is a Jacobson ring.

3.18 Differentials

Chapter 4

Topology and Differential Geometry

Many of the constructions in algebraic geometry are analogues of constructions in topology and differential geometry. Therefore we review these, but slanted from the point of view of algebraic geometry.

4.1 Topological Spaces

Topology is useful in algebraic geometry, but often the natural topologies are usually much coarser so the theory looks rather different.

Definition 4.1.1 (Topological Space)

A topological space (X, \mathcal{T}_X) consists of a set X and family of open sets $\mathcal{T}_X \subseteq \mathcal{P}(X)$ satisfying the following properties

- $X, \emptyset \in \mathcal{T}_X$
- $U_i \in \mathcal{T}_X \implies \bigcup_{i \in I} U_i \in \mathcal{T}_X$
- $U, V \in \mathcal{T}_X \implies U \cap V \in \mathcal{T}_X$

A subset $Z \subset X$ is said to be closed iff $X \setminus Z$ is open. We may equivalently define the topology in terms of closed sets.

Definition 4.1.2 (Continuous)

A map $f : X \rightarrow Y$ is continuous if the inverse image of an open (closed) set is open (closed).

Remark 4.1.3

In the case of \mathbb{R}^n this can be shown to be equivalent to the usual $\delta - \epsilon$ definition.

Definition 4.1.4 (Subspace topology)

Let $Y \subset X$, then we may define the subspace topology on Y by

$$\mathcal{T}_Y := \{U \cap Y \mid U \in \mathcal{T}_X\}$$

when Y is open then this is given by

$$\mathcal{T}_Y = \{U \subseteq Y \mid U \in \mathcal{T}_X\}$$

Definition 4.1.5 (Base)

We say $\mathcal{B} \subseteq \mathcal{P}(X)$ is a base (of open sets) on X if

- For every $x \in X$ there is a $U \in \mathcal{B}$ such that $x \in U$
- Suppose $U, V \in \mathcal{B}$ and $x \in U \cap V$ then there exists $W \in \mathcal{B}$ such that $x \in W \subseteq U \cap V$

Proposition 4.1.1 (Topology generated by a base)

Let \mathcal{B} be a base, then the following is a topology on X

$$\mathcal{T}_{\mathcal{B}} := \left\{ \bigcup_{U_i \in I} U_i \mid I \subseteq \mathcal{B} \right\}$$

i.e. the set of arbitrary unions of sets in \mathcal{B} .

Proposition 4.1.2 (Base generating topology)

A base \mathcal{B} satisfies $\mathcal{T}_{\mathcal{B}} = \mathcal{T}_X$ if and only if for every $x \in U$ and $U \in \mathcal{T}_X$ there exists $V \in \mathcal{B}$ such that $x \in V \subseteq U$.

In this case we say \mathcal{B} is a base for X .

Definition 4.1.6 (Limit point)

For $Y \subset X$ we say x is a limit point of Y if $(x \in U \implies Y \cap U \neq \emptyset)$. NB every point of Y is necessarily a limit point.

Remark 4.1.7

In the case of \mathbb{R}^n this is equivalent to x being the limit of a convergent sequence $x_n \in Y$.

Proposition 4.1.3 (Topological Closure)

Let $Y \subset X$ then the following sets are equal

$$\text{cl}_X(Y) := \bar{Y} := \bigcap_{\substack{Z \supseteq Y \\ Z \text{ closed}}} Z = \{x \in X \mid x \text{ limit point of } Y\}$$

Furthermore

1. $Y \subseteq \bar{Y}$ and \bar{Y} is closed
2. $Y = \bar{Y}$ if and only if Y is closed
3. $(Y \cap U \neq \emptyset \iff \bar{Y} \cap U \neq \emptyset)$ for any U open

Proof. Suppose Z is a closed set containing Y and x is a limit point of Y . Then $x \notin Z \implies x \in X \setminus Z \implies (X \setminus Z) \cap Y \neq \emptyset$ a contradiction. Conversely assume $x \notin \bar{Y}$ then there exists $Z \supseteq Y$ closed such that $x \notin Z \implies x \in X \setminus Z$. This means x is not a limit point.

1. An arbitrary intersection of closed sets is closed
2. This follows because \bar{Y} is the smallest closed superset.
3. One implication is clear because $Y \subseteq \bar{Y}$. Conversely if $x \in \bar{Y} \cap U$ then x must be a limit point of Y hence $U \cap Y \neq \emptyset$ as required.

□

Remark 4.1.8

In \mathbb{R}^n this is simply adjoining limit points, e.g. $[a, b] \setminus T \rightarrow [a, b]$ where T is a finite set.

Proposition 4.1.4 (Dense subset)

Let $Y \subset X$ then the following are equivalent

1. $\bar{Y} = X$
2. $Y \cap U \neq \emptyset$ for any U open

and we say Y is dense.

Proof. 1 \implies 2) Follows from Proposition 4.1.3 criteria 3.

2 \implies 1). Suppose $Y \subseteq \bar{Y} \subsetneq X$ then $X \setminus \bar{Y}$ is an open set not intersecting Y a contradiction.

□

Proposition 4.1.5 (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 4.1.9

For a topological space X let X° denote the subset of closed points.

4.1.1 Continuous Maps**4.1.2 Irreducible Topological Spaces****Proposition 4.1.6** (Irreducible space)

Let X be a topological space. Then the following are equivalent

1. $X = Z_1 \cup Z_2$ closed implies either $Z_1 = X$ or $Z_2 = X$
2. $U, V \neq \emptyset \implies U \cap V \neq \emptyset$ for open sets U, V
3. $U \neq \emptyset \implies \bar{U} = X$ i.e. every non-empty open set is dense

and we say X is irreducible.

Proof. 1 \implies 2) Suppose U, V are open sets such that $U \cap V = \emptyset$. Then $X = U^c \cup V^c$. By hypothesis $X = U^c$ or $X = V^c$ whence either U or V is empty.

2 \implies 1) Similar.

3 \iff 2) Follows directly from Proposition 4.1.4

□

Proposition 4.1.7 (Irreducible Subset)

Let $Y \subset X$ be a subset of a topological space. Then the following conditions on Y are equivalent

1. Y is irreducible in the subspace topology.
2. $Y \subseteq Z_1 \cup Z_2$ closed implies either $Y \subseteq Z_1$ or $Y \subseteq Z_2$
3. $U \cap Y \neq \emptyset, V \cap Y \neq \emptyset \implies (U \cap V) \cap Y \neq \emptyset$ for U, V open

and we say Y is an irreducible subset.

Proof. This follows by applying Proposition 4.1.6 along with the definition of the subspace topology. □

Remark 4.1.10

Singletons $\{x\}$ are always irreducible.

Definition 4.1.11 (Irreducible Component)

We say that Y is an irreducible component if it is a maximal irreducible subset.

<https://stacks.math.columbia.edu/tag/004W>

Proposition 4.1.8 (Decomposition into Irreducible Components)

A topological space X may be decomposed into irreducible components. More precisely

- Y irreducible $\implies \overline{Y}$ irreducible
- Y irreducible component $\implies Y$ is closed
- Every irreducible subset is contained in an irreducible component
- X is the union of irreducible components

Proof. We prove each in turn

- Suppose $\overline{Y} \subseteq Z_1 \cup Z_2$ then by irreducibility $Y_1 \subseteq Z_1$ say. By 4.1.3 then $\overline{Y} \subseteq Z_1$ as required.
- Since an irreducible component is maximal and \overline{Y} is irreducible we see that for Y irreducible and maximal we must have $Y = \overline{Y}$. Proposition 4.1.3 implies that such a Y is closed.
- By Zorn's Lemma it's enough to show that if T_i is a chain (i.e. I is totally ordered and $i \leq j \implies T_i \subseteq T_j$) of irreducible subsets then $T := \cup_i T_i$ is irreducible. Suppose $T \subseteq Z_1 \cup Z_2$. Then for every i we have $T_i \subseteq Z_1$ or $T_i \subseteq Z_2$. Suppose for some i , $T_i \not\subseteq Z_1$, then for $j \geq i$ we have $T_j \not\subseteq Z_1$ whence $T_j \subseteq Z_2$ which implies $T \subseteq Z_2$ as required.
- As $\{x\}$ is irreducible every element is contained in an irreducible component by the previous step.

□

Corollary 4.1.9

Let $x \in X$ be a point then the closure $\overline{\{x\}}$ is an irreducible closed subset.

Corollary 4.1.10

X is irreducible if and only if it has a single irreducible component.

Definition 4.1.12 (Generic Point)

Let Z be an irreducible closed subset of X , then we say $\eta \in X$ is a generic point of Z if

$$Z = \overline{\{\eta\}}$$

Definition 4.1.13 (Sober)

A topological space is said to be sober if the mapping

$$x \longrightarrow \overline{\{x\}}$$

is bijective mapping from the set of points to irreducible closed subsets.

4.2 Sheaves

For what follows we assume \mathcal{C} is an algebraic category.

Definition 4.2.1 (Sheaf [War13, Defn 5.7] [For81, Defn 6.3])

A \mathcal{C} -valued sheaf \mathcal{F} on a topological space X is a mapping

$$U \longrightarrow \mathcal{F}(U) \in \text{ob}(\mathcal{C})$$

together with a collection of restriction morphisms $\rho_{UV} \in \text{Mor}(\mathcal{F}(U), \mathcal{F}(V))$, for any pair of open sets $V \subset U$ satisfying the following properties

1. $\rho_{VW} \circ \rho_{UV} = \rho_{UW}$. Write

$$\sigma|_V := \rho_{UV}(\sigma)$$

2. 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 $\sigma = \tau$.

3. 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

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

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 $\phi : \mathcal{F} \rightarrow \mathcal{G}$ consists of a family of morphisms

$$\phi_U : \mathcal{F}(U) \rightarrow \mathcal{G}(U)$$

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

$$\text{PSh}(X; \mathcal{B})$$

and the (full subcategory) of sheaves by

$$\text{Sh}(X; \mathcal{B})$$

When $\mathcal{B} = \mathcal{T}_X$ we may omit \mathcal{B} .

Definition 4.2.5 (Stalk of a (pre)sheaf)

Let \mathcal{F} be a (\mathcal{B} -)presheaf then define the stalk \mathcal{F}_x for $x \in X$ to be the directed limit

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

under the directed system $\{\mathcal{F}(U) \rightarrow \mathcal{F}(V)\}_{V \subseteq U}$. Explicitly this may be constructed as

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

where $(U, \sigma) \sim (V, \tau)$ if there is an open set $x \in W \subset U \cap V$ such that $\sigma|_W = \tau|_W$. It comes equipped with a family of morphisms $\rho_{Ux} : \mathcal{F}(U) \rightarrow \mathcal{F}_x$ such that

$$\rho_{Vx} \circ \rho_{UV} = \rho_{Ux}$$

Moreover for any open set U and family of morphisms $\{\phi_V : \mathcal{F}(V) \rightarrow A\}_{V \subseteq U}$ there is a unique morphism $\phi_x : \mathcal{F}_x \rightarrow A$ such that $\phi_U = \phi_x \circ \rho_{Ux}$.

