Ring Theory

Jacob Denson

October 16, 2018

Table Of Contents

Chapter 1

Basic Definitions

Rings are algebraic structures closed under addition, subtraction, and multiplication, but not necessarily under division. They can be noncommutative, such as the ring of square matrices of a fixed dimension, or commutative, like the ring of integers. Specifically, a ring is a set under which an additive and multiplicative operation is defined, where the addition gives the ring a structure of a group with identity 0, and the multiplication gives the ring a structure of a semigroup. The multiplicative structure and additive structure play nice with one another thanks to the distributive law, which saw that $a(b+c) = ab + ac$, 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. It is often the case that rings have a multiplicative identity, and provided that it is not also the additive identity, we denote it by 1. Studying rings with identity is normally no more general than studying rings without identity, since any ring can be extended to have an identity in a canonical way.

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. *All the number systems* $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{F}_p$, *and* $\mathbf{C}$ *are rings, in which case every nonzero element is invertible. Such rings are known as* **division rings**, *and if the multiplicative operation is commutative,* **fields**.

Example. *For any ring A, the algebra of $n \times n$ matrices $M_n(A)$ with entries in A forms a ring. If A is a field, then the analysis of this ring becomes a topic of the field of linear algebra. The canonical form of matrices generalizes to an important 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 $a_0+a_1X+\dots+a_NX^N$, where $a_n \in A$. We view two polynomials as being equal precisely when their coefficients are equal. More generally, we can discuss their multivariate counterparts $A[X_1,\dots,X_n]$, the ring of formal sums in the monomials $X_1^{m_1}\dots X_n^{m_n}$. The addition of two polynomials is defined by taking the sum over each monomial separately, and the product is obtained by expanding and multiplying monomials together in the obvious way. The polynomial ring is the 'most general' way to add elements to a ring, since it has the universal property that for any homomorphism $f: A \to B$, and $x_1,\dots,x_n \in B$, there is a unique extension of f to a homomorphism on $A[X_1,\dots,X_n]$ with $f(X_n) = x_n$.*

Example. *If A is a ring, and M is a multiplicative semigroup, then we can consider a ring $A[M]$, whose elements are finite formal sums of the form $\sum a_n x_n$, with $x_n \in A$, $x_n \in M$, with the obvious additive structure, and with multiplicative structure defined by multiplying elements of the monoid termwise. We calculate that*

$$\left(\sum_{x\in M} a_x x\right)\left(\sum_{y\in M} b_y y\right) = \sum_{x,y\in M} a_x b_y xy = \sum_{z\in M}\left(\sum_{xy=z} a_x b_y\right) z$$

So multiplicative is given by a form of convolution in the coefficients. In the case where $M = \mathbf{N}$ or $M = \mathbf{N}^n$, we obtain the ordinary natural numbers. There are multiple ways to generalize this. If M is a monoid such that for each k, there are only finitely many g,h such that $gh = k$, then we can extend the group to the set of all formal sums with infinitely many terms. In these cases one can think of elements as functions $f: M \to A$, and $g: M \to A$, and then the multiplication operation on $A[M]$ extends to convolution $f * g: M \to A$ defined by

$$(f*g)(z) = \sum_{xy=z} f(x)g(y)$$

This often occurs in number theory over $M = \mathbf{N}$, which is often disguised via the introduction of the power series ring $A[[X]]$. If we do not have a finiteness *condition, we could still interpret the sums as an infinite sum, provided A has some analytic structure. Better yet, if M is a locally compact group with a Haar measure, we can interpret*

$$(f * g)(x) = \int f(y) g(y^{-1}x)\, d\mu(y)$$

This is where harmonic analysis takes over.

Example. *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 a quotient of the group algebra* $\mathbf{R}[Q]$*, where*

$$Q = \langle \overline{e}, i, j, k : \overline{e}^2 = e, i^2 = j^2 = k^2 = ijk = \overline{e} \rangle$$

The quotient is taken over the ideal $(\overline{e} + e, \overline{e}i + i, \overline{e}j + j, \overline{e}k + k)$. Invented by the Irishman, lord Hamilton, in the mid 19th century, to algebrize 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 induce the classical development of abstract algebra.

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 the set of all equivalence classes of logical statements (two statements being equivalent if they both imply each other), and consider conjunction as a multiplication, and exclusive disjunction as an additive structure, then we obtain a ring satisfying $x^2 = x$ for all statements x, where 0 is a statement that is always false, and 1 a statement the 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 $yx = xy$. They are essentially the same as Boolean algebras studied in logic and measure theory, and the exact correspondence is provided by the Stone representation theorem, employing tools of topology!*

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. The ring* $C_c(\mathbf{R})$ *of compactly supported continuous functions on the real line provides our first natural example of a ring without identity.*

Example. *If B is a commutative subring of a ring A, then for any subset S of A, we can consider the ring generated by B and S, denoted by $B[S]$. Interesting examples of these include the* **Gaussian integers** $\mathbf{Z}[i]$*, whose points form a lattice in the plane, and the* **Dyadic numbers** $\mathbf{Z}[1/2]$*, which are the fractions expressible with a denominator a power of two, which form a dense subset of the real line. In algebraic number theory, if d is a squarefree integer, one studies the ring $\mathbf{Z}[\sqrt{d}]$ in more detail, which is the set of all numbers of the form $n + m\sqrt{d}$.*

Remark. There is only a single example of a ring in which the multiplicative identity equals the additive identity. This is because for any a,

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

From which we conclude $a \cdot 0 = 0$. But if 0 is also a multiplicative identity, we conclude that $a = a \cdot 0$. This means the only ring for which the additive and multiplicative identities correspond is the ring consisting 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* $\text{End}(G)$ *of all homomorphisms from G to itself. We define a ring structure on this group. Given $f, g \in$* $\text{End}(G)$*, 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* $\text{End}(G)$ *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 $\text{End}(A)$ of group homomorphisms on the abelian additive structure of A. Consider the map $\varphi : A \to \text{End}(A)$ where $\varphi(x)(y) = xy$. The distributive law implies

$$\varphi(x)(y + z) = x(y + z) = xy + xz = \varphi(x)(y) + \varphi(x)(z)$$

so $\varphi(x) \in \text{End}(A)$. What's more, φ is a ring homomorphism (a homomorphism of rings is defined exactly how you think it should be), since

$$\varphi(x+y)(z) = (x+y)(z) = xz + yz = [\varphi(x) + \varphi(y)](z)$$

$$\varphi(xy)(z) = (xy)z = x(yz) = (\varphi(x) \circ \varphi(y))(z)$$

The map φ is injective assuming that there is no nonzero element $x \in A$ with $xy = 0$ for all y. In particular, this is true if A has an identity, for then $x = x \cdot 1 = 0$. Thus $\text{End}(A)$ naturally contains A as a subring. □

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.

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. For example, when A is the ring of endomorphisms on a ring, $ab = 1$ implies b is injective, whereas $ba = 1$ implies b is surjective, and when the set is infinite injectivity is not equivalent to surjectivity. Thus we need to distinguish between the left invertible and right invertible elements, though if an element is both left and right invertible, it is a unit. We let $U(A)$ denote the set of all units in a ring. It forms a multiplicative group.

- The group of units in $\mathbf{Z}$ is ± 1.

- In the ring $\mathbf{Z}[i]$ of Gaussian integers, the only units are ± 1 and $\pm i$.

- In the ring $\mathbf{Z}[1/2]$ of dyadic numbers, the invertible elements are precisely of the form $\pm 2^n$ for some $n \in \mathbf{Z}$.

- The group of units in $\mathbf{Z}_n$ is the set of equivalence classes of integers coprime to n.

- If A is a unital ring with no zero divisors, then the units of $A[X_1, \dots, \dots, X_n]$ are precisely the elements of A.

- If A is a ring with identity, then a power series $f \in A[[X]]$ is a unit in $A[[X]]$ if and only if $f(0)$ is a unit in A.

- If A is a ring with identity, then Cramer's rule tells us that the units of $M_n(A)$ are precisely those matrices whose determinant is a unit in A. In particular, if K is a field, then the group of units in $M_n(K)$ is the set of matrices with nonzero determinant, forming the general linear group $GL_n(K)$.

