Ring Theory

Jacob Denson

June 7, 2017

Table Of Contents

Chapter 1

Basic Definitions

The simplest algebraic operation is counting, and leads to the set of integers. On the integers, we can perform addition and multiplication, but not division (without ending up with a rational number). Rings are the abstract objects which abstract the operations of addition and multiplication. More specifically, a **ring** is a set R upon which an additive and multiplicative operation is defined (with respective identities 0 and 1). The additive structure forms an abelian group, the multiplicative structure a (not-necessarily commutative) monoid structure. The additive and multiplicative structures play nice with each other thanks to the 'distributive law': for any $a, b, c \in R$, $a(b+c) = ab + ac$, 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 aspects of ring theory we will encounter. They have a nontrivial theory of divisibility, but still have a unique factorization property of integers into prime elements, an idea we will study in the more general situation of 'unique factorization domains'. More generally, the number systems* $\mathbf{Q}$, $\mathbf{R}$, *and* $\mathbf{C}$ *are all rings, in which all nonzero elements are invertible. We call these rings* **fields**.

Example. *Your favourite number systems, be they* $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{Q}$, *or the finite fields* $\mathbf{F}_p$ *are rings, as are the set of all* $n \times n$ *matrices* $M_n(K)$ *over an arbitrary field* K.

It is often assume that $1 \neq 0$ in a ring. This is because if $1 = 0$, then the ring structure is particularly trivial. This is because in any ring, $a \cdot 0 = 0$

for all elements $a \in R$. The proof of this follows from the distributive law: $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$, and subtracting $a \cdot 0$ from both sides gives $a \cdot 0 = 0$. If $1 = 0$, then $a = a \cdot 1 = a \cdot 0 = 0$, so the ring consists of a single element: just a single zero! Some mathematicians do not necessarily assume that $1 \neq 0$, but we know that the theory is essentially the same, except for the single space in which there is a single zero.

You already know many examples of rings. Your favourite number systems, be they $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{Q}$, or the finite fields $\mathbf{F}_p$, are rings, as are the set of all matrices $M_n(\mathbf{F})$, and polynomials $K[X]$ over some field. 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, though we have axiomatized rings abstractly, every ring can be seen as a set of symmetries over some abelian group.

Example. *Let G be an abelian group, and consider* $\mathrm{End}(G)$*, the set of all homomorphisms from G to itself. We define a ring structure on this set. Let $(f+g)$ be defined pointwise, and let composition $f \circ g$ be the multiplicative structure. The fact that* $\mathrm{End}(G)$ *satisfies the laws of a ring are trivial, with the identity endomorphism 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 R be a ring, and consider the set $\mathrm{End}(R^+)$ of group homomorphisms on the abelian additive structure of R. We will show that R can be embedded in $\mathrm{End}(R^+)$ in a natural way. Consider the map $\varphi : R \to R^R$ defined by $\varphi(y) = f_y$, where $f_y : R \to R$ is a map defined by $x \mapsto yx$. Since the distributive law in R holds, we have that

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

which means exactly that f_y is a morphism, so that $\varphi(R)$ is contained in $\mathrm{End}(R^+)$. What's more, φ is a ring morphism (which by now, you should be able to provide a definition for), 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 what's more, φ is injective, since if $f_x = f_y$, then

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

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

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.

Definition. The **units** of a ring R are the elements x which possess a multiplicative inverse x^{-1}, a number such that $xx^{-1} = 1 = x^{-1}x$ (both ends of the equation need to be satisfied since ab may not equal ba). We shall denote the set of units by $R^\times$ or $U(R)$. This set always forms a group. though not necessarily a subring. Every non-zero element of a **division ring** (also called a **skew field**) is a unit. Commutative division rings are called **fields**.

Example. *The group of units in $M_n(\mathbf{F})$ is the general linear group $GL_n(\mathbf{F})$.*

Left invertible elements need not be right invertible.

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 $R \circ L(x_0, x_1, \dots) = (0, x_1, \dots)$, and L could never have an inverse, since it is not bijective.

