Ring Theory

Jacob Denson

March 1, 2018

Table Of Contents

1 Basic Definitions **1**
- 1.1 Basic Algebraic Structure of Rings . . . 3
- 1.2 Ideals . . . 7

2 Commutative Rings **11**
- 2.1 Euclidean Domains . . . 12
- 2.2 Maximal Ideals . . . 13
- 2.3 Uniqueness of Congruences . . . 14
- 2.4 Factorial Rings . . . 15
- 2.5 Nilradicals . . . 18
- 2.6 Localization . . . 18
- 2.7 Properties Preserved Under Localization . . . 23
- 2.8 Local Rings . . . 26
- 2.9 Dedekind Rings . . . 34

3 Modules **36**
- 3.1 Abelian Categories . . . 39

4 Algebras **42**
- 4.1 Matrix Rings . . . 42

5 Linear Algebra **45**

Chapter 1

Basic Definitions

The simplest operation one can perform is counting, which leads to the analysis of addition and multiplication on the integers. Rings are abstract objects which abstract operations possessing qualities common to addition and multiplication. More specifically, a **ring** is a set upon which an additive and multiplicative operation is defined, with respective identities often denoted by 0 and 1. The additive structure forms an abelian group, the multiplicative structure a not-necessarily commutative monoid structure, which play nice with one another thanks to the distributive law, that for any a, b, c, $a(b+c) = ab + ac$, and $(b+c)a = ba + ca$. Note that one equation does not imply the other due to the fact that the multiplicative operation is in general not abelian.

Example. *The integers* $\mathbf{Z}$ *form the classical example of a ring, and we find they exhibit most of the basic properties of rings. They have a nontrivial divisibility theory, yet still possess the property of unique factorization into prime elements, an idea we will study in the more general situation of 'unique factorization domains'.*

Example. *Your favourite number systems* $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{F}_p$, *and* $\mathbf{C}$ *are all rings, which provide the best examples of fields.*

Example. *If* K *is a field, the algebra of* $n \times n$ *matrices* $M_n(K)$ *forms a ring under addition and multiplication. The analysis of this ring forms the field of basic linear algebra. We shall find the discussion of canonical forms for matrices forms a particular application to the theory of modules over subrings of matrices.*

Example. *A key way to analyze the algebraic structure of a ring A is to introduce encodings of algebraic structure through the theory of polynomials $A[X]$ over that ring, formal sums of the form*

$$a_0 + a_1 X + \cdots + a_N X^N$$

where $a_n \in A$. We will discuss these rings, and their multivariate counterparts $A[X_1, \ldots, X_n]$, later on in these notes.

Example. *The theory of rings arises very often in the study of functions. If A is a ring, and X is a set then one can make the set A^X of maps from X to A into a ring, by definining addition and multiplication pointwise. Thus, for instance, the set $\mathbf{R}^{\mathbf{N}}$ of real valued sequences forms a ring, as does $\mathbf{R}^{\mathbf{R}}$. Subrings of these rings occur all the time in analysis.*

Remark. It is often assumed that $1 \neq 0$ in a ring. This is because if $1 = 0$, then the ring structure is particularly trivial. In any ring, $a \cdot 0 = 0$; the proof follows from the distributive law, since

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Multiplying the equation $1 = 0$ by a, we conclude that $a = 0$ for all elements a of the ring, which implies the ring consists of a single element: the number zero! We denote the zero ring by (0).

Rings arise naturally when we start studying symmetries of preexisting algebraic structures. Matrices are symmetries of vector spaces, which themselves can be seen as shifting symmetries of space. Polynomials are symmetries over a field of numbers, which themselves are also very well behaved symmetries. In fact, like groups, all rings can be represented as symmetries of some abelian group.

Example. *Let G be an abelian group, and consider the set $\mathrm{End}(G)$ of all homomorphisms from G to itself. We define a ring structure on this group. Given $f, g \in \mathrm{End}(G)$, we define $f + g$ to be the endomorphism on G defined by $(f + g)(x) = f(x) + g(x)$, and where composition $f \circ g$ is the multiplicative structure. The fact that $\mathrm{End}(G)$ satisfies the laws of a ring are trivial, with the identity behaving as 1, and the trivial homomorphism acting as 0.*

Theorem 1.1. *All rings naturally arise as endomorphism of an abelian group.*

Proof. Let A be a ring, and consider the set $\mathrm{End}(A^+)$ of group homomorphisms on the abelian additive structure of A. We will show that A can be embedded in $\mathrm{End}(A^+)$ in a natural way. Consider the map $\varphi : A \to \mathrm{End}(A^+)$ defined by $\varphi(y) = f_y$, where $f_y : A \to A$ is a map defined by $x \mapsto yx$. Since the distributive law in R holds, we findt

$$f_y(x+z) = y(x+z) = yx + yz = f_y(x) + f_y(z)$$

which means exactly that f_y is a morphism. What's more, φ is a ring morphism (a morphism is defined exactly how you think it should be), since

$$f_{y+z}(x) = (y+z)x = yx + zx = (f_y + f_z)(x)$$

$$f_{yz}(x) = (yz)x = y(zx) = (f_y \circ f_z)(x)$$

$$f_1 = \mathrm{id}_R \qquad f_0(x) = 0x = 0$$

And φ is injective, for if $f_x = f_y$, then

$$f_x(1) = x = f_y(1) = y$$

Thus $\mathrm{End}(A^+)$ naturally contains A. □

The problem with this proof is that the theorem doesn't really give a 'nice' answer to what a ring really is. Groups are already abstract, so we may not necessarily be able to visualize what a symmetry of an arbitrary abstract object is. Alas, most general theories in mathematics do not have natural correspondences with a single object of study, unlike the niceities of group theory. This is to be expected, since ring theory arose from many fields of study, like number theory, geometry, and logic. We will just have to accept this theorem as a little tidbit of intuition, and move on. We will return to this idea in the theory of modules, where one studies a ring 'acting' on an abelian group, just like Cayley's theorem gives us group actions on sets and the corresponding representation theory of groups on symmetric groups.

1.1 Basic Algebraic Structure of Rings

We begin with discussing an operation that seems left out of the definition of a ring – divisibility. In the ring of rational numbers, we can divide a

rational number by any *non-zero* rational number, and still get a rational number. On the other hand, an integer divided by an integer is only in very special cases an integer. If A is a ring, the **units** are the elements x which possess a multiplicative inverse x^{-1} such that $xx^{-1} = 1 = x^{-1}x$; note both ends of the equation need to be satisfied since ab may not equal to ba. In terms of functions, a function may be injective but not surjective, or vice versa.

Example. *Consider the set $\mathbf{R}^{\mathbf{N}}$ of real-valued sequences, which form an abelian group under pointwise addition. Take the set of morphisms on this set. This consists of two maps – the left shift L and the right shift R:*

$$L(x_0, x_1, x_2, \dots) = (x_1, x_2, \dots) \qquad R(x_0, x_1, \dots) = (0, x_0, x_1, \dots)$$

Then $L \circ R = \mathrm{id}_{\mathbf{R}^{\mathbf{N}}}$, yet $R \circ L(x_0, x_1, \dots) = (0, x_1, \dots)$. L could never have an inverse, since it is not bijective.

Theorem 1.2. *If an element a in a ring has a left and a right inverse, then these inverses are equal, and a is a unit.*

Proof. Suppose $x, y \in A$ satisfies $xa = 1$ and $ay = 1$. Then $x = xay = y$. □

We shall denote the set of units of a ring by $A^\times$ or $U(A)$. This set always forms a multiplicative group, and never a subring. If $U(A) = A - \{0\}$, and $A \neq (0)$, then we say A is a **division ring**, or **skew field**. This is as many units as we can possibly hope to get, because if $0 \cdot a = a \cdot 0 = 1$, then $0 = 1$. Commutative division rings are called **fields**.

Example. *Here are basic examples of units in the field.*

1. *The group of units in $M_n(K)$ is the general linear group $GL_n(K)$, the space of invertible n by n matrices. In this ring, it is true that if $yx = I$, then $xy = I$, but this is certainly not true in all rings.*

2. *The group of units in $\mathbf{Z}$ is $\{0, 1\}$. The group of units in $\mathbf{F}_n$ is the set of integers coprime to n, and their study marks an important part of number theory.*

Not all division rings need be commutative.

Example. *Let G be a group, and K a field. The group ring $K[G]$ is the set of all finite sums $\sum a_n g_n$, with $a_n \in K$, and $g_n \in G$, with an obvious additive structure, and such that*

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh = \sum_{k\in G}\left(\sum_{gh=k} a_g b_h\right)k$$

This multiplication is given by a form of convolution in the coefficients. The quaternion division ring $\mathbf{H}$*, named after their creator, Hamilton, are quantities of the form $a+bi+cj+dk$, and with algebraic operations induced as $\mathbf{R}[Q]$, where Q is the group of unit quaternions $\{1,i,j,k\}$, where $i^2=j^2=k^2=ijk=-1$. Every non-zero quaternion is invertible, since if we define $\overline{z}=a-bi-cj-dk$ for $z=a+bi+cj+dk$, then a simple calculation reveals $z\overline{z}=a^2+b^2+c^2+d^2$, which is nonzero if one of a,b,c, or d is nonzero. Quaternions are not commutative, since $ij=k$, $ji=-k$. Invented by the irishman, lord Hamilton, in the mid 19th century, to algebricate the rotations in three dimensional space, the quaternions have a special place in an algebraist's heart for they are one of the first truly strange algebraic structures to occur in mathematics.*

Example. *George Boole began the modern study of logic by studying the algebraic notions of truth. He saw that the logical operations of conjunction and disjunction behaved very similarily to the algebraic operations of multiplication and addition. If we consider conjunction as the multiplicative structure in a set of statements, and exclusive disjunction as an additive structure (where two statements are equivalent if they both imply each other), then we obtain a ring, satisfying $x^2=x$ for all statements x, and where 0 is a statement that is always false, and 1 a statement which is always true. In his honour, we call a ring* **Boolean** *if this equation is satisfied. Any Boolean ring is commutative, since $1=xyxy$, which implies, by multiplying by yx on the right $yx=xy$. These are essentially the same as the Boolean algebras studied in logic and measure theory, and the exact correspondence is provided by the Stone representation theorem, employing tools of topology!*

Example. *In number theory, it is natural to consider data defined on the positive integers, functions $f:\mathbf{Z}^+\to A$, where A is some commutative ring. Often, given two functions g, sums come up of the form*

$$(f*g)(N)=\sum_{mn=N} f(m)g(n)$$

known as the **Dirichlet convolution** *of f and g. This turns the family of all functions into a commutative ring, whose unit element is the function $\delta(N) = [N = 1]$. We say a function f is* **multiplicative** *if $f(mn) = f(m)f(n)$ whenever m and n are coprime integers. If f and g are both multiplicative functions, then $f * g$ is also multiplicative, since if N and M are coprime, then*

$$(f*g)(NM) = \sum_{ab=NM} f(a)g(b) = \sum_{\substack{n_1n_2=N \\ m_1m_2=M}} f(n_1m_1)g(n_2m_2)$$
$$= \sum_{n_1n_2=N} f(n_1)g(n_2) \sum_{m_1m_2=M} f(m_1)g(m_2) = (f*g)(N)(f*g)(M)$$

The **Möbius function** *μ is the function such that $\mu(1) = 1$, $\mu(p_1 \dots p_n) = (-1)^n$ if the p_n are distinct, and $\mu(n) = 0$ if p^2 divides n for some prime p. If 1 denotes the constant 1 function on $\mathbf{Z}^+$, then 1 is easily seen to be multiplicative. μ is also multiplicative, since if n and m are coprime, and a perfect square divides neither integer, then $n = p_1 \dots p_N$, $m = q_1 \dots q_M$, and then $nm = p_1 \dots p_N q_1 \dots q_M$, so $\mu(nm) = (-1)^{N+M} = (-1)^N(-1)^M$. If a perfect square divides n or m, a perfect square divides nm, and so $\mu(nm) = 0 = \mu(n)\mu(m)$. This means that $1 * \mu$ is multiplicative, and we find*

$$(1*\mu)(p^N) = \sum_{m=0}^{N} \mu(p^m) = 1 - 1 = 0$$

so $1 * \mu = \delta$. The Möbius inversion formula says $f = g * \mu$ if and only if $f * 1 = g$, and this is nothing more than saying that 1 is invertible with inverse μ.

As with groups, one may consider subrings of a ring, and homomorphisms between rings. By now, you should be able to figure out the definitions yourself, but for completeness, we now specify them. A **subring** of a ring is a subset of a ring which also possesses a ring structure. That is, a subring is closed under addition and multiplication.

Example. *The most fundamental chain of commutative subrings is $\mathbf{Z} < \mathbf{Q} < \mathbf{R} < \mathbf{C}$. If you want things to get really interesting, you can identify $\mathbf{C}$ as a subring of the ring $\mathbf{H}$ of Hamiltonians.*

Example. *The family of diagonal matrices in $M_n(K)$ form a subring. Since the map $\lambda \mapsto diag(\lambda, \lambda, \dots, \lambda)$ is an isomorphism of K with the family of diagonal matrices, it is often convinient to let $\lambda \in K$ denote the diagonal matrix in*

$M_n(K)$ with elements λ. This notation is often used when discussing algebras over a ring – in this case, $M_n(K)$ is an algebra over K.