- In number theory, one considers functions $f : \mathbf{N} \to \mathbf{C}$ which behave nicely with respect to the Dirichlet convolution

  $$(f * g)(k) = \sum_{nm=k)} f(n)g(m)$$

  Then the space of functions with pointwise addition and convolution as multiplication form a ring. This ring has a multiplicative identity, the function

  $$\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{otherwise} \end{cases}$$

  If μ is the *Möbius function*

  $$\mu(n) = \begin{cases} 0 & p^2 \text{ divides } n \text{ for some prime } p \\ (-1)^k & n \text{ has } k \text{ distinct prime factors} \end{cases}$$

  and 1 is the constant 1 function, then one proves that $1 * \mu = \delta$. The Möbius inversion formula states that $f = g * \mu$ if and only if $f * 1 = g$, and this is nothing more than the fact than saying that μ is a unit in the convolution ring, with 1 as it's inverse.

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 classical chain of commutative subrings is*

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

The other subrings in this chain are still actively researched today, most importantly in the theory of algebraic number theory.

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 semigroup structure on the two spaces. If the rings are unital, we also assume that they map the identity to the identity. As with groups and vector spaces, the kernel $\text{Ker}(f)$ of the map f is defined to be the set of all a such that $f(a) = 0$. As with groups, determining the structure of the kernel of a homomorphism will enable us to obtain a variant of the isomorphism theorems for rings, which we carry out in the next section.

Example. *If A is a unital ring, there is a unique homomorphism of unital rings from $\mathbf{Z}$ to A, since $\mathbf{Z}$ is generated by the unit. We identify elements of $\mathbf{Z}$ with elements of A. Even if A is non-unital, we can still define an action of $\mathbf{Z}$ on the additive structure of R by defining $nx = x + \dots + x$ as the n fold sum of x's. Thus we can consider the additive group $\mathbf{Z} \oplus R$ with an additional multiplication operation $(n \oplus x)(m \oplus y) = nm \oplus (mx + ny + xy)$. One verifies that this gives the structure of a ring, which now has an identity $1 \oplus 0$. The resultant ring is known as the* **unitization** *of R, and has the universal property that every homomorphism of R into a unital ring extends to a homomorphism of the unitization of R.*

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 say $\mathfrak{a}$ is an **ideal** if it is an additive subgroup of R closed under multiplication on the left and the right. In a commutative ring, of course, we need only prove that an ideal is closed by multiplication on the left.

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.*

Example. *Every additive subgroup of $\mathbf{Z}$ is a set of multiples of some number n, which we denote by (n). It is also an ideal of $\mathbf{Z}$, and so these describe all multiples of the integers. In general, if A is a commutative ring, and $x \in A$, we find $(x) = Ax = \{ax : a \in A\}$ is an ideal, known as a* **principal ideal**. *If A is a ring such that every ideal is principal, we say that A is a* **principal ideal ring**. *The integers are an example, as we have just argued. We can also consider the ideal $(x_1, \dots, x_n)$, the smallest ideal containing the elements $x_1, \dots, x_n$.*

Example. *If M is a nonzero rank k square matrix, then there exists two invertible square matrices N and K such that*

$$NMK = \begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}$$

Then for any for $j \leqslant k$, $e_{ij}NMK = e_{ij}$. Similarily, if $i \leqslant k$, $NMKe_{ij} = e_{ij}$. In particular, we conclude that the two sided ideal generated by M over $M_n(K)$

contains all e_{ij}, so in particular $M_n(K)$ has only two ideals, (0) and (1). In particular, this means that every homomorphism from $M_n(K)$ to another ring A must be injective, or zero.

Example. *The last example is a phenomenon which very rarely happens in the field of commutative unital rings. This is because if (0) and A are the only ideals of a ring A, then for any nonzero x, $(x) = A$, so there is an element $y \in A$ such that $yx = 1$, which implies that x is invertible. Thus A must be a field. It follows from similar reasoning to the example above that every homomorphism from a field into another ring must be injective.*

The intersection of a family of 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 $\mathfrak{a}\mathfrak{b}$ 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 $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. We need not have equality here. For instance, in $\mathbf{Z}$, $(a)(b) = (ab)$, yet $(a) \cap (b) = (\text{lcm}(a,b))$. However, if a and b are relatively prime, the two ideals are equal, and more generally, if A is a unital ring such that $\mathfrak{a} + \mathfrak{b} = A$, then we can find $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ such that $a + b = 1$ and $c \in \mathfrak{a} \cap \mathfrak{b}$, then $c = c(a+b) = ca + cb \in \mathfrak{a} + \mathfrak{b}$. The distributive law $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$ 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 $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$ in the integers, but we only have $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}$ in general rings.

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 there is a unique induced homomorphism $f_* : A/\mathfrak{a} \to B$ satisfying the commutative diagram*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d] & B \\
A/\mathfrak{a} \arrow[ur, "f_*"] &
\end{tikzcd}$$

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

Theorem 1.3 (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 1.4 (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, and for any ideal $\mathfrak{a}$ in B, $A/f^{-1}(\mathfrak{a}) \cong B/\mathfrak{a}$.*

The third isomorphism shows that we can 'introduce relations' in an essentially commutative way, by either quotienting by a kernel, then by further relationships, or by quotienting by the ideal generated by both. The resulting ring will be the same.

Example. *Consider the ring $\mathbf{Z}[i]/(i-2)$. The third isomorphism theorem tells us that this ring is isomorphic to $\mathbf{Z}[X]$, quotiented by the ideal $(X^2+1, X-2)$. But if we consider the projection $\pi : \mathbf{Z}[X] \to \mathbf{Z}$ by mapping X to 2, the kernel is $(X-2)$, and since $\pi((X^2+1, X-2)) = (2^2+1, 0) = (5)$, we conclude that $\mathbf{Z}[X]/(X^2+1, X-2) \cong \mathbf{Z}/(5) \cong \mathbf{Z}_5$.*

If A is a unital ring, we can consider the unique homomorphism from $\mathbf{Z}$ to A, whose kernel is of the form (n) for some positive integer n. We call n the **characteristic** of the ring. The ring A therefore contains a subring isomorphism to $\mathbf{Z}_n$ for some integer n, known as the **prime ring**. The reason for the terminology is that, if A has no zero divisors, then n must necessarily be prime.

Chapter 2

Divisibility in Commutative Rings

We now assume all rings under discussion are commutative. A commutative ring with identity 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**. In this case, ideals provide a way to extend the theory of divisibility over the integers to larger classes of rings. For instance, if A is an integral domain, and $a, b \neq 0$, then $(a) = (b)$ if and only if there is a unit x such that $a = xb$. In the case of the integers, this means that $(a) = (b)$ if and only if $b = \pm a$. We shall find that the integers form a principal ideal domain, which means that the ideals of this ring perfectly model the divisibility theory in this ring. In particular $(a) \subset (b)$ if and only if the element b divides a.

As another example, given two $x, y \in A$, we say a is a **greatest common divisor** if a divides x and y, and for any b dividing x and y, b divides a. If A is a principal ideal domain, and $(x, y) = (a)$, then a is a greatest common divisor of x and y. The fact that b divides x and y, is expressed by saying $(x, y) \subset (b)$, hence $(a) = (x, y) \subset (b)$, so b divides a. Thus we see that the greatest common divisor in a principal ideal domain exists and is unique up to a unit in a principal ideal domain. Similarily, if $x, y \in A$, we say a is a **least common multiple** of x and y if x and y divide a, and any b with x and y dividing b is divisible by a. In a principal ideal domain, if $(x) \cap (y) = (a)$, then a is a least common multiple of x and y.

An ideal $\mathfrak{p}$ of a commutative ring A 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 p divides nm, then p divides n or m. An alternative definition, clear from the definition, is that $A/\mathfrak{p}$ is an integral domain.

Theorem 2.1. *The inverse image of a prime ideal is prime.*

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

One of the tenents of commutative ring theory is that the structure of the ring according to the prime ideals tells us everything we need to know about the ring.

2.1 Euclidean Domains

If A is an integral domain, a **Euclidean function** is a positive integer valued function ord 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 an integral domain possessing a Euclidean function. For convinience, we define $\text{ord}(0) = -\infty$.