Lemma 4.2.1 (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 4.2.2

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

$$\rho_x : (\mathcal{F}|_{\mathcal{B}_2})_x \rightarrow \mathcal{F}_x$$

It satisfies

$$[(U, \sigma)]_{x, \mathcal{B}_2} \rightarrow [(U, \sigma)]_{x, \mathcal{B}_1}$$

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 Proposition 4.1.2 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 Proposition 4.1.2 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. \square

Proposition 4.2.3

Let $\phi : \mathcal{F} \rightarrow \mathcal{G}$ be a morphism of (\mathcal{B}) -pre-sheaves then there exists a unique map on stalks

$$\phi_x : \mathcal{F}_x \rightarrow \mathcal{G}_x$$

such that $\phi(\sigma)_x = \phi_x(\sigma_x)$ for all $\sigma \in \mathcal{F}(U)$ and U neighbourhoods of x . Furthermore if $\psi : \mathcal{G} \rightarrow \mathcal{H}$ is another morphism of (pre-)sheaves then

$$\psi_x \circ \phi_x = (\psi \circ \phi)_x$$

Definition 4.2.6 (Push-forward sheaf)

Let $f : X \rightarrow Y$ be a continuous map and \mathcal{F} a sheaf on X . Then we may define the push-forward sheaf on Y by

$$(f_*\mathcal{F})(V) = \mathcal{F}(f^{-1}V)$$

Proposition 4.2.4 (Stalks on a push-forward sheaf)

Let $f : X \rightarrow Y$ be a continuous map and \mathcal{F} a sheaf on X . Then for $x \in X$ there is a unique morphism

$$\rho_x : (f_*\mathcal{F})_{f(x)} \rightarrow \mathcal{F}_x$$

such that $\rho_x(\sigma_{f(x)}) = \sigma_x$ for all $\sigma \in \mathcal{F}(f^{-1}V)$ and V nbhds of $f(x)$.

Proposition 4.2.5 (Sheafification)

Given a \mathcal{B} -presheaf \mathcal{F} define the sheafification \mathcal{F}^+ on \mathcal{T}_X by

$$\mathcal{F}^+(U) := \{(s_x)_{x \in U} \mid s_x \in \mathcal{F}_x\}$$

where we only consider “sections” (s_x) such that there is an open cover $U = \bigcup_i U_i$ with $U_i \in \mathcal{B}$ and sections $\sigma_i \in \mathcal{F}(U_i)$ such that $s_y = (\sigma_i)_y$ for all $y \in U_i$. We say the section s is determined by the sections (U_i, σ_i) . This constitutes a functor

$$(-)^+ : \text{PSh}(X; \mathcal{B}) \rightarrow \text{Sh}(X)$$

Furthermore there is a natural transformation $\eta : \mathbf{1} \Rightarrow (-)^+|_{\mathcal{B}}$ given by

$$\begin{aligned}\eta_{\mathcal{F}} : \mathcal{F} &\rightarrow (\mathcal{F}^+)|_{\mathcal{B}} \\ \sigma &\rightarrow (\sigma_x)\end{aligned}$$

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

$$\begin{array}{ccc}\mathrm{Mor}(\mathcal{F}^+, \mathcal{G}) & \longrightarrow & \mathrm{Mor}(\mathcal{F}, \mathcal{G}|_{\mathcal{B}}) \\ \alpha & \longrightarrow & \alpha|_{\mathcal{B}} \circ \eta_{\mathcal{F}} \\ \epsilon_{\mathcal{G}} \circ \beta^+ & \longleftarrow & \beta\end{array}$$

where we have used the counit natural transformation, which is in fact an isomorphism,

$$\begin{array}{ccc}\epsilon_{\mathcal{G}} : (\mathcal{G}|_{\mathcal{B}})^+ & \longrightarrow & \mathcal{G} \\ (\rho_x(\sigma_x)) & \longleftarrow & \sigma\end{array}$$

Finally there is an isomorphisms of stalks which commutes with restrictions, namely for all $U \in \mathcal{B}$ and $x \in U$ there is a commutative diagram

$$\begin{array}{ccc}\mathcal{F}(U) & \xrightarrow{\eta_U} & \mathcal{F}^+(U) \\ \rho_x \downarrow & & \downarrow \rho_x \\ \mathcal{F}_x & \xrightarrow{\eta_x} & (\mathcal{F}^+)_x\end{array}$$

where the bottom arrow is uniquely determined by this condition.

Proof. \mathcal{F}^+ is clearly a sheaf. The fact $(-)^+$ is functorial follows from Proposition 4.2.3, 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

$$\begin{aligned}\Phi_{\mathcal{F}, U}^{\mathcal{B}_2} : \mathcal{F}(U) &\rightarrow (\mathcal{F}|_{\mathcal{B}_2})^+(U) \quad U \in \mathcal{B}_1 \\ \sigma &\rightarrow (\rho_x^{-1}(\sigma_x))_{x \in U}\end{aligned}$$

where we have used the isomorphism from Proposition 4.2.2 $\rho_x : (\mathcal{F}|_{\mathcal{B}_2})_x \rightarrow \mathcal{F}_x$.

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 it is an isomorphism if \mathcal{F} is a sheaf. Suppose that $\rho_x^{-1}(\sigma_x) = \rho_x^{-1}(\tau_x)$ for all $x \in U$, then $\sigma_x = \tau_x$. By Lemma 4.2.1 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 Lemma 4.2.1 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.

Finally we may define the unit and counit natural transformations as follows

$$\begin{aligned}\epsilon_{\mathcal{G}, U} &:= (\Phi_{\mathcal{G}, U}^{\mathcal{B}})^{-1} & U \in \mathcal{T}_X \\ \eta_{\mathcal{F}, U} &:= \Phi_{\mathcal{F}, U}^{\mathcal{B}} & U \in \mathcal{B}\end{aligned}$$

By abstract nonsense (Proposition 2.3.16) 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

$$\alpha_1(s)|_{U_i} = \alpha_1(s|_{U_i}) = \alpha_2(s|_{U_i}) = \alpha_2(s)|_{U_i}$$

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 $\mathcal{F}(U) \rightarrow \mathcal{F}^+(U) \rightarrow (\mathcal{F}^+)_x$ 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 Lemma 4.2.1 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 Lemma 4.2.1 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. \square

Remark 4.2.7

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 $U \rightarrow \coprod_{x \in U} \mathcal{F}_x$.

We note a corollary, which may be proved more directly

Corollary 4.2.6

The functor

$$(-)|_{\mathcal{B}}: \text{Sh}(X) \rightarrow \text{PSh}(X; \mathcal{B})$$

is full and faithful.

Proof. This follows because it is a right-adjoint with a counit isomorphism by Proposition 2.3.15. \square

Corollary 4.2.7

There is an equivalence of categories

$$\text{Sh}(X; \mathcal{B}) \xrightleftharpoons[(-)^+]{(-)|_{\mathcal{B}}} \text{Sh}(X)$$

4.3 Spaces of k -functions

Often sheaves arise in the following more concrete way

Definition 4.3.1 (Space of k -functions)

Let X be a topological space. We say (X, \mathcal{O}_X) is a space of k -functions if \mathcal{O}_X is a presheaf such that

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

with restriction maps corresponding to restriction of functions and

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

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

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

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

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

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

Proposition 4.3.1 (Stalks are local)

Let (X, \mathcal{O}_X) be a space of k -functions there is an evaluation map

$$\mathcal{O}_{X,x} \longrightarrow k$$

given by

$$(U, f) \rightarrow f(x)$$

Define

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

Then \mathfrak{m}_x is the unique maximal ideal making $\mathcal{O}_{X,x}$ a local ring.

Definition 4.3.2 (Morphisms of spaces of k -functions)

Let (X, \mathcal{O}_X) and (Y, \mathcal{O}_Y) be spaces of k -functions. A morphism is a continuous mapping $f : X \rightarrow Y$ such that

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

This determines a sheaf morphism

$$f^\# : \mathcal{O}_Y \rightarrow f_* \mathcal{O}_X$$

Using (...) there is a unique homomorphism

$$f_x^\# : \mathcal{O}_{Y,f(x)} \rightarrow \mathcal{O}_{X,x}$$

such that $f_U^\#(\sigma)_x = f_x^\#(\sigma_{f(x)})$ for all $\sigma \in \mathcal{O}_Y(V)$. Then this is a local homomorphism in the sense that

$$f_x^\#(\mathfrak{m}_{f(x)}) \subseteq \mathfrak{m}_x$$

4.4 Differentiable Manifolds

We consider two types of manifold in parallel

- A \mathcal{C}^∞ manifold modelled on $\mathbf{E} = \mathbb{R}^n$ with ground field $k = \mathbb{R}$
- A complex-analytic surface modelled on $\mathbf{E} = \mathbb{C}$ with ground field $k = \mathbb{C}$

Definition 4.4.1 (Locally Euclidean Space [War13, Defn 1.3])

A Locally Euclidean Space X of dimension d is a Hausdorff topological space X for which each point has a neighbourhood homeomorphic to an open subset of \mathbf{E} . Such a homeomorphism is a pair $(U, \phi : U \rightarrow \mathbf{E})$, which we call a coordinate system. The functions $x_i = \pi_i \circ \phi$ are the “local coordinates” relative to this coordinate system.

Definition 4.4.2 (Real Smooth Manifold [War13, Defn 1.3])

A differentiable manifold is a pair (X, \mathcal{F}) where X is a d -dimensional locally Euclidean space and \mathcal{F} is a differentiable structure, namely a collection of coordinate systems

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

with

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

Example 4.4.3 (Euclidean space)

\mathbf{E} is a canonical example of smooth manifold, where the differentiable structure is the maximal one containing the identity map on \mathbf{E} .

Definition 4.4.4 (Riemann Surface [For81, Defn 1.1])

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

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

Definition 4.4.5 (Smooth (resp. holomorphic) functions [War13, Defn 1.6], [For81, Defn 1.6])

Let X be a Smooth Manifold (resp. Riemann Surface) and $U \subset X$ an open set then a function

$$f : U \rightarrow k$$

is smooth (resp. holomorphic) if

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

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

Definition 4.4.6 (Coordinate functions)

Let X be a smooth manifold and (U, ϕ) be a coordinate chart then the local coordinates x_i are functions

$$x_i : U \rightarrow k$$

given by

$$x_i(y) = \phi(y)_i \quad \forall y \in U$$

Proposition 4.4.1

Let X be a smooth manifold over k then the pair (X, \mathcal{O}_X) is a space of k -functions.