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 $\sum k_i g_i$, with $k_i \in K$ and $g_i \in G$, where the additive structure is obvious, and*

$$\left(\sum_i k_i g_i\right)\left(\sum_j k'_j h_i\right) = \sum_{i,j} k_i k'_j g_i h_j$$

The quaternion group is $Q = \{1, i, j, k\}$, where

$$i^2 = j^2 = k^2 = ijk = -1$$

The general quaternions are the group ring $\mathbf{R}[Q]$. Every non-zero quaternion is invertible, since

$$\begin{aligned}(a + bi + cj + dk)(a - bi - cj - dk) &= a^2 + b^2 + c^2 + d^2 \\ &= (a - bi - cj - dk)(a + bi + cj + dk)\end{aligned}$$

Quaternions are not commutative, since $ij = k$, $ji = -k$. Invented by the Irishman, lord Hamilton, quaternions were one of the first truly abstract algebraic structures, and therefore have a special place in an algebraist's heart.

Example. *George Boole began the modern study of logic by studying 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 (where 0 is a statement which 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 boolean algebras studied in logic.*

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, they are included below.

Definition. 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.

The most fundamental chain of subrings are

$$\mathbf{Z} < \mathbf{Q} < \mathbf{R} < \mathbf{C}$$

Diagonal matrices in $M_n(\mathbf{F})$ form a subring, as do the continuous functions in $\mathrm{Mor}(\mathbf{R}, \mathbf{R})$.

Definition. A ring homomorphism from a ring A to a ring B is a function $f : A \to B$ such that

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

1.1 Ideals

We wish to establish a quotient structure on rings, to obtain analogies to the isomorphism theorems for groups. Let $\mathfrak{a}$ be a subset of a ring A. In order to obtain a well defined addition operation, we first need $\mathfrak{a}$ to be an additive subgroup of the additive group structure on $\mathfrak{a}$. We also require that the act of multiplication is well defined:

$$(a + \mathfrak{a})(b + \mathfrak{a}) = (ab + \mathfrak{a})$$

So, in terms of sets,

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

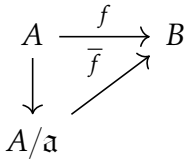
Thus we require $xb + ax' + xx' \in \mathfrak{a}$. Clearly, not only do we need $\mathfrak{a}$ to be closed under multiplication, but also closed under multiplication by any element of A. This is the definition of an ideal.

Definition. A **left ideal** $\mathfrak{a}$ is an additive subgroup of a ring A, with $A\mathfrak{a} = \mathfrak{a}$. A **right ideal** satisfies $\mathfrak{a}A = \mathfrak{a}$. A **double-sided ideal** (shortened to **ideal**) is a left and right ideal, and is the structure we use to form a quotient ring $A/\mathfrak{a}$.

We shall focus mostly on double sided ideals (which are the same as single sided ideals in the commutative case). One sided ideals come into play most importantly when we analyze modules.

The kernel of a ring homomomorphism is a double sided ideal. A ring homomorphism is an isomorphism if and only if the kernel is trivial. Just as in the group-theoretic case, we obtain the first isomorphism theorem.

Theorem 1.2 (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 we have an induced homomorphism $\overline{f} : A/\mathfrak{a} \to B$ satisfying the commutative diagram*



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

Theorem 1.3 (Second Isomorphism Theorem)**.** *Let $B < A$ be a subring, and $\mathfrak{a}$ an ideal of A. Then $B + \mathfrak{a}$ is a subring, $\mathfrak{a}$ 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 1.4 (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.*

A ring itself (denoted (1) when viewed as an ideal), and its trivial subring $(0) = \{0\}$, are always ideals, and are called trivial. In a field, these are the only ideals (from which we can deduce that a non-trivial ring homomorphism whose domain is a field is injective). Other examples in a

ring R are Ra, where a is a ring element. This ideal is called the principal ideal generated by a, and in the commutative case, is denoted (a). If a ring is such that all ideals are of this form, we say the ring is principal. Any ideal can be generated by these ideals in the sense that all ideals are $(S) = \bigoplus_{s \in S} Rs$ 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.

There is one and only one homomorphism from the integers to any ring (a simple proof by induction). They are in some sense 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 this is the smallest subring.

Quite a bit of elementary ring theory is an attempt to generalize what makes the integers so nice. Integers are universal objects in ring theory – they are the initial objects in the category. Since homomorphisms relate properties of rings, integers should naturally possess nice properties.

A 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.