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 the polynomial ring $K[X]$, for any field K. If $f(X) = a_0 + \dots + a_N X^N$, $g(X) = b_0 + \dots + b_M X^M$, and $N \geqslant M$, then we can write*

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

which has order 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 2.2. *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. □

The fact that $\mathbf{Z}$ was a principal ideal domain was known since the time of the greeks. Gauss was the first to realise that $\mathbf{Z}[i]$ was a principal ideal domain, and he used it to prove some interesting results about the ordinary integers, solving congruences modulo primes.

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 2.3. *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 2.4. *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. □

Over non-commutative rings, this need not be the case.

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.*

2.3 Uniqueness of Congruences

In classical number theory, one takes a series of integers $k_1, \dots, k_m$ and values $a_1, \dots, a_m$, 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 $\mathfrak{a}_1, \dots, \mathfrak{a}_N$ over a commutative ring A, and we consider the corresponding projection π of A onto the product ring $A/\mathfrak{a}_1 \times \dots \times A/\mathfrak{a}_N$. The generalization of the Chinese remainder theorem is summarized in the next theorem. We saw two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are **coprime** if $\mathfrak{a} + \mathfrak{b} = A$.

Theorem 2.5. 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 $a \in \mathfrak{a}, b \in \mathfrak{b}$ 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 $\pi(b) = (1,0)$. This means that the homomorphism is surjective. Given any $x, y \in A$, $\pi(ya + xb) = (x,y)$, so π is surjective. In general, we note it suffices to find elements a_n such that $\pi(a_n)_m = \delta_{nm}$, because then $\pi(\sum x_n a_n) = (x_1, \dots, x_n)$. 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 is congruent to zero in each $\mathfrak{a}_n$ if and only if it contained in the intersection of all of the ideals. Conversely, if π is surjective, then for any $\mathfrak{a}_n$ and $\mathfrak{a}_m$, then we can find $a \in \mathfrak{a}_m$ such that $1 - a \in \mathfrak{a}_n$, which means $1 \in \mathfrak{a}_n + \mathfrak{a}_m$, implying coprimality. □

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 $a \in \{0, \dots, p-1\}$, $ap^n + 1$ 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 $p_1 p_2 \dots p_N$, for some irreducibles p_n, and such that if $p_1 \dots p_N = q_1 \dots q_M$, then $N = M$, and, after a permutation, each p_n differs from q_n by a unit.

Theorem 2.6. *Let A be a principal factorial ring. If $(a, b) = (c)$, then every d dividing a and b also divides c. The number 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

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

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 2.7. *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 $x_N \mid \dots \mid x_2 \mid x_1 \mid x_0$, 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.

The fact that every ideal in $K[X_1, \dots, X_n]$ is finitely generated was discovered by Hilbert. However, the importance of every ideal being finitely generated in an arbitrary commutative ring was discovered by Emmy Noether. We therefore call a ring **Noetherian** if every ideal is finitely generated. Equivalently, a ring is Noetherian if there does not exist an infinite strictly increasing family of ideals $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \dots$, a fact known as the *ascending chain condition*. If every ideal is finitely generated, the limit of these ideals must also be finitely generated, and hence be contained in some $\mathfrak{a}_n$, which is impossible. Conversely, if we take an ideal $\mathfrak{a}$ which is not finitely generated, then we can consider an infinite chain $(f_1) \subsetneq (f_1, f_2) \subsetneq (f_1, f_2, f_3) \subsetneq \dots \to \mathfrak{a}$, which is a counterexample to the ascending chain condition.

Theorem 2.8. *If R is a Noetherian ring, then $R[X]$ is a Noetherian ring.*

Proof. For any ideal $\mathfrak{a}$ in $R[X]$, we can consider the *leading coefficient ideal* $\mathfrak{b}$ consisting of all elements of R which form the leading coefficients of polynomials in $\mathfrak{a}$, together with the zero element. The set $\mathfrak{b}_d$ of all elements of R which form the leading coefficients of polynomials in $\mathfrak{a}$ of degree d also forms an ideal, and $\mathfrak{b} = \lim \mathfrak{b}_d$. Since R is Noetherian, $\mathfrak{b} = \mathfrak{b}_N$ for some sufficiently large N. Each of the $\mathfrak{b}_1, \dots, \mathfrak{b}_N$ is finitely generated, and we can therefore consider a family of polynomials $f_1, \dots, f_M$ such that for each $b \in \mathfrak{b}_n$, there exists polynomials g_n such that $\sum f_n g_n$ has degree n, and has leading coefficient b. We claim that the $f_1, \dots, f_M$ generate $\mathfrak{a}$. If f is an element of minimal degree d in $\mathfrak{a} - (f_1, \dots, f_M)$, then the leading coefficient of f is an element of $\mathfrak{b}_d$, and so there exists polynomials g_n such that $\sum f_n g_n$ has degree n and has the same leading coefficient as g. In particular, this means that $f - \sum f_n g_n$ has degree less than f, implying it cannot be an element of $\mathfrak{a} - (f_1, \dots, f_M)$. But it certainly an element of $\mathfrak{a}$, hence an element of $(f_1, \dots, f_M)$, but this implies that

$$f = (f - \sum f_n g_n) + \sum f_n g_n \in (f_1, \dots, f_M) + (f_1, \dots, f_M) = (f_1, \dots, f_M)$$

which is impossible. □

The ideal of leading coefficients of an ideal $\mathfrak{a}$ in $R[X]$ is extremely useful to understanding $\mathfrak{a}$, and the higher dimensional analysis of such coefficients leads to a very rich area of computable operations on ideals of polynomial rings, known as the theory of Gröbner bases.

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.*

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 A-module. A representation of a ring A on an abelian group M is a ring homomorphism from A into $\text{Hom}(M)$. If such a representation is fixed, we can define a 'scalar multiplication' structure on M by elements of A, for $x \in M$ and $a \in A$, letting ax denote the action of a on x via the representation. We obtain the relations

$$a(x+y) \quad (ab)x = a(bx) \quad (a+b)x = ax + bx$$

and if A has a multiplicative unit, we assume $1 \cdot x = x$. Conversely, any multiplication map from $A \times M$ to M satisfying these properties induces a representation of A on $\text{Hom}(M)$, and we call any such M with a fixed scalar multiplication an A **module**. If A is a field, then these are just the axioms which give M the structure of a **vector space** over A, and any such module over a field will be referred to as a vector space.

If we fix A, we can give the family of all A modules the structure of a category, denoted $\mathbf{Mod_A}$. A homomorphism f between two A modules M and N is a group homomorphism satisfying $f(ax) = af(x)$. The family of all morphisms between M and N is denoted $\text{Hom}_A(M,N)$, or just $\text{Hom}(M,N)$ if the underlying ring is obvious. Since one can add morphisms, one can verify that $\text{Hom}(M,N)$ forms an abelian group. Unfortunately, if A is noncommutative, $\text{Hom}(M,N)$ has no natural module structure over A, since if we define $(af)(x) = af(x)$, then af need not be a morphism, since we would require $abf(x) = (af)(bx) = baf(x)$ for all b and x, but if A is commutative, $\text{Hom}(M,N)$ does form a module.

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

$$nx = x + x + \dots + x$$

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 the category* $\mathbf{Ab}$ *of abelian groups in disguise. Thus results about modules automatically give results about abelian groups, and one should keep mind intuition about abelian groups when developing the more general theory of modules.*

Example. *If V is a vector space over a field K with a fixed endomorphism T, then V has a natural structure of a $K[X]$ module, by defining $f(X)x = f(T)(x)$. More generally, if M is a monoid, and we have a monoid representation of M on $End_A(N)$, then any A module N naturally has the structure of an $A[M]$ module. If $C^\infty(a,b)$ is the ring of infinitely differentiable function on an open interval, an infinite dimensional example of this is provided by the homomorphism $Tf = f'$, and then* $\mathbf{R}[X]$ *acts as the rings of differentiable operators. More generally, if we set $T_1, \dots, T_n$ is partial derivative with respect to all n variables, then* $\mathbf{R}[X_1, \dots, X_n]$ *acts on $C^\infty(U)$. If we consider the submodule consisting of the Schwartz functions, then the Fourier transform establishes an isomorphism of this submodule with the ring of Schwartz functions under which* $\mathbf{R}[X_1, \dots, X_n]$ *acts by pointwise multiplication by a polynomial, up to a change in scale. If H is a complex Hilbert space, then the representation of* $\mathbf{C}[X]$ *on $B(H)$ extends to a representation of the ring $\mathcal{O}(\sigma(T))$ of functions analytic in a neighbourhood of the spectrum of T on $B(H)$, and if T is self adjoint, this further extends to a representation of $C(\sigma(T))$.*

Both $K[T]$ and $\mathbf{Z}$ form principal ideal domains, and we shall find that the classification of finitely generated modules over principal ideal domains generalizes the classification of endomorphisms over a vector space, and the classification of finite abelian groups.

