PIECING TOGETHER CRUMBS: INTRODUCTION TO SOME HIGHER ALGEBRA TOPICS

JUAN SERRATOS

ABSTRACT. Originally, this paper was meant to be an introduction to basic notions of the tensor product between modules and some closely related material (e.g., biadditive functions, the $\text{Hom}_R(A, B)$ set between two R-modules A and B, the category R-**Mod**, etc...) — a lot of the early sections for module theory and the appendices were written when I was a first year — but now I think this paper is best understood as a paper that gives you a quick "What is this thing? And how does it work?" of common *things* in higher algebra.

Now, with that out of the way, the topics that I've taken particular interest to discuss are: module theory (that is, essentially linear algebra but taken over a ring R rather than a field, say, F), rudimentary topology to grasp at the notions of sheaves, category theory, (co)homology, homotopy theory, and ∞-categories — motivated by reading early segments of Jacob Lurie's *Higher Topos Theory*. (However, I hope to further revise this *paper* to include some sort of introduction to p-adic Hodge theory and the work of Peter Scholze with his notion of *perfectoid rings and spaces*, but that'll require me to explain/develop the machinery in algebraic and arithmetic geometry, so I don't know).

CONTENTS

1. Motivation

An introduction to learning about the tensor product and *pure* tensors themselves are often times, in my experience, difficult to comprehend — or at least daunting. For example, if you're to pickup Eisenbud's *Commutative Algebra with a View Toward Algebraic Geometry* you'll encounter the tensor product quickly enough and if you don't know already what it *is* and *does*, you might go the appendix and try to comprehend the definition.

Definition 1 (Eisenbud)**.** *Let M and N be R-modules. The **tensor product** of M and N over R, written $M \otimes_R N$, is the R-module generated by symbols $m \otimes n$ for $m \in M$ and $n \in N$, with relations*

$$rm \otimes n = m \otimes rn$$
$$(m + m') \otimes n = m \otimes n + m' \otimes n$$
$$m \otimes (n + n') = m \otimes n + m \otimes n'.$$

Eisenbud then states, immediately, that "these relations say precisely that the natural map $b \colon M \times N \to M \otimes_R N$ taking (m, n) to $m \otimes n$ is **bilinear**." Now, as for me, I immediately thought "What the fuck is bilinear?" I had taken a computationally focused linear algebra course in high school so the theoretical ideas didn't really stick, and so it took some formal linear algebra enlightenment to further understand what Eisenbud was talking about. Really what this exposition is all about is an introduction, or refreshment, of the formal linear algebra ideas that mathematicians seems to always bring up — you simply cannot avoid linear algebra in any of the natural science, nor mathematics (this is a topic that is milked so much).

Now, another aspect of this exposition that may be useful is the categorical foundations that I may get into since they're as well used so often in say commutative algebra, homological algebra, algebraic geometry, K-theory, algebraic topology, and by god this list can likely stretch so far out. And well you probably suspected it, they're also integral in understanding different perspectives (or you may argue the main perspective) of the tensor product. For example, as Eisenbud continues talking about the tensor product in his appendix (Appendix A2. Multilinear Algebra): "It is elementary that a bilinear map $M \times N \to P$ is the same as a homomorphism $M \to \mathrm{Hom}_R(N, P)$, so we may rewrite the natural isomorphism above as a natural isomorphism

$$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

In categorical language this says that the functor $- \otimes_R N$ is the left adjoint functor of the functor $\mathrm{Hom}_R(N, -)$. "

Although I've mentioned the case of approaching Eisenbud's tensor product definition, there are some other examples that I think are fruitful in mentioning since I'll be trying to really, in a way, comprehend them (myself included) in later sections.

One that comes to mind is provided in Joseph Rotman's *An Introduction to Homological Algebra*. This definition, however, requires more machinery; first we need to describe what we mean by bilinear, and thus we also need to know what biadditive is. This is all in having the idea of describing the tensor product as a biadditive function between modules, or in the *special case*, between vector spaces.

Definition 2 (Rotman)**.** *Let R be a ring , let A_R be a right R-module, let $_R B$ be a left R-module, and let G be an (additive) abelian group. A function $f \colon A \times B \to G$ is called R-**additive** if, for all $a, a' \in A, b, b' \in B$, and $r \in R$, we have*

$$f(a + a', b) = f(a, b) + f(a', b),$$
$$f(a, b + b') = f(a, b) + f(a, b'),$$
$$f(ar, b) = f(a, rb).$$

If R is commutative and A, B, and M are R-modules, then a function $f\colon A \times B \to M$ is called R-**bilinear** if f is R-biadditive and also

$$f(ar, b) = f(a, rb) = rf(a, b)$$

[$rf(a, b)$ makes sense here because $f(a, b)$ now lies in the R-module M].