In particular $\mathcal{O}_{X,p}$ is a local ring with maximal ideal

$$\mathfrak{m}_p := \{f_p \mid f(p) = 0\}$$

such that $k \rightarrow \mathcal{O}_{X,p} \rightarrow \mathcal{O}_{X,p}/\mathfrak{m}_p =: k(p)$ is an isomorphism.

Definition 4.4.7 (Smooth maps)

Let (X, \mathcal{O}_X) and (Y, \mathcal{O}_Y) be smooth manifolds, then a smooth map is simply a morphism of a space of k -functions. That is a continuous map $f : X \rightarrow Y$ which induces a sheaf morphism

$$f^\# : \mathcal{O}_Y \longrightarrow f_* \mathcal{O}_X$$

By (...) this induces a local homomorphism

$$f_p^\# : \mathcal{O}_{Y,f(p)} \longrightarrow \mathcal{O}_{X,p}$$

Given a point $p \in X$, a chart (U, ϕ) and a vector $v \in k^n$ we may determine a directional derivative

$$D_{v,p} : \mathcal{O}_{X,p} \longrightarrow k$$

$$D_{v,p}(f_p) = \frac{d}{dt}(f \circ \phi^{-1})(\phi(p) + tv)|_{t=0} = \nabla(f \circ \phi^{-1})(\phi(p))v$$

A different chart and vector may determine the same functional on $\mathcal{O}_{X,p}$. So we define an equivalence relation which (we will show) still makes this correspondence well-defined and indeed injective.

Definition 4.4.8 (Tangent Space)

Let X be a smooth manifold define the tangent space at $p \in X$ to be $T_p X$ the set of triples (U, ϕ, v) where (U, ϕ) is a chart and $v \in \mathbf{E}$, under the equivalence relation

$$(U, \phi, v) \sim (V, \psi, w)$$

if

$$\nabla(\psi \circ \phi^{-1})(\phi p)v = w$$

Proof. We briefly show that the equivalence relation is reflexive, symmetric and transitive. Recall the multivariate chain rule means in general

$$\nabla(f \circ g)(p) = \nabla(f)(g(p))\nabla(g)(p)$$

So if $(U, \phi, v) \sim (V, \psi, w) \sim (W, \chi, z)$ then

$$\nabla(\chi \circ \phi^{-1})(p)v = \nabla(\chi \circ \psi^{-1})(\psi(p))\nabla(\psi \circ \phi^{-1})(p)v = \nabla(\chi \circ \psi^{-1})(\psi(p))w = z$$

and the relation is transitive as required. Clearly it's reflexive. Observe that the chain rule also implies that

$$\nabla(f)^{-1}(p) = \nabla(f^{-1})(f(p))$$

Therefore

$$\nabla(\psi \circ \phi^{-1})(\phi p)v = w \implies v = \nabla(\phi \circ \psi^{-1})(\psi(p))w$$

and the relation is symmetric. □

If we fix coordinates then there is a canonical basis for $T_p X$

Proposition 4.4.2 (Tangent Vectors as derivatives of germs)

Each coordinate chart (U, ϕ) induces a bijection

$$\begin{aligned} \mathbf{E} &\rightarrow T_p X \\ v &\rightarrow [(U, \phi, v)] \end{aligned}$$

In particular $T_p X$ inherits the structure of a k -vector space and the given map is an isomorphism. In particular $\dim_k T_p X = n$. Let x_i denote the coordinates for this chart, and denote the image of the standard basis as

$$\left\{ \left. \frac{\partial}{\partial x_i} \right|_p \right\}_{i=1 \dots n}$$

Furthermore there is a canonical k -linear map

$$\begin{aligned} T_p X &\rightarrow \mathcal{D}_p X \\ [(U, \phi, v)] &\rightarrow D_{v,p} \end{aligned}$$

where $\mathcal{D}_p X$ is the set of k -linear functionals $D : \mathcal{O}_{X,p} \rightarrow k$ satisfying the Liebniz rule

$$D(fg) = f(p)D(g) + g(p)D(f)$$

Under this map

$$\left. \frac{\partial}{\partial x_i} \right|_p f = \left. \frac{\partial(f \circ \phi^{-1})}{\partial x_i} \right|_p$$

in the usual calculus sense, motivating the terminology.

Proof. We show that the map $\mathbf{E} \rightarrow T_p X$ is surjective. Given a tangent vector (V, ψ, w) and a coordinate chart (U, ϕ) . Define $v = \nabla(\phi \circ \psi^{-1})(\psi(p))w$. Then $(V, \psi, w) \sim (U, \phi, v)$ and the map is surjective. We claim the map is injective for consider two tangent vectors $(U, \phi, v) \sim (U, \phi, v')$ then since the transition map is the identity $v = v'$.

We show that the map $T_p X \rightarrow \mathcal{D}_p X$ is well-defined. For suppose $(U, \phi, v) \sim (V, \psi, w)$ then by the chain rule

$$D_{w,p}(f_p) = \nabla(f \circ \psi^{-1})(\psi(p))w = \nabla(f \circ \phi^{-1})(\phi(p))\nabla(\phi \circ \psi^{-1})(\psi(p))w = \nabla(f \circ \phi^{-1})(\phi(p))v = D_{v,p}(f_p)$$

and so the mapping is well-defined. □

In order to devise a more intrinsic definition we may introduce the cotangent space

Proposition 4.4.3 (Tangent and Cotangent space are dual)

Let X be a smooth manifold and $p \in X$ define the cotangent space

$$T_p^* X := \mathfrak{m}_p / \mathfrak{m}_p^2$$

which is a k -vector space.

- $\dim_k T_p^* X = n$, more specifically given a coordinate chart (U, ϕ) with local coordinates x_i the following determines a basis

$$(dx_i)_p := \overline{(x_i - x_i(p))_p}$$

- There is a sequence of canonical isomorphisms

$$T_p X \xrightarrow{\sim} \mathcal{D}_p X \xrightarrow{\sim} \text{Hom}_k(T_p^* X, k)$$

given by

$$[(U, \phi, v)] \rightarrow D_{v,p}$$

and

$$D \rightarrow (\bar{f} \rightarrow D(f))$$

The composite is given by

$$[(U, \phi, v)] \rightarrow (f_p \rightarrow \nabla(f \circ \phi^{-1})(\phi(p))v)$$

- There is a corresponding perfect pairing

$$\psi : T_p X \times T_p^* X \rightarrow k$$

with

$$([(U, \phi, v)], \bar{f}_p) \rightarrow D_{v,p}(\bar{f}_p)$$

for which ψ_L is equal to the isomorphism described above. In particular there is a corresponding isomorphism

$$\psi_R : T_p^* X \xrightarrow{\sim} \text{Hom}_k(T_p X, k)$$

Proof. The fact $\dim_k T_p^* X = n$ follows essentially from the multivariate version of Taylor's Theorem and the fact the remainder term vanishes to second order.

Given a derivation D define $\theta_D \in \text{Hom}_k(T_p^* X, k)$ by $\theta_D(\bar{f}) = D(f)$. Observe D annihilates \mathfrak{m}_p^2 (since $D(fg) = f(p)D(g) + g(p)D(f)$) so this is well-defined. Further θ is clearly k -linear. Conversely given θ define $D_\theta(f) := \theta(\overline{f - f(p)})$. Observe that

$$(fg - f(p)g(p)) = (f - f(p))(g - g(p)) + f(p)(g - g(p)) + g(p)(f - f(p))$$

and as the first term lies in \mathfrak{m}_p^2 we see that $D_\theta(f)$ satisfies the product rule. It's easily seen that these are mutual inverses (as any D annihilates k) so the second map is a bijection. Further it's clearly k -linear and so a vector space isomorphism.

Recall, given a chart (U, ϕ) , that $T_p X$ has basis $\left. \frac{\partial}{\partial x_i} \right|_p$. It's clear that under the composite map stated that

$$\left. \frac{\partial}{\partial x_i} \right|_p (dx_j)_p = \delta_{ij}$$

which means by 3.4.58 that a basis of $T_p X$ is mapped to the basis $(dx_j)^*$ of $\text{Hom}_k(T_p^* X, k)$. By Proposition 3.4.44 the composite is then an isomorphism. \square

Remark 4.4.9

We have exhibited natural isomorphism between the more concrete tangent space construction and the more algebraic version as dual to the cotangent space.

Proposition 4.4.4 (Functoriality of Cotangent Space)

Let $f : X \rightarrow Y$ be a smooth map and $p \in X$ a point. Then there is a corresponding linear map

$$\begin{aligned} (df)_p^* = \overline{f_p^\sharp} : T_{f(p)}^* Y &\longrightarrow T_p^* X \\ \overline{g_{f(p)}} &\longrightarrow \overline{(g \circ f)_p} = \overline{f_p^\sharp(g_{f(p)})} \end{aligned}$$

Proof. By Definition 4.4.7 the homomorphism f_p^\sharp is local, that is $(f_p^\sharp)(\mathfrak{m}_p) \subseteq \mathfrak{m}_{f(p)}$. It's easy to show that $(f_p^\sharp)(\mathfrak{m}_p^2) \subseteq \mathfrak{m}_{f(p)}^2$. This shows that the given map is well-defined. \square

A key property is that a smooth map of manifolds induces linear maps of the tangent space at every point. We demonstrate this for each construction of the tangent space.

Proposition 4.4.5 (Functoriality of Tangent Space)

Let $f : X \rightarrow Y$ be a smooth map and $p \in X$ a point. Then there are corresponding linear maps $df_p, \tilde{df}_p, (df)_p^{**}$ making the following diagram commute, for any pair of charts $(U, \phi), (V, \psi)$ on X and Y respectively

$$\begin{array}{ccccccc} \mathbf{E} & \xrightarrow{\sim} & T_p X & \xrightarrow{\sim} & \mathcal{D}_p X & \xrightarrow{\sim} & \text{Hom}_k(T_p^* X, k) \\ \downarrow v \rightarrow \nabla(\psi f \phi^{-1})(p)v & & \downarrow df_p & & \downarrow \tilde{df}_p & & \downarrow (df)_p^{**} \\ \mathbf{F} & \xrightarrow{\sim} & T_{f(p)} Y & \xrightarrow{\sim} & \mathcal{D}_{f(p)} Y & \xrightarrow{\sim} & \text{Hom}_k(T_{f(p)}^* Y, k) \end{array}$$

given by

$$\begin{aligned} df_p : (U, \phi, v) &\longrightarrow (V, \psi, \nabla(\psi f \phi^{-1})(\phi(p))v) \\ \tilde{df}_p : D &\longrightarrow (g_{f(p)} \rightarrow D((g \circ f)_p)) \\ (df)_p^{**} : \theta &\longrightarrow \theta \circ \overline{f_p^\sharp} \end{aligned}$$

where $(df)_p^{**}$ is the dual map to $(df)_p^*$ defined in Proposition 4.4.4.