Example. *If A is a ring, then the cartesian product A^n forms a module over A. The morphisms of $Hom(A^n, A^m)$ can be identified with matrices in $M_{n,m}(A)$. A* *module isomorphic to A^n is known as a* **free module**. *Those modules M are those for which there exists $x_1, \dots, x_n$ such that every elements of M is uniquely expressible as $\sum a_n x_n$, for $a_n \in A$. This is known as a* **basis** *for M. Just as with vector spaces, we can consider linearly independant sets in modules, which are those for which if $\sum a_n x_n = 0$, then $a_n = 0$. Unfortunately, over exotic rings, the cardinality of a basis need not be unique. More generally, we can consider bases of infinite cardinality, and we shall refer to these variants as free modules also, though it is rare that these can be analyzed by algebraic means. For other module, we can still talk about generating sets, which may not be independant, and we say the module is finitely generated if it has a finite generating set.*

Unfortunately, over exotic rings, the cardinality of a basis is not an invariant of a free module. However, over almost any ring you would ever want to work with, the cardinality of a basis is an invariant property. We say a ring has the **invariant basis property** if this is true. All commutative rings have the invariant basis property, for if A is commutative, it has a maximal ideal $\mathfrak{m}$, and if A^n is isomorphic to A^m as an A module, then as $A/\mathfrak{m}$ modules,

$$(A/\mathfrak{m})^n \cong A^n/\mathfrak{m}A^n \cong A^m/\mathfrak{m}A^m \cong (A/\mathfrak{m})^m$$

If A is a algebra over a field, which is also finite dimensional over that field viewed as a vector space, then A has the invariant basis property, for if A is k dimensional, and $A^n \equiv A^m$ as A modules, then they are also isomorphic as K modules, and $A^n \equiv K^{kn}$, $A^m \equiv K^{km}$, hence $kn = km$, so $n = m$. Here is an example of a ring without the invariant basis property. It must, of course, be an infinite dimensional construction over a field. For a free module M over a ring A with the invariant basis property, the **dimension** $\dim_A(M)$ is well defined.

Example. *Consider the ring A of endomorphisms of the sequence space $V = \bigoplus_{n=1}^\infty K$. Then as A modules, we claim $A \oplus A \cong A$. Let $e_1, e_2, \dots$ denote a basis for V. Partition the standard basis of V into two infinite sets $I = \{f_1, f_2, \dots\}$ and $J = \{g_1, g_2, \dots\}$, and define two endomorphisms F and G by setting $F(f_n) = G(g_n) = e_n$, and $F(g_n) = G(f_n) = 0$. If $TF + SG = 0$, then*

$$0 = (TF)(f_n) + (SG)(f_n) = T(e_n) + S(0) = T(e_n)$$

So $T = 0$. Conversely,

$$0 = (TF)(g_n) + (SG)(g_n) = T(0) + S(e_n) = S(e_n)$$

So $S = 0$. Thus F and G and linearly independant. If T is an arbitrary endomorphism in A, we can write $T(f_n) = T_0(e_n)$ and $T(g_n) = T_1(e_n)$ for two endomorphisms T_0 and T_1, and then $T = T_0 f + T_1 g$. Thus the morphism $(T \oplus S) \mapsto TF + SG$ is an A isomorphism between $A \oplus A$ and A.

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 $\text{Ker}(f)$ and $\text{Im}(f)$ are submodules of their respective modules.

Example. *Given a ring A, the submodules of A are precisely the additive subgroups $\mathfrak{a}$ of A such that if $x \in \mathfrak{a}$ and $a \in A$, then $ax \in \mathfrak{a}$. If A is commutative, this is precisely an ideal. Over a noncommutative ring, these are known as* **left ideals***. Thus the left ideals are the only submodules of A.*

Example. *Given an endomorphism T acting on a vector space V, the $K[X]$ submodules of V are precisely the T invariant subspaces of V. We have a decomposition of V into minimal T invariant subspaces, a fact we will obtain as a corollary of our exploration of modules over a principal ideal domain.*

Example. *If M is a module over an integral domain, we define the* **torsion submodule** *M_{tor} to be the set of all $x \in M$ for which there is a nonzero scalar a with $ax = 0$. Then M_{tor} is a submodule of M. If this submodule is the zero module, we say that M is* **torsion free***. For any module M, M/M_{tor} is torsion free.*

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. The natural analogues of the isomorphism theorems for abelian groups hold for modules. In a similar correspondence, we can define the coproduct and product of modules in a categorical manner, in the same way as for abelian groups. And we have direct and inverse limits of a family of modules as well. The coproduct consists of all finite formal sums of elements of M_α, and the product consists of all tuples with elements in M_α. The two notions coincide in the case of a finite product.

3.1 Exact Sequences and Homomorphisms

For a fixed M, the map $N \mapsto \text{Hom}(M, N)$ is a covariant functor from the category of modules to the category of abelian groups, in the following way. Given a morphism $f : N \to L$, we obtain a morphism f_* from

$\mathrm{Hom}(M,N)$ to $\mathrm{Hom}(M,L)$ by setting $f_*(T) = f \circ T$. On the other hand, the map $M \mapsto \mathrm{Hom}(M,N)$ for a fixed N is a contravariant functor, for given $M \to L$, we obtain $f^* : \mathrm{Hom}(L,N) \to \mathrm{Hom}(M,N)$ by setting $f^*(T) = T \circ f$. Almost all the structure of the modules over a ring can be seen through the structure of the homomorphism groups,

Over the category of modules, we have kernels and images of homomorphisms, and so we can consider exact sequences of modules. We have a relationship between exact sequences of modules and exact sequences of their morphisms. A functor is called exact if it maps exact sequences to exact sequences. The homomorphism functors are not exact, but preserve exactness in certain useful scenarios.

Theorem 3.1. *A sequence $M_0 \to M_1 \to M_2 \to 0$ is exact if and only if $0 \to Hom(M_2,N) \to Hom(M_1,N) \to Hom(M_0,N)$ is exact for all modules N, and a sequence $0 \to N_0 \to N_1 \to N_2$ is exact if and only if $0 \to Hom(M,N_0) \to Hom(M,N_1) \to Hom(M,N_2)$ is exact for all modules M.*

Proof. Exercise. □

We now consider short exact sequences of modules

$$0 \to M \to N \to L \to 0$$

given by maps $f : M \to N$ and $g : N \to L$. We say such a diagram **splits** if the following of three equivalent conditions hold:

- There exists a section $\psi : L \to N$ such that $g \circ \psi$ is the identity.
- There exists a section $\eta : N \to M$ such that $\eta \circ f$ is the identity.

We now prove that if either of these conditions hold, then the other must hold, and then N decomposes as $\mathrm{Ker}(g) \oplus \mathrm{Im}(\psi)$ and as $\mathrm{Im}(f) \oplus \mathrm{Ker}(\eta)$, and is therefore isomorphic to $M \oplus L$. Surely the existence of ψ implies the direct sum decomposition, because $g(\psi(x)) = x$, so $\mathrm{Ker}(g)$ is disjoint from $\mathrm{Im}(\psi)$, and $x - \psi(g(x)) \in \mathrm{Ker}(g)$. The second condition implies the second decomposition in a similar manner. To prove the equivalence of the two splitting conditions, we note that if $N = \mathrm{Ker}(g) \oplus \mathrm{Im}(\psi) = \mathrm{Im}(f) \oplus \mathrm{Im}(\psi)$, we can define $\eta(f(x) + \psi(y)) = x$, since f is injective. If $N = \mathrm{Im}(f) \oplus \mathrm{Ker}(\eta) = \mathrm{Ker}(g) \oplus \mathrm{Ker}(\eta)$, since g is surjective, setting $\psi(x)$ to be the unique element of $\mathrm{Ker}(\eta)$ with $g(\psi(x)) = x$. Such an element exists because g is surjective, and such an element is unique since if $\eta(x) = \eta(y) = 0$ and $g(x) = g(y)$, then $x - y = f(z)$, and so $0 = \eta(x) - \eta(y) = z$, so $x = y$.