An element x is nilpotent if $x^n = 0$ for some integer $n > 0$. If $1 \neq 0$ in a ring, then a nilpotent element is not invertible. The set of all nilpotent elements in a **commutative** ring R is an ideal, denoted $\sqrt{R}$ and called the nilradical of the ring. The additive closure of $\sqrt{R}$ follows from the binomial theorem. If $x^n = 0$ and $y^m = 0$, then

$$(x-y)^{nm} = \sum_{k=0}^{nm} \binom{n+m}{k} x^{n+m-k} y^k (-1)^k$$

each element in the sum has some nilpotent power in. Hence $(x-y)^{nm} = 0$.

Given any ring R, there is a unique homomorphism from $\mathbf{Z}$ to R. The kernel of this homomorphism is an ideal of $\mathbf{Z}$, and since $\mathbf{Z}$ is a principal ideal domain, can be denoted $n\mathbf{Z}$ for some integer n. n is the characteristic of the ring R.

The property of idealness is preserved by many set theoretic operations. For instance, if A is a set of ideals, then so is

$$\bigcap A$$

and provided A forms a chain linearly ordered by inclusion, so is

$$\bigcup A$$

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, we define an operation of multiplication

$$\mathfrak{a}\mathfrak{b} = \{\sum a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

This is the smallest ideal containing all $a_i b_i$. $\mathfrak{a} + \mathfrak{b}$ is similarily an ideal. More generally, so is $\bigoplus \mathfrak{a}_i$ for any so specified family of ideals. Given any subset of a ring, we can generate a smallest ideal containing it by the same mathematical trick used in all disciplines of mathematics - just take the intersection of all possible candidates.

As an example of this process, consider ideals in $\mathbf{Z}$. Since $\mathbf{Z}$ is a principal ideal domain, we need only consider products of the form

$$\prod_{i \in I} p_i \mathbf{Z}$$

which is generated by all integers that can be written

$$\prod_{i \in I} s_i p_i$$

with s_i in $\mathbf{Z}$. Since all of the products can be written $\prod s_i \prod p_i$, we get that $\prod p_i \mathbf{Z} \subset \mathbf{Z}(\prod p_i)$. Since we may take all $s_i = 1$, we obtain that $\prod \mathbf{Z} p_i = \mathbf{Z} \prod p_i$.

A prime number is a number p such that if p divides ab, p divides a or p divides b. Equivalently, it is a number such that if $p = ab$, then a or b are ± 1. A prime ideal is an ideal in a ring which is not the entire, ring, and such that if the ideal contains ab, it also contains a and b. It is a small exercise to verify that a ring is entire if and only if (0) is a prime ideal. If a ring is an integral domain, the characteristic of the ring is 0 or a prime number.

An ideal is maximal if it does not contain all ring elements, 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 ideal is contained in some maximal ideal. Maximal ideals in some sense take the nastiness out of a ring.

Theorem 1.5. *I is a maximal ideal of a ring R if and only if R/I is a field.*

Proof. We will verify that R/I is a field, and leave the converse to the reader. In R/I, $1 \neq 0$, since $1 \notin I$. Consider $x + I$, where $x \notin I$. Then $I + Rx$ is an ideal strictly bigger than I, so that $I + Rx = R$. Thus there is $y \in R$, $z \in I$ such that $z + yx = 1$. But then $yx + I = 1 + I$, so $y + I = (x + I)^{-1}$. □

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.

We can also use Zorn's lemma to generalize the nilradical of a commutative ring to noncommutative cases. We define the Jacobson radical $J(R)$ of a (not necessarily commutative) ring R to be the intersection of all prime ideals in the ring; it is the smallest prime radical. In the commutative case, $J(R) = \sqrt{R}$.

Theorem 1.6. *In a commmutative ring, the Jacobson radical is equal to the nilradical of the ring.*

Proof. First we must show that every prime ideal contains every nilpotent element. If $x^n = 0$, then, since every prime ideal I contains 0, $x^n \in I$. By definition of the prime ideal, $x \in I$. Conversely, suppose $x \notin \sqrt{R}$. Consider the set $S = \{x^n : n \in \mathbf{N}\}$. Let L be the set of all (not necessarily prime) ideals in R disjoint from S. L is not empty, since $(0) \in L$, and L is inductively ordered, so we may consider some upper bound P. Given any $a, b \notin P$, $P + Ra$ and $P + Rb$ are strictly bigger than P, and thus there is p_1, r_1 and p_2, r_2 such that $p_1 + r_1 a = x^n$ and $p_2 + r_2 b = x^m$. But then

$$x^{m+n} \in (P + Ra)(P + Rb) = P + P(Ra) + P(Rb) + Rab = P + Rab$$

And therefore $ab \notin P$. Thus P is prime, and does not contain x, so that $J(R)$ does not contain x. □

Chapter 2

Commutative Rings

Definition. A factorial ring A is an integral domain such that every a can be written

$$a = \prod_{i=1}^{n} p_i$$

where p_i is irreducible, and if

$$\prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$$

Then $n = m$, and, after a permutation, each p_i differs from q_i by a unit.