These maps are well-defined and independent of the local charts. Furthermore they are functorial in the sense that

$$d(\mathbf{1}_X)_p = \mathbf{1}_{T_p X}$$

and

$$dg_{f(p)} \circ df_p = d(g \circ f)_p$$

Let $\left\{ \frac{\partial}{\partial x_i} \Big|_p \right\}_{i=1 \dots n}$ and $\left\{ \frac{\partial}{\partial y_j} \Big|_{f(p)} \right\}_{j=1 \dots m}$ be the standard bases for $T_p X$ and $T_{f(p)} Y$ then

$$df_p \left(\frac{\partial}{\partial x_i} \Big|_p \right) = \sum_{j=1}^m \frac{\partial(y_j \circ f \circ \phi^{-1})}{\partial x_i}(\phi(p)) \frac{\partial}{\partial y_j} \Big|_{f(p)}$$

and more succinctly has matrix representation

$$\frac{\partial f^i}{\partial x_j}(p)$$

with respect to the standard basis just given.

Proof. Suppose that $(U', \phi', v') \sim (U, \phi, v)$. Then this means precisely that $\nabla(\phi' \circ \phi^{-1})(\phi(p))v = v'$. Then by the chain rule

$$\nabla(\psi \circ f \circ \phi^{-1})(\phi(p))v = \nabla(\psi \circ f \circ (\phi')^{-1})(\phi'(p))\nabla(\phi' \circ \phi^{-1})(\phi(p))v = \nabla(\psi \circ f \circ (\phi')^{-1})(\phi'(p))v'$$

so the map is independent of the choice of chart (U, ϕ) . Similarly if (V', ψ') is another chart then we claim that

$$(V', \psi', \nabla(\psi' \circ f \circ \phi^{-1})(\phi(p))v) \sim (V, \psi, \nabla(\psi \circ f \circ \phi^{-1})(\phi(p))v)$$

This follows from the chain rule

$$\nabla(\psi' \circ \psi^{-1})(\psi(p))\nabla(\psi \circ f \circ \phi^{-1})(\phi(p)) = \nabla(\psi' \circ f \circ \phi^{-1})(\phi(p)).$$

Note that $g_{f(p)} = g'_{f(p)} \implies g|_V = g'|_V$ in some neighbourhood V of $f(p)$, which implies $(g \circ f)|_{f^{-1}(V)} = (g' \circ f)|_{f^{-1}(V)} \implies (g \circ f)_p = (g' \circ f)_p$. Therefore the mapping \tilde{df}_p is well-defined. Note

$$\tilde{df}_p(D_{v,p})(g_{f(p)}) = D_{v,p}((g \circ f)_p) = \nabla(g \circ f \circ \phi^{-1})(\phi(p))v = \nabla(g \circ \psi^{-1})(\psi(f(p)))\nabla(\psi \circ f \circ \phi^{-1})(\phi(p))v = D_{w,f(p)}(g_{f(p)})$$

where $w = \nabla(\psi \circ f \circ \phi^{-1})(\phi(p))$. This means the map \tilde{df}_p commutes with the rest of the diagram. \square

Definition 4.4.10 (Regular Point)

Let $f : X \rightarrow k^d$ be a smooth map then we say p is a regular point for f if the differential map

$$df_p : T_p X \longrightarrow T_p k^d$$

is surjective (if and only if $\text{rank}(df_p) = d$ by Corollary 3.4.43). Otherwise it is a critical point. NB by the rank-nullity theorem we require $\dim T_p X \leq d$ for any regular point.

We say $c \in k^d$ is a regular value if $f^{-1}(c)$ consists of regular points. When $f^{-1}(c)$ is empty then c is automatically regular.

It's possible to show that a regular level set $Y = f^{-1}(c)$ is an embedded (smooth) submanifold. We may identify the tangent space of Y with $T_p Y = \ker(df_p)$. When $X = \mathbb{R}^n$ then $\ker(df_p)$ has a geometric interpretation as lines on which f is locally constant. The regular points are where $\ker(df_p)$ has the minimal possible rank.

4.5 Locally Ringed Spaces

Chapter 5

Algebraic Geometry

Throughout we assume that k is perfect and contained in an algebraic closure \bar{k} . In particular we may assume any algebraic extension K/k is contained in \bar{k} and is separable. However we don't assume that k is algebraically closed which makes the development of "classical algebraic geometry" slightly more complex than e.g. Hartshorne Chap I.

5.1 Algebraic Sets over a Field

Proposition 5.1.1

Let $A = k[X_1, \dots, X_n]$ be the polynomial ring in n -variables over a field k . For a set $S \subset k[X_1, \dots, X_n]$ and an algebraic field extension K/k define the **zero-locus**

$$V_K(S) := \{\alpha \in K^n \mid f(\alpha) = 0 \quad \forall f \in S\}.$$

Similarly for a subset $Y \subset K^n$ define

$$I_K(Y) := \{f \in A \mid f(y) = 0 \quad \forall y \in Y\}$$

Therefore we may consider the pair of maps

$$\mathcal{P}(k[X_1, \dots, X_n]) \xrightleftharpoons[V_K]{I_K} \mathcal{P}(K^n)$$

V_K and I_K constitute a Galois Connection

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 subscript K)

4. $VIV = V$ and $IVI = I$
5. $I(Y)$ is a radical ideal and $\sqrt{\langle S \rangle} \subseteq I(V(S))$
6. $V(S) = V(\langle S \rangle) = V(\sqrt{\langle S \rangle})$ and $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$
7. $\bigcap_i V(S_i) = V(\bigcup_i S_i)$ and $\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$
8. $\bigcap_i I_K(W_i) = I_K(\bigcup_i W_i)$
9. $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$
10. $V((0)) = K^n$ and $V(A) = \emptyset$

The sets of the form $V_K(\mathfrak{a})$ constitute the closed sets of a topology on K^n , denoted by $\text{Zar}_k(K^n)$. In this case we have the following form for the topological closure

$$V_K(I_K(Y)) = \overline{Y}$$

Furthermore this restricts to a Galois connection

$$\text{Rad}(k[X_1, \dots, X_n]) \xrightleftharpoons[V_K]{I_K} \text{Zar}_k(K^n)$$

such that $V_K \circ I_K = \mathbf{1}$.

Proof. We make use of general results on Galois connections (Section 2.1.5), though many results may be shown more directly.

1-3. These follow directly from the definitions

4. This follows from Proposition 2.1.18.

5. It's clear that $I(Y)$ is an ideal. It is radical because K is reduced (...). The second statement follows from Proposition 2.1.19 by considering the closure operator $\sqrt{\langle - \rangle}$.

6. This follows from Proposition 2.1.19 by considering the closure operators $\sqrt{\langle - \rangle}$ and $\langle - \rangle$.

7. The first equality follows from Proposition 2.1.21. The second equality follows from Proposition 3.4.7.

8. This follows from Proposition 2.1.21.

9. Observe that $\mathfrak{m}_x = I(\{x\})$ 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 Proposition 3.4.10 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 $\text{Zar}_k(K^n) := \text{Im}(V_K)$ constitute the closed sets of a topology precisely because they are closed under arbitrary intersections and finite unions. Furthermore by Proposition 2.1.18 $V_K \circ I_K$ is a closure operator with image precisely the closed sets. Therefore by Proposition 2.1.15

$$(V_K \circ I_K)(Y) = \bigcap_{Y \subseteq Z \in \text{Zar}_k(K^n)} Z$$

which is the definition of the topological closure. □

For a fixed ideal $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$ we may vary the field K to obtain families of solutions in different fields.

Definition 5.1.1 (Algebraic Set, Coordinate Ring and K -rational points)

We say $X \subset k^n$ is an algebraic set if it is of the form $V(\mathfrak{a})$ for $\mathfrak{a} \triangleleft k[X_1, \dots, X_n]$ a radical ideal.

Define the coordinate ring to be $k[X] := k[X_1, \dots, X_n]/\mathfrak{a}$. Note $k[X]$ is a reduced f.g. k -algebra

For K/k an algebraic field extension define the K -rational points to be

$$X(K) := V_K(\mathfrak{a}) \subset K^n$$

For a point $x \in X(K)$ define the degree of x to be

$$\deg(x) = \dim_k k(x_1, \dots, x_n)$$

Note if we have a tower $k \subset K_1 \dots \subset K_n \subset \bar{k}$ then we have a tower of sets

$$X(k) \subset X(K_1) \dots \subset X(K_n) \subset X(\bar{k})$$

Remark 5.1.2

$X = \mathbb{A}_k^n := V((0))$ is an algebraic set and $\mathbb{A}_k^n(K) = K^n$.

Proposition 5.1.2 (Coordinate ring as functions)

Let $X = V(\mathfrak{a})$ be a k -algebraic set with coordinate ring $k[X]$. Then there is a well-defined embedding

$$\begin{aligned} k[X] &\hookrightarrow \text{Fun}(X(K), K) \\ \bar{f} &\longrightarrow \text{ev}_x(f) \end{aligned}$$

given by function evaluation.

For completeness we also consider sub-algebraic sets in the same way as before

Definition 5.1.3 (Sub-algebraic sets)

For X an algebraic set with coordinate ring $k[X]$. For $\mathfrak{b} \triangleleft k[X]$ and K/k algebraic define

$$V_K(\mathfrak{b}; X) := \{x \in X(K) \mid f(x) = 0 \quad \forall f \in \mathfrak{b}\}$$

Similarly for $Y \subset X(K)$ define

$$I_K(Y; X) := \{f \in k[X] \mid f(y) = 0 \quad \forall y \in Y\}$$

Note in the case $X = \mathbb{A}_k^n$ then this is exactly the same notion as before.