A clear example, that Rotman provides, is that if we have a ring R, then we will get, naturally, that its multiplication $\varphi\colon R \times R \to R$ is R-additive — as Rotman says, "the first two axioms are the right and left distributive laws, while the third axiom is associativity." You can check these easily on your own. Now, since we didn't assume R to be commutative, we can then suppose that it is and then we'll get that φ is bilinear since $\varphi\colon R \times R \to R$ is biadditive and $\varphi(ar, b) = (ar)b = a(rb) = \varphi(a, rb) = r(ab) = r\varphi(a, b)$ also holds.

The purpose of describing all this machinery is to simply explain the tensor product as a sort of conversion process between biadditive functions and linear functions.

Remark 1 (Rotman). *The tensor product converts biadditive functions into linear ones.*

Definition 3 (Rotman). *Given a ring R and modules A_R and $_RB$, then their **tensor product** is an abelian group $A \otimes_R B$ and an R-biadditive function*

$$h\colon A \times B \to A \otimes_R B$$

such that, for every abelian group G and every R-biadditive $f\colon A \times B \to G$, there exists a unique $\mathbb{Z}$-homomorphism $\tilde{f}\colon A \otimes_R B \to G$ making the following diagram commute.

A $\mathbb{Z}$-homomorphism is an abelian homomorphism. Moreover, if you can't recall immediately what a linear function is, as it's important to know for Remark 1:

Definition 4. *A **linear function** is a mapping $\lambda\colon A \to M$ between R-modules A and M such that it satisfies the properties*

$$\lambda(a + b) = \lambda(a) + \lambda(b),$$
$$\lambda(\alpha b) = \alpha\lambda(b),$$

for all $a, b \in A$ and $\alpha \in R$.

Rotman's definition of the tensor product gave us a look at how categorical methods (specifically, diagram chasing) are going to be a great tool. For example, the following proposition uses categorical methods in its proof:

Proposition 1. *If $A \otimes_R B$ and $\mathfrak{T}$ are tensor products of A and B (R-modules) over R, then $A \otimes_R B \cong \mathfrak{T}$.*

Proof. Suppose that $\partial\colon A \times B \to \mathfrak{T}$ is an R-biadditive function such that, for every abelian group G and every R-biadditive $f\colon A \times B \to G$, there exists a a unique $\mathbb{Z}$-homomorphism $\tilde{f}\colon \mathfrak{T} \to G$ such that f commutes via $\tilde{f}\partial$, i.e., $\tilde{f}\partial = f$.

However, rather than going through nearly the same process of defining all the same assumptions for $A \otimes_R B$ being a tensor product of R-modules of A and B, we can just justify all our assumptions with the fact that the following diagram

commutes with two unique $\mathbb{Z}$-homomorphisms $\tilde{f}$ and $\tilde{h}$, and that $\eta\colon A \times B \to A \otimes_R B$ is an R-biadditive function with the obvious assumption that for every R-biadditve $f\colon A \times B \to G$, it commutes with $\tilde{h}\colon A \otimes_R B \to G$.

Now setting $A \otimes_R B = G$ and $f = h$, since $A \otimes_R B$ is an abelian group so we can since we made no assumptions about G, we get, trivially, that there's a unique $\mathbb{Z}$-homomorphism $\tilde{f}\colon \mathfrak{T} \to A \otimes_R B = G$; thus, $f = \tilde{f}\partial$. Furthermore, we do something very similar with the fact that $A \otimes_R B$ is a tensor product: we can set $G = \mathfrak{T}$ and there will be, with the usual assumptions made about the tensor product above, a unique $\mathbb{Z}$-homomorphism $\tilde{h}\colon A \otimes_R B \to \mathfrak{T}$ that commutes via $h = \tilde{h}\eta$. (If you didn't catch the assumptions made, it follows formally as: Suppose $\eta\colon A \times B \to A \otimes_R B$ is an R-biadditive function such that, for every abelian group G and every R-biadditive $h\colon A \times B \to G$, there exists a unique $\mathbb{Z}$-homomorphism $\tilde{h}\colon \mathfrak{T} \to G$.)