Example. *If A is a ring, the center $Z(A)$ is defined to be the set of elements a such that, for all $b \in A$, $ab = ba$. Then $Z(A)$ is a commutative subring of A.*

Example. *The continuous functions form a subring of $\mathbf{R}^{\mathbf{R}}$, as do the polynomial functions, or differentiable functions, and so on and so forth.*

A ring homomorphism from a ring A to a ring B is a function $f : A \to B$ which is a homomorphism of abelian groups, and a homomorphism of the multiplicative monoid structure on the two spaces. In other words, f must satisfy

$$f(a+b) = f(a) + f(b) \qquad f(ab) = f(a)f(b)$$
$$f(1) = 1 \qquad f(0) = 0$$

As with groups and vector spaces, the kernel $\mathrm{Ker}(f)$ of the map f is defined to be the set of all a such that $f(a) = 0$.

1.2 Ideals

We wish to establish a quotient structure on rings, and obtain analogies of the isomorphism theorems for groups. Let's consider $\mathfrak{a}$ as a subset of a ring A, and try to determine which properties allow the cosets $A/\mathfrak{a}$ of the form $x + \mathfrak{a}$ allow the operations on A to be well defined on the quotient. In order to even define these cosets, we first need $\mathfrak{a}$ to be an additive subgroup of the additive group structure on $\mathfrak{a}$. Since all subgroups of abelian groups are normal, this means the operation of addition on the quotient is well defined. In order for multiplication to be well defined, we need to conclude $(a + \mathfrak{a})(b + \mathfrak{a}) = (ab + \mathfrak{a})$. In terms of sets, this says

$$\{(a+x)(b+y) = ab + xb + ay + xy : x, y \in \mathfrak{a}\} = \{ab + x : x \in \mathfrak{a}\}$$

Thus we require $xb + ay + xy \in \mathfrak{a}$ for any $x, y \in \mathfrak{a}$. This implies that $\mathfrak{a}$ not *only* needs to be closed under multiplication, but also closed under multiplication by an element of A, both on the left and the right. We define a **left ideal** of a ring A to be an additive subgroup $\mathfrak{a}$, with $A\mathfrak{a} = \mathfrak{a}$, in the sense that if $a \in A$, and $x \in \mathfrak{a}$, then $ax \in \mathfrak{a}$. A **right ideal** satisfies $\mathfrak{a}A = \mathfrak{a}$,

and a **double-sided ideal** is a left and right ideal, which is the structure we use to form the quotient ring $A/\mathfrak{a}$. We shall focus mostly on double sided ideals, for which the quotient ring is well defined. One sided ideals come into play most importantly when we analyze modules.

The intersection of a family of (left/right/two-sided) ideals is easily seen to be an ideal. A consequence is we can talk about a generating set of an ideal. We say a set S generates $\mathfrak{a}$ if $\mathfrak{a}$ is the smallest ideal containing S (If S is finite, we say $\mathfrak{a}$ is finitely generated). Using this fact, we can define algebraic operations on ideals. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, then $\mathfrak{a}+\mathfrak{b}$, viewed as a set theoretic addition, is an ideal, and is the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$. More generally, we can take infinite sums of ideals, often using the notation $\bigoplus \mathfrak{a}_\alpha$, which is just the smallest ideal containing all the ideals in the sum. Together with intersection, we find that the family of ideals forms a complete lattice on the subsets of a ring. More interestingly, we can form the product $\mathfrak{ab}$ of ideals, which is the ideal generated by products of the form ab, for $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Note that these operations are *not* sufficient to define a ring structure on the family of ideals, though they do form a monoid under addition and multiplication.

If $\mathfrak{a}$ and $\mathfrak{b}$ are two sided ideals in a ring, then one trivially verifies that $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. In the case of the integers, one obtains a strict equality here. On the other hand, in general we do not have inequality, but if $\mathfrak{a}+\mathfrak{b} = A$ (we say $\mathfrak{a}$ and $\mathfrak{b}$ are **coprime**, most often in the commutative case), then we do have equality, for if $a+b=1$, and $c \in \mathfrak{a} \cap \mathfrak{b}$, then $c = c(a+b) = ca+cb$, and both the quantities in this sum are in $\mathfrak{ab}$. The distributive law $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{ab}+\mathfrak{ac}$ is always satisfied. On the other hand, we do not always know that $\mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ (though in the integers this is true). We can conclude this is true if $\mathfrak{a} \supset \mathfrak{b}$ or $\mathfrak{a} \supset \mathfrak{c}$, a fact known as the *modular law*. We also find that $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{ab}$ in the integers, but we only have $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{ab}$ in general rings.

Example. *In a commutative ring A, two-sided ideals and one sided ideals correspond, and for any $x \in A$, the set $(x) = \{ax : a \in A\}$ is an ideal of A, known as a* **principal ideal**. *If A is a commutative ring where every ideal is principal, we say it is a* **principal ideal ring**. *The notation (x) isn't used too often in non-commutative ring theory, where we do not know whether to interpret (x) as the left ideal, the right ideal, or the two sided ideal, except in the case of (1) and (0). But in the commutative case, the notation is very nice, and allows us to very algebraically discuss the theory of divisiblity, since (x) is the set of*

elements which x 'divides', in notation generalized from the integers. In the non-commutative case, we often use the notation Ax, or xA, as a subtitute, and AxA as the two sided ring, which is really defined to be the set

$$\{a_1xb_1 + \cdots + a_Nxb_N : a_n, b_n \in A\}$$

for otherwise the set might not be an ideal. Any ideal can be generated by principal ideals in the sense that all ideals are of the form

$$ASA = \bigoplus_{s\in S} AsA$$

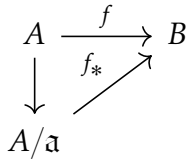
for some set S, and we say that S generates the ideal. In particular, if S can be selected as a finite set, we say the ideal is finitely generated.

Example. *In number theory, one learns Bezout's theorem, that the greatest common denominator of two integers a and b is the smallest positive integer c which can be written in the form $na + mb$, for some integers n and m. This implies that every ideal in $\mathbf{Z}$ is closed under the operation of taking greatest common denominators. If $\mathfrak{a}$ is a non-zero ideal of $\mathbf{Z}$, let $a \in \mathfrak{a}$ be it's smallest positive element. Then if $x \in \mathfrak{a}$ is nonzero, then $gcd(x, a)$ is a positive integer in $\mathfrak{a}$ no larger than a, and in particular, this means we must have $gcd(x, a) = a$, so $x \in (a)$, and so $\mathfrak{a} = (a)$.*

Example. *As should be expected, if $f : A \to B$ is a ring homomorphism, then the kernel $Ker(f)$ is a double sided ideal of A. Conversely, if $\mathfrak{a}$ is a two-sided ideal, then $A/\mathfrak{a}$ is a ring, and the projection $\pi : A \to A/\mathfrak{a}$ is a homomorphism with kernel $\mathfrak{a}$. A ring homomorphism is an isomorphism if and only if the kernel is trivial.*

Just as in group theory, we obtain a family of isomorphism theorems.

Theorem 1.3 (First Isomorphism Theorem)**.** *Let $f : A \to B$ be a homomorphism of rings. If $\mathfrak{a}$ is a double-sided ideal contained in the kernel of f, then there is a unique induced homomorphism $f_* : A/\mathfrak{a} \to B$ satisfying the commutative diagram*



If $\mathfrak{a}$ is the kernel, then f_* is injective.

Theorem 1.4 (Second Isomorphism Theorem)**.** *Let B be a subring of A, and $\mathfrak{a}$ an ideal of A. Then $B + \mathfrak{a}$ is a subring of A, $\mathfrak{a}$ is an ideal in $B + \mathfrak{a}$, $B \cap \mathfrak{a}$ is an ideal in B, and*

$$B/(B \cap \mathfrak{a}) \cong (B + \mathfrak{a})/\mathfrak{a}$$

Theorem 1.5 (Third Isomorphism Theorem)**.** *If $f : A \to B$ is a surjective homomorphism, there is a one-to-one correspondence with ideals of B and ideals of A that contain the kernel of f.*

Example. *In any ring A, the ideals $(1) = A$ and $(0) = \{0\}$ are known as* **trivial***. If K is a division ring, these ideals are the only ones which exist (one sided or two sided). This is because if $\mathfrak{a}$ is an ideal, and $x \in \mathfrak{a}$ is non-zero, then there is $y \in A$ such that $xy = yx = 1$, so $1 \in \mathfrak{a}$, and if 1 is in an ideal, every element $a \in A$ is $a \cdot 1 \in \mathfrak{a}$. The last example gives the important consequence that every ring homomorphism from a division ring into a nonzero ring is injective.*

A simple proof by induction shows that there is a unique homomorphism from the integers to any ring A, which in a sense, means they are the fundamental ring. They are in certain senses the fundamental ring object. The kernel of such a map is of the form (n), for a unique positive integer n. We call n the **characteristic** of the ring, and $\mathbf{Z}_n$ the **prime ring** contained within the ring. Note that since the characteristic of a ring is preserved by subrings, the prime ring is the smallest subring contained in A. We can think of these integers as actually being contained in A, so that 1 denotes the identity, 2 denotes $1 + 1 \in A$, and so on and so forth. Furthermore, since $\mathbf{Z}_n$ contains zero divisors if n is not prime, the characteristic of an integral domain is always either zero or a prime.

Chapter 2

Commutative Rings

We now assume all rings under discussion are commutative. A commutative ring is **entire**, or forms an **integral domain**, if it contains no zero-divisors. That is, if $ab = 0$ for two elements a and b, then $a = 0$ or $b = 0$. In particular, if a principal ring is entire it is called a **principal ideal domain**. This removes some of the nasty properties inherent in the general definition of rings. Here is an example.

Theorem 2.1. *If A is entire, and $a, b \neq 0$, then $(a) = (b)$ if and only if there is a unit $x \in U(A)$ such that $a = xb$.*

Proof. If $a = xb$ and $b = ya$, then $a = xya$, hence $(1 - xy)a = 0$, and since $a \neq 0$, we conclude that $1 - xy = 0$, so $x, y \in U(A)$. On the other hand, if $x \in U(A)$, then we find that

$$(a) = Aa = (Ax^{-1})(xb) = Ab = (b)$$

and so the two ideals are equal. □

An ideal $\mathfrak{p}$ is **prime** if $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. This mimics the definition of prime integers as those p such that if $nm \mid p$, then $n \mid p$ or $m \mid p$. An alternative definition is that $A/\mathfrak{p}$ is entire, which is easily verified.

Theorem 2.2. *The inverse image of a prime ideal under a homomorphism is prime.*

Proof. If $f : A \to B$, and $\mathfrak{p} \subset B$ is a prime ideal, then $f(ab) = f(a)f(b) \in \mathfrak{p}$ implies that $f(a) \in \mathfrak{p}$ or $f(b) \in \mathfrak{p}$, hence $f^{-1}(\mathfrak{p})$ is prime. □

The fact that prime ideals tell us almost everything we need to know about a ring is one of the tenets of commutative ring theory.

2.1 Euclidean Domains

If A is an integral domain, a **Euclidean function** on A is a function ord : $A - \{0\} \to \mathbf{Z}^+$ such that if $a, b \neq 0$, then there is q, r such that $a = qb + r$, where $\text{ord}(r) < \text{ord}(q)$. A **Euclidean domain** is a ring possessing a Euclidean function. For convinience, we define $f(0) = -\infty$.

Example. *The function $ord(n) = |n|$ is a Euclidean function on $\mathbf{Z}$, which is easily verified because of the Euclidean division algorithm. This is the first example of a Euclidean domain.*

Example. *The function $ord(f) = deg(f)$ is a Euclidean function on $K[X]$, for any field K. If*

$$f(X) = a_0 + a_1 X + \cdots + a_N x^N \qquad g(X) = b_0 + b_1 X + \cdots + b_M x^M$$

where $a_N, b_M \neq 0$. If $N < M$, we're done, for $f = 0 \cdot g + f$. If $N \geqslant M$, we can write

$$f = b_M^{-1} x^{N-M} g + (f - b_M^{-1} x^{N-M} g)$$

and the order of $f - b_M^{-1} x^{N-M} g$ is less than N.

Example. *The ring $\mathbf{Z}[i]$ of Gaussian integers of the form $n + im$, where $n, m \in \mathbf{Z}$, is a Euclidean domain if we define $ord(z) = |z|$. To verify this, given $z, w \in \mathbf{Z}[i]$ with $|z| \geqslant |w|$, pick $u \in \{w, iw, -w, -iw\}$ with an angle of $\leqslant \pi/4$ with z. Then*

$$|z-u|^2 = |z|^2 + |u|^2 - 2\langle z, u\rangle \leqslant |z|^2 + |w|^2 - \cos(\pi/4)|z||w| \leqslant (2-\sqrt{2})|z|^2 < |z|$$

and so $|z - u| < |z|$.