Lemma 2.1. *An element $x \in A$ is invertible in $S^{-1}A$ if and only if $(x) \cap S \neq \varnothing$.*

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

Lemma 2.2. *If 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 that $p \mid mx$. 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 2.3. *Let A be factorial. 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, then some p_i is irreducible in $S^{-1}A$, and the other combined factors are a unit. But this implies exactly that p_i is irreducible in A, and $(p_i) \cap S = \varnothing$. □

Lemma 2.4. *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 2.5. *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 $S^{-1}A$. □

2.1 Localization

Let A be a commutative ring with identity. Even if an element $a \in A$ is not invertible, we may still want to find a way to embed A in a larger ring B in which a has an inverse. This is not always possible. For instance, if $a^2 = 0$, then it is impossible for a to be 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 an invertible map, then a cannot have any zero divisors. However, if we remove the condition that f is injective, then the only condition that prevents $f(a)$ from having an inverse is if $a = 0$.

Considering this problem in a more general viewpoint, we consider some set $S \subset A$, and try to find a '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**. The technique of adding invertible elements in this manner is known as **localization**.

The classical situation where we apply localization is in the case where A is an integral domain, in which case the problems of zero divisors disappear. If we consider the set B which consists of all (a, b), where $b \neq 0$, and identifying (a, b) with (c, d) if $ad - bc = 0$. Because of the relation to fractions, it is customary to denote (a, b) by a/b. After the identification of ratios, we can define a multiplication and addition operation by setting $(a, b)(c, d) = (ac, bd)$, and by setting $(a, b)+(c, d) = (ad+bc, bd)$. These operations are well defined, because if $(a_0, b_0) = (a_1, b_1)$ and $(c_0, d_0) = (c_1, d_1)$, then $a_0c_0/b_0d_0 = a_1c_1/b_1d_1$ and $(a_0d_0 + b_0c_0)/b_0d_0 = (a_1d_1 + b_1c_1)/b_1d_1$,

because

$$a_0b_1c_0d_1 - a_1b_0c_1d_0 = a_1b_0c_0d_1 - a_1b_0c_1d_0 = a_1b_0(c_0d_1 - c_1d_0) = 0$$

$$(a_0d_0 + b_0c_0)b_1d_1 = a_1b_0d_0d_1 + b_0b_1c_1d_0 = b_0d_0(a_1d_1 + b_1c_1)$$

Then B has the structure of a ring, in which every nonzero element has an inverse – that is $(a,b)^{-1} = (b,a)$. Thus B is not only a ring, but a field, and we call B the **field of fractions** with coefficients in A. We have an embedding of A in B by mapping a to $a/1$.

Example. *The first use of the field of fractions was the construction of the rational numbers from the integers. This is validified because* $\mathbf{Z}$ *is an integral domain. Constructing the field of fractions is essentially just a generalization of the technique of forming* $\mathbf{Q}$ *from* $\mathbf{Z}$*, now taken over arbitrary integral domains.*

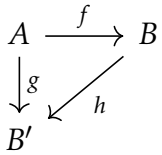
Example. *If* $A[X_1,\ldots,X_n]$ *is the polynomial ring with coefficients in some integral domain* A*, then the polynomial ring is an integral domain, and performing localization gives the field* $A(X_1,\ldots,X_n)$ *of rational functions, which consists of all finitary expressions of the form*

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

These can be considered as functions mapping certain elements of A *into* K*, where* K *is the field of fractions of the ring* A*. In particular,* f/g *is defined at* $a \in A$ *if* $g(a) \neq 0$*, because then* $f(a)/g(a)$ *is defined. For each* $a_1,\ldots,a_n$*, there is a unique homomorphism from* $A[X_1,\ldots,X_n]$ *to* K *fixing elements of* A*, and mapping* X_i *to* a_i*. As an example, the field of fractions of* $\mathbf{Z}[X_1,\ldots,X_n]$ *is* $\mathbf{Q}(X_1,\ldots,X_n)$*.*