Conisder the following diagram

The diagram commutes since we have that $\tilde{f}\colon A \otimes_R B \to \mathfrak{T}$ and $\tilde{h}\colon \mathfrak{T} \to A \otimes_R B$ both exist due to our assumptions. Moreover, we see that that the big triangle commutes by $\eta = \tilde{h}\tilde{f}$ but also by $1_{A\otimes_R B}$, and thus $1_{A \otimes_R B} = \tilde{h}\tilde{f}$. As an exercise, you should prove that the other part of the isomorphism holds true, i.e., $1_{\mathfrak{T}} = \tilde{f}\tilde{h}$. However, I'll also sort of do it here: In the diagram defining $A \otimes_R B$, we set $\mathfrak{T} = G$ and get that the following diagram

commutes with $1_{\mathfrak{T}} = \tilde{f}\tilde{h}$. Therefore, $A \otimes_R B \cong \mathfrak{T}$. (**Revise Proof:** fix definitions of $\tilde{f}$ and $\tilde{h}$.) $\qquad\square$

2. Module Theory

2.1. **Definition and Examples.** To establish some common notation, and provide a general refresher, we'll go through an introduction to the ideas of module theory. If this topic is unknown to you, it's a *weaker* theory of vector spaces: a vector space takes its scalars from a field (e.g., $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, etc...), while a module takes its scalars from a ring (e.g., $\mathbb{Z}$, $\mathbb{Z}[i]$, etc...).

Some lore from the famous *Abstract Algebra* by Dummit & Foote: "The use of modules was pioneered by one of the most prominent mathematicians of the first part of this century, Emmy Noether, who led the way in demonstrating the power and elegance of this structure. We shall see that vector spaces are just special types of modules which arise when the underlying ring is a field. If R is a ring, the definition of an R-module M is closely analogous to the definition of a group action where R plays the role of the group and M the role of the set. The additional axioms for a module require that M itself have more structure (namely that M be an abelian group). Modules are the 'representation objects' forrings, i.e., they are, by definition, algebraic objects on which rings act. As the theory develops it will become apparent how the structure of the ring R (in particular, the structure and wealth of its ideals) is reflected by the structure of its modules and vice versa in the same way that the structure of the collection of normal subgroups of a group was reflected by its permutation representations."

Definition 5. *Let R be a ring. By an R-**module** M, we mean an additive abelian group M together with a map $R \times M \to M$, $(a, x) \mapsto ax$, called **scalar multiplication**, satisfying the following conditions for all $a, b \in R$, and $x, y \in M$:*

$$a(x + y) = ax + ay,$$
$$(a + b)x = ax + bx,$$
$$a(bx) = (ab)x,$$
$$1x = x.$$

*If R is not necessarily commutative then the above conditions define a **left** R-**module**; commonly denoted as $_R M$. For a **right** R-**module**, the third condition $(xb)a = x(ba)$ defines the right R-module, which is commonly denoted M_R. Elements in a R-module M are called **vectors** and elements in the underlying ring are called **scalars**.*

Remark 2. *We call the map $R \times M \to M$ an R-action.*

In this paper, we focus our discussion on commutative rings, and so the notions of right and left don't need to be specified since commutivity will provide that they coincide; that is, $a(bx) = (ab)x = (xb)a = x(ba)$. However, there may be some remarks of some properties that also hold for modules where their ring of scalars are not necessarily commutative.

Some examples of R-modules — if said without context, you should assume R is a commutative ring with unity:

- A ring R is an R-module over itself

For an R-module M, properties of the following type are deduced easily from the above axioms: $a0 = 0 = 0x$, $(-1)x = -x$, $(-a)x = a(-x) = -(ax)$, $(a-b)x = ax - bx$, $a(x-y) = ax - ay$, $a\left(\sum x_i\right) = \sum ax_i$, $\left(\sum a_i\right)x = \sum a_i x$, etc. Here $a, a_i, b \in R$, $x, x_i, y \in M$, and the symbol 0 is used to denote the additive identity of both R and M.

Definition 6. *Let M be an R-module. A nonempty subset N of M is called a **submodule** (more precisely, an R-submodule) of M if for any $a \in R$ and $x, y \in N$, we have $x + y \in N$ and $ax \in N$, that is, N is itself an R-module.*

Remark 3. *Submodules of M are therefore just subsets of M which are themselves modules under the restricted operations. In particular, if $R = F$ is a field, submodules are the same as subspaces. Every A-module M has the two submodules M and 0 (the latter is called the **trivial submodule**).*

Proposition 2. *Suppose R is a ring. Let $\{M_i\}$ be a family of submodules of a module M. Then $\bigcap_i M_i$ is also a submodule of M*

Proof. Clearly $\bigcap_i M_i$ is nonempty since 0 is in every submodule. Let $x, y \in \bigcap_i M_i$. Then x, y are contained in every submodule of $\{M_i\}$, and so let $x, y \in M_\alpha$ for some $M_\alpha \in \{M_i\}$. But then $x + y \in M_\alpha$ by mere definition of a submodule, and so $x + y \in \bigcap_i M_i$. Moreover, let $a \in R$ and $x \in M_\alpha$. Then, once again, by definition, we have that $ax \in M_\alpha$, and so $ax \in \bigcap_i M_i$. Therefore $\bigcap_i M_i$ is a submodule of M. $\qquad\square$

Example 1 ($\mathbb{Z}$-modules)**.** *Let $R = \mathbb{Z}$, let A be any abelian group (finite or infinite) and write the operation of R as $+$. Make R into a $\mathbb{Z}$-module as follows: for any $n \in \mathbb{Z}$ and $a \in R$ define*

$$
na = \begin{cases} a + a + \cdots + a \ (n \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a - a - \cdots - a \ (-n \text{ times}) & \text{if } n < 0 \end{cases}
$$

(here 0 is the identity of the additive group A). This definition of an action of the integers on A makes A into a $\mathbb{Z}$-module.