Theorem 2.3. *If A if a Euclidean domain, then A is principal.*

Proof. We mimic the proof that $\mathbf{Z}$ is principal. Let $\mathfrak{a}$ be a nonzero ideal in A, and let a be an element of smallest order. If $b \in \mathfrak{a}$, then we can write $b = qa + r$, where $\text{ord}(r) < \text{ord}(a)$. But $r = b - qa \in \mathfrak{a}$, so $r = 0$, and so a divides b. □

2.2 Maximal Ideals

An ideal $\mathfrak{m}$ is **maximal** if $\mathfrak{m} \neq A$, and there is no ideal strictly containing $\mathfrak{m}$ except the entire ring. and there is no ideal containing it but the entire ring, and the ideal itself is not the entire ring. Using Zorn's lemma in the classical manner, one may verify that any proper ideal of a ring is contained in some maximal ideal. The most useful fact about maximal ideals to use in basic proofs is to use the fact that if $a \notin \mathfrak{a}$, then $(a) + \mathfrak{m} = A$. Thus (0) is a prime ideal if and only if A is entire to begin with.

Theorem 2.4. *Every maximal ideal is prime.*

Proof. If $\mathfrak{m}$ is maximal, let $ab \in \mathfrak{m}$. If $a \notin \mathfrak{m}$, then $(a) + \mathfrak{m} = A$, and so we can write $xa + m = 1$ for some $x \in A$, $m \in \mathfrak{m}$. But this implies that $b = 1 \cdot b = xab + mb \in \mathfrak{m}$. □

Theorem 2.5. *An ideal $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ is a field.*

Proof. Suppose $\mathfrak{m}$ is maximal, and $a \notin \mathfrak{m}$. Then $(a) + \mathfrak{m} = A$, and so we can write $xa + m = 1$, which implies that $xa \cong 1$ modulo $\mathfrak{m}$. This verifies that all nonzero residues in the quotient ring have inverses. On the other hand, the third isomorphism theorem says there is a one to one correspondence between ideals in $A/\mathfrak{m}$ and ideals in A containing $\mathfrak{m}$. If $A/\mathfrak{m}$ is a field, then the only ideals are (0) and (1), implying that the only ideals containing $\mathfrak{m}$ are $\mathfrak{m}$ and A. This verifies $\mathfrak{m}$ is maximal. □

Example. *In the case of the ring $\mathbf{Z}$, the maximal ideals are $p\mathbf{Z}$, where p is a prime number. We already know that $\mathbf{Z}/p\mathbf{Z}$ is a field, and the theory of maximal ideals allows us to understand this from a different perspective.*

Example. *In the ring $C(X)$ of continuous functions on a locally compact Hausdorff space X, one finds that the ideals which form closed sets under the L^∞ metric are in one to one correspondence with closed subsets of X, such that for each set $C \subset X$, the ideal is the family of continuous functions vanishing on C. If $\mathfrak{m}$ is a maximal ideal in $C(X)$, then $\mathfrak{m}$ is closed, because the units of $C(X)$ form an open neighbourhood of the multiplicative identity. Thus if $\mathfrak{m}$ was dense in $C(X)$, it would contain a unit, which is impossible. The maximal ideals in $C(X)$ thus correspond to points in X, and the homomorphisms from $C(X)$ to the field formed by the quotient can be seen as the evaluation of the functions at that point.*

2.3 Uniqueness of Congruences

In classical number theory, one takes a series of integers $k_1, \ldots, k_m$ and values $a_1, \ldots, a_m$, and asks to find an integer N such that $N \equiv a_n$ modulo k_n for all n. The classical Chinese remainder theorem says that if the k_n are coprime, this can always be done. These ideas can be extended to solve congruences over general rings. In the general setup, we are given a family of ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_N$ over a commutative ring A, and we consider the corresponding projection π of A onto the product ring $A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_N$. The generalization of the Chinese remainder theorem is summarized in the next theorem.

Theorem 2.6. *π is surjective if and only if the ideals $\mathfrak{a}_n$ are pairwise coprime, and is injective if $\bigcap \mathfrak{a}_n = (0)$.*

Proof. Consider the case of two coprime ideals $\mathfrak{a}$ and $\mathfrak{b}$. Then there are a, b such that $a + b = 1$. This means a is congruent to 1 modulo $\mathfrak{b}$, and b is congruent to 1 modulo $\mathfrak{a}$, so $\pi(a) = (0, 1)$ and $\pi(b) = (1, 0)$. Given any $x, y \in A$, $\pi(ya + xb)$, we find $\pi(ya + xb) = y(0, 1) + x(1, 0) = (x, y)$, which solves our problem. In general, we note that it suffices to find elements a_n such that $\pi(a_n)_m = \delta_{nm}$, because then $\pi(\sum x_n a_n) = (x_1, \ldots, x_n)$. But if for each m, we find a_n^m such that $\pi(a)_n = 1$ and $\pi(a)_m = 0$, then the product over all $m \neq n$ satisfies the properties we desire of a_n. The injectivity property is obvious, because something congruent to zero in each $\mathfrak{a}_n$ is contained in the intersection. □

Example. *Given an integer n, the units of $\mathbf{Z}_n$ are in one to one correspondence with the set of integers $1 \leqslant m \leqslant n$ which are relatively prime to n. The Euler phi function $\varphi(n)$ is the number of such integers. The Chinese remainder theorem proves that φ is multiplicative. The map $\mathbf{Z} \mapsto \mathbf{Z}_n \prod \mathbf{Z}_m$, whose kernel is $(n) \cap (m) = (nm)$. Thus $\mathbf{Z}_{nm}$ is isomorphic to $\mathbf{Z}_n \times \mathbf{Z}_m$. In any two rings A and B, $U(A \times B) = U(A) \times U(B)$, which implies the number of units in $U(\mathbf{Z}_{nm})$ is the same as the product of the number of units in $U(\mathbf{Z}_n)$ with the number of units in $U(\mathbf{Z}_m)$. This implies the theorem.*

The function can be calculated by noting that $\varphi(p^n) = p^{n-1}(p-1)$, because there are p^n integers between 1 and p^n, and they are all relatively prime except for the multiples of p. An alternative, ring theoretic proof uses induction. If $n = 1$, then $\mathbf{Z}_p$ is a field, with every element invertible, so $\varphi(p) = p - 1$. The projection $\mathbf{Z} \to \mathbf{Z}_{p^n}$ induces a surjective homomorphism from $\mathbf{Z}_{p^{n+1}}$ to $\mathbf{Z}_{p^n}$,

with an induced surjective group homomorphism from $U(\mathbf{Z}_{p^{n+1}})$ to $U(\mathbf{Z}_{p^n})$. If x is invertible, and congruent to one modulo p^n, it is of the form $ap^n + 1$. For any $a \in \{0, \ldots, p-1\}$, $ap^n + 1$ is relatively prime to p^{n+1}, and so we conclude that that the kernel of the homomorphism has size p.

Example. *For each $n \in \mathbf{Z}$, the map $f_n : \mathbf{Z}_N \to \mathbf{Z}_N$ given by $f_n(m) = nm$ is an endomorphism of $\mathbf{Z}_N$. The map $n \mapsto f_n$ induces an isomorphism of $End(\mathbf{Z}_N)$ with $\mathbf{Z}_N$, and a group isomorphism $U(\mathbf{Z}_n)$ with the automorphisms of $\mathbf{Z}_N$. To see this, it is easy to see it is a homomorphism, and if nm is congruent to zero for all m, then in particular, $n \cdot 1 = n$ is congruent to zero.*

Thus, if $\bigcap \mathfrak{a}_n = (0)$ and the $\mathfrak{a}_n$ are coprime, A is isomorphic to the product of it's quotients, which indicates we only have to understand each of it's quotients to understand the entire ring. In particular, one can understand the set $\mathbf{Z}$ of integers once one can understand the quotients $\mathbf{Z}_p$ modulo a prime.

2.4 Factorial Rings

A **factorial ring** A is an integral domain such that every a can be written as $p_1 p_2 \ldots p_N$, for some irreducibles p_n, and such that if $p_1 \ldots p_N = q_1 \ldots q_M$, then $N = M$, and, after a permutation, each p_n differs from q_n by a unit. A principal, factorial ring is the place where the basic facts of number theory are best exposited.

Theorem 2.7. *Let A be a principal factorial ring. If $(a, b) = (c)$, then every d dividing a and b also divides c (such a c is known as a* **greatest common divisor***).*

Proof. If d divides a and b, then $(c) = (a, b) \subset (d)$, so d divides c. □

We say a ring is **Noetherian** if it satisfies the *ascending chain condition*. That is, there do not exist an infinite linear chain $\{\mathfrak{a}_\alpha\}$ of distinct ideals. This can be reworded by saying that every infinite chain of ideals

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$$

eventually has $\mathfrak{a}_N = \mathfrak{a}_M$ for sufficiently large N and M. Noetherian rings have a factorization theory, but this factorization need not be unique.

Theorem 2.8. *Every nonzero element of a Noetherian ring may be factored into irreducible elements.*

Proof. Fix some $x_0 \neq 0$. If x_0 is irreducible, we're done. Otherwise, we can write $x_0 = a_0 x_1$, where a and x_1 are both not units. If x_1 is not irreducible, we can write $x_1 = a_1 x_2$, where neither $a_1 x_2$ are not units. It is clear that if this process never stops, we can find elements $x_N \mid \cdots \mid x_2 \mid x_1 \mid x_0$, but none of these differ by a unit, which corresponds to an infinite chain

$$(x_0) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \dots$$

which is impossible since the ring is Noetherian. □

An equivalent definition of a Noetherian ring is one for which every ideal is finitely generated. If a ring satisfies the ascending chain condition, and an ideal $\mathfrak{a}$ was *not* finitely generated, then we could, by successively picking elements of $\mathfrak{a}$, find an infinite chain of increasing ideals, contradicting the ascending chain condition. Conversely, if we have an infinite chain of ideals

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \dots$$

then $\lim \mathfrak{a}_n = \mathfrak{a}_\infty$ is an ideal, hence finitely generated with $\mathfrak{a}_\infty = (x_1, \dots, x_n)$, and since the x_i lie in $\mathfrak{a}_N$ for large enough N (the limit of the ideals is just the union), we conclude that $\mathfrak{a}_N = \mathfrak{a}_\infty$ for large enough N. A consequence of this is that every principal ideal domain is Noetherian.

Theorem 2.9. *Every principal ideal domain is factorial.*

Proof. The fact that every principal entire ring *has* a factorization is justified because it is Noetherian. It now suffices to prove such a factorization is unique. Let $p_1 \dots p_N = q_1 \dots q_M$. We proceed by induction on N. If $p = q_1 \dots q_M$, then p divides one of the quantities on the right, implying p must divide one of the q_n, which, without loss of generality, we may assume is q_M. Then $q_M = ap$, so, dividing by p on both sides of the equation, we conclude that $1 = aq_1 \dots q_{M-1}$, so each q_n is a unit, which is a contradiction unless $M = 1$. Now in general, suppose $p_1 \dots p_{N+1} = q_1 \dots q_M$. Then p_{N+1} divides one of the quantities on the right, say q_M, so $q_M = ap_{N+1}$, hence, dividing out, we conclude $p_1 \dots p_N = aq_1 \dots q_{M-1}$, hence by induction, $N = M - 1$, and by permutation, we can assume $p_n = a_n q_n$. But then $p_1 \dots p_{N+1} = aa_1 \dots a_{M-1} p_1 \dots p_N q_M$, hence $p_{N+1} = aa_1 \dots a_{M-1} q_M$, so p_{N+1} differs from q_M by a unit. □

The *primes* of a factorial ring can be broken up into equivalence classes, where we identify two primes that differ by a unit. Picking one element p_α from each equivalence class allows us to literally uniquely decompose a nonzero element of the ring into a product of powers of p_α, multiplied by a unit at the end.

Example. *The integers are a principal ideal domain, so they are factorial. It groups of units are* 1 *and* -1*, so the equivalence class of primes consist of* p *and* $-p$*. It is canonical to take the positive primes as representatives, and so we find every positive integer can be uniquely decomposed as a product of primes, and every negative integer is the negation of a product of primes.*

In most rings of functions that form integral domains, being non factorial normally indicates the presence of some singularity.