We can reduce to the case \mathbb{A}_k^n easily as follows

Proposition 5.1.3 (Transitivity of algebraic sets)

Let $X = V(\mathfrak{a})$ be an algebraic set and $\pi : k[X_1, \dots, X_n] \rightarrow k[X]$ be the canonical surjective homomorphism with kernel \mathfrak{a} . Then if we regard $X(K) \subset K^n$

$$V_K(\mathfrak{b}; X) = V_K(\pi^{-1}(\mathfrak{b})) \cap X$$

$$I_K(Y \cap X; X) = \pi(I_K(Y))$$

and in particular

$$I_K(V_K(\mathfrak{b}; X); X) = \pi(I_K V_K(\pi^{-1}(\mathfrak{b})))$$

Proposition 5.1.4 (Galois connection on sub-algebraic set)

Let $X = V(\mathfrak{a})$ be an algebraic set with $\mathfrak{a} \in \text{Rad}(k[X_1, \dots, X_n])$. Then for any algebraic extension K/k there is a Galois connection

$$\mathcal{P}(k[X]) \xleftrightarrow[V_K(-; X)]{I_K(-; X)} \mathcal{P}(X(K))$$

which satisfies all the same properties as Proposition 5.1.1. The image of $V_K(-; X)$ constitutes a topology on $X(K)$, which we denote by $\text{Zar}_k(X(K))$, whence we have a Galois connection

$$\text{Rad}(k[X]) \xleftrightarrow[V_K(-; X)]{I_K(-; X)} \text{Zar}_k(X(K))$$

such that $V_K(-; X) \circ I_K(-; X) = \mathbf{1}$. Furthermore the induced topology on $X(K)$ is precisely the subspace topology inherited from $\text{Zar}_k(K^n)$.

Remark 5.1.4

When $\mathfrak{a} = (0)$ then this coincides with the previous definition.

5.1.1 Nullstellensatz

For this section fix a **non-algebraically closed** base field k . We refine the statement of Proposition 5.1.4 when the extension field K is \bar{k} . In this case we may establish a lattice isomorphism between maximal ideals (resp. radical ideals) and Galois orbits (resp. “closed sets”). Note that this is a more general form of the usual Nullstellensatz which requires $k = \bar{k}$. Clearly the statement of results in this section simplifies substantially in this case, because the action of $\text{Aut}(\bar{k}/k)$ is then trivial.

First we establish a precise form of the so-called Weak Nullstellensatz

Proposition 5.1.5 (Weak Nullstellensatz II)

Let $X = V(\mathfrak{a})$ be a k -algebraic set with $k[X]$ the coordinate ring. There is a pair of mutually inverse maps

$$\text{Specm}(k[X]) \xleftrightarrow[V_{\bar{k}}(-; X)]{I_{\bar{k}}(-; X)} X(\bar{k}) / \text{Aut}(\bar{k}/k)$$

between maximal ideals of $k[X]$ and $\text{Aut}(\bar{k}/k)$ -orbits of \bar{k} -rational points. Explicitly we write

$$I_{\bar{k}}([x]; X) = I_{\bar{k}}(\{x\}; X) =: M_{X,x}$$

Proof. First we claim that $I_{\bar{k}}([x]; X) = I_{\bar{k}}(\{x\}; X)$. For if $x = \sigma(y)$ then $f(y) = \sigma(f(x))$ and $f(y) = 0 \iff f(x) = 0$. This also holds when $X = k^n$.

Let $M_{k^n, x} = I_{\bar{k}}(\{x\})$ then by Weak Nullstellensatz I it is maximal. Further $x \in X(\bar{k}) \implies \{x\} \subseteq V_{\bar{k}}(\mathfrak{a}) \implies \mathfrak{a} \subseteq M_{k^n, x}$. Consider the canonical surjective homomorphism with kernel \mathfrak{a}

$$\pi : k[X_1, \dots, X_n] \rightarrow k[X]$$

then by Proposition 5.1.3

$$M_{X,x} = \pi(M_{k^n, x}) \quad M_{k^n, x} = \pi^{-1}(M_{X,x})$$

and by 3.4.19 $M_{X,x}$ is a maximal ideal. If $M_{X,x} = M_{X,y}$ then $M_{k^n, x} = M_{k^n, y}$ which by the Weak Nullstellensatz implies $x = \sigma(y)$, and therefore the map is injective.

Similarly suppose $M_X \triangleleft k[X]$ is a maximal ideal then $M := \pi^{-1}(M_X)$ is a maximal ideal (3.4.19) containing \mathfrak{a} . By the Weak Nullstellensatz I it is of the form $M_{k^n, x}$ for $x \in \bar{k}^n$. And because $\mathfrak{a} \subseteq M_{k^n, x}$ we have $x \in X(\bar{k})$. Furthermore $M_X = \pi(M_{k^n, x}) = M_{X,x}$, and the map is surjective as required.

Note $I_{\bar{k}} V_{\bar{k}}(M_{X,x})$ is an ideal containing $M_{X,x}$. By maximality it is either $M_{X,x}$ or $k[X]$. But as $V_{\bar{k}}(M_{X,x})$ is non-empty it must be the former (since 1 does not have any zeros). Therefore the maps given are mutual inverses and $V_{\bar{k}}(M_{X,x}) = [x]$. \square

Corollary 5.1.6 (Weak Nullstellensatz III)

Every proper ideal $\mathfrak{b} \triangleleft k[X]$ has a common zero in $X(\bar{k})$, i.e. $V_{\bar{k}}(\mathfrak{b}) \neq \emptyset$.

In particular when $k = \bar{k}$ then \mathfrak{b} proper implies $V(\mathfrak{b}) \neq \emptyset$.

Proof. By Proposition 3.4.9 \mathfrak{b} is contained in a maximal ideal \mathfrak{m} . By Proposition 5.1.5 it is of the form $M_{X,x}$ for $x \in X(\bar{k})$. By definition x is a zero of \mathfrak{b} . \square

Proposition 5.1.7 (Characterization of closed set)

Let $\mathfrak{b} \triangleleft k[X]$ and $x \in X(\bar{k})$ then

$$x \in V_{\bar{k}}(\mathfrak{b}) \iff \mathfrak{b} \subseteq M_{X,x}$$

In particular

$$I_{\bar{k}}V_{\bar{k}}(\mathfrak{b}) = \bigcap_{\mathfrak{b} \subseteq \mathfrak{m}} \mathfrak{m} = \sqrt{\mathfrak{b}}^J$$

Proof. This follows by definition and the correspondence between maximal ideals and \bar{k} -rational points. \square

Furthermore we have noted before that in general $\sqrt{\mathfrak{a}} \subseteq IV(\mathfrak{a})$. The more refined version is that these are equal when $K = \bar{k}$. The proof uses the Rabinowitsch Trick, which we slightly abstract here.

Lemma 5.1.8 (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 $\bar{\cdot} : A \rightarrow A/\mathfrak{a}$ and the corresponding map $A[Y] \rightarrow (A/\mathfrak{a})[Y]$. Applying this to the above shows $1 - Y\bar{f}$ is invertible in $(A/\mathfrak{a})[Y]$. So by 3.6.2 \bar{f} is nilpotent in (A/\mathfrak{a}) whence $f \in \sqrt{\mathfrak{a}}$. \square

Proposition 5.1.9 (Strong Nullstellensatz)

Let $\mathfrak{b} \triangleleft k[X]$ then

$$I_{\bar{k}}V_{\bar{k}}(\mathfrak{b}) = \sqrt{\mathfrak{b}} = \bigcap_{\mathfrak{b} \subseteq \mathfrak{m}} \mathfrak{m} = \sqrt{\mathfrak{b}}^J$$

Proof. Note the second equality has already been demonstrated in Proposition 5.1.7.

First we consider the case $X = k^n$ and $k[X] = k[X_1, \dots, X_n]$. Let $\mathfrak{a} \triangleleft k[X]$ and choose $f \in I_{\bar{k}}V_{\bar{k}}(\mathfrak{a})$. Consider the ring $B := k[X_1, \dots, X_n, Y]$ and the ideal $\tilde{\mathfrak{a}} = \mathfrak{a}B + (1 - Yf)$. Clearly this has no zeros in \bar{k}^{n+1} , so by the Weak Nullstellensatz it is not proper. By the previous Lemma $f \in \sqrt{\mathfrak{a}}$ as required. The reverse inclusion is clear.

Now suppose that $X = V(\mathfrak{a})$, $k[X] = k[X_1, \dots, X_n]/\mathfrak{a}$ and $\mathfrak{b} \triangleleft k[X]$ is proper. Using Propositions 5.1.3 and 3.4.16 together with the result just proven, shows

$$I_{\bar{k}}(V_{\bar{k}}(\mathfrak{b}; X); X) = \pi(I_{\bar{k}}V_{\bar{k}}(\pi^{-1}\mathfrak{b})) = \pi(\sqrt{\pi^{-1}(\mathfrak{b})}) = \sqrt{\mathfrak{b}}$$

where $\pi : k[X_1, \dots, X_n] \rightarrow k[X]$ is canonical surjective morphism. \square

Corollary 5.1.10

Let $k[X]$ be any finitely generated reduced k -algebra, then $k[X]$ is a Jacobson ring, i.e.

$$\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}}^J$$

Corollary 5.1.11 (Irreducible \iff prime)

An algebraic subset $V_{\bar{k}}(\mathfrak{b}; X)$ is irreducible in the (k) -Zariski topology for $X(\bar{k})$ if and only if $\sqrt{\mathfrak{b}}$ is a prime ideal.

Proof. Let $Y = V(\mathfrak{b}; X) = V(\sqrt{\mathfrak{b}}; X)$. Then we may assume without loss of generality that \mathfrak{b} is radical. Suppose that $Y = V(\mathfrak{b})$ is irreducible and $\mathfrak{c}\mathfrak{d} \subseteq \mathfrak{b}$ then

$$V(\mathfrak{b}) \subseteq V(\mathfrak{c}\mathfrak{d}) = V(\mathfrak{c}) \cup V(\mathfrak{d})$$

By the irreducibility criterion (Proposition 4.1.7) we find, say $V(\mathfrak{b}) \subseteq V(\mathfrak{c})$. Apply I to find $\mathfrak{c} \subseteq \sqrt{\mathfrak{c}} \subseteq \sqrt{\mathfrak{b}} = \mathfrak{b}$. This shows by the prime ideal criterion 3.4.11 that \mathfrak{b} is prime. The converse is similar. \square

Corollary 5.1.12

Let $X = V(\mathfrak{a})$ be a k -algebraic set, then there is a dual isomorphism between radical ideals and “Zariski”-closed subsets of $X(\bar{k})$.

$$\text{Rad}(k[X]) \xleftrightarrow[V_{\bar{k}}(-; X)]{I_{\bar{k}}(-; X)} \text{Zar}_k(X(\bar{k}))$$

under which

- maximal ideals correspond to $\text{Aut}(\bar{k}/k)$ -orbits of single points $x \in X(\bar{k})$
- prime ideals correspond to irreducible subsets of $X(\bar{k})$

Proof. The content of the Strong Nullstellensatz is precisely that $I_{\bar{k}}(-; X) \circ V_{\bar{k}}(-; X) = \mathbf{1}$. The other direction was already proven so we have a dual order isomorphism. The statement about maximal ideals was already shown in Proposition 5.1.5. \square

Remark 5.1.5

When $k = \bar{k}$ the $\text{Aut}(\bar{k}/k)$ -orbits are just the singleton sets, and we obtain the “classical” nullstellensatz results.