Example 2. *Let $_RM$ be an R-module and let $M_1, M_2, \ldots, M_n$ be submodules of $_RM$. Define*

$$M_1 + M_2 + \cdots + M_n = \{x_1 + x_2 + \cdots + x_n \mid x_i \in M_i, i = 1, 2, \ldots, n\}.$$

*It is easy to see that $M_1 + M_2 + \cdots + M_n$ is a submodule of $_RM$, which is called the **sum** of $M_1 + M_2 + \cdots + M_n$. More generally, let $\{M_i \mid i \in \Lambda\}$ be a family of submodules of M. Define*

$$\sum_i M_i = \{x_{i_1} + x_{i_2} + \cdots + x_{i_n} \mid x_{i_k} \in M_{i_k}, i_k \in \Lambda, n \in \mathbb{Z}_{>0}\}.$$

*Then $\sum_{i \in \Lambda} M_i$ is a submodule of M, which is called the **sum** of $\{M_i \mid i \in \Lambda\}$*

Since ever ideal of R is a submodule of R, the above sum of submodules can be applied to R. Therefore we have the same definition of the sum of ideals of R, and so we do not have to repeat it.

An element x of the sum $\sum_{i \in \Lambda} M_i$ of submodules can be often expressed as $\sum_{i \in \Lambda} x_i$, where $x_i \in M_i$ and only finitely many $x_i \neq 0$.

Example 3. *Let I be an ideal of R and let $_RM$ be an R-module. Define*

$$I_R M = \left\{ \sum_{i=1}^m a_i x_i \,\middle|\, m \in \mathbb{Z}_{>0}, a_i \in I, x_i \in {}_RM \right\}$$

Then $I_R M$ is a submodule of $_RM$, which is called the **product** of I and M.

Sometimes it is convenient to write a general element of $I_R M$ as $\sum_i a_i x_i$, where $a_i \in I$, $x_i \in {}_RM$, and indicate that only a finite number of $a_i x_i \neq 0$.

If I and J are ideals of R, we also have the same argument of the product IJ of two ideals of R. But we can continue this approach. More generally, let $I_1, I_2, \ldots, I_n$ be ideals of R. Define inductively:

$$I_1 I_2 \cdots I_n = (I_1 I_2 \cdots I_{n-1}) I_n.$$

Naturally $I_1 I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$. Given an ideal I of R, we define:

$$I^0 = R, \ I^1 = I, \ I^2 = II, \ I^n = (I^{n-1})I.$$

Let N be a submodule of $_RM$. We have a factor group M/N. For each $x \in {}_RM$, we use $\overline{x}$ to denote the coset $x + N$. So in M/N,

$$\overline{x} + \overline{y} = \overline{x + y}, \ x, y \in {}_RM.$$

For $r \in R$, define

$$r\overline{x} = \overline{rx}, \ r \in R, x \in {}_RM.$$

Then M/N becomes an R-module ($_RM/N$), which is called the **factor module** of M modulo N.

Let $_RM$ be an R-module and $s \in R$. Then s is called a **zero-divisor** of $_RM$ if there exists an $x \in M_R \setminus \{0\}$ such that $sx = 0$. Naturally, $s = 0$ is called the trivial zero-divisor of M. Let X be a subset of $_RM$. For $r \in R$, we write $rX = \{rx \mid x \in X\}$. Define

$$\operatorname{ann}_R(X) = \{r \in R \mid rX = 0\},$$

which is an ideal R, called the **annihilator** of X. Correspondingly, for a subset A of R, define

$$\operatorname{ann}_{RM}(A) = \{x \in_R M \mid Ax = 0\},$$

which is a submodule of M, called the **annihilator** of A.