Example. *Consider the curve in* $\mathbf{A}^2 = K^2$ *defined as the locus of points satisfying the equation* $Y^2 = X^3$*. Then the curve has a singularity at the origin. The corresponding ring* $K[X,Y]/(Y^2 - X^3)$*, often viewed as the ring of polynomial functions in two dimensions restricted to the curve, is not factorial, since* $X \neq Y$ *are both irreducible elements not differing by primes, yet* $X^3 = Y^2$*.*

Example. *The relation* $\sin^2 x = (1+\cos x)(1-\cos x)$ *indicates that the ring* $\mathbf{R}[\sin x, \cos x]$ *of functions generated by* $\sin x$ *and* $\cos x$ *is not a factorial ring. The fact that* $\sin x$*,* $1-\cos x$*, and* $1+\cos x$ *are irreducible follows from the fact that we have a* **trigonometric degree** *of a polynomial*

$$f(x) = a + b_1\cos(x) + \cdots + b_N\cos(Nx) + c_1\sin(x) + \cdots + c_M\sin(Mx)$$

where $b_N, c_M \neq 0$*, as* $\max(N,M)$*. One can show* $\deg(fg) = \deg(f) + \deg(g)$ *directly, but it is easier to extend to the complex algebra* $\mathbf{C}[e^{ix}]$*, which contains* $\mathbf{R}[\cos x, \sin x]$ *as a subring. The degree is well defined because* e^{ix} *is trancendental over* $\mathbf{R}$*, so the degree is just the degree of the polynomial. This follows from the integral calculation*

$$\int_{-\pi}^{\pi} e^{nix}e^{-mix} = \begin{cases} 2\pi & n = m \\ 0 & n \neq m \end{cases}$$

So given $f(x) = \sum a_n e^{nix}$*,*

$$a_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-nix}$$

And now it is easy to see that $\deg(fg) = \deg(f) + \deg(g)$. *This implies that* $\mathbf{R}[\sin x, \cos x]$ *has no zero divisors, and all degree one trigonometric polynomials are irreducible.*

2.5 Nilradicals

Recall that the nilradical of a commutative ring A is the ideal $\sqrt{A}$ of all *nilpotent* x, i.e. those elements with $x^n = 0$. The reason for the interest in a nilradical is that it removes nilpotent elements from the quotient. We now show a way to generalize the nilradical of a commutative ring to noncommutative cases, by showing the nilradical is equivalent to another construction. The **Jacobson radical** $J(R)$ of a (not necessarily commutative) ring R to be the intersection of all prime ideals in the ring. In the commutative case, we find $J(R) = \sqrt{R}$.

Theorem 2.10. *In a commmutative ring, the Jacobson radical is equal to the nilradical of the ring.*

Proof. If $\mathfrak{a}$ is a prime ideal, and $x^n = 0$, then $x^n \in \mathfrak{a}$, hence $x \in \mathfrak{a}$, showing $\sqrt{A} \subset J(A)$. Conversely, suppose $x \notin \sqrt{A}$. Consider the set S of all powers x^n. Let L be the set of all (not necessarily prime) ideals in A disjoint from S. Then L is nonempty, since (0) is in L, and L is inductively ordered, so we can consider some maximal element $\mathfrak{a}^*$. Given $a, b \notin \mathfrak{a}^*$, $\mathfrak{a}^* + (a)$ and $\mathfrak{a}^* + (b)$ are both strictly larger than $\mathfrak{a}^*$, and so there is x_1, y_1 and x_2, y_2 such that $x_1 + ay_1 = x^n$ and $x_2 + by_2 = x^m$. But then

$$x^{m+n} \in (\mathfrak{a}^* + (a))(\mathfrak{a}^* + (b)) = \mathfrak{a}^* + (a)\mathfrak{a}^* + (b)\mathfrak{a}^* + (ab)$$

And therefore $ab \notin \mathfrak{a}^*$, so $\mathfrak{a}^*$ is prime, not containing x, and so $J(R)$ does not contain x. □

2.6 Localization

In many situations, we study a commutative ring A with identity, and wish to invert elements of the ring which aren't necessarily units. Thus, given an element $a \in A$, we may wish to embed A in a larger ring B in which a has an inverse. Unfortunately, this is not always possible. For instance, if $a^2 = 0$, then we cannot possibly embed A in such a way that makes

a invertible. More generally, if $f : A \to B$ is a homomorphism in which $f(a)$ is invertible, and $ab = 0$, then we must have $f(b) = 0$. This implies that if we desire f to be injective, then the ring A cannot have any zero divisors. Nonetheless, if we remove this condition, then the only condition that prevents $f(a)$ from having an injective, then the only condition that prevents $f(a)$ from having an inverse is if $a = 0$. Identifying certain maps by a not necessarily injective map f is a process in algebra we now called localization.

Considering this problem in a more general viewpoint, we consider a set $S \subset A$, and try to find the 'most general' homomorhpism $f : A \to B$ such that $f(s)$ is invertible for each $s \in S$. If $f(s)$ and $f(t)$ are invertible, then $f(st) = f(s)f(t)$ is invertible, so we may assume from the outset that S is closed under multiplication. We may also assume that $1 \in S$, because $f(1)$ is always invertible. In this case, S is a multiplicative submonoid of A, which we call a **multiplicative set**. By 'localizing' S, we mean extending A to a space B in which all elements of S have an inverse.

The classical situation where we can localize is in the case where A is an integral domain, in which case the problems of zero divisors disappear completely. In this case, we can embed A into it's **field of fractions** B, which consist of formal quotients a/b, with $b \neq 0$, where a/b is identified with c/d if $ad - bc = 0$. After identification, we can define a multiplication and addition operation by setting $(a/b)(c/d) = ac/bd$, and by setting $(a/b) + (c/d) = (ad + bc)/bd$. It is simple to check these operations are well defined on B. Then B is given the structure of a commutative ring in which every nonzero element has an inverse. Thus B is not only and ring, but a field! We embed A by mapping a to the formal quotient $a/1$.

Example. *The localization of* $\mathbf{Z}$ *produces a field of fractions which is obviously just the rational numbers* $\mathbf{Q}$ *in disguise. Constructing the field of fractions over an integral domain is essentially just a generalization of this process.*

Example. *If* $A[X_1, \ldots, X_n]$ *is a polynomial ring with coefficients in some integral domain* A*, then the polynomial ring is an integral domain, and performing localization gives the field* $K(X_1, \ldots, X_n)$ *of rational functions over the field of fractions* A*, which consists of all finitary expressions of the form*

$$\frac{\sum a_\alpha X^\alpha}{\sum b_\beta X^\beta}$$

These can be considered as functions mapping certain 'nonsingular' elements of A into it's field of fractions K. In particular, f/g is defined at $x \in K$ if $g(a) \neq 0$, because then the quotient $f(a)/g(a) = f(a)g(a)^{-1}$ is well defined. As an example, the field of fractions of $\mathbf{Z}[X_1,\ldots,X_n]$ is the field $\mathbf{Q}(X_1,\ldots,X_n)$ of rational functions over the rationals.

Example. *Let $A(D)$ denote the complex algebra of functions holomorphic in some connected open region D of $\mathbf{C}$. Then $A(D)$ is an integral domain, for if $fg = 0$, where $f, g \neq 0$, then $f^{-1}(0)$ and $g^{-1}(0)$ are two discrete sets whose union is D, which is impossible. We may therefore form the field of fractions of $A(D)$, which is precisely the set of meromorphic functions on D. These functions f/g are defined except for certain points upon which $g(z) = 0$, except in the case that z is a removable singularity of g, which means that we can write $f/g = f_1/g_1$, where $g_1(z) \neq 0$.*

More generally, suppose that a commutative ring A has zero divisors. Then forming the field of fractions is impossible – we cannot give every element of A an inverse simultaneously. More generally, we might hope to find the 'most general' homomorphism $i : A \to S^{-1}A$ such that $i(s)$ is invertible for each element s in some multiplicative set S. In particular, we hope to find an object i and $S^{-1}A$ such that for *any* homomorphism $f : A \to B$ such that $f(s)$ is invertible for each $s \in S$, there is a homomorphism $f_* : S^{-1}A \to B$ such that $f = f_* \circ i$. This is an initial object in the category of homomorphisms from A which map S to units, which means it is unique up to isomorphism.

Often, the correct technique to finding a universal object is to determine what properties the object must have, and then trying to form a formal structure based on these properties. Given what we know, this object will either fail to be constructed in general, in which case we must try and find more properties of the object, or the formal object we construct will often be the required universal object. Let us try and derive what our initial object $S^{-1}A$ should be 'forced to have'. Note that if $f : A \to S^{-1}A$ is the required morphism, then the set B of elements of $S^{-1}A$ of the form $i(a)i(s)^{-1}$, for $a \in A$ and $s \in S$ is a subring of $S^{-1}A$ (an easy calculation left to the reader). This means that $i : A \to B$ is a map in which each $f(s)$ is invertible, and so there must be a map $i_* : S^{-1}A \to B$ such that $i = i_* \circ i$. Clearly i_* must be the identity map, which implies $B = S^{-1}A$. Now, let us determine when $i(a)i(s)^{-1} = i(b)i(t)^{-1}$. If this is true, then $i(at - bs) = 0$. One condition guaranteeing this to be true is if there is $u \in S$ for which

$u(at-bs)=0$, because then $f(u)f(at-bs)=0$, and multiplying by $f(u)^{-1}$ gives the required property. It turns out that these properties are sufficient to formally define $S^{-1}A$.

Consider the set $S^{-1}A$ whose objects are fractions a/s, as in the field of fractions of an integral domain, but where $a \in A$ and $s \in S$. We identify two fractions a/s and b/t if there is an element $u \in S$ such that $u(at-bs)=0$. We define multiplication by setting $(a/s)(b/t)=(ab/st)$, and addition by $a/s+b/t=(at+bs)/ts$. This gives $S^{-1}A$ a ring structure, and we have a map $i : A \to S^{-1}A$ given by $i(a)=a/1$, and then $i(s)^{-1}=1/s$. If $f : A \to B$ is any ring homomorphism in which $f(s)$ is invertible for each $s \in S$, then we can define $f_* : S^{-1}A \to B$ by $f_*(a/s)=f(a)f(s)^{-1}$, and then it is a simple procedure to verify that the required diagram commutes, and that f is unique. Thus $S^{-1}A$ is exactly the initial object we required.

Example. *Let X be a topological space, and let $C(X)$ denote the ring of all (real/complex valued) continuous functions defined on X. If $p \in X$, then set the set S of all functions f with $f(p) \neq 0$ is a multiplicative set containing 1, closed under multiplication, and not containing 0. Thus we can consider the localization $S^{-1}C(X)$, which we denote by $C(X)_p$. Since $C(X)$ is almost never an integral domain, the map $C(X) \to C(X)_p$ will likely not be injective. Indeed, two functions f and g will be identified in $C(X)_p$ if there is a function h with $h(p) \neq 0$, and with $h(f-g)=0$. Since $h(p) \neq 0$, the set of points q where $h(q) \neq 0$ contains an open neighbourhood of zero, and this implies that $(f-g)(q)=0$ on this neighbourhood. Conversely, it suitably nice topological spaces (where Urysohn's theorem applies), if f agrees with g in a neighbourhood of p, we can find a function h such that h vanishes outside this neighbourhood, and then $h(f-g)=0$. Thus functions are identified in $C(X)_p$ precisely when they are locally equal around p, and this is the context in which the term localization emerged, because localization takes a ring of functions, and identifies those functions which locally agree. More generally, if we set S to be the set of all functions with $f(p) \neq 0$ for all p in some $Y \subset X$, then $C(X)_Y$ consists of the equivalence class of all functions which agree on a neighbourhood of Y, provided we can construct functions vanishing outside of a neighbourhood of Y, with no zeroes on Y.*

Example. *Similarily, if M is a differentiable manifold, then the space $C^\infty(M)$ of (real/complex valued) differentiable functions on M forms a ring. For a fixed $p \in M$, the space of functions not vanishing at p forms a multiplicative set, and the corresponding localization corresponds to the equivalence class of*

differentiable functions which agree in a neighbourhood of p, known as the space of germs of differentiable functions at p. Viewed as a vector space over the real numbers, the dual space of germs of differentiable functions is used to construct the tangent space of a manifold at a point. A similar process is used to construct the germ of analytic functions on an analytic/holomorphic manifold, where we replace $C^\infty(M)$ with $C^\omega(M)$.

Perhaps this formal approach is not so intuitive from a more geometric perspective. There is a more 'natural' approach to forming $S^{-1}A$, but it is much more messy. When learning fractions for the first time, you viewed them as ways to 'divide' certain integers into other integers. If you have 6 apples, you can 'apply' the fraction $1/2$ to divide the apples into two sets of three apples, the fraction $1/3$ to divide the 6 apples into three sets of two, but one cannot apply the fraction $1/5$. In other words, we can view a fraction $1/n$ as a partial function on $\mathbf{Z}$ (defined on $n\mathbf{Z}$, to be precise), which outputs m when given input nm. Similarily, n/m is the partial function defined on the set of integers k such that nk is divisible by m, in which case applying n/m to k results in nk/m. It seems reasonable to set fractions equal if they agree on the common input upon which they are defined. That is, we should set $1/2 = 2/4$, because they have the same domain, and are equal to one another on this domain. To abstract these ideas to form $S^{-1}A$, we let Φ denote the set of all A-module homomorphisms from $(s) \to A$, for some $s \in S$. We then form a family of equivalence classes on Φ by identifying $f : (s) \to A$ and $g : (t) \to A$ if f and g agree on (st). On these equivalence classes, we can define addition between $f : (s) \to A$ and $g : (t) \to A$ by letting $f + g$ be the addition of the functions as morphisms from (st) to A. Similarily, we define fg to be $f \circ g$, once f and g are restricted to the proper ideals. We then embed A in Φ by mapping $a \in A$ to the 'multiplication by a' homomorphism from A to itself. Given $s \in S$, the inverse of s is the homomorphism with domain (s) mapping sa to a. Unfortunately, if A has zero divisors, then this approach does not work, in which case one must first quotient A by the ideal of all elements of A which are annihilated by elements of S.