Example. *If we consider the complex algebra of functions holomorphic in some connected open region* D *of the complex plane, then* $A(D)$ *is an integral domain. If* $fg = 0$*, where* f *and* g *are not equal to zero 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, which is the set of meromorphic functions on* D*. These functions* f/g *are defined except for certain points upon which* $g(z) = 0$*, and for which* z *is not a removable singularity of* g*, which means exactly that* $f/g = f'/g'$*, where* $g'(z) \neq 0$*.*

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 $f : A \to B$ into some ring B such that $f(s)$ is invertible for each element s in some multiplicative set S. To find this object, we apply category theory. Consider the category whose objects are ring homomorphisms $f : A \to B$, such that for each $s \in S$, $f(s)$ is invertible, and a homomorphism between f and another homomorphism $g : A \to B'$ is a map $h : B \to B'$ such that $g = h \circ f$.



An initial object in this category 'should be' the simplest ring in which every element of S has an inverse. We shall construct such an object, and we shall denote it by $S^{-1}A$.

Let us try and derive what our initial object $S^{-1}A$ should look like. First, 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 $f(a)f(s)^{-1}$, for $a \in A$ and $s \in S$ is a subring of $S^{-1}A$. This follows because

$$\begin{aligned} f(a)f(s)^{-1}f(b)f(t)^{-1} &= f(ab)f(st)^{-1} \\ f(a)f(s)^{-1} + f(b)f(t)^{-1} &= f(at+bs)f(st)^{-1} \\ f(a)f(s)^{-1} + f(-a)f(s)^{-1} &= f(0)f(s)^{-1} = 0 \\ f(1)f(1)^{-1} &= f(1) = 1 \end{aligned}$$

This implies that $f : A \to B$ is actually an object in our required category, and we must therefore have an isomorphism from $g : B \to S^{-1}A$ respecting the induced functions. This implies that $S^{-1}A$ consists exactly of elements of the form $f(a)f(s)^{-1}$. Next, we must deduce the property that $f(a)f(s)^{-1} = f(b)f(t)^{-1}$. If this is true, then $f(at - bs) = 0$. One condition guaranteeing this will occur is if there is an element $u \in S$ for which $u(at - bs) = 0$, because then $f(u)f(at - bs) = 0$, and multiplying by $f(u)^{-1}$ gives the property. Often, the correct technique to find 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 which case we must try and find more properties of the object, or the object will be correctly constructed, and will often be the required universal object. Let us try and construct $S^{-1}A$ based on the properties we have considered.

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 $a/s + b/t = (at + bs)/ts$. Provided that $0 \notin S$ in which $su = 0$, in $S^{-1}A$ $1/1$ will not be equal to $0/1$, in which case $S^{-1}A$ will have a ring structure (if $0 \in S$, then $S^{-1}A$ consists of a single equivalence class), and we have a map $f : A \to S^{-1}A$ given by $f(a) = a/1$, and then $f(s)^{-1} = 1/s$. If $g : A \to B$ is any ring homomorphism in which $f(s)$ is invertible for each $s \in S$, then we can define $h : S^{-1}A \to B$ by $h(a/s) = g(a)g(s)^{-1}$, and then it is a simple procedure to verify that the require diagram commutes. 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 containining 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, these two conditions are equivalent in a topological space where we can construct functions at a point vanishing outside of a specified neighbourhood. Thus functions are identified if 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.

If A is an integral domain, and $a/1 = 0$, then there is $s \in S$ with $sa = 0$, and provided that $0 \notin S$, we conclude that $a = 0$, hence the homomorphism $A \to S^{-1}A$ is injective. If no element of S has any zero divisors, then the homomorphism is still injective, but otherwise we can guarantee that the homomorphism is not injective. There is a certain converse to this result. If A is an integral domain, and $f : A \to B$ is an injective homomorphism such that $f(s)$ is invertible for each $s \in S$, then the induced homomorphism $f : S^{-1}A \to B$ is injective, hence $S^{-1}A$ is isomorphic to the subring of B generated by elements of the form $f(a)f(s)^{-1}$.