2.2. Module Homomorphisms.

Definition 7. *Let A be a ring and M, N A-modules. A function $\varphi \colon M \to N$ is an R-module homomorphism if*

- $\varphi(x + y) = \varphi(x) + \varphi(y)$,
- $\varphi(rx) = r\varphi(x)$ *for all $x \in M$ and $r \in R$.*

One can easily prove this simple lemma from the definition:

Lemma 1. *A function $\phi \colon M \to N$ mapping A-modules M, N is an A-module homomorphism if and only if $\varphi(x + ry) = \varphi(x) + \varphi(ry)$ for all $x, y \in M$ and $r \in A$.*

Proposition 3. *$\varphi(0) = 0$ for any R-module homomorphism φ.*

Proof. $\varphi(0 + 0) = \varphi(0) + \varphi(0) = 2\varphi(0) = 0$. $\qquad\square$

Example. Some examples:

- A group homomorphism of abelian groups is a $\mathbb{Z}$-module homomorphism.
- If K is a field (implying a vector space), then K-module homomorphism is a linear transformation.

Definition 8. *Let $\varphi \colon M \to N$ be a homomorphism of R-modules. Then the **kernel** of φ is*

$$\ker \varphi := \{x \in M \colon \varphi(x) = 0\}.$$

*The **image** of φ is*

$$\operatorname{im} \varphi := \{y \in N \colon \varphi(x) := y \text{ for some } x \in M\}.$$

The use of the kernel and image of a R-module homomorphism will be used well enough in the following sections when talking about how a complex requires that, essentially, $\operatorname{im} \partial_n \subset \ker \partial_{n+1}$ for a chain complex $(C_\bullet, \partial_\bullet)$, and the same thing goes for an exact sequence for which $\operatorname{im} \partial_n = \ker \partial_{n+1}$.

2.3. Direct Products and Direct Sums.
Let $\{A_i\}_{i \in I}$ be a family of rings. The product set $\prod_{i \in I} A_i$ has the structure of a ring with addition and multiplication defined component-wise, that is, $(a_i) + (b_i) = (a_i + b_i)$ and $(a_i)(b_i) = (a_i b_i)$. This ring is called the **direct product** of the family $\{A_i\}_{i \in I}$. The multiplicative identity of this ring should be pretty obvious: $(1_i) \in \prod_{i \in I} A_i$.

If we want to investigate the product set where the structure is focused on modules we let $\{M_i\}_{i \in I}$ be a family of modules and A be a ring, so that the product set $\prod_{i \in I} M_i$ has the structure of an A-module with addition and scalar multiplication defined component-wise: $(x_i) + (y_i) = (x_i + y_i)$ and $a(x_i) = (ax_i)$ for all $x_i, y_i \in \prod_{i \in I} M_i$ and $a \in A$. This module is called the **direct product** of the family $\{M_i\}_{i \in I}$.

Remark 4. *The A-submodule*

$$\bigoplus_{i \in I} M_i := \{(x_i) \in \prod_{i \in I} M_i \mid x_i = 0 \text{ for almost all } i\}$$

*of $\prod_{i \in I} M_i$ is called the **direct sum** of the family $\{M_i\}_{i \in I}$.*

The direct product and direct sum of a finite family of modules $M_1, M_2, \ldots, M_n$ are also written, respectively, as

$$M_1 \times M_2 \times \cdots \times M_n \ \text{ and } \ M_1 \oplus M_2 \oplus \cdots \oplus M_n.$$

Now, if the indexing set I is finite then the direct product and the direct sum coincide, and so either term is can be used; but we use the convention of using the direct sum for modules and the direct product for rings.

To include a further note about the direct sum $\bigoplus_{i \in I} M_i$, we should define what I mean by a *projection*.

Definition 9. *A **projection** is a mapping of a set (or a mathematical structure) that is idempotent, that is, a map ψ such that $\psi \circ \psi = \psi$.*

Now, the direct sum $\bigoplus_{i \in I} M_i$ comes equipped with a projection homomorphism $\pi_j \colon \bigoplus_{i \in I} M_i \to M_i$ for each $j \in I$ and a coprojection $\alpha_j \colon M_j \to \bigoplus_{i \in I} M_i$ for each $j \in I$.

Additionally, on that note, the abelian group of A-linear (module) homomorphisms from the direct sum to some A-module N is naturally isomorphic to the direct product of the the abelian groups of A-linear homomorphisms from M_i to N:

$$\mathrm{Hom}_A \left(\bigoplus_{i \in I} M_i, N \right) \cong \prod_{i \in I} \mathrm{Hom}_A(M_i, N).$$

2.4. **Exact Sequences.** Consider a finite or infinite sequence

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\partial_{i+1}} M_i \xrightarrow{\partial_i} M_{i-1} \longrightarrow \cdots$$

of A-homomorphisms, or, of A-modules. We say that M_i is an **intermediary** term of this sequence if ∂_{i+1} and ∂_i exist — additionally, i is called the intermediary index. The sequence is said to be a **complex** if $\partial_i \partial_{i+1} = 0$; that is, $\mathrm{im}(\partial_{i+1}) \subset \ker(\partial_i)$ for every intermediary i. The sequence is said to be **exact at** an intermediary M_i if $\mathrm{im}(\partial_{i+1}) = \ker(\partial_i)$, and is said to be **exact** if it is exact at every intermediary M_i.