Remark. Localization can be done in noncommutative rings. However, the resulting rings $S^{-1}A$ are extremely nontrivial to analyze, and as such we do not consider them. This follows because expressions of the form $rs^{-1}t + uv^{-1}w$ cannot in general be reduced to having a single common denominator. Thus one may have to repeat the process of localization

many times to obtain inverses for all elements of S, and even if we repeat the process finitely many times we may still not end up with all the right inverses. What's more, even if A has no zero divisors, it can still be difficult to determine if the localization of A is nontrivial. However, one can in certain situations achieve success, by generalizing the 'partial homomorphism' technique of the last paragraph. The general technique is known as Ore localization, and is left for another time.

2.7 Properties Preserved Under Localization

We have a map $\mathfrak{a} \to S^{-1}\mathfrak{a}$ from the ideals in A to the ideals in $S^{-1}A$, such that $S^{-1}\mathfrak{a}$ is the ideal generated by $i(\mathfrak{a})$. We can also described it as

$$S^{-1}\mathfrak{a} = \{a/s : a \in \mathfrak{a}, s \in S\}$$

The map also has nice algebraic properties, in that it represents sums, products, and intersections of ideals, so

$$S^{-1}(\mathfrak{a} + \mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b} \quad S^{-1}(\mathfrak{a}\mathfrak{b}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$$

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

and respects inclusions. Every ideal in $S^{-1}A$ is of the form $S^{-1}\mathfrak{a}$, because

$$S^{-1}(i^{-1}(\mathfrak{a})) = \{a/b : a \in \mathfrak{a}, b \in S\} = \mathfrak{a}$$

Thus localization doesn't add any new ideal structure to a ring.

Proposition 2.11. *If A is principal, then $S^{-1}A$ is principal.*

Proof. This follows because all ideals in A are of the form $S^{-1}\mathfrak{a}$, and if $\mathfrak{a} = (a)$, then $S^{-1}\mathfrak{a} = (a)$. □

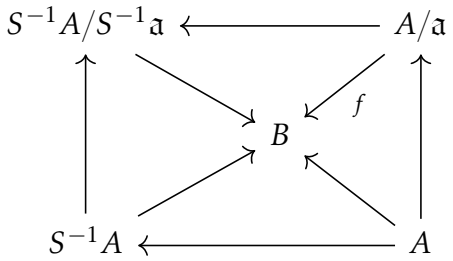
Proposition 2.12. *If A is Noetherian, then $S^{-1}A$ is Noetherian.*

Proof. If $S^{-1}(\mathfrak{a}_0) \subset S^{-1}(\mathfrak{a}_1) \subset \ldots$ is a chain of ideals in $S^{-1}A$, then $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots$, so eventually the $\mathfrak{a}_N$ are constant, so $S^{-1}\mathfrak{a}_N$ are constant. □

Because localization relates to a universal property of rings, it respects many of the useful transformations in the category of rings.

Proposition 2.13. *If A is a ring, S is a multiplicative subset, and $\mathfrak{a}$ is an ideal containing no elements in common with S, then $S^{-1}A/S^{-1}\mathfrak{a}$ is isomorphic to $(S/\mathfrak{a})^{-1}(A/\mathfrak{a})$, in a way which preserves the embedding of $A/\mathfrak{a}$ into the two sets.*

Proof. Let $f : A/\mathfrak{a} \to B$ be a ring homomorphism such that for each $s \in S/\mathfrak{a}$, $f(s)$ is invertible. Applying lifting techniques and universal properties, one can verify that given the canonical maps between the numerous rings associated with A, a function f on $A/\mathfrak{a}$ induces a unique diagram



where the left, bottom, and right triangles commute, as does the overall rectangle. But this implies that the top triangle, and thus the whole diagram, commutes, because we can make the upper triangle commute if we first apply the projection from A into $A/\mathfrak{a}$, and this map is surjective so the triangle itself must commute. Now conversely, any function from $S^{-1}A/S^{-1}\mathfrak{a}$ to B making the upper triangle commute induces a unique set of maps making the whole diagram above commute, so this map must be unique, and therefore $S^{-1}A/S^{-1}\mathfrak{a}$ is an initial object in the category defining the localized ring $(S/\mathfrak{a})^{-1}(A/\mathfrak{a})$, so the two rings must be isomorphic. □

Now let's show the localization of a factorial ring is factorial.

Lemma 2.14. *If A is entire, then $x \in A \cap U(S^{-1}A)$ if and only if $(x) \cap S \neq \varnothing$.*

Proof. If $x(m/n) = 1$, $xm = n \in S$. If $xm \in S$, then $x(m/xm) = 1$. □

Lemma 2.15. *If A is entire, and p is prime in A, then it is irreducible in $S^{-1}A$, provided it is not a unit.*

Proof. If $p = (m/n)(x/y)$, and it is not a unit, then $nyp = mx$, so $p \mid mx$. It follows that $p \mid m$ or $p \mid x$. In either case, we divide by p to conclude either m/n or x/y is a unit. □

Lemma 2.16. *Let A be factorial. Then a/b is irreducible if and only if $a/b = up$, where $u \in U(S^{-1}A)$, and p is irreducible in A and $S^{-1}A$.*

Proof. Let $a = p_1 \dots p_n$, and $b = q_1 \dots q_n$, where p_i and q_i are irreducible in A. Because a/b is irreducible, it follows that exactly one of the p_i is irreducible in $S^{-1}A$, and the other combined factors are units. But this means that p_i is irreducible in A as well. The converse is obvious. □

Lemma 2.17. *If y differs from x by a unit, and y is uniquely factorizable, then x is uniquely factorizable.*

Proof. Write $x = yu$, where y is factorizable, $y = p_1 \dots p_n$, then $x = up_1 \dots p_n$. Now suppose that x can be factorized in two ways

$$x = p_1 \dots p_n = q_1 \dots q_m$$

Then,

$$ux = (up_1)p_2 \dots p_n = p_1' \dots p_n' = (uq_1)q_2 \dots q_m = q_1' \dots q_n'$$

so, up to a permutation, $p_i' = u_i q_{\pi(i)}'$. But one verifies, by taking the vary cases, that this implies that $p_i = v_i q_{\pi(i)}$, where v_i is a unit. □

Theorem 2.18. *If A is factorial, and S is a multiplicative set with $0 \notin S$, then $S^{-1}A$ is factorial.*

Proof. Let a/b be given. We need only verify that a/b differs from a uniquely factorizable element by a unit. a differs from a/b by a unit. Write $a = p_1 \dots p_n$, where p_i is irreducible in A. We know that each p_i is either still irreducible, or a unit, so without loss of generality we may as well assume all p_i are irreducible in $S^{-1}A$. Suppose

$$p_1 \dots p_n = (u_1 q_1) \dots (u_m q_m) = (u_1 \dots u_m q_1)q_2 \dots q_m$$

Let $u_1 \dots u_m = x/y$. If $u_1 \dots u_m$ can be written as the quotient of two units in A, then we are done, for then the p_i and q_i differ by units in A, and thus the p_i differs from $u_i q_i$ by a unit. We show this is the only case that could happen, since we assume the p_i are irreducible in $S^{-1}A$.

If y is not a unit in A, write $y = y_1 \dots y_k$. If x is a unit in A, then when we apply unique factorization in A, we see y_1 differs from some p_i by a unit in A. But y_1 is a unit in $S^{-1}A$, so that p_i is a unit in $S^{-1}A$. If x is not a unit, then we may consider $x = x_1 \dots x_l$, and may assume no x_i and y_j

differ by a unit (by cancelling like terms), so that when we apply unique factorization, y_1 is mapped to p_i again, contradicting the irreducibility of p_i. Thus y must be a unit in A, and when we expand x as we have already done, and write

$$(p_1/y)\dots p_n = x_1 \dots x_l q_1 \dots q_m$$

But then some x_i differs from a p_j by a unit in A, hence p_j is a unit in $S^{-1}A$. □

2.8 Local Rings

Originally, localization was used to construct the field of fractions of an integral domain. However, it has been studied in more detail to understand the **local rings**, which occur in areas such as complex analysis and algebraic geometry. A ring A is **local** if it is commutative, and has a unique, maximal ideal. This condition is equivalent to saying that the set $A - U(A)$ of non-invertible elements in A forms an ideal, because if A has a unique maximal ideal $\mathfrak{m}$, then for any $a \in A - U(A)$, (a) is an ideal not equal to A (because if $1 \in (a)$ then a is a unit), so $a \in (a) \subset \mathfrak{m}$. Another equivalent condition is that there exists a maximal ideal $\mathfrak{m}$ such that $1 + \mathfrak{m} \subset U(A)$, because if $x \notin \mathfrak{m}$, then there is y such that $xy \equiv 1$ modulo $\mathfrak{m}$, hence xy is invertible and in particular, x is invertible, so $\mathfrak{m} = U(A)^c$. Conversely, if, in a local ring, $1 + x$ is not invertible, where $x \in \mathfrak{m}$, then $1 + x \in \mathfrak{m}$, so $1 \in \mathfrak{m}$, which is absurd.

Recalling our intuition that maximal ideals in a ring of functions corresponds to a 'point' that the functions operate over, we see that a local ring can be seen as a ring of functions taking values in a unique ring, concentrated at a single point – this is the reason why local rings are called 'local', because they represent the properties of a ring of functions locally around a single point. Indeed, this means that, up to isomorphism, there is a unique field K, and a unique homomorphism from A into K. If a homomorphism $f : A \to K$ corresponds to some 'evaluation map' over elements of A, where K is some field, then we find that A has only a single evaluation map. The main context in which local rings occur is in the study of the localization of certain rings. If $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}^c$ is certainly a multiplicative subset of A containing 1, so we can form the localization with respect to $\mathfrak{p}^c$, which we denote by $A_\mathfrak{p}$, and call the local ring at $\mathfrak{p}$.

Theorem 2.19. *If $\mathfrak{p}$ is a prime ideal, then $A_{\mathfrak{p}}$ is a local ring.*

Proof. Since $\mathfrak{p}$ is an ideal, $U(A) \subset \mathfrak{p}^c$, and we can argue that no element of $\mathfrak{p}$ is invertible in $A_{\mathfrak{p}}$. If $a \in \mathfrak{p}$, and $ab = 1$ in $A_{\mathfrak{p}}$, then there is $u \in \mathfrak{p}^c$ such that $u(ab-1) = 0 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $ab-1 \in \mathfrak{p}$ and so we conclude $1 \in \mathfrak{p}$, which is impossible. Thus the set of elements of the form a/b with $a \in \mathfrak{p}$ is *precisely* the set $U(A_{\mathfrak{p}})^c$ of noninvertible elements. If $a \in \mathfrak{p}$, then $(a/b)(c/d) = ac/bd$, and $ac \in \mathfrak{p}$, so $ac/bd \notin \mathfrak{p}$. If $c \in \mathfrak{p}$, then $a/b+c/d = (ad+bc)/bd$, and $ad+bc \in \mathfrak{p}$, so $(ad+bc)/bd$ is not invertible. We conclude that $U(A_{\mathfrak{p}})^c$ is an ideal of $A_{\mathfrak{p}}$, so $A_{\mathfrak{p}}$ is a local ring. □

Example. *If $A(D)$ is the set of analytic functions on some open set D, then the set of functions $f \in A(D)$ such that $f(p) = 0$ forms a prime ideal, so we can form the local ring on this ideal, which is commonly denoted $\mathcal{O}_p(D)$. The invertible elements of $\mathcal{O}_p(D)$ are exactly those functions which are nonzero at p (or, viewing the functions as direct quotients, have a nonzero removable singularity at p). This ring is isomorphic to the subring of the ring $\mathbf{C}[[X - p]]$ of power series in $X - p$, consisting of elements which are convergent in a neighbourhood of p.*

Example. *On $\mathbf{Z}$, we can view elements $a \in \mathbf{Z}$ as functions on the set of prime integers, mapping a prime p to the congruence class of a modulo p in $\mathbf{F}_p$. Thus the integer $1984 = 2^6 \cdot 31$ is a function on the primes which has two zeros at 2 and 31, where 2 to a 'zero of multiplicity six'. This corresponds to the fact that 1984 is invertible in $\mathbf{Z}_{(p)}$ except for $p = 2$ and $p = 31$, where $1984/31$ is invertible in $\mathbf{Z}_{(1984)}$, and $1984/2^6$ is invertible in $\mathbf{Z}_{(2)}$.*

In modern commutative algebra, one takes the set of prime ideals in a space and views them as points, through which the elements of the ring act as functions mapping into integral domains.