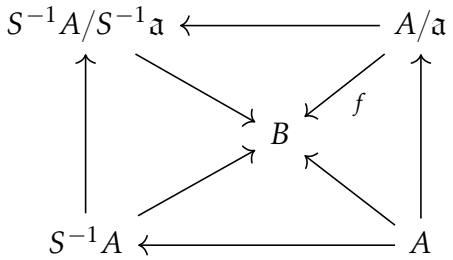
Perhaps this formal approach is not so intuitive from a more geometric perspective. There is a more 'natural' approach to forming $S^{-1}A$, but it is much more messy. When learning fractions for the first time, you viewed them as ways to 'divide' certain integers into other integers. If you have 6 apples, 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.

Using the universal property of localization, we can prove that the action of 'localization' is preserved under quotients.

Proposition 2.6. *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. □

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.

If $J(A)$ is the set of ideals in A, then we have a map from $J(A)$ to $J(S^{-1}A)$, where we map the ideal $\mathfrak{a}$ in A to the ideal generated by the image of these elements in $S^{-1}A$, which, more precisely, is the set of elements of the form a/s, where $a \in \mathfrak{a}$. The image of this map is often denote $S^{-1}\mathfrak{a}$, and respect intersections, sums, products, and inclusions of ideals. That is,

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

and if $\mathfrak{a} \subset \mathfrak{b}$, $S^{-1}\mathfrak{a} \subset S^{-1}\mathfrak{b}$. This essentially shows that the localization of rings with certain properties for their ideals will also have these properties.

Proposition 2.7. *If A is principal, then $S^{-1}A$ is principal.*

Proof. If $\mathfrak{a} \subset S^{-1}A$ is an ideal, then the inverse image of $\mathfrak{a}$ in A is an ideal, hence equal to (a) for some element $a \in A$. This means exactly that if $b/1 \in \mathfrak{a}$, then a divides b. But this means that a generates $\mathfrak{a}$, because for any $b/s \in \mathfrak{a}$, $b/1 = s(b/s) \in \mathfrak{a}$, hence we can write $b = ca$, and then $b/s = (c/s)a$, hence $\mathfrak{a} = (a)$. □

Proposition 2.8. *If A is Noetherian, then $S^{-1}A$ is Noetherian.*

Proof. The proof of this proposition is analogous to the proof of the last proposition, and is left to the reader. □

Proposition 2.9. *If A is a factorial ring, then $S^{-1}A$ is factorial.*

Proof. Let X be the set of irreducible elements x of A with $(x) \cap S \neq \varnothing$ (these are easily proved invertible in $S^{-1}A$), and Y the set of irreducibles with $(x) \cap S = \varnothing$. Then the elements of X cannot differ from elements

of Y by a unit, because this doesn't change the principal ideal generated by X and Y. Then all elements of Y are irreducible in A. To prove this, consider $a \in Y$. If $a = (b/s)(c/t) = (bc/st)$, then $ast = bc$. Because A is factorial, we may write $bc = stb'c'$ for some $b', c' \in A$ with b' dividing b and c' dividing c, so we conclude $a = b'c'$, hence either b' or c' is a unit. We may assume b' is a unit, and then b is the product of two units in $S^{-1}A$, hence b itself is a unit in $S^{-1}A$. This shows that every element of $S^{-1}A$ has a factorization into irreducibles, because $1/s$ is a unit, and any element $a \in A$ has a factorization $p_1^{n_1} \dots p_m^{n_m} q_1^{l_1} \dots q_k^{l_k}$, where $p_i \in X$ and $q_i \in Y$, and then we have a product of units and irreducibles.

If a/s is a unit in $S^{-1}A$, we can write $a = p_1^{n_1} \dots p_m^{n_m}$, with $p_i \in X$, and this describes the set of all units in $S^{-1}A$. Conversely, if a/s is irreducible in $S^{-1}A$, then a is irreducible in $S^{-1}A$, and $a = p_1^{n_1} \dots p_m^{n_m} q_1^{k_1} \dots q_l^{k_l}$ has a factorization as in the last paragraph. Since the q_i are not units, it turns out that we can only have one factor q, so $a = p_1^{n_1} \dots p_m^{n_m} q$.