5.1.2 Morphisms of Algebraic Sets**5.1.3 Structure Sheaf for Algebraic Sets with $k = \bar{k}$**

For this section assume $k = \bar{k}$ is algebraically closed.

Definition 5.1.6 (Principal Open Set)

For $X = V(\mathfrak{a})$ and $f \in k[X]$, define the principal open set

$$D(f) := \{x \in X(k) \mid f(x) \neq 0\} = X \setminus V(f)$$

Lemma 5.1.13

The principal open sets form a basis for the Zariski topology, closed under finite intersection.

Proof. Let $U = X \setminus V(\mathfrak{b})$ be an open set. Then $f \in \mathfrak{b} \implies V(\mathfrak{b}) \subseteq V(f) \implies D(f) \subseteq U$ as required. Furthermore $V(\mathfrak{b}) = \bigcap_{f \in \mathfrak{b}} V(f)$ whence $\bigcup_{f \in \mathfrak{b}} D(f) = U$. \square

Definition 5.1.7 (Structure Sheaf)

Let $X = V(\mathfrak{a})$ be an algebraic set. We say a function $f : U \rightarrow k$ is regular at $x \in X$ if there exists $g, h \in k[X]$ and a neighbourhood $V \ni x$ such that

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

We say f is regular on U if it is regular at all $x \in U$. Then we may define the structure sheaf

$$\mathcal{O}_X(U) := \{f : U \rightarrow k \mid f \text{ regular}\}$$

It's clear that by definition this is a sheaf, and furthermore that (X, \mathcal{O}_X) is a space of functions.

Proposition 5.1.14

Let $X = V(\mathfrak{a})$ be an algebraic set and $f \in k[X]$. There is a canonical map

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

which is an isomorphism.

Proof. The map is given by

$$\frac{a}{f^n} \longrightarrow (y \mapsto a(y)f(y)^{-n})$$

Note that

$$\begin{aligned} \frac{a}{f^n} = \frac{b}{f^m} &\iff f^r(f^m a - f^n b) \quad \text{some } r > 0 \\ &\iff f^r(y)(f^m(y)a(y) - f^n(y)b(y)) \quad \forall y \in X \\ &\iff f^r(y)(f^m(y)a(y) - f^n(y)b(y)) \quad \forall y \in D(f) \\ &\iff a(y)f(y)^{-n} = b(y)f(y)^{-m} \quad \forall y \in D(f) \end{aligned}$$

which shows that the map is both well-defined and injective.

In order to show that the given map is surjective, consider $\sigma \in \mathcal{O}_X(D(f))$

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

If $f \in J$ then $\phi(f)\sigma = \phi(g/f^r) \implies \sigma = \phi(g/f^{r+1})$ as required.

Suppose $f \notin J$ then as J is proper it's contained in a maximal ideal \mathfrak{m}_x . Observe $x \in D(f)$. By definition there is an open neighbourhood $x \in W \subseteq D(f)$ and elements h_1, h_2 such that

$$\sigma(y) = \frac{h_1(y)}{h_2(y)} \quad \forall y \in W$$

Now choose h_3 such that $x \in D(h_3) \subseteq W$. then $\phi(h_3 h_2)\sigma = \phi(h_1 h_3)$. Therefore $h_3 h_2 \in J$. But by construction $h_3(x)h_2(x) \neq 0$ a contradiction. \square

5.1.4 Rational points over finite fields and the Zeta Function

For this section let $k = \mathbb{F}_p$ be the finite field of order p and $\phi : \overline{\mathbb{F}_p} \rightarrow \overline{\mathbb{F}_p}$ be the Frobenius automorphism. Let $k_d = \mathbb{F}_{p^d}$ be the unique subfield of $\overline{\mathbb{F}_p}$ order p^d (3.16.44).

By Proposition 3.16.45 we have a tower of Galois extensions

$$k \subset k_d \subset \bar{k}$$

$\text{Gal}(\bar{k}/k)$ acts on each, restricting to an action on $\text{Gal}(k_d/k)$ on k_d/k preserving degree.

Let $X = V(\mathfrak{a}) \subset \mathbb{A}_k^n$ be an algebraic set (defined over k), then we have an inclusion

$$X(k) \subset X(k_d) \subset X(\bar{k})$$

It will be useful to partition solutions more precisely by degree, so we use the following lemma

Lemma 5.1.15

Let $x \in X(\bar{k})$ then

$$\deg(x) = \text{lcm}(\deg_k(x_i))$$

Furthermore for $n > 0$

$$\deg(x) \mid d \iff x \in X(k_d) \iff \phi^d(x) = x$$

and $\text{Gal}(k_d/k)$ acts freely on the elements of degree exactly d .

Proof. Let $k(x) := k(x_1, \dots, x_n)$, then recall (5.1.1) by definition that $\deg(x) = [k(x) : k] = d$ for some d . Similary define $d_i := \deg(x_i) = [k(x_i) : k]$.

Note $k(x_i) \subseteq k(x)$ is a subfield therefore by 3.16.1 we have $d_i \mid d$, so $\text{lcm}_i(d_i) \mid d$.

Let $d' := \text{lcm}_i(d_i)$ then by 3.16.44 we have $k(x_i) \subseteq k_{d'}$ which implies $k(x) \subseteq k_{d'}$. By 3.16.1 again $d' \mid d$ and $d = d'$.

For the second statement

$$\begin{aligned} \deg(x) \mid d &\iff \text{lcm}(\deg_k(x_i)) \mid d \\ &\iff \deg_k(x_i) \mid d \quad \forall i \\ &\iff x_i \in k_d \quad \forall i \quad 3.16.47 \\ &\iff \phi^d(x_i) = x_i \quad \forall i \quad 3.16.47 \\ &\iff \phi^d(x) = x \end{aligned}$$

First by (...) $\text{Gal}(k_d/k)$ preserves degree. Suppose $\deg(x) = d$ and $\text{Gal}(k_d/k) = \langle \phi \rangle$ is a cyclic group of order d . Suppose $\phi^r(x) = x$ for $0 < r < d$. Then we have shown $x \in X(k_r)$, which implies $d = \deg(x) \mid r$ and therefore $d \mid r$ a contradiction. That is $\text{Gal}(k_d/k)$ acts freely on elements of degree exactly d . \square

Let

$$X_d := \{x \in X(\bar{k}) \mid \deg(x) = d\}$$

Then $\text{Gal}(k_d/k)$ acts freely on X_d so that by Proposition 3.3.16 the orbits have order d . The restriction map

$$\text{Gal}(\bar{k}/k) \longrightarrow \text{Gal}(k_d/k)$$

is surjective by Proposition 3.16.38, and the two actions on X_d commute. Therefore X_d also has orbits of order d under the action of the absolute Galois Group. Furthermore we see

$$\#X(k_m) = \sum_{d|m} \#X_d$$

Recall there is a bijection preserving degree

$$X(\bar{k})/\text{Gal}(\bar{k}/k) \longrightarrow \text{Specm}(k[X])$$

Then since the orbits of X_d have order d we have $\#X_d = d \times \#B_d$ where

$$B_d = \{\mathfrak{m} \in \text{Specm}(k[X]) \mid \deg(\mathfrak{m}) = d\}$$

and

$$\#X(k_m) = \sum_{d|m} d \times \#B_d$$

Proposition 5.1.16 (Zeta function of an algebraic set over a finite field)

Formally as elements of the power series ring $\mathbb{Q}[[T]]$ we have

$$Z(X, T) := \prod_{\mathfrak{m} \in \text{Specm}(k[X])} (1 - T^{\deg(\mathfrak{m})})^{-1} = \exp \left(\sum_{m=1}^{\infty} \frac{\#X(k_m)}{m} T^m \right)$$

Proof. Let $Z(X, T)$ be the right hand side then

$$\begin{aligned} \log(Z(X, T)) &= \sum_{m=1}^{\infty} \#X(k_m) \frac{T^m}{m} \\ &= \sum_{m=1}^{\infty} \sum_{d|m} (d \times \#B_d) \frac{T^m}{m} \\ &= \sum_{d=1}^{\infty} \#B_d \sum_{r=1}^{\infty} \frac{T^{rd}}{r} \\ &= - \sum_{d=1}^{\infty} \#B_d \log(1 - T^d) \end{aligned}$$

□

Example 5.1.8

For $X(k) = k^n$ we have $\#X(k_m) = p^{mn}$. Then

$$Z(X, T) = \exp \left(\sum_{n=1}^{\infty} \frac{p^{mn} T^m}{m} \right) = \exp(-\log(1 - p^n T)) = \frac{1}{1 - p^n T}$$

5.1.5 Cotangent Space

Proposition 5.1.17

Let A be a ring with maximal ideal \mathfrak{m} . Then there exists a canonical ring isomorphism

$$A/\mathfrak{m}^k \xrightarrow{\sim} A_{\mathfrak{m}}/\mathfrak{m}^k A_{\mathfrak{m}}$$

given by

$$a + \mathfrak{m}^k \longrightarrow \frac{a}{1} + \mathfrak{m}^k A_{\mathfrak{m}}$$

Proof. This will follow from Corollary ?? if we show that $x \in A \setminus \mathfrak{m}$ is co-prime to \mathfrak{m}^k . First of all by maximality it is clearly true for $k = 1$. The general case follows from (...). □

Proposition 5.1.18

Let $X = V(\mathfrak{a})$ be an algebraic set with coordinate ring $k[X]$. Then for the maximal ideal $M_{X,x}$ there are canonical isomorphisms

$$k[X_1, \dots, X_n]/M_x^k \longrightarrow k[X]/M_{X,x}^k \longrightarrow k[X]_{M_{X,x}}/m_x^k$$

where $m_x = M_{X,x}k[X]_{M_{X,x}}$

5.1.6 Tangent Space

Proposition 5.1.19

Let $F \in k[X_1, \dots, X_n]$ and $g_i \in k[T]$. Then

$$\frac{d}{dT} F(g_1(T), \dots, g_n(T)) = \sum_{i=1}^n \frac{\partial F}{\partial X_i}(g_1(T), \dots, g_n(T)) g'_i(T)$$

Let $F \in k[X_1, \dots, X_n]$ and $x, v \in k^n$. Then we claim the following are equivalent

- $F(x) = 0$ and $0 = \sum_{i=1}^n \frac{\partial F}{\partial X_i}(x) v_i$
- $P(T) := F(x + vT)$ has zero as a root of multiplicity ≥ 2 , i.e. $v_T(P) \geq 2$.
- $P(0) = P'(0) = 0$

In this case we say the line $L_{x,v} = \{x + vt \mid t \in k\}$ is tangent to $X = V(F)$ at x .