Remark. If we are considering the short exact sequence

$$0 \to M \to M \oplus L \to L \to 0$$

Then the existence of the splitting maps is obvious. The splitting argument above shows that this situation is essentially the only case where a short exact sequence can split.

A module P such that for any short exact sequence

$$0 \to M \to N \to P \to 0$$

splits is known as a **projective module**. These are the modules that are easy to define maps out of.

Theorem 3.2. *Fix a module P. Then the following are equivalent.*

- *For any map $f : P \to N$ and a surjective map $g : M \to N$, there exists a map $h : P \to M$ such that $g \circ h = f$.*

- *Any short exact sequence $0 \to M \to N \to P \to 0$ splits.*

- *There is a module N such that $N \oplus P$ is a free module.*

- *The functor $M \mapsto Hom(P,M)$ is exact.*

If any of these conditions are satisfied, we say P is a **projective module**.

Proof. Consider the first condition. Then given any $0 \to M \to N \to P \to 0$, we can take $N = P$ in the triangle condition to obtain the splitting map, showing P is projective. If any short exact sequence terminating at P splits, there certainly exists a free module M with a surjective map $M \to P \to 0$, and then M is isomorphic to the direct sum of P and the kernel of the homomorphism. If N is a free module, then the functor $M \mapsto \text{Hom}(N,M)$ is obviously exact, and since $\text{Hom}(N \oplus P,M) \cong \text{Hom}(N,M) \oplus \text{Hom}(P,M)$. Thus if we have $M_0 \to M_1 \to M_2$ is exact, then

$$\text{Hom}(N \oplus P, M_0) \to \text{Hom}(N \oplus P, M_1) \to \text{Hom}(N \oplus P, M_2)$$

is exact. Restricting the domain of our homomorphisms gives an exact sequence

$$\text{Hom}(P, M_0) \to \text{Hom}(P, M_1) \to \text{Hom}(P, M_2)$$

Finally, assume that the functor is exact. Then we have an exact sequence $M \to N \to 0$, so we have an exact sequence $\text{Hom}(P,M) \to \text{Hom}(P,N) \to 0$. In particular, for any homomorphism from P to N, there exists a homomorphism from $P \to M$ which completes the triangle, so the first property is proved. □

Since projective modules are those for which it is easy to define maps out of, all free modules are projective. Assuming certain circumstances on the ring underlying the module, we can prove that all projective modules are free.

3.2 Modules over Principal Ideal Domains

We could proceed to define more of the general theory of modules, but this gets kind of dry. Instead, to develop our intuition, we use our knowledge of principal ideal domains to come up with a complete classification of the finitely generated modules over a principal ideal domain. In particular, this has applications to modules over the polynomial rings $K[X]$, the integers $\mathbf{Z}$ (and therefore to abelian groups). Thus we assume a principal ideal domain A has been fixed, and we study modules over it.

Theorem 3.3. *Every submodule of a finite dimensional free module is free, with dimension less than the dimension of the module it contains.*

Proof. We prove by induction. Consider the case where the free module is generated by a single element, so it is isomorphic to A. Any submodule is therefore an ideal of A, and is therefore of the form (a). If $a = 0$, then the submodule is free with dimension 0, and if $a \neq 0$, since A has no zero divisors, then a forms the basis of (a). Thus the theorem is true for one dimensional free modules. For the induction, if M is generated by a basis $x_1, \dots, x_N, x_{N+1}$, then for a submodule N, then by induction, $N' = N \cap (x_1, \dots, x_N)$ is freely generated by $y_1, \dots, y_M$. We can consider the ideal in $\mathfrak{a}$ consisting of all a_{N+1} such that there are a_n such that $a_1 x_1 + \dots + a_n X_N + a_{N+1} x_{N+1} \in N$. Thus $\mathfrak{a} = (a)$. If $a = 0$, $N \subset (x_1, \dots, x_N)$, and we are done. Otherwise, we can pick some $y_{M+1} = a_1 x_1 + \dots + a_N x_N + a x_{N+1}$, so that for any $x \in N$, there is a unique b such that $x - b y_{M+1} \in N'$, and so $x - b y_{M+1}$ has a unique expression as a sum of $y_1, \dots, y_M$, showing $y_1, \dots, y_{M+1}$ is a basis for N. □

Remark. If A has an infinite basis, then by well ordering it, and letting N denote an ifninite ordinal in the proof above, the proof essentially extends to the case of an arbitrary free module, except for the case of limit ordinals. But this is proven fairly easily from the fact that a direct limit of free modules is free.

If A is a commutative ring such that every submodule of a free module is free, then A must be a principal ideal domain, for if $\mathfrak{a}$ is a left ideal of A, then $\mathfrak{a}$ cannot contain more than a single independant element, since for any a and b, $ba - ab = 0$. Thus if $\mathfrak{a}$ is free, it must be principal, and if this is true for all $\mathfrak{a}$, then A is a principal ideal domain.

Corollary 3.4. *Every submodule of a f.g. module is f.g.*

Proof. If M is finitely generated, then M is the quotient of a free module. The correspondence theorem shows that every submodule of M corresponds to the quotient of a submodule of the free module, which is therefore the quotient of a free module. □

The classification of finitely generated modules over a principal ring is essentially a generalization of the classification of finitely generated abelian group. The generalization of a finite abelian group is a finitely generated torsion module.

Lemma 3.5. *If M is a finitely generated torsion free module, then M is free.*

Proof. Out of a series of generators $x_1, \dots, x_N$ for M, select a finite independent set $y_1, \dots, y_M$ of maximal cardinality. Then for any x_n, there exists constants $a_n, b_1, \dots, b_M$ such that $a_n x_n + b_1 y_1 + \dots + b_M y_M = 0$. We must have $a_n \neq 0$, and if we consider $a = a_1 \dots a_n$, then we find that for any x_n, $ax_n \in (y_1, \dots, y_M)$, so $aM \subset (y_1, \dots, y_M)$. But the map $x \mapsto ax$ embeds M in aM, so M is isomorphic to aM as a module, and as a submodule of a free module, aM is free. □

Theorem 3.6. *If M is finitely generated, M decomposes as a direct sum of M_{tor} and submodule of M isomorphic to M/M_{tor}.*

Proof. We have a short exact sequence

$$0 \to M_{\text{tor}} \to M \to M/M_{\text{tor}} \to 0$$

Then M/M_{tor} is finitely generated and torsion free, hence free, and therefore splits this diagram, giving the result. □

Thus every finitely generated module is uniquely the direct sum of a free module of a certain finite dimension, and a finitely generated torsion module. The dimension of the free module is known as the **rank** of the module. Two modules will be isomorphic if they isomorphic torsion submodules, and they have the same rank. It therefore suffices to classify the finitely generated torsion modules over a principal ring.

The remainder of the proof essentially carries over exactly the same as the classification of finite abelian groups. First, we note that if x is fixed, the **annihilators** of x, the elements $a \in A$ such that $ax = 0$, form a left ideal of A, and therefore is of the form (a). We call a a **period** for x. We set $M(p)$ to be the submodule of M consisting of all x such that $p^n x = 0$. Thus the annihilators of any element of $M(p)$ are of the form (p^n) for some n.