To formalize much of what has been said, and to include further information,

Definition 10. *A **chain complex** (or simply a **complex**) of R-modules is a sequence*

$$(C_\bullet, \partial_\bullet) = \left(\cdots \to C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \cdots \right),$$

where for each $n \in \mathbb{Z}$, C_n is an R-module and $\partial_n \in \mathrm{Hom}_R(C_n, C_{n-1})$ satisfies $\partial_n \partial_{n+1} = \{0\} := 0$. We often write $C_\bullet$ instead of $(C_\bullet, \partial_\bullet)$.

*The integer n is called the **degree** of the R-modules C_n. The R-linear maps ∂_n ($n \in \mathbb{Z}$) are called the **differential maps**. A complex $C_\bullet$ is called **non-negative** (resp. **positive**) if $C_n = 0$, for all $n \in \mathbb{N}$ (resp. for all $n \in \mathbb{Z}_{n \geq 0}$).*

Definition 11. *A sequence*

$$\cdots \to G_{n+1} \xrightarrow{\varrho_{n+1}} G_n \xrightarrow{\varrho_n} G_{n-1} \xrightarrow{\varrho_{n-1}} \cdots$$

*of modules together with homomorphisms ϱ_i between them is said to be **exact at** G_n if $\mathrm{im}\, \varrho_{n+1} = \ker \varrho_n$. A sequence that is exact at every stage is said to be an **exact sequence**.*

Remark 5. *A **short exact sequence** is an exact sequence with $\{0\} := 0$'s at either end:*

$$0 \to G_2 \xrightarrow{\varrho_2} G_1 \xrightarrow{\varrho_1} G_0 \to 0.$$

*And a **split short exact sequence** is a short exact sequence where $G_1 \cong G_1 \oplus G_0$.*

I'll list some examples to get your mind thinking about (short) exact sequences:

- Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a ring R. Then

$$0 \longrightarrow \mathfrak{a} \cap \mathfrak{b} \longrightarrow \mathfrak{a} \oplus \mathfrak{b} \longrightarrow \mathfrak{a} + \mathfrak{b} \longrightarrow 0$$

  is an exact sequence of R-modules, where the module homomorphism $\mathfrak{a} \cap \mathfrak{b} \longrightarrow \mathfrak{a} \oplus \mathfrak{b}$ maps each element $x \in \mathfrak{a} \cap \mathfrak{b}$ to the element (x, x) of the direct sum $\mathfrak{a} \oplus \mathfrak{b}$, and the homomorphism $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{a} + \mathfrak{b}$ maps each element (x, y) of $\mathfrak{a} \oplus \mathfrak{b}$ to $x - y \in \mathfrak{a} + \mathfrak{b}$.
- An example that concerns this paper's interest, and quite possibly nearly all branches of mathematics, is that if we have vector space V and W over the same field K and if $U \subseteq V$ is a subspace of V, then

$$0 \longrightarrow U \longrightarrow V \longrightarrow V/U \longrightarrow 0$$

  is a short exact sequence. And, additionally, it can turn into another short exact sequence with the use of the tensor product:

$$0 \longrightarrow U \otimes W \longrightarrow V \otimes W \longrightarrow (V/U) \otimes W \longrightarrow 0$$

- Now, if the reader is more experienced, then a noteable example would be to let k be a field with separable closure $\bar{k}$ and X a quasi-compact, quasi-separated k-scheme. So, if $\bar{x}$ is a geometric point of X and the base change $X_{\bar{k}}$ is connected, then there is a (*short*) exact sequence of profinite topological groups:

$$1 \longrightarrow \pi_1^{\acute{e}t}(X_{\bar{k}}, \bar{x}) \longrightarrow \pi_1^{\acute{e}t}(X, \bar{x}) \longrightarrow \pi_1^{\acute{e}t}(\operatorname{Spec} K, \bar{x}) \simeq \operatorname{Gal}(\bar{k}/k) \longrightarrow 1.$$

One of the goals of this paper is to establish some elementary notions in homological algebra, and, because of what has been recently said, we can define now define an important concept. Since we know that $\operatorname{im} \partial_{i+1} \subset \ker \partial_i$, then we can naturally take a quotient: Let $H_n(C_\bullet) = \ker(\partial_n)/\operatorname{im}(\partial_{n+1})$. We call $H_n(C_\bullet)$ the **nth homology group** of the chain complex $C_\bullet$.