Theorem 2.20. *If S is multiplicative, and $\mathfrak{p}$ is a maximal ideal not containing elements of S, then $\mathfrak{p}$ is prime.*

Proof. We claim $S^{-1}\mathfrak{p}$ is a maximal ideal. If $S^{-1}\mathfrak{p} \subsetneq S^{-1}\mathfrak{a}$, then $\mathfrak{p} \subsetneq \mathfrak{a}$, implying $\mathfrak{a}$ contains element of S, so $S^{-1}\mathfrak{a} = S^{-1}A$. Now we claim $i^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$. If $b = a/s$, where $a \in \mathfrak{p}$, $s \in S$, and $b \notin \mathfrak{p}$, then $(b) + \mathfrak{p}$ contains elements in S, hence $xb + y = t$, for $y \in \mathfrak{p}$, $t \in s$. But then $xa + ys = ts$, with the left hand in $\mathfrak{p}$, and the right hand side in S, contradicting the construction of $\mathfrak{p}$. Thus we conclude $\mathfrak{p}$ is prime. □

Proposition 2.21. *If A is local, and $f : A \to B$ a surjective homomorphism, then B is local.*

Proof. If $\mathfrak{m}$ is a maximal ideal in B, then $f^{-1}(\mathfrak{m})$ is an ideal, and the isomorphism theorem guarantees that $A/f^{-1}(\mathfrak{m}) \cong B/\mathfrak{m}$, and since $B/\mathfrak{m}$ is a field, we conclude $f^{-1}(\mathfrak{m}) = U(A)^c$ is the unique maximal ideal in A. If $\mathfrak{n}$ is another maximal ideal in B, then $f^{-1}(\mathfrak{m}) = f^{-1}(\mathfrak{n})$, implying $\mathfrak{m} = \mathfrak{n}$ because f is surjective. □

Local rings were originally designed to analyze rings of functions, such as the ring $\mathcal{O}_p(D)$ of meromorphic functions on an open, connected subset of D, defined at the point p. As discovered in single variable complex analysis, it is in this ring that the concept of orders of poles and zeroes occur. In particular, if f is a meromorphic function holomorphic in a neighbourhood of p, and if $f(p) = 0$, then we can write $f = (X - p)g$ for some meromorphic function g. Since $f \in \mathcal{O}_p(D)$ is non-invertible precisely when $f(p) = 0$, we conclude that the maximal ideal of non-invertible elements is principal, of the form $(X - p)$. More generally, we know that if f is a meromorphic function holomorphic in a neighbourhood of p, then there is a non-negative integer n such that we can write $f = (X - p)^n g$ for some meromorphic function g with $g(p) \neq 0$, and we call n the order of the zero at g. This implies that if $\mathfrak{a}$ is any proper ideal in $\mathcal{O}_p(D)$, then it is of the form $((X-p)^n)$ for some integer n, so $\mathcal{O}_p(D)$ is principal. Thus the smallest ideal in $A_\mathfrak{p}$ containing a function corresponds to it's order at the point p. Here's another example.

Example. *Let A be a factorial ring, and (p) a principal ideal, where p is prime. Then the ring A_p is principal, and also has the properties that $\mathcal{O}_p(D)$ has. Every principal ideal in A_p is of the form (p^N), because if $a = p^n q$, where $p \nmid q$, then $q \in U(A_p)$ and so $(a) = (p^n)$. But now if $\mathfrak{a}$ is any ideal, and we define the order of a to be the integer $ord(a)$ such that $(a) = (p^n)$, then*

$$\mathfrak{a} = \bigoplus_{a \in \mathfrak{a}} (a) = \bigoplus_{a \in \mathfrak{a}} (p^{ord(a)}) = (p^{\min ord(a)})$$

so every ideal is principal, and in particular, generated by a power of p. Thus the order of an element of the ring measures it's place in the linear heirarchy

$$(1) \supset (p) \supset (p^2) \supset \cdots \supset (0)$$

which consists of all ideals.

We want to consider rings where we can discuss the phenomenon of 'multiplicities of zeroes'. Since we are focusing on a ring, such a ring shuold be localized at the point where we want to measure zeroes, so our ring should be local. If the ring is Noetherian domain, but not a field, which maximal ideal is principal, we call the ring a **discrete valuation ring**. These are the rings having the properties we wish.

Proposition 2.22. *If A is a discrete valuation ring, then there exists an element $t \in A$ such that every nonzero element of A can be uniquely written as ut^n, where u is a unit in A.*

Proof. Let (t) be the maximal ideal of A. Suppose that $ut^n = vt^m$. If $n = m$, then $u = v$. Otherwise, if $n > m$, then $u = vt^{m-n}$, and this implies that (t) contains a unit, hence is not a maximal ideal. Thus it suffices to prove that every element of A has a required expansion of the form above. If $a \in A$ is a unit, we can write $a = at^0$, and we are done. If a is not a unit, then (a) is an ideal contained in (t), so we can write $a = a_1 t$ for some $a_1 \in A$. Then (a) is a proper subideal of (a_1), because if $a_1 = ba$, then $a = bat$, hence $1 = bt$, so t is invertible. If a_1 is a unit, we are done, otherwise we can write $a_1 = a_2 t$. Continuing this process, if this process does not terminate, we end up with an infinite ascending chain

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$$

and this is impossible in a Noetherian ring. □

If A is a domain, the condition that we have a unique expansion of the form ut^n for each element of A is exactly the condition which guarantees that the ring is a discrete valuation ring. If this is true, then (t) is certainly a unique maximal ideal in A, so A is a local ring whose maximal ideal is principal. To prove that A is Noetherian, it suffices to notice that the proper ideals of A are exactly $(0), (t), (t^2), (t^3)$, and so on and so forth, so that the ring is actually principal. The element t in the theorem is known as a **uniformizing parameter** for A. Any other uniformizing parameter for A differs from t by a unit, so if $s = ut$ is another uniformizing parameter, then if $a = vt^n = rs^m$, then $rs^m = ru^m t^m$, so $v = ru^m$ and $n = m$. Since this value is invariant of the uniformizing parameter, it depends only on the element a, and we call this the **order of a**. We define the order of 0 to be ∞. If we consider the field B of fractions of A, then every nonzero element

b of B can be written as ut^n for a unique integer $n \in \mathbf{Z}$, and we define this to be the order of b. If $n < 0$, we say that b has a pole of order $-n$.

Example. *Consider the ring $K[X] = K[\mathbf{A}^1]$. Then for any $a \in \mathbf{A}^1$, the ring $\mathcal{O}_a(\mathbf{A}^1)$ of rational functions defined at a (those polynomials f/g with $g(a) \neq 0$) is a discrete valuation ring. If we consider any function f/g with $g(a) \neq 0$, then $f = (X-a)^n h(X)$ for some $n \geqslant 0$ and since h with $h(a) \neq 0$. This gives us a decomposition $f/g = (h/g)(X-a)^n$, so $X-a$ is a uniformizing parameter, and $\mathcal{O}_a(\mathbf{A}^1)$ is a discrete valuation domain.*

Example. *Consider the ring $\mathcal{O}_\infty(\mathbf{A}^1)$ of rational functions of the form $f/g \in K(X)$, with $\deg g \geqslant \deg f$. This rings models the set of rational functions which converges to a well defined quantity 'near infinity'. The only invertible functions in this ring are those with $\deg g = \deg f$, and so the noninvertible functions are generated by $(1/X)$, because if $\deg g - \deg f = n$, then $X^n(f/g) = (X^n f/g)$ is invertible, and contained in $\mathcal{O}_\infty(\mathbf{A}^1)$.*

Example. *If p is a prime number, then the local ring $\mathbf{Z}_{(p)}$ is a discrete valuation ring, because if $a/b \in \mathbf{Z}_{(p)}$, with $b \notin (p)$, we can write $a = p^n c$ with c and p relatively prime, and then $a/b = p^n(c/b)$ has c/b invertible. This gives an order function on $\mathbf{Q}$ defined by taking the order of a number $m = p^n(a/b)$ with respect to p to be n. This can be used to define a metric on $\mathbf{Q}$, and the completion is the field of p-adic numbers.*

The order function on the resulting field of fractions of a discrete valuation domain satisfies useful algebraic properties.

- $\mathrm{ord}(x) = 0$ if and only if $x = 0$.
- $\mathrm{ord}(xy) = \mathrm{ord}(x) + \mathrm{ord}(y)$.
- $\mathrm{ord}(x+y) \geqslant \min(\mathrm{ord}(x), \mathrm{ord}(y))$.

We will show that these properties are essentially the defining properties of a discrete valuation domain. Given any field K, an order function is a $\mathbf{Z} \cup \{\infty\}$ valued function φ on K with the properties above, and with $\varphi(x) = \infty$ if and only if $x = 0$.

Proposition 2.23. *For any order function φ on a field K, the ring A of elements $x \in K$ with $\varphi(x) \geqslant 0$ forms a discrete valuation domain, with K it's field of fractions.*

Proof. A is certainly closed under multiplication and addition. Since $\varphi(x) = \varphi(1 \cdot x) = \varphi(1) + \varphi(x)$, we conclude that $\varphi(1) = 0$. We use this to conclude that $\varphi(xx^{-1}) = \varphi(x) + \varphi(x)^{-1} = 0$, so an element $x \in A$ is invertible if and only if $\varphi(x) = 0$. This shows that the set of noninvertible elements forms an ideal, hence the ring A is local. The ring is certainly a domain. We may assume that there is $x \in K$ with $\varphi(x) = 1$, because otherwise every noninfinite value of the order function is a multiple of some integer, and we obtain another order function by dividing by this integer. If $\varphi(x) = 0$, then for every $x \in A$, there is n such that $\varphi(xt^{-n}) = 0$, hence $xt^{-n} = u$ is a unit, and $x = ut^n$. We have justified that this proves A is a discrete valuation domain, and since $\varphi(x^{-1}) = -\varphi(x)$, every element of K is either an element of A, or of the form $1/x$ for some $x \in A$, showing that K is the field of fractions of A. □

Proposition 2.24. *If $ord(a) < ord(b)$, then $ord(a + b) = ord(a)$.*

Proof. $a = t^n u$, $b = t^m s$, then $a+b = t^n(u+t^{m-n}s)$, and $u+t^{m-n}s$ is invertible because it is congruent to u in the maximal ideal. This is analogous to the addition law for polynomials in $K[X]$. □

Often, a discrete valuation ring models the germ of functions around a point, and the evaluation map at this points gives us the maximal ideal, as well as an isomorphism between the ring of constant functions and the field upon which the functions are defined. In this situation, we can obtain some useful properties of the ring of constant functions, related to the Taylor expansion of functions around a point.

Proposition 2.25. *Suppose that a discrete valuation ring A contains a subfield K, such that if $\mathfrak{m}$ is the maximal ideal of A, then $K \to A \to A/\mathfrak{m}$ gives an isomorphism of fields. If t is a uniformizing parameter for A, then for any $n \geqslant 0$, every $x \in A$ has a unique expansion as $x = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}$, where $z_n \in A$.*

Proof. For any $x \in A$, there is $\lambda \in K$ such that x is congruent to λ modulo $\mathfrak{m} = (t)$, so $x = \lambda + z_0 t$. This gives the proposition for the case $n = 0$. For the inductive case, we write $x = \sum \lambda_i t^i + z_n t^{n+1}$. Then using the $n = 0$ case we can write $z_n = \lambda_{n+1} + z_{n+1} t$, and this gives the expansion for x one degree higher. To prove uniqueness, we note that if $\sum \lambda_i t^i + z_n t^{n+1} = 0$, then $\sum \lambda_i t^i = -z_n t^{n+1}$, and if $z_n \neq 0$, the right side has order greater than or equal to $n + 1$, whereas the right side has order equal to the minimum index i such that $\lambda_i \neq 0$, and these two values cannot be equal. □

The ring of formal power series over a field K is written $K[[X]]$, and is the ring of 'infinite power series' $\sum_{k=0}^{\infty} a_k X^k$, with $a_k \in K$. Then $K[[X]]$ is a ring containing $K[X]$ as a subring, and is a discrete valuation ring. To prove this, suppose $\left(\sum a_i X^i\right)$ is invertible, so there is a power series such that $\left(\sum a_i X^i\right)\left(\sum b_i X^i\right) = 1$. This is equivalent to being able to solve the infinite series of equations

$$a_0 b_0 = 1 \quad a_1 b_0 + a_0 b_1 = 0 \quad a_2 b_0 + a_1 b_1 + a_0 b_2 = 0$$

The first equation guarantees that we must have $a_0 \neq 0$, but if this is true the first equation is uniquely solvable for b_0, and this value is nonzero. Once b_1 is fixed, the equation $a_0 b_1 = -a_1 b_0$ is uniquely solvable for b_1. Continuing this, we find that given that the previous equations are solvable, there is a unique value of b_n which satisfies the n'th equation, and so an element of $K[[X]]$ is invertible precisely when its constant coefficient is nonzero. This shows that the non-invertible elements of $K[[X]]$ are precisely (X), so the ring is local. We can write an arbitrary power series $\sum a_i X^i$ as $X^n \sum b_i X^i$, where $b_0 \neq 0$, so the ring is a discrete valuation domain, where the order function is precisely the degree corresponding to the smallest non-zero coefficient. The quotient field of $K[[X]]$ is denoted $K((X))$.