Theorem 3.7. *Let M be a finitely generated torsion module. Then M is the direct sum of $M(p)$, where p ranges over all equivalence classes of primes in A.*

Proof. Let a be such that $aM = 0$, which exists since M is finitely generated and is a torsion module. If $a = a_0 a_1$, with $(a_0, a_1) = 1$, then $b_0 a_0 + b_1 a_1 = 1$ for some b_0 and b_1. We claim $M \equiv M_{a_0} \oplus M_{a_1}$, where M_{a_0} is the submodule of elements annihilated by a_0, and M_{a_1} the submodule annihilated by a_1. Given any $x \in M$, $x = b_0 a_0 x + b_1 a_1 x$, and $a_1(b_0 a_0 x) = 0$, $a_0(b_1 a_1 x) = 0$,so certainly $M = M_{a_0} + M_{a_1}$. But if $a_0 x = 0$ and $a_1 x = 0$, then any element of $(a_0, a_1) = (1)$ annihilates x, so in particular $x = 0$. Thus we really do have a direct sum representation. Carrying out the entire prime decomposition gives the direct sum result. □

Lemma 3.8. *Let M be a torsion module with $p^n M = 0$, and suppose x has period p^n, and suppose there are $y_1, \dots, y_M$ such that $M/(x)$ can be written as $(y_1 + (x)) \oplus \dots \oplus (y_M + (x))$. Then we can select y_n having the same period as $y_n + (x)$ and with $M = (y_1) \oplus \dots \oplus (y_M) \oplus x$.*

Proof. Suppose $y + (x)$ has period p^m. Then $p^m y \in (x)$, so $p^m y = p^k c x$, where c does not divide p. If $k = n$, y has the same period as $y + (x)$, since $p^{m-1} y \notin (x)$, and so in particular is nonzero. Otherwise, $p^m y$ has period p^{n-k}, and so y has period p^{m+n-k}. We must have $m + n - k \leqslant n$, hence $m \leqslant k$, and so $y' = y - p^{k-m} c x$ has y' the same period as $y + (x)$ and $y' + (x) = y + (x)$. Thus given $y_1 + (x), \dots, y_M + (x)$, we may assume y_n has the same period as $y_n + (x)$. Suppose that $ax + a_1 y_1 + \dots + a_m y_M = 0$. Then $a_n y_n \in (x)$ for all n, hence a_n is divisible by the period of y_n, and so in particular, $a_n y_n = 0$. Thus $ax = 0$. This completes the proof of the decomposition. □

Theorem 3.9. *For any finitely generated p module M, there is a sequence of integers such that*

$$M \equiv A/(p^{n_1}) \oplus \cdots \oplus A/(p^{n_m})$$

and $n_1 \geqslant \cdots \geqslant n_m$.

Proof. We prove by induction on the maximal exponent of M. If p is the exponent of M, then $M = M_p$ is a vector space over $A/(p)$, and therefore isomorphic to a direct sums of $A/(p)$. Now we prove the theorem for p^{N+1} by a second induction on the dimension of M_p over $A/(p)$. If $M_p = (0)$, then $M(p)$ is isomorphic to $pM(p)$, which by induction has a required decomposition. Otherwise, consider x with maximal period p^N. If we consider $M' = M/(x)$, then we contend that M'_p has dimension strictly less than M_p over $A/(p)$. If we consider a basis $y_1 + (x), \dots, y_M + (x)$ for M'_p, then we can be the last lemma assume $py_n = 0$, then $p^{N-1}x, y_1, \dots, y_M$ are linearly independant over M_p. Thus by induction M' is the direct sum of $(x_1) \oplus \cdots \oplus (x_M)$ for some M, and the last lemma implies we can choose $x_1, \dots, x_M$ such that $M = (x) \oplus (x_1) \oplus \cdots \oplus (x_M)$. The decreasing integer condition then holds. □

Such a decomposition is unique, as proved by this next lemma which reduces the argument to a different, equivalent decomposition of a finitely generated torsion module M.

Lemma 3.10. *If M is a finitely generated torsion module, then M is uniquely isomorphic to a direct sum of $A/(n_1) \oplus \cdots \oplus A/(n_N)$, where n_1 divides n_2, which divides n_3, and so on up to n_N.*

Proof. We decompose M into $M(p)$, and decompose $M(p)$ into the modules $A/(p_i^{n_{ij}})$, with n_{ij} increasing in j. Arrange these modules into a matrix with rows i and columns j. The existence of the result is obtained by taking the direct sum of modules over each column, since the direct sum of cyclic modules with relatively prime exponents is also cyclic. To prove uniqueness, consider a decomposition of M as $A/(n_1) \oplus \cdots \oplus A/(n_N)$. If $x = x_1 \oplus \cdots \oplus x_N$, then $x \in M_p$ if and only if $px_n = 0$ for all n, so M_p is the direct sum of $(A/n_m)_p$. In particular, the dimension of M_p over $A/(p)$

is precisely the number of n_m such that p divides n_m. Given another sequence $m_1, \dots m_M$, such that M is decomposed as $A/(m_1) \oplus \dots \oplus A/(m_M)$, consider a prime p such that p divides m_1, hence all m_n, we conclude that the dimension of M_p is M, and so $N \geqslant M$. By symmetry $N = M$, and also p divides all the n_n and m_n. The module pM is decomposed by removing a factor of p from each element in the decomposition. Once we continue this process, we reach relative primality, hence we must reach relative primality in the other decomposition by the dimensionality argument, and continuing this process shows that up to a unit, all the n_n were uniquely specified. □

Example. *Let G be a finitely generated abelian group. Then, since $\mathbf{Z}$ is principal, all of our results apply. Thus G has a rank n, and is isomorphic to the product of $\mathbf{Z}^n$ and a finite abelian group, i.e. a finitely generated torsion module over $\mathbf{Z}$. To classify the finite abelian groups, we can either prick integers n_1 divides n_2 dividing up to n_M, and considering $\mathbf{Z}_{n_1} \oplus \dots \oplus \mathbf{Z}_{n_M}$, or we can decompose our abelian groups into products of cyclic groups of prime order.*

Example. *Let T be an endomorphism of a vector space V. Then V has the structure of a $K[X]$ module. If V is finite dimensional, then V is a torsion module over $K[X]$, which is a principal ring, so there exists a unique decomposition of V into T invariant subspaces, and on each subspace W in the decomposition, there exists an irreducible polynomial f such that W is isomorphic to $K[X]/(f^N)$. If K is algebraically closed, then there is an element $\lambda \in K$ such that W is isomorphic to $K[X]/((X-\lambda)^N)$, and the elements v_n corresponding to $(X-\lambda)^n$ are a vector space basis over K of W, and $Tv_n = \lambda v_n + v_{n+1}$. Thus we obtain the Jordan normal form an endomorphism over an algebraically closed field. Over the real numbers, we either have a T invariant subspace of this form, or isomorphic as a $\mathbf{R}[X]$ module to $\mathbf{R}[X]/((X^2 + 2Re(\lambda)X + |\lambda|^2)^N)$ for some N and complex λ.. TODO: GIVING RISE TO THE REAL CANONICAL FORM OF A MATRIX, where the jordan blocks are formed by a basis $v_1, w_1, v_2, w_2, \dots, v_n, w_m$, with $T(v_n + iw_n) = \lambda(v_n + iw_n) + (v_n + iw_n)$. Thus the Jordan blocks corresponds to rotation matrices and two by two identity matrices.*

Chapter 4

Commutative Algebra

4.1 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 4.1. *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. □

4.2 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.

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* $A[X_1, \dots, X_n]$ *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* $K(X_1, \dots, X_n)$ *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 $\mathbf{Z}[X_1,\dots,X_n]$ is the field $\mathbf{Q}(X_1,\dots,X_n)$ 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 $g_1(z) \neq 0$.*

Considering this problem in a more general viewpoint, we consider a set $S \subset A$, and try to find the 'most general' homomorphism $f : A \to B$ 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. By a localization of A by S, we mean a ring $S^{-1}A$ together with a map $i : A \to S^{-1}A$ such that for any homomorphism $f : A \to B$ such that $f(s)$ is invertible for each $s \in S$, there is a unique homomorphism $S^{-1}f : S^{-1}A \to B$ for which $f = S^{-1}f \circ i$. This is an initial object in a certain category, and is therefore unique up to isomorphism.

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 $f : A \to B$ into a commutative ring B such that $f(s)$ is invertible for each $s \in S$, there is a homomorphism $S^{-1}f : S^{-1}A \to B$ such that $f = S^{-1}f \circ i$. This is an initial object in the category of homomorphisms from A into some other ring B 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 $S^{-1}i : S^{-1}A \to B$ such that $i = S^{-1}i \circ i$. Clearly $S^{-1}i$ 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 $S^{-1}f : S^{-1}A \to B$ by $S^{-1}f(a/s) = f(a)f(s)^{-1}$, 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.