Definition 5.1.9

For $X = V(\mathfrak{a})$ and $x \in X$ define the linear subspace of k^n by

$$\Theta_{X,x} = \{v \in k^n \mid \sum_{i=1}^n v_i \frac{\partial F}{\partial X_i}(x) = 0 \quad \forall F \in \mathfrak{a}\}$$

Geometrically this is an affine hyperplane at x which is tangent to the algebraic set X . We expect the dimension of this hyperplane to be constant as a function of x except at a few isolated points (cusps or singularities). Certainly it's finite-dimensional

Proposition 5.1.20

Suppose $\mathfrak{a} = (F_1, \dots, F_m)$, $X = V(\mathfrak{a})$ and $x \in X$ then

$$\Theta_{X,x} = \{v \in k^n \mid \sum_{j=1}^n v_j \frac{\partial F_i}{\partial X_j}(x) = 0 \quad i = 1 \dots m\}$$

i.e. it is the kernel of the matrix acting on $k^n \rightarrow k^m$

$$\left(\frac{\partial F_i}{\partial X_j}(x) \right)$$

Proof. Clearly LHS is contained in the RHS. Conversely suppose v is in the RHS. For an arbitrary $F \in \mathfrak{a}$ we have $F = \sum_{i=1}^m g_i F_i$. Then

$$\frac{\partial f}{\partial X_j}(x) = \sum_{i=1}^m F_i(x) \frac{\partial g_i}{\partial X_j}(x) + \sum_{i=1}^m g_i(x) \frac{\partial F_i}{\partial X_j}(x) = \sum_{i=1}^m g_i(x) \frac{\partial F_i}{\partial X_j}(x)$$

Taking scalar product with v shows that v is contained in the LHS. □

Corollary 5.1.21

Let $X = \mathbb{A}_k^n$ and $x \in X$ then $\Theta_{X,x} = k^n$.

$$M_{X,x} = \{f \in k[X] \mid f(x) = 0\}$$

Define the k -bilinear map

$$\begin{aligned} M_{X,x}/M_{X,x}^2 \times \Theta_{X,x} &\rightarrow k \\ (\bar{F} + M_{X,x}^2, v) &\rightarrow \sum_{i=1}^n \frac{\partial F}{\partial X_i}(x) v_i \end{aligned}$$

We claim it's well-defined for suppose $\bar{F} = \bar{G}$ then by definition $F - G \in \mathfrak{a}$. In particular the definition of the tangent space implies $\sum_{i=1}^n \frac{\partial F}{\partial X_i}(x) v_i = \sum_{i=1}^n \frac{\partial G}{\partial X_i}(x) v_i$. Suppose $\bar{F} \in M_{X,x}^2$, then $\bar{F} = \sum_{i=1}^n \bar{G}_i \bar{H}_i$ for $G_i, H_i \in M_{\mathbb{A}_k^n, x}$.

5.2 Abstract Varieties and Schemes

We observed that for X an (affine) algebraic set that the coordinate ring $k[X]$ is an algebraic invariant which quite rigidly determines the regular functions. The idea behind the abstract approach is to reverse the direction, and construct a geometric object from an algebraic one in an “essentially inverse” way. First this will be just reduced k -algebras, and secondly for schemes this will be for arbitrary commutative rings.

5.2.1 Maximal Spectrum

We observed that for X an algebraic set that $k[X]$ is a finitely generated reduced k -algebra. It's possible to reverse the construction in some sense

Definition 5.2.1 (Maximal Spectrum)

Let A be a ring. Define

$$\text{Specm}(A) := \{[\mathfrak{m}] \mid \mathfrak{m} \triangleleft A\}$$

For $S \subseteq A$ define

$$V(S) := \{[\mathfrak{m}] \mid S \subseteq \mathfrak{m}\}$$

and for $Y \subseteq \text{Specm}(A)$ define

$$I(Y) = \bigcap_{[\mathfrak{m}] \in Y} \mathfrak{m}$$

Proposition 5.2.1 (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

$$\mathcal{P}(A) \xrightleftharpoons[V]{I} \mathcal{P}(\text{Specm}(A))$$

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 Proposition 5.1.1. The relation $IV(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ results from the Strong Nullstellensatz, or from the definition of a Jacobson ring. \square

Proposition 5.2.2 (Maximal ideals are closed)

All the points of $\text{Specm}(A)$ are closed.

Proof. $V(\mathfrak{m}) = \{[\mathfrak{m}]\}$ by maximality. \square

We see that this construction is equivalent

Proposition 5.2.3

Let $X = V(\mathfrak{a})$ be an algebraic set with coordinate ring $k[X]$. If $k = \bar{k}$ then there is a commutative diagram

$$\begin{array}{ccc} \text{Specm}(k[X]) & \xrightleftharpoons[I]{V} & k[X] \\ \uparrow \simeq & & \downarrow = \\ X & \xrightleftharpoons[I]{V} & k[X] \end{array}$$

where the left arrow is the bijection described in Proposition 3.17.3 and is in fact a homeomorphism. For general k we still have a commutative diagram

$$\begin{array}{ccc}
\mathrm{Specm}(k[X]) & \xleftarrow[V]{I} & k[X] \\
\uparrow \simeq & & \downarrow = \\
X(\bar{k})/G_k & \xleftarrow[V_{\bar{k}}]{I_{\bar{k}}} & k[X]
\end{array}$$

5.2.2 Prime Spectrum

The maximal spectrum construction is only useful when A is a f.g. k -algebra.

Definition 5.2.2

Let A be a ring, then define the prime spectrum of A to be the set

$$\mathrm{Spec}(A) = \{[\mathfrak{p}] \mid \mathfrak{p} \triangleleft A\}$$

For $\mathfrak{a} \triangleleft A$ define

$$V(\mathfrak{a}) := \{[\mathfrak{p}] \mid \mathfrak{a} \subseteq \mathfrak{p}\}$$

and for $Y \subseteq \mathrm{Spec}(A)$ define

$$I(Y) = \bigcap_{[\mathfrak{p}] \in Y} \mathfrak{p}$$

Proposition 5.2.4 (Properties of Prime Spectrum)

Consider $(\mathrm{Spec}(A), A)$ for a ring A then we have a Galois connection

$$\mathcal{P}(A) \xleftarrow[V]{I} \mathcal{P}(\mathrm{Spec}(A))$$

That is

- V and I are order-reversing
- $S \subseteq I(V(S))$
- $Y \subseteq V(I(Y))$

and furthermore

- $I(Y)$ is a radical ideal
- $V(S) = V(\langle S \rangle) = V(\sqrt{\langle S \rangle})$
- $IV(\mathfrak{a}) = \sqrt{\mathfrak{a}}$
- $\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$
- $\bigcap_i I(W_i) = I(\bigcup_i W_i)$
- $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$

In particular the closed sets $V(\mathfrak{a})$ induce a topology (Zariski) on $\mathrm{Spec}(A)$. Furthermore

- $VI(Y) = \bar{Y}$

Proof. The proof is the same as Proposition 5.2.1, except for the relation $IV(\mathfrak{a}) = \mathfrak{a}$ which is precisely Proposition 3.4.14.

Last bit TODO □

The Zariski topology differs to the maximal case because not all points are closed. More precisely

Proposition 5.2.5 (Closed points are maximal ideals)

$[\mathfrak{p}] \in \mathrm{Spec}(A)$ is a closed point if and only if \mathfrak{p} is a maximal ideal. In other words

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

More precisely

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}) = \{\mathfrak{q} \mid \mathfrak{q} \supseteq \mathfrak{p}\} \tag{5.1}$$

Proof. Equation (5.1) follows from the definitions and the fact $V(\mathfrak{p}) = VI(\{\mathfrak{p}\}) = \overline{\{\mathfrak{p}\}}$ from the final result in Proposition 5.2.4.

Then by Proposition 4.1.3 $\{\mathfrak{p}\}$ is closed if and only if $\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}}$ if and only if \mathfrak{p} is contained in no proper prime ideals, i.e. if and only if it is maximal (see Lemma (...)) \square

Similarly to Proposition ?? we may characterize irreducible subsets of $\text{Spec}(A)$ as the zero-locus of prime ideals

Proposition 5.2.6 (Irreducible subsets)

Let A be a ring (resp. Jacobson ring) and $X = \text{Spec}(A)$ (resp. $\text{Specm}(A)$).

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 Corollary 5.1.11. \square

Corollary 5.2.7

$\text{Spec}(A)$ (resp. $\text{Specm}(A)$) 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 Proposition 5.2.6 \square

We may summarize in a correspondence much as in the classical case

Corollary 5.2.8 (Closed set and ideal correspondence)

Let A be a ring (resp. Jacobson ring) and $X = \text{Spec}(A)$ (resp. $\text{Specm}(A)$) then there is a bijective correspondence

$$\{Y \subset X \text{ closed}\} \xleftrightarrow[\text{I}]{\text{V}} \{\mathfrak{a} \triangleleft A \text{ radical}\}$$

under which

- Prime ideals correspond to irreducible closed subsets
- Minimal prime ideals correspond to irreducible components
- Maximal ideals correspond to closed points

Proof. The correspondence follows directly from 5.2.4. The first statement follows from 5.2.6 \square

There is another way of viewing the non-closed points :

Proposition 5.2.9 (Prime Spectrum is Sober)

The prime spectrum $\text{Spec}(A)$ is sober, i.e. there is a bijection

$$\mathfrak{p} \rightarrow \overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$$

between points and irreducible closed subsets. Minimal primes correspond to irreducible components and maximal ideals correspond to closed singleton sets.

Proof. It's well-defined and surjective by Proposition 5.2.6. 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. \square

Definition 5.2.3 (Principal Open Sets of Prime Spectrum)

Let A be a ring (resp. Jacobson ring) and $X = \text{Spec}(A)$ (resp. $\text{Specm}(A)$) 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 $D(f) = X \iff f \in A^*$.

Proposition 5.2.10 (Principal Open Sets from a Base)

Let A be a ring (resp. Jacobson ring) and $X = \text{Spec}(A)$ (resp. $\text{Specm}(A)$). 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 Proposition 4.1.2 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) $D(g) \subseteq D(f) \iff V((f)) \subseteq V((g)) \iff \sqrt{(g)} \subseteq \sqrt{(f)} \iff g \in \sqrt{(f)} \iff f \mid g^N$.