Assuming that we have an isomorphism $K \to A \to A/\mathfrak{m}$, the previous proposition shows that we have a natural injective homomorphism from A to $K[[X]]$. This shows that the class of discrete valuation domains which contain a field corresponding to the quotient by their maximal ideal are precisely the rings where we can consider 'power series' of elements. Furthermore, we obtain a map of K into $K((X))$, because the homomorphism is injective, and the order function on $K[[X]]$ agrees with the one induced from K. This essentially corresponds to the fact that all holomorphic functions can be expanded as power series, and here we also have additional analytic relationships between these expansions and their convergence around a point.

Example. *In complex analysis, one memorizes the power series expansion*

$$(1 - X)^{-1} = (1 + X + X^2 + \dots)$$

This equation holds in the ring $K[[X]]$ of power series over any field, because

of the telescoping series properties of $(1-X)(1+X+X^2+\dots)$. *Similarily,*

$$\begin{aligned}(1-X)(1+X^2)^{-1} &= (1-X)(1+iX)^{-1}(1-iX)^{-1}\\ &= (1-X)\left(\sum(-i)^kX^k\right)\left(\sum i^kX^k\right)\\ &= (1-X)\left(\sum(-1)^kX^{2k}\right)\\ &= (1-X-X^2+X^3+X^4-X^5-X^6+\dots)\end{aligned}$$

Proposition 2.26. *Suppose that A is a discrete valuation ring, with quotient field K. Then there are no local rings B with $A \subsetneq B \subset K$, such that the maximal ideal of B contains the maximal ideal of A.*

Proof. If a nonzero x is in K, but not in A, then x has some order $-n < 0$, so x^{-1} has order n, and is consequently in A. This means that $x^{-1} \in A$ for each $x \in A$. Iif the maximal ideal $\mathfrak{m}$ of B contains the maximal ideal $\mathfrak{n}$ of A, we claim that $\mathfrak{m} = \mathfrak{n}$. Otherwise, we can pick $x \in \mathfrak{m} - \mathfrak{n}$, and then $x^{-1} \in A$, so $1 = xx^{-1} \in \mathfrak{m}$, contradicting the fact that $B \neq K$. Now let t be a uniformizing parameter for A. Every element of K, and in particular B, can be written as xt^n, where x is a unit in A. In particular, if $B - A$ is nonempty, it contains some element ut^{-n}, where $n > 0$, and u is a unit in A. But then B contains t^{-n}, and hence all elements of the form $t^{k-mn} = t^k(t^{-n})^m$, so $B = K$, which is impossible. □

Example. *Using this theorem, we can classify the discrete valuation rings with quotient field $K(X)$ which contain K, where K is algebraically closed. Let A be a discrete valuation ring, and suppose the uniformizing parameter is some irreducible $t \in A$. If A contains X, then A contains $K[X]$, and the set of elements of $K[X]$ which are not invertible in A forms a prime ideal, which is therefore of the form (f) for some irreducible monic polynomial f. Since K is algebraically closed, $f(X) = X - a$, for some $a \in K$, and so A contains $\mathcal{O}_a(\mathbf{A}^1)$, implying the two are equal to one another. If A does not contain X, then A contains X^{-1}. Since the order of any nonzero $a \in K$ is zero, and the order of X^{-1} is greater than zero because it is not invertible, $a_0+a_1X^{-1}+\dots+a_nX^{-n} = (a_0X^n+\dots+a_n)/X^n$ is invertible in A, hence $X^n/(a_0X^n+\dots+a_n) \in A$. Multiplying by $b_0+b_1X^{-1}+\dots+b_nX^{-n}$, we conclude that $(b_0X^n+\dots+b_n)/(a_0X^n+\dots+a_n) \in A$ for any $a_0 \neq 0$. This shows that A contains $\mathcal{O}_\infty(\mathbf{A}^1)$, and if $f(X)/g(X)$ has $\deg g > \deg f$, then g/f is not in A, for otherwise we may write $g = (X-a_1)\dots(X-a_m)$, $f = (X-b_1)\dots(X-b_l)$, and then $h = (X-a_1)\dots(X-a_{m-1})/(X-b_1)\dots(X-b_l) \in A$,*

so $hg/f = X - a_m \in A$, implying $X \in A$, contradicting our assumption. Thus the maximal ideal of A contains the maximal ideal of $\mathcal{O}_\infty(\mathbf{A}^1)$, and this implies that A is in fact equal to $\mathcal{O}_\infty(\mathbf{A}^1)$.

Example. *The only discrete valuation rings with quotient field $\mathbf{Q}$ are the local rings $\mathbf{Z}_{(p)}$. If A is any such discrete valuation ring, then A contains all the integers $\mathbf{Z}$. Because A is a local ring, the set of non-invertible integers in A forms a prime ideal in $\mathbf{Z}$, and hence is of the form (p) for some prime integer. But then A contains $\mathbf{Z}_{(p)}$, which implies $A = \mathbf{Z}_{(p)}$.*

Similar techniques to the classifications above allow us to classify the set of all discrete valuation rings which are obtained from extensions of principal ideal domains. These valuation rings are exactly of the form A_p, where (p) is a prime ideal in the PID.

2.9 Dedekind Rings

In the understanding of integral solutions to polynomial equations such as $X^n - Y^n$ can be factored over $\mathbf{Z}[\zeta_n]$, where ζ_n is a primitive n th root of unity. In 1847 Gabriel Lumé used the fact that $\mathbf{Z}[\zeta_n]$ is a unique factorization domain to provide a proof of Fermat's last theorem, with one catch; $\mathbf{Z}[\zeta_n]$ is not always a unique factorization domain, and so his proof only works for certain values of n for which the ring is such a domain; in 1844 Ernst Kummer showed that $\mathbf{Z}[\zeta_{23}]$ is *not* a unique factorization domain. However, Ernst Kummer also showed that there are certain techniques which allow us to extend UFD type arguments to more general rings, including the rings $\mathbf{Z}[\zeta_{23}]$; rather than factorizing individual elements of a ring, we can factor ideals in the ring into prime ideal components.

Example. *Consider the ring $\mathbf{Z}[\sqrt{-5}]$, in which*

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

all of 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible in $\mathbf{Z}[\sqrt{-5}]$, because we know $|a + b\sqrt{-5}|^2 = a^2 + 5b^2$, and there are no solutions in $\mathbf{Z}^2 + 5\mathbf{Z}^2$ to the equations $XY = 4$, 9, or 6, except for the trivial ones corresponding to a unit multiplied by a constant. Thus $\mathbf{Z}[\sqrt{-5}]$ is not a unique factorization domain. However, consider the corresponding relationship between the ideals, i.e.

$$(2)(3) = (6) = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Even though these numbers are irreducible element of the ring, they are not prime elements, since, for instance, 2 divides $6 = (1+\sqrt{-5})(1-\sqrt{-5})$*, but can't divide* $1+\sqrt{-5}$ *or* $1-\sqrt{-5}$*. On the other hand,* $(2, 1+\sqrt{-5})$ *is a prime ideal, because* $\mathbf{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5})$ *is isomorphic to* $\mathbf{Z}_2$*, which is obtained from the fact that the embedding of* $\mathbf{Z}$ *into* $\mathbf{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5})$ *is surjective, with kernel* (2)*, as is* $(3, 1-\sqrt{-5})$*, and we have*

$$(6) = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$

which is a unique factorization of ideals.

A **Dedekind ring** is precisely a domain where one can factor ideals uniquely into products of prime ideals. An equivalent definition, more interesting, occurs in the theory of ideal class groups in algebraic number theory. If A if a domain with a field of fractions K, we say an A submodule $\mathfrak{a}$ of K is a **fractional ideal** if there is $x \in A$ with $x\mathfrak{a} \subset A$, so that $\mathfrak{a}$ has 'bounded denominator'. The family of fractional ideals forms a monoid, with A as the identity element, if we take products just as in the case of normal ideals, $\mathfrak{ab}$ is the subgroup of K generated by elements of the form ab, for $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. If the family of fractional ideals forms a group under this product, we will find that the ideals have a unique factorization theory.

To see this, let's explore some consequences of the group property. If $\mathfrak{a}$ is an ideal of A, this means there is a fractional ideal $\mathfrak{b}$ with $\mathfrak{ab} = A$, so that there are $x_1, \ldots, x_n \in \mathfrak{a}$, $y_1, \ldots, y_n \in \mathfrak{b}$ with $x_1y_1 + \cdots + x_ny_n = 1$. If $x \in \mathfrak{a}$ is arbitrary, then $x = x_1(y_1x) + \cdots + x_n(y_nx)$, and we know because of the product formula $\mathfrak{ab} = A$ that $y_kx \in A$, hence we have found $\mathfrak{a} = (x_1, \ldots, x_n)$. We conclude that any ring whose fractional ideals form a group is Noetherian.

Chapter 3

Modules

All groups are really sets of bijective maps in disguise. Regardless of the complex nature that grants us a specific group, we can still relate it back to some symmetric group, by Cayley's theorem. This leads to the study of group actions. It turns out that all rings can be seen as a set of endomorphisms over an abelian group. The counterpart to a group action on a G-set is then a ring action on an R-module.

Theorem 3.1. *Every ring is isomorphic to a subring of the ring of endomorphisms on an abelian group.*

Proof. Let R be a ring. Let us denote by R^+ the same object, but viewed solely as an abelian group (the ring's additive structure). For each $r \in R$, consider the group endomorphism $f_r : R^+ \to R^+$ defined by $a \mapsto ra$. The distributive law tells us that f_r really is an endomorphism, because

$$f_r(a+b) = r(a+b) = ra + rb = f_r(a) + f_r(b)$$

The map $f_{(\cdot)} : r \mapsto f_r$ is a ring homomorphism of R in $\mathrm{End}(R^+)$.

$$f_{a+b}(x) = (a+b)x = ax + bx = f_a(x) + f_b(x)$$

$$f_1(x) = 1x = x$$

$$f_{ab}(x) = (ab)(x) = a(bx) = f_a(f_b(x))$$

Now if $f_a = f_b$, then $f_a(1) = f_b(1)$, so $a = b$. Thus our homomorphism really is an embedding. □

The axioms for a ring seem, magically, to perfectly align with the construction of a ring of endomorphisms. It leads to the notion of a 'ring action' on an abelian group. A representation of a ring R on an abelian group A is a ring homomorphism of R into $\mathrm{Hom}(A)$. If R is a ring, then a **left R-module** is an abelian group M together with a fixed representation of R in $\mathrm{End}(M)$, which gives a scalar multiplication structure. We write λx for the application of the representation of $\lambda \in R$ on x. Axiomatically, an R-module satisfies the relations

$$r(x+y) = rx + ry \qquad (ru)x = r(ux) \qquad (r+u)x = rx + ux \qquad 1x = 1$$

If R is a field, we often call an R-module an R-**vector space**.

The morphisms in the category of R-modules are the group homomorphisms that fix the representation of R. In exact, a map $f : M \to N$ is an R-module morphism if it is a group homomorphism, and

$$f(\lambda x) = \lambda f(x)$$

for all $\lambda \in R$, $x \in M$. This is just a morphism of representations as in category theory. If $\pi : R \to \mathrm{End}(M)$ and $\rho : R \to \mathrm{End}(N)$ are the representations that give M and N there module structure, then f is a morphism if it is a morphism in **Ab**, and for each $\lambda \in R$,

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \pi(\lambda)} & & \downarrow{\scriptstyle \rho(\lambda)} \\ M & \xrightarrow{f} & N \end{array}$$

commutes. The category of R-modules is denoted $\mathbf{Mod_R}$. Sets of morphisms in this category are denoted $\mathrm{Hom}_R(M,N)$, or just $\mathrm{Hom}(M,N)$ if the ring is obvious.

Example. *Any abelian group is a* $\mathbf{Z}$ *module, for we may define*

$$nx = x + x + \cdots + x$$

These properties were used to classify finitely generated Abelian groups. We shall show that this classification can be widely generalized to classify finitely generated modules. A $\mathbf{Z}$*-morphism is just an abelian group morphism, so that the category* $\mathbf{Mod_Z}$ *is just* **Ab** *in disguise.*

Example. *If R is a ring, then R^n might not be a ring, but it is still an Abelian group, and is an R-module. Any morphism in $Hom(R^n, R^m)$ can be identified with a matrix in $M_{n,m}(R)$.*

Example. *If V is a vector space over $\mathbf{F}$ with a fixed endomorphism T, then we have a representation of $\mathbf{F}[X]$ in $End(V)$ obtained by mapping $\sum a_i X^i$ to $\sum a_i T^i$. More generally, if M is a monoid, and we have a representation of M on $End_R(N)$, then the representation extends to a representation of the monoid algebra $R[M]$ on $End_R(N)$.*

Example. *If $C^\infty(U)$ is the ring of infinitely differentiable functions on an open subset U of $\mathbf{R}$, then $\mathbf{R}[X]$ acts on $C^\infty(U)$ after fixing the differentiable endomorphism*

$$T = \frac{d}{dt}$$

Similarily, if U is an open subset of $\mathbf{R}^n$, then $\mathbf{R}[X_1, \ldots, X_n]$ acts on $C^\infty(U)$. If H is a complex Hilbert space, and T a self-adjoint operator, then the representation of $\mathbf{C}[X]$ on $B(H)$ extends to a representation of $C(\sigma(T))$ on $B(H)$, where $\sigma(T)$ is the spectrum of T.