Finally, we remark that localization acts not only on a ring, but also on the modules over a ring. Given a module M over a ring A with multiplicative set S, we can find a natural module $S^{-1}M$ over $S^{-1}A$ which is the initial module in the category of A module maps $f : M \to N$ such that for any $s \in S$, the map $x \mapsto sx$ is an isomorphism of N. To construct this initial object, we consider elements of the form x/s, with $x \in M$ and $s \in S$, and we identify x/s and y/s' if there is $s'' \in S$ such that $s''(xs' - ys) = 0$. The map $M \mapsto S^{-1}M$ is a functor from the category of A modules to $S^{-1}A$ modules, since if $f : M \to N$, then given the map $i : N \to S^{-1}N$, the map $f \circ i$ induces a morphism of $S^{-1}M$ with $S^{-1}N$.

As we have seen, a ring need not embed in its localization when the ring has zero divisors. In fact, zero divisors precisely describe when the embedding exists. Suppose that the annihilators of any $s \in S$ in M are trivial. Two elements $x, y \in M$ are identified in $S^{-1}M$ if and only if there is $s \in S$ such that $s(x - y) = 0$, so $x - y = 0$, hence $x = y$. Conversely, if $sx = 0$, then x is identified with zero in $S^{-1}M$. In particular, if S has no zero divisors in A, then A embeds in $S^{-1}A$.

4.3 Properties Preserved Under Localization

The universal description of the localization of a ring allows us to prove many useful properties of the localization. Given any family of A modules M_α, we find that $S^{-1}(\bigoplus M_\alpha)$ is isomorphic to $\bigoplus S^{-1}M_\alpha$ in a way that the embeddings of $\bigoplus M_\alpha$ in these rings corresponds with one another. A morphism $f : \bigoplus M_\alpha \to N$ corresponds to a unique sequence of morphisms $f_\alpha : M_\alpha \to N$. Because of the properties of localization, f_α extends uniquely to a morphism $f_\alpha : S^{-1}M_\alpha \to N$, and hence f extends unique to a morphism from $\bigoplus S^{-1}M_\alpha \to N$. Thus this direct sum has the properties of localization which $S^{-1}\bigoplus M_\alpha$ possesses, so they are both isomorphic in the required manner.

Remark. Since finite products and coproducts of modules correspond, this identity also holds if we swap the direct sum operation with a *finite* direct product. Unfortunately, this need not be true for infinite direct products. If we consider the fraction field of the integers generated by $S = \mathbf{Z} - \{0\}$, with $M_1 = M_2 = \dots = \mathbf{Z}$ then the two rings we get from the direct product above are $S^{-1}(\mathbf{Z}^\infty)$ and $\mathbf{Q}^\infty$. The inclusion of $\mathbf{Z}^\infty$ in $\mathbf{Q}^\infty$ certainly identifies $S^{-1}(\mathbf{Z}^\infty)$ with a subspace of $\mathbf{Q}^\infty$, but this subspace is proper; it consists of all infinite sequences of rational numbers with bounded denominator. Since $S^{-1}(\mathbf{Z}^\infty)$ is countable, whereas $\mathbf{Q}^\infty$ is uncountable, these spaces cannot be isomorphic.

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 4.2. *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 4.3. *If A is Noetherian, then $S^{-1}A$ is Noetherian.*

Proof. If $S^{-1}(\mathfrak{a}_0) \subset S^{-1}(\mathfrak{a}_1) \subset \dots$ is a chain of ideals in $S^{-1}A$, then $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \dots$, 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 4.4. *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

$$\begin{tikzcd}
S^{-1}A/S^{-1}\mathfrak{a} \arrow[dr] & & A/\mathfrak{a} \arrow[ll] \arrow[dl, "f"] \\
& B & \\
S^{-1}A \arrow[uu] \arrow[ur] & & A \arrow[ll] \arrow[ul] \arrow[uu]
\end{tikzcd}$$

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 4.5. *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 4.6. *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 4.7. *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 4.8. *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 4.9. *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 $S^{-1}A$. □

4.4 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 4.10. *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 4.11. *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 4.12. *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

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

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 4.13. *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.

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

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 4.14. *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 4.15. *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 4.16. *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 4.17. *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.

4.5 Tensor Products

Given two A modules M and N, the **tensor product** $M \otimes_A N$, or $M \otimes N$ if the module A is implicit (or over $\mathbf{Z}$, if M and N are just abelian groups), is the most general way we can form a 'bilinear space' corresponding to M and N. More specifically, $M \otimes N$ is the initial object in the category of bilinear maps $f : M \times N \to L$ into a module L. We can construct $M \otimes N$ by consider the quotient of the free module with basis elements $M \times N$, subject to the submodule generated by $(x+y,z)-(x,z)-(y,z)$, $a(x,y)-(ax,y)$, and $a(x,y)-(x,ay)$. We let the image of (x,y) in the quotient be denoted by

$x \otimes y$, so that $(x+y) \otimes z = x \otimes z + y \otimes z$, $a(x \otimes y) = (ax) \otimes y = x \otimes (ay)$. The embedding of $M \times N$ in the free abelian group obviously descends to a bilinear map from $M \times N$ to $M \otimes N$, which is bilinear precisely because of the quotients defining $M \otimes N$. If $f : M \times N \to L$ is bilinear, then f extends uniquely to a map on the free group generated by $M \times N$. Furthermore, the relations which make f bilinear precisely mean that f descends to a map from $M \otimes N$ to L, so we get a unique morphism from $M \otimes N$ to L which represents f. However, this definition is the 'wrong' definition to use in most cases when understanding the tensor product, because it's quite a strange definition to work with.

Example. *Given the abelian groups $\mathbf{Z}_{10}$ and $\mathbf{Z}_{12}$, we find that $\mathbf{Z}_{10} \otimes \mathbf{Z}_{12}$ is isomorphic to $\mathbf{Z}_2$. We find that for any integers n, m,*

$$n \otimes m = (11n) \otimes m = n \otimes (11m) = -n \otimes m$$

Thus 2 annihilates all of $\mathbf{Z}_{10} \otimes \mathbf{Z}_{12}$, and so we get the natural structure of $\mathbf{Z}_{10} \otimes \mathbf{Z}_{12}$ as a vector space over $\mathbf{Z}_2$. Yet

$$n \otimes m = n(1 \otimes m) = (nm)(1 \otimes 1)$$

so the vector space is generated by a single element $1 \otimes 1$. The element $1 \otimes 1$ doesn't equal to zero in $\mathbf{Z}_{10} \otimes \mathbf{Z}_{12}$. We have a bilinear map $f : \mathbf{Z}_{10} \times \mathbf{Z}_{12} \to \mathbf{Z}_2$ given by $f(x,y) = xy$, which is well defined because $(x+10)y = x(y+12) = xy$ modulo 2. Thus we have an induced map $f_* : \mathbf{Z}_{10} \otimes \mathbf{Z}_{12} \to \mathbf{Z}_2$ where $f_*(1 \otimes 1) = f(1,1) = 1$, which is different from $f_*(0 \otimes 0) = 0$, so $1 \otimes 1 \neq 0$. In particular, our calculation shows that for any bilinear map $f : \mathbf{Z}_{10} \times \mathbf{Z}_{12} \to M$, there exists a unique morphism $g : \mathbf{Z}_2 \to M$ such that $f(x,y) = g(xy)$.

The tensor product is a covariant bifunctor on the category of modules, since if $f : M_0 \times M_1$ and $g : N_0 \times N_1$, then we have a unique morphism $(f \otimes g) : (M_0 \otimes N_0) \to (M_1 \times N_1)$ obtained by $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$. If we fix a module N on the right, then we obtain a covariant functor which is known as **right exact**. More specifically, given an exact sequence

$$M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \longrightarrow 0$$

The induced exact sequence

$$M_0 \otimes N \xrightarrow{f \otimes \text{id}} M_1 \otimes N \xrightarrow{g \otimes \text{id}} M_2 \otimes N \longrightarrow 0$$

is also exact. The surjectivity is easy to prove. Since g is surjective, given for any $y \in M_2$, there is $x \in M_1$ with $g(x) = y$, so $(g \otimes \mathrm{id})(x \otimes z) = y \otimes z$ for any $z \in N$. Now we prove that the image of $(f \otimes \mathrm{id})$ is the kernel of $(g \otimes \mathrm{id})$. Certainly the image, which we denote by L, is a subset of the kernel, which we denote by K. So we get an induced surjective map from $(M_1 \otimes N)/L \to (M_2 \otimes N)$. We claim it is an isomorphism, which would show that $L = K$. To define a left inverse, given $y \otimes z \in M_2 \otimes N$, choose $x \in M_1$ such that $g(x) = y$. The map $h(y \otimes z) = x \otimes z + L$ is a well defined map into the quotient, because if $x, x' \in M_1$ are such that $f(x) = f(x') = y$, then $x - x'$ is in the kernel of g, so $(x - x') \otimes z$ is in L. The map is clearly bilinear, and thus extends to a complete map h on $M_2 \otimes N$, and it is easy to check this is a left inverse on a generating set, hence everywhere.