Finally, assume we have an equality $(a_1/s_1) \dots (a_n/s_n) = (b_1/t_1) \dots (b_m/t_m)$, where a_i/s_i, b_j/t_j is irreducible. Then we can cross multiply, rewriting the equation over A as $t_1 \dots t_m a_1 \dots a_n = b_1 \dots b_m s_1 \dots s_n$. We know that the only factorizations of t_i and s_j contain factors of the form p_i, which we can safely ignore when factoring over $S^{-1}A$. Each a_i has a single factor $q_i \in Y$, and each b_i has a single factor $r_i \in Y$. Since the elements of X are not equivalent to factors over B, the q_i and r_i must factor together, so $n = m$, and there is a permutation of the b_i such that q_i and r_i differ from each other by a unit. This completes the proof of unique factorization. □

2.2 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 $a \in (a) \subset \mathfrak{m}$. 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 $A_\mathfrak{p}$ and call the local ring at $\mathfrak{p}$. An element in $A_\mathfrak{p}$ will be invertible precisely when it can be written as a/b, where $a \notin \mathfrak{p}$. If two elements $a/b, c/d \in A_\mathfrak{p}$ are not invertible, but $(ad + bc)/bc = x/y$, where $x \notin \mathfrak{p}$, then $y(ad + bc) = xbc$, and $ad + bc \in \mathfrak{p}$, because $a, c \in \mathfrak{p}$, hence $y(ad + bc) \in \mathfrak{p}$ so we conclude that $bc \in \mathfrak{p}$, hence $b \in \mathfrak{p}$ or $c \in \mathfrak{p}$, which is impossible. Thus the sum of two noninvertible elements is noninvertible. If a/b is not invertible, then ac/bd is not invertible, because if $ac/bd = x/y$, where $x \notin \mathfrak{p}$, then $acy = bdx$, and since $a \in \mathfrak{p}$, we conclude that either $b \in \mathfrak{p}$ or $d \in \mathfrak{p}$ again, which is impossible. Thus the set of noninvertible elements is an ideal, and $A_\mathfrak{p}$ 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 $\mathbf{Z}_{(2)}$.*

Proposition 2.10. *If A is a local ring, and $f : A \to B$ is a surjective homomorphism, then B is local.*

Proof. Let A be a local ring with maximal ideal $\mathfrak{m}$, and let $\mathfrak{a}$ be any proper ideal. For any $x \in \mathfrak{m}$, we cannot have $x-1 \in \mathfrak{m}$, because then $1 = x-(x-1) \in \mathfrak{m}$, so $\mathfrak{m}$ is not a proper ideal. Then $A/\mathfrak{a}$ is a ring, and $\mathfrak{m}/\mathfrak{a}$ is an ideal in $A/\mathfrak{a}$. This ideal is in fact a proper ideal of $A/\mathfrak{a}$, because if there was $x \in \mathfrak{m}$ such that x is congruent to 1 modulo $\mathfrak{a} \subset \mathfrak{m}$, which we already showed was impossible. If $\mathfrak{ba}$ is a proper ideal of $A/\mathfrak{a}$, it corresponds to a proper ideal of A containing $\mathfrak{a}$, and hence we find $\mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{m}$, so $\mathfrak{b}/\mathfrak{a} \subset \mathfrak{m}/\mathfrak{a}$, so $\mathfrak{m}/\mathfrak{a}$ is the unique maximal ideal of $A/\mathfrak{a}$. The first isomorphism theorem then gives us the result for general surjective maps from a local ring to another ring. □

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.

Local rings occur widely in mathematics when we want to look at 'local' properties of functions. For instance, we call a Noetherian local ring, which isn't a field-= but which is a domain, whose maximal ideal is principal a **discrete valuation ring**. It turns out that this is the class of rings where we can discuss the phenomenon of 'multiplicities of zeroes'.

Proposition 2.11. *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 function 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*.*

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, such that $\varphi(xy) = \varphi(x) + \varphi(y)$, $\varphi(x+y) \geqslant \min(\varphi(x), \varphi(y))$, and $\varphi(x) = \infty$ if and only if $x = 0$.

Proposition 2.12. *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 2.13. *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 2.14. *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,

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

Proposition 2.15. *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, $a_0 + a_1X^{-1} + \cdots + a_nX^{-n} = (a_0X^n + \cdots + a_n)/X^n$ is invertible in A, hence $X^n/(a_0X^n + \cdots + a_n) \in A$. Multiplying by $b_0 + b_1X^{-1} + \cdots + b_nX^{-n}$, we conclude that $(b_0X^n + \cdots + b_n)/(a_0X^n + \cdots + a_n) \in A$ 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 $g = (X - a_1)\ldots(X - a_m)$, $f = (X - b_1)\ldots(X - b_l)$, and then $h = (X - a_1)\ldots(X - a_{m-1})/(X - b_1)\ldots(X - b_l) \in A$, 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.

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 $W/T(W)$. $\square$