A **submodule** of a module M is a subgroup N which is closed under multiplication by a scalar. Given a morphism $f : M \to N$, both $\ker(f)$ and $\mathrm{im}(f)$ are submodules of their respective modules. Submodules are the natural object to quotient by in the category of modules. If N is a submodule of M, then we can define a module structure on M/N, in the canonical way.

Example. *If M is a module over an entire ring R, then we define the* **torsion submodule** *M_{tor} to be the set of all $x \in M$ such that there is $\lambda \in R$ for which $\lambda x = 0$.*

Example. *If R is a ring, then it is a module over itself. Every left ideal $\mathfrak{a}$ is a submodule of R, and $R/\mathfrak{a}$ is therefore also a module over R.*

Modules satisfy the isomorphism theorems just like groups. If $f : M \to N$ is a module morphism with kernel K, then it is an group homomorphism, so we may take factors to obtain a group homomorphism $\tilde{f} : M/K \to N$, and since $\tilde{f}([\lambda x]) = f(\lambda x) = \lambda f([x])$, the map is also a module homomorphism. By similar tricks, we find that for submodules K and L of M,

$$K/(K \cap L) \cong (K + L)/L$$

If M is a submodule of N, which is a submodule of L,

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

hence modules behave almost exactly the same as abelian groups.

3.1 Abelian Categories

If M and N are modules over the same ring, then $\mathrm{Hom}(M,N)$ is an abelian group. If $f,g \in \mathrm{Hom}(M,N)$, then define

$$(f+g)(x) = f(x) + g(x)$$

The zero homomorphism $0(x) = 0$ is the identity in this group. Given $\lambda \in \mathbf{R}$, we may define

$$(\lambda f)(x) = \lambda f(x)$$

but this is only in $\mathrm{Hom}(M,N)$ if R is commutative, so $\mathrm{Hom}(M,N)$ is an R module only if R is commutative. Given $f : M \to N$, and a fixed module X, we obtain a morphism $f^* : \mathrm{Hom}(N,X) \to \mathrm{Hom}(M,X)$, mapping g to $g \circ f$. Similarily, we get a morphism $f_* : \mathrm{Hom}(X,M) \to \mathrm{Hom}(X,N)$, by letting $g \mapsto f \circ g$. This follows because composition is bilinear,

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

It follows that Hom is a functor in two variables, contravariant in the first, and covariant in the second. We shall also make use of the relations

$$(g\circ f)_* = g_* \circ f_* \qquad (g\circ f)^* = f^* \circ g^*$$

Arrow theoretic arguments are very common in module theory. We consider exact sequences just as in group theory.

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_n$$

If $\ker(f_{i+1}) = \mathrm{im}(f_i)$ for each i.

Theorem 3.2. *If*

$$A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is exact, then

$$Hom(A,X) \xleftarrow{f^*} Hom(B,X) \xleftarrow{g^*} Hom(C,X) \leftarrow 0$$

is also exact.

Proof. Since $g \circ f = 0$, $(g \circ f)^* = 0$. Thus $\ker(f^*) \supset \mathrm{im}(g^*)$. Suppose that $f^*(T) = 0$. We claim that $T = g^*(S)$ for some $S \in \mathrm{Hom}(C, X)$. If $x = g(y)$, then define

$$Sx = Ty$$

This is well-defined, since if $g(y) = g(z)$, $g(y-z) = 0$, so there is some $a \in A$ such that $y - z = f(a)$. It then follows that

$$T(y - z) = (T \circ f)(a) = 0(a) = 0$$

Thus $Ty = Tz$. Since g is surjective, S is defined on all of C, is easily checked to be a module homomorphism, and satisfies $T = g^*(S)$.

We must also show g^* is injective. Suppose $T \circ g = 0$. If $x \in C$ is given, then there is $y \in b$ such that $g(y) = 0$. Then

$$0 = (T \circ g)(y) = T(x) = 0$$

so $T = 0$. □

Theorem 3.3. *If*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C$$

is exact, then

$$0 \to Hom(X, A) \xrightarrow{f_*} Hom(X, B) \xrightarrow{g_*} Hom(X, C)$$

is also exact.

Proof. We have the relation

$$g_* \circ f_* = (g \circ f)_* = 0_* = 0$$

Hence $\ker(g_*) \subset \mathrm{im}(f_*)$. Suppose $g \circ T = 0$. We claim $T = f \circ S$ for some $S \in \mathrm{Hom}(X, A)$. For each $x \in X$, define $Sx = y$, where $f(y) = Tx$. y must be necessarily unique, for f is injective, and exists because $g(Tx) = 0$, and the exactness of f and g. The map is easily checked to be a homomorphism, and satisfies $f_*(S) = T$.

Now we prove f_* is injective. Suppose $f \circ T = 0$. Then $f(T(x)) = 0$ for each x, implying $T(x) = 0$ since f is injective. Thus $T = 0$. □

A Category $\mathcal{C}$ is **Additive** if for any two objects X and Y, $\mathrm{Mor}(X, Y)$ is an abelian group, such that composition is bilinear, there exists an object 0 which is both initial and terminal, and finite products and coproducts exist. An additive category is **Abelian** if kernels and cokernels exist, and if 0 is the kernel of $f : X \to Y$, then f is the kernel of its cokernel, and if 0 is the cokernel of f, then f is the cokernel of its kernel, and if 0 is the kernel and cokernel of f, then f is an isomorphism. Most module arguments can be made into abelian categorical arguments, which is useful when other abelian categories appear, such as the category of chain complexes in homology theory.

Chapter 4

Algebras

4.1 Matrix Rings

Let R be a ring. Then the set of all endomorphisms from R^n to itself is the prime example of an R-module, and the set of endomorphisms from R^n to itself is an R-algebra. Every endomorphism $T : R^n \to R^n$ can be identified as an $n \times n$ matrix M with coefficients in R, such that $Mx = T(x)$. We denote the set of all $n \times n$ matrices as $M_n(R)$. The tractable case is really only when R is a commutative ring, those noncommutative examples do occur in certain problems. For now, we shall assume R is commutative.

The units of $M_n(R)$ are the invertible matrices, and the set of all matrices forms the general linear group $GL_n(R)$. The determinant operator $\det : M_n(R) \to R$ still applies, and satisfies $\det(AB) = \det(A)\det(B)$, since

$$\begin{aligned}
\det(AB) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (A_{i1}B_{1\sigma(i)} + A_{i2}B_{2\sigma(i)} + \cdots + A_{in}B_{n\sigma(i)}) \\
&= \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \left(\sum_{\sigma \in S_n} \operatorname{sgn}(\tau^{-1}\sigma) \sum_{i=1}^{n} B_{\tau(i)\sigma(i)} \right) A_{1\tau(1)} \ldots A_{n\tau(n)} \\
&= \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \sum_{i=1}^{n} B_{i\sigma(i)} \right) A_{1\tau(1)} \ldots A_{n\tau(n)} \\
&= \det(A)\det(B)
\end{aligned}$$

If $M \in GL_n(R)$, then $\det(M) \in U(R)$, because

$$\det(M)\det(M^{-1}) = \det(MM^{-1}) = \det(I) = 1$$

For instance, $M \in GL_n(\mathbf{Z})$ can only be invertible if $\det(M) = \pm 1$. In this case, we know by Cramer's rule that the inverse of M in $GL_n(\mathbf{R})$ is given by

$$\frac{1}{\det(M)} A$$

where the coefficient A_{ij} is the determinant of the submatrix of M obtained by removing row j and column i, multiplied by $(-1)^{i+j}$. This matrix lies in $GL_n(\mathbf{Z})$ if $\det(M) = \pm 1$, so $GL_n(\mathbf{Z})$ consists exactly of the matrices whose determinant is ± 1. We essentailly can apply Cramer's rule to all rings.

Theorem 4.1. *M is invertible in $M_n(R)$ if and only if $\det(M)$ is a unit in R.*

Proof. Consider the adjoint matrix A described above. Let M^{jk} be the matrix obtained by deleting row j and column k.

$$(MA)_{ij} = \sum_{k=1}^{n} M_{ik} A_{kj} = \sum_{k=1}^{n} (-1)^{j+k} M_{ik} \det(M^{jk})$$

If $i = j$, then this is just the Laplace expansion of the determinant, so $(MA)_{ii} = \det(A)$. If $i \neq j$, this is the Laplace expansion of the matrix obtained by replacing row j with row i, causing a repeated row, and so the Laplace expansion will be zero. Thus $MA = \det(A)$, and M is invertible provided $\det(A)$ is invertible, i.e. it is a unit. □

The group $GL_n(R)$, together with its action on R^n, make it somewhat tractable to study. In the field of representation theory, we try and understand all groups by their homomorphisms into $GL_n(R)$. The determinant allows us to understand some properties of the group. For instance, since the determinant is a group homomorphism from $GL_n(R)$ to $U(R)$, we have a normal subgroup $SL_n(R)$ consisting of matrices with determinant one, and since the map from $GL_n(R)$ to $U(R)$ is surjective, the index of $SL_n(R)$ in $GL_n(R)$ is the same as the number of invertible elements in R.

Theorem 4.2. *$M_n(M_m(R))$ is isomorphic $M_{nm}(R)$.*

Proof. The algebra $M_n(M_m(R))$ is isomorphic to the set of endomorphisms on $M_m^n(R)$. But the module $M_m^n(R)$ is isomorphic to $M^{nm}(R)$, so the set of endomorphisms on $M_m^n(R)$ is isomorphic to the set of endomorphisms on $M^{nm}(R)$. □

We note that the isomorphism from $M_{nm}(R)$ to $M_n(M_m(R))$ coagulates blocks of submatrices in a way which preserves the algebraic structure. For instance, $M_4(R)$ is isomorphic to $M_2(M_2(R))$, such that

$$\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix} \begin{pmatrix} \mathbf{N} & \mathbf{M} \\ \mathbf{O} & \mathbf{P} \end{pmatrix} = \begin{pmatrix} \mathbf{AN} + \mathbf{BO} & \mathbf{AM} + \mathbf{BD} \\ \mathbf{CN} + \mathbf{DO} & \mathbf{CM} + \mathbf{DP} \end{pmatrix}$$

where the left side is multiplication in $M_4(R)$, and the algebra on the right side done over matrices in $M_2(R)$.

Chapter 5

Linear Algebra

Theorem 5.1. *Let $T : V \to V$ be an injective linear map. If W if a T stable subspace of V, and V/W and $W/T(W)$ is finite dimensional, then $V/T(V)$ is finite dimensional, and the dimension is equal to the dimension of $W/T(W)$.*

Proof. The map T induces a surjective map from V to $T(V)/T(W)$ whose kernel is W, so V/W is isomorphic to $T(V)/T(W)$ by the first isomorphism theorem. Since $W \subset W + T(V) \subset V$ and $T(W) \subset W \cap T(V) \subset T(V)$, we conclude that

$$\dim \frac{V}{W} = \dim \frac{V}{W + T(V)} + \dim \frac{W + T(V)}{W}$$

$$\dim \frac{T(V)}{T(W)} = \dim \frac{T(V)}{W \cap T(V)} + \dim \frac{W \cap T(V)}{T(W)}$$

The second isomorphism theorem tells us that $T(V)/[W \cap T(V)]$ is isomorphic to $[W + T(V)]/W$. Putting this together with the fact that V/W is isomorphic to $T(V)/T(W)$, we conclude that $\dim V/[W + T(V)] = \dim[W \cap T(V)]/T(W)$. But now, since $T(V) \subset W + T(V) \subset V$ and $T(W) \subset W \cap T(V) \subset W$, we conclude that

$$\dim \frac{V}{T(V)} = \dim \frac{W + T(V)}{T(V)} + \dim \frac{V}{W + T(V)}$$

$$\dim \frac{W}{T(W)} = \dim \frac{W \cap T(V)}{T(W)} + \dim \frac{W}{W \cap T(V)}$$

But $V/[W + T(V)]$ has the same dimension as $[W \cap T(V)]/T(W)$, and the second isomorphism theorem implies that $[W + T(V)]/T(V)$ is isomorphic

to $W/[W \cap T(V)]$, and we conclude that $V/T(V)$ has the same dimension as $W/T(W)$. $\square$