Tensoring commutes with the direct sum operation, a fact easy to prove by the universal property. That is, we have $M \otimes \bigoplus N_\alpha$ isomorphic to $\bigoplus (M \otimes N_\alpha)$. Any bilinear map f from $M \times \bigoplus N_\alpha$ to L corresponds to a unique family of bilinear maps f_α from $M \times N_\alpha$ to L, inducing a map from $M \otimes N_\alpha$ to L, which can be put together to form a unique map from $\bigoplus (M \otimes N_\alpha)$ to L. Thus multiplication and addition of modules is 'distributive'. Considering the tensor product of modules as a multiplication operation, and addition as a direct sum, the family of modules over an abelian group is given a sort of ring structure, which becomes very important in the field of K theory.

4.6 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, $\mathfrak{a}\mathfrak{b}$ 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 $\mathfrak{a}\mathfrak{b} = A$, so that there are $x_1,\dots,x_n \in \mathfrak{a}$, $y_1,\dots,y_n \in \mathfrak{b}$ with $x_1y_1 + \dots + x_ny_n = 1$. If $x \in \mathfrak{a}$ is arbitrary, then $x = x_1(y_1x) + \dots + x_n(y_nx)$, and we know because of the product formula $\mathfrak{a}\mathfrak{b} = A$ that $y_kx \in A$, hence we have found $\mathfrak{a} = (x_1,\dots,x_n)$. We conclude that any ring whose fractional ideals form a group is Noetherian.

4.7 Abelian Categories

If M and N are modules over the same ring, then $\text{Hom}(M,N)$ is an abelian group. If $f,g \in \text{Hom}(M,N)$, 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 $\text{Hom}(M,N)$ if R is commutative, so $\text{Hom}(M,N)$ is an R module only if R is commutative. Given $f : M \to N$, and a fixed module X, we obtain a morphism $f^* : \text{Hom}(N,X) \to \text{Hom}(M,X)$, mapping g to $g \circ f$. Similarily, we get a morphism $f_* : \text{Hom}(X,M) \to \text{Hom}(X,N)$, 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 $\ker(f_{i+1}) = \text{im}(f_i)$ for each i.

Theorem 4.18. *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 $\ker(f^*) \supset \text{im}(g^*)$. Suppose that $f^*(T) = 0$. We claim that $T = g^*(S)$ for some $S \in \text{Hom}(C, X)$. 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 4.19. *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 $\ker(g_*) \subset \text{im}(f_*)$. Suppose $g \circ T = 0$. We claim $T = f \circ S$ for some $S \in \text{Hom}(X, A)$. 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 5

Algebras

5.1 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

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

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 essentaily can apply Cramer's rule to all rings.

Theorem 5.1. *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 5.2. *$M_n(M_m(R))$ 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 6

Linear Algebra

Theorem 6.1. *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 $W/T(W)$. □

Chapter 7

K Theory

Theorem 7.1 (Steinitz). *Let R be a Dedekind domain. Let $P = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$, and let $Q = \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ be finitely generated projective modules, where the ideals is the direct sum are nonzero. Then P is isomorphic to Q if and only if $r = s$ and $\mathfrak{a}_1 \dots \mathfrak{a}_r = \mathfrak{b}_1 \dots \mathfrak{b}_s$.*

Proof. The last result implies P is isomorphic to $\mathbf{R}^{r-1} \oplus \mathfrak{a}_1 \dots \mathfrak{a}_r$, and Q is isomorphic to $\mathfrak{r}^{s-1} \oplus \mathfrak{b}_1 \dots \mathfrak{b}_s$. Just because P is isomorphic to Q does not imply that $\mathfrak{a}_1 \dots \mathfrak{a}_r$ is isomorphic to $\mathfrak{b}_1 \dots \mathfrak{b}_s$ over *general rings*, but we find that such is true when working over Dedekind domains. First, we remark that for an R linear map $\phi : \mathfrak{a} \to \mathfrak{b}$, there is an element q in the fraction field K such that $\phi(a) = qa$ for all $a \in \mathfrak{a}$. To see this take any nonzero $a_0 \in \mathfrak{a}$. Then, in K,

$$\phi(a) = \frac{a_0 \phi(a)}{a_0} = \frac{\phi(a_0 a)}{a_0} = a \frac{\phi(a_0)}{a_0}$$

Therefore, associated to any R linear map ϕ there is an $r \times s$ matrix M with entries in K. If ϕ is an isomorphism, then M^{-1} exists, and so $r = s$. We now claim that $\det(M)\mathfrak{a}_1 \dots \mathfrak{a}_r$ □

Corollary 7.2. *If R is a Dedekind domain, then $K_0(R) \cong \mathbf{Z} \oplus \widetilde{K_0}(R)$, and as a group, $\widetilde{K_0}(R)$ is isomorphic to the class group of R. Moreover, the product of any two elements of the reduced group is zero.*

Proof. The group $\widetilde{K_0}(R)$ is the kernel of the map from $K_0(R)$ to $\mathbf{Z}$. There is a correspondence $[\mathfrak{a}_1 \oplus \dots \mathfrak{a}_r] \mapsto r$ (taking the rank of the module) which extends to an isomorphism from $K_0(R)$ to $\mathbf{Z} \oplus \mathrm{Cl}(R)$. To prove the product of any two elements of $\tilde{K_0}(R)$ is zero, we consider $[\mathfrak{a}]-1$ and $[\mathfrak{b}]-1$ in $\tilde{K_0}(R)$. Then

$$([\mathfrak{a}-1])([\mathfrak{b}]-1) = [\mathfrak{a}\otimes\mathfrak{b}]-[\mathfrak{a}]-[\mathfrak{b}]+1$$

Since $\mathfrak{a}\oplus\mathfrak{b} \cong R\oplus\mathfrak{a}\mathfrak{b} \cong R\oplus(\mathfrak{a}\otimes\mathfrak{b})$, this is zero. Because the elements $[\alpha]-1$ generate $\tilde{K_0}(R)$. □

7.1 Invertible Modules

A finitely generated module M over an commutative ring is invertible if there exists some module N such that $M\otimes N$ is isomorphic to R. We have a canonical homomorphism from $M\otimes M^*$ to R. Whenever M is invertible, this is precisely an isomorphism.

Lemma 7.3. *If P is a finitely generated projective module then P^* is finitely generated and projective, and $(P^*)^* \cong P$.*

Proof. If P is finitely generated, we have an exact diagram

$$0 \to Q \to R^n \to P \to 0$$

which induces an exact diagram

$$0 \to P^* \to (R^n)^* \to Q^* \to 0$$

and if the first diagram splits, the second one splits. Thus $R^n = P\oplus Q$, and $(R^n)^* \cong P^*\oplus Q^*$, and $(R^n)^*$ is isomorphic to R^n, showing P^* is projective. The double dual map $\nu : M \to M^{**}$ is an isomorphism if $M = R^n$. If P is finitely generated and projective, then $\nu : P \to P^{**}$. If $\mathfrak{p}$ is a prime ideal of R, then $R_{\mathfrak{p}}\otimes P \to R_{\mathfrak{p}}\otimes P^{**}$. □

M is an invertible R module if and only if M is finitely generated and projective of rank 1. TODO: ADD PROOF.

The Picard group of a commutative ring R is the group of isomorphism classes of invertible R modules, with the operation being the tensor product. We have an inclusion from the Picard group of R to $K_0(R)$, which is a morphism of multiplicative monoids. It is an inclusion of groups, but not necessarily an isomorphism.