3. CATEGORY THEORY

3.1. Definition and Examples.

Definition 12. *A **category** $\mathbf{C}$ is a collection of **object** and **morphisms**, which are maps between objects. These must satisfy the following conditions:*

(i) *Given objects $x, y \in \mathbf{C}$, $\operatorname{Hom}_{\mathbf{C}}(x, y)$ denotes the morphisms from x to y. This may be an empty.*
(ii) *Given objects $x, y, z \in \mathbf{C}$ and morphisms $f \colon x \to y$ and $g \colon y \to z$, the composition $g \circ f \colon x \to z$ is defined. That is, a dotted arrow exists in the following diagram that makes it commute*

(iii) *Given objects $x, y, z, w \in \mathbf{C}$ and morphisms $f \colon x \to y$, $g \colon y \to z$, $h \colon z \to w$, composition is associative; that is, $h \circ (g \circ f) = (h \circ g) \circ f \colon x \to w$. These morphisms are represented by the following commutative diagram (note, no dotted line):*

(iiii) *Every object, $x \in \mathbf{C}$, has an identity map $1_x \colon x \to x$ such that, for any $f \colon x \to y$, $f \circ 1_x = 1_y \circ f = f \colon x \to y$. This saying that the following diagram commutes*
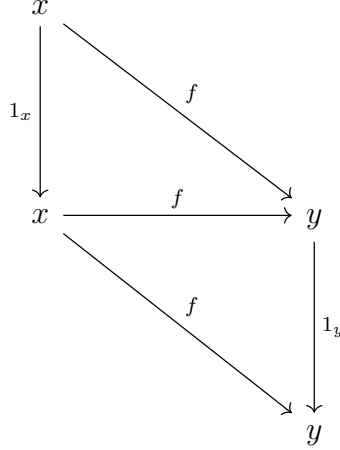
Remark 6. *Categories who's only morphisms are identity morphisms/maps are called **discrete**. Given a little thought, discrete categories are essentially just the objects of the category.*

Example 4 (Objects and Morphisms from Algebra). **Ring** *is the category of rings where the morphisms are ring-homomorphisms;* **Grp** *is the category of groups where the morphisms are group-homomorphisms;* **Field** *is the category of fields where the morphisms are field-homomorphisms.*

Example 5. *The category,* **Sets**, *of sets where the morphisms are functions mapping one set to another (e.g., $\varphi \colon A \to B$, where A and B are sets and φ is a function).*

Example 6. *The category,* **Top**, *of topological spaces where the morphisms are continuous maps.*

Definition 13. *A category,* $\mathbf{C}$, *is called **concrete** if*

(i) *its objects are sets (possibly with additional structure), and*
(ii) *morphisms that are equal as set-mappings are equal in* $\mathbf{C}$.

Remark 7. *Examples 1-3 are all concrete.*

Definition 14. *Let $\mathbf{C}$ be a category and let X_1 and X_2 be objects of $\mathbf{C}$. A **product** of X_1 and X_2 is an object X (often denoted $X_1 \times X_2$) together with a pair of morphisms $\pi_1 \colon X \to X_1$, $\pi_2 \colon X \to X_2$ that satisfy the following universal property:*

- *for every object Y and every pair of morphisms $f_1 \colon Y \to X_1$, $f_2 \colon Y \to X_2$ there exists a **unique** morphism $f \colon Y \to X_1 \times X_2$ such that the following diagram commutes:*
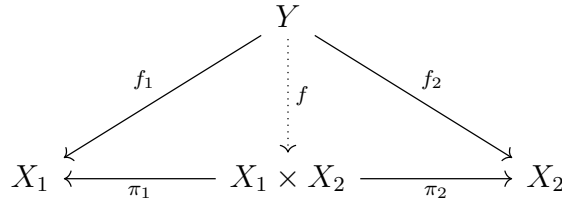
Remark 8. *The unique arrow f making this diagram commute is called the **product of morphisms** and is denoted $f = \langle f_1, f_2 \rangle$. The morphisms π_1 and π_2 are called the **canonical projections** or **projection morphisms**.*

Definition 15. *Let $\mathbf{C}$ be a category and let X_1 and X_2 be objects of $\mathbf{C}$. An object is called the **coproduct** of X_1 and X_2, written $X_1 \coprod X_2$ or $X_1 \oplus X_2$, if*

(i) *there exists maps $i_1 \colon X_1 \to X_1 \coprod X_2$, $i_2 \colon X_2 \to X_1 \coprod X_2$, and*
(ii) *for any object Y and any morphisms $f_1 \colon X_1 \to Y$ and $f_2 \colon X_2 \to Y$, there exists a unique morphism $f \colon X_1 \coprod X_2 \to Y$ such that $f_1 = f \circ i_1$ and $f_2 = f \circ i_2$.*