If $f \mid g^N$ then clearly $S_f \subseteq \overline{S_g}$ which implies $\overline{S_f} \subseteq \overline{S_g}$ by Proposition 3.5.10. Conversely we see $f \in \overline{S_g} \implies af \in S_g$ by Proposition 3.5.10 which implies $f \mid g^N$ as required. \square

Proposition 5.2.11 (Functoriality)

Let $\phi : A \rightarrow B$ be homomorphism then there is a natural map

$$\text{Spec}(\phi) : \text{Spec}(B) \rightarrow \text{Spec}(A)$$

$$\mathfrak{p} \rightarrow \phi^{-1}(\mathfrak{p})$$

and satisfies

$$\text{Spec}(\phi)^{-1}(D(f)) = D(\phi(f))$$

It is continuous with respect to the Zariski topology. If any one of the following conditions holds

- ϕ is surjective.
- B is integral over A
- 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

$$\text{Specm}(B) \rightarrow \text{Specm}(A)$$

Proof. That the map is well-defined follows from Proposition 3.4.18. The same result shows that when ϕ is surjective then it maps maximal ideals to maximal ideals. Suppose that B is integral over A then we have an injective ring homomorphism

$$\bar{A} := A/\phi^{-1}(\mathfrak{m}) \rightarrow B/\mathfrak{m} =: \bar{B}$$

which is integral and for which \bar{B} is a field. Therefore by Proposition 3.15.4 \bar{A} is a field and $\phi^{-1}(\mathfrak{m})$ is maximal by Proposition 3.4.22 as required.

TODO final case \square

Proposition 5.2.12

The canonical morphism $i_f : A \rightarrow A_f$ induces a homeomorphism

$$\text{Spec}(i_f) : \text{Spec}(A_f) \longrightarrow D(f) \subset \text{Spec}(A)$$

Proof. We claim that

$$D(f) = \{\mathfrak{p} \mid \overline{S_f} \cap \mathfrak{p} = \emptyset\}$$

then the bijection would follow from Corollary 3.5.9. 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. \square

5.2.3 Abstract Structure Sheaf (Integral Case)

Note in the case of an algebraic set X with coordinate ring $k[X]$ we associated to it a natural structure sheaf \mathcal{O}_X (5.1.7) such that $\mathcal{O}_X(D(f)) = k[X]_f$. We may mimic this for an arbitrary ring A replacing the coordinate ring $k[X]$. First we illustrate the results for an integral domain A , as this is a bit easier and demonstrates the essential argument.

Proposition 5.2.13

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 (...) 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 3.4.14 it's enough to show that $I \subseteq \mathfrak{p} \implies f \in \mathfrak{p}$. But $I \subseteq \mathfrak{p} \implies f_i \in \mathfrak{p} \implies \mathfrak{p} \notin D(f_i) \implies \mathfrak{p} \notin D(f)$ by hypothesis. Therefore \mathcal{O}'_X is a \mathcal{B} -sheaf as required. \square

5.2.4 Abstract Structure Sheaf (General Case)

For this section we generalize the structure sheaf construction to a general ring A , and let $X = \text{Spec}(A)$. We will also consider the case A a Jacobson ring and $X = \text{Specm}(A)$.

The main result is the following

Proposition 5.2.14 (Structure Sheaf)

Let A be a ring and $X = \text{Spec}(A)$. Recall from 5.2.10 that

$$D(f) \subseteq D(g) \iff \overline{S_f} \subseteq \overline{S_g}$$

There is a \mathcal{B} -presheaf \mathcal{O}'_X , defined over the principal open sets by

$$\mathcal{O}'_X(D(f)) := A_f$$

with the canonical restriction maps defined in Proposition 3.5.18. It is in fact a 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

$$\text{Mor}(\mathcal{O}_X, \mathcal{G}) \rightarrow \text{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}})$$

$$\phi \longrightarrow \phi|_{\mathcal{B}} \circ \eta_A$$

for all sheaves \mathcal{G} . Further there is an isomorphism of stalks (at $x = [\mathfrak{p}]$) yielding a commutative diagram for $f \notin \mathfrak{p}$

$$\begin{array}{ccccc} A_f & \xlongequal{\quad} & \mathcal{O}'_X(D(f)) & \xrightarrow{\sim} & \mathcal{O}_X(D(f)) \\ \downarrow & & \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\sim} & \mathcal{O}'_{X,x} & \xrightarrow{\sim} & \mathcal{O}_{X,x} \end{array}$$

where the left hand diagram is given in Proposition 3.5.21. Finally the canonical map $i_f : A \rightarrow A_f$ induces a homeomorphism

$$\tilde{i}_f : \text{Spec}(A_f) \rightarrow D(f)$$

and an isomorphism of sheaves

$$\tilde{i}_{f*}(\mathcal{O}_{\text{Spec}(A_f)}) \longrightarrow \mathcal{O}_X|_{D(f)}$$

Explicitly for $D(h) \subseteq D(g) \subseteq D(f)$ we have a commutative diagram

$$\begin{array}{ccccccc} \mathcal{O}_{\text{Spec}(A_f)}(\text{Spec}(A_f)) & \xleftarrow{\eta_{A_f,1}} & (A_f)_1 & \xleftarrow{\sim} & A_f & \xleftarrow{\eta_{A,f}} & \mathcal{O}_X(D(f)) \\ \downarrow & & \downarrow i_{1(g/1)} & & \downarrow i_{fg} & & \downarrow \\ \mathcal{O}_{\text{Spec}(A_f)}(D(g/1)) & \xleftarrow{\eta_{A_f,g/1}} & (A_f)_{g/1} & \xleftarrow{\sim} & A_g & \xleftarrow{\eta_{A,g}} & \mathcal{O}_X(D(g)) \\ \downarrow & & \downarrow i_{(g/1)(h/1)} & & \downarrow i_{gh} & & \downarrow \\ \mathcal{O}_{\text{Spec}(A_f)}(D(h/1)) & \xleftarrow{\eta_{A_f,h/1}} & (A_f)_{h/1} & \xleftarrow{\sim} & A_h & \xleftarrow{\eta_{A,h}} & \mathcal{O}_X(D(h)) \end{array}$$

where the inner diagram is from Proposition 3.5.19, 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. Observe that $D(f) = D(g) \iff \overline{S_f} = \overline{S_g}$, so we may construct a \mathcal{B} -presheaf

$$\mathcal{O}'_X(D(f)) = A_f = \overline{S_f}^{-1} A$$

with restriction maps the canonical maps from Proposition 3.5.18. 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 Proposition 4.2.5 there is a sheaf \mathcal{O}_X together with a canonical isomorphism of sheaves

$$\eta_A : \mathcal{O}'_X \rightarrow \mathcal{O}_X|_{\mathcal{B}}$$

such that there is a bijection (natural in \mathcal{G})

$$\text{Mor}(\mathcal{O}_X, \mathcal{G}) \longrightarrow \text{Mor}(\mathcal{O}'_X, \mathcal{G}|_{\mathcal{B}})$$

$$\alpha \rightarrow \alpha|_{\mathcal{B}} \circ \eta_A$$

This shows the existence of the required isomorphism and its universal property. Furthermore the isomorphism of stalks is also the content of Propositions 4.2.5 and 3.5.21.

We claim there is an isomorphism of \mathcal{B} -presheaves

$$\tilde{i}_{f*}(\mathcal{O}'_{\text{Spec}(A_f)}) \longrightarrow \mathcal{O}'_X|_{D(f)} \quad (5.2)$$

This is precisely the inner part of the commutative diagram stated and is demonstrated in Proposition 3.5.19. 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 Lemma 5.2.15

$$1 = \sum_i g_i f_i^N$$

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 sufficiently large N . Observe the canonical map

$$A_{f_i} \rightarrow A_{f_i f_j}$$

is given by

$$a / f_i^r \rightarrow a f_j^r / (f_i f_j)^r$$

Therefore by the compatibility assumption we have

$$(f_i f_j)^M (f_j^N a_i - f_i^N a_j) = 0 \quad (5.3)$$

for sufficiently large M . By Lemma 5.2.15 there is a partition of unity

$$1 = \sum_j g_j f_j^{N+M}$$

Define

$$a := \sum_j g_j f_j^M a_j$$

Then using Equation (5.3)

$$f_i^{N+M} a = f_i^{N+M} \sum_j g_j f_j^M a_j = a_i f_i^M \sum_j g_j f_j^{N+M} = a_i f_i^M$$

and therefore $f_i^M(f_i^N a - a_i) = 0$, which means precisely $\sigma|_{D(f_i)} = \sigma_i$ as required. Therefore \mathcal{O}'_X is a \mathcal{B} -sheaf.

The statement about A_f is a somewhat tedious and formal consequence of the results already shown.

Let $\mathcal{B}|_f$ be the principal open sets contained in $D(f)$, which is therefore a base for $D(f)$ in the subspace topology. Note that as functors of sheaves

$$(-)|_{\mathcal{B}|_f} \circ (-)|_{D(f)} = (-)|_{D(f)} \circ (-)|_{\mathcal{B}}$$

Similarly let \mathcal{B}_f be the base for $\text{Spec}(A_f)$ then as functors we have

$$(-)|_{\mathcal{B}|_f} \circ \tilde{i}_{f*} = \tilde{i}_{f*} \circ (-)|_{\mathcal{B}_f}$$

By 4.2.6 $(-)|_{\mathcal{B}|_f}$ is full and faithful when acting on sheaves so there is a bijection

$$\text{Mor}(\tilde{i}_{f*}(\mathcal{O}_{\text{Spec}(A_f)}), \mathcal{O}_X|_{D(f)}) \xrightarrow{(-)|_{\mathcal{B}|_f}} \text{Mor}(\tilde{i}_{f*}(\mathcal{O}_{\text{Spec}(A_f)}|_{\mathcal{B}_f}), \mathcal{O}_X|_{\mathcal{B}|_{D(f)}})$$

and by Proposition 2.3.8 it reflects isomorphisms. We may compose isomorphisms as follows

$$\tilde{i}_{f*}(\mathcal{O}_{\text{Spec}(A_f)}|_{\mathcal{B}_f}) \xrightarrow{\tilde{i}_{f*}(\eta_{A_f})^{-1}} \tilde{i}_{f*}(\mathcal{O}'_{\text{Spec}(A_f)}) \xrightarrow{\sim} \mathcal{O}'_X|_{D(f)} \xrightarrow{\eta_A|_{D(f)}} \mathcal{O}_X|_{\mathcal{B}|_{D(f)}}$$

(where the middle was shown in (5.2)) and reflect it back to get the stated isomorphism. □

We used the following Lemma

Lemma 5.2.15 (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

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

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