That is, the following commutative diagram commutes:

$$
\begin{array}{ccccc}
 & & Y & & \\
 & \nearrow \ \uparrow \ \nwarrow & & & \\
f_1 & f & & f_2 & \\
X_1 & \xrightarrow{\ i_1\ } & X_1 \coprod X_2 & \xleftarrow{\ i_2\ } & X_2
\end{array}
$$

Remark 9. *The unique arrow f making this diagram commute may be denoted by $f = f_1 \coprod f_2$ or $f = f_1 \oplus f_2$.*

Remark 10. *Although, in Definition 3, I've chosen $\coprod$ to represent the coproduct, I will be choosing $\oplus$ for later matters. The main reason I did this was to show how the coproduct of a set of objects is essentially their union — $\coprod$ vaguely represents $\bigcup$, and this was appropriate since coproducts have the structural properties of a union.*

4. HOMOLOGY

5. The Grothendieck Revolution

This chapter will introduce some of the basic themes of *IDA*. The geometry we are interested in concerns *affine varieties*, which are curves and surfaces (and higher dimensional objects) defined by polynomial equations. To understand affine varieties, we need some algebra, and in particular, we will need to study ideals in the polynomial ring $k[x_1, \ldots, x_n]$.

5.1. **Polynomials and Affine Space.** The most commonly used fields will be:

- The rational numbers $\mathbb{Q}$: the field for most of our counter examples.
- The real numbers $\mathbb{R}$: the field for drawing pictures of curves and surfaces
- The complex numbers $\mathbb{C}$: the field for proving many of our theorems.
- The polynomial ring $R[x]$: should be read as "Ring of polynomials in the indeterminant x over the field R."

I feel as if we should first discuss a little about the polynomial ring $k[x_1, \ldots, x_n]$ before we proceed into later topics since they're a prominent and frequent concept.

Firstly, $k[x]$ means the ring containing all the polynomials whose coefficients are in the field k and in a single variable/indeterminant x. For example, if k is the field $\mathbb{R}$ in the indeterminant x, then the polynomials such as $x^2 + 2x$ or $x^{10} - 1$ all belong to our indeterminant x since its coefficients belong to $\mathbb{R}$ and it's in one indeterminant, i.e., x_1.

Then, more generally, a polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in k[x]$ if and only if the coefficients $a_0, a_1, \ldots, a_n \in k$ (are in the ring k).

In $k[x, y]$, the only difference is that we are in two variables.; you'll have the polynomial $g(x) = b_0 y + b_1 x^2 y^3 + \cdots + b_n x^n y^{n+1} \in k[x, y]$ if and only if its coefficients $b_0, b_1, \ldots, b_n$ are in the field k.

Example 7.

$$f(x) = x^2 - 3$$

From this polynomial, we see that the coefficients are 1, "in front" of x^2, and the constant coefficient is -3. Since $-3, 1 \in \mathbb{R}$, and in conjunction with our polynomial, we have $f(x) = x^2 - 3 \in \mathbb{R}[x]$. Furthermore, the polynomial also belongs to the polynomial field $\mathbb{Q}$, $f(x) = x^2 - 3 \in \mathbb{Q}[x]$, since -3 and 1 are also rational numbers. Lastly, the polynomial also belong to the polynomial field $\mathbb{C}$, $f(x) = x^2 - 3 \in \mathbb{C}[x]$, since $-3, 1 \in \mathbb{C}$. Recall

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Example 8.

$$a(x, y) = x^{10} y - y^{10} x$$

We see that $(x, y) = x^{10} y - y^{10} x \notin \mathbb{R}[x]$ since, although the coefficients surely are real, we are in two indeterminants, not just one. However, $(x, y) = x^{10} y - y^{10} x \in \mathbb{R}[x, y]$ because its coefficients belong to $\mathbb{R}$ and it's in two indeterminants. Using the same reasoning from the previous example, we see that $(x, y) = x^{10} y - y^{10} x \in \mathbb{Q}[x, y]$. Furthermore, we could assert that $a(x, y) = x^{10} y - y^{10} x \in \mathbb{R}[x, y, z]$. Weird, right? The reason that it also lies in the indeterminant z is because z is evaluated at $z^0 = 1$. Looking at $a(x, y, z) = x^{10} y - y^{10} x \in \mathbb{R}[x, y, z]$, we have the same polynomial as $a(x, y)$, however, z is being evaluated at z^0 again. (This phenomenon is going to be very common in algebraic geometry. For instance, when we look at projective geometry, it's quite often that we will see $a(x, y, z)$ but z being evaluated at $z^0 = 1$, and we'll end up with something which belongs to some ring of polynomials in only two indeterminants rather than three.)

Definition 16. *A **monomial** in $x_1, \ldots, x_n$ is a product of the form*

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdots x_n^{\alpha_n},$$

*where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. The **total degree** of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$.*

The notion of a monomial can be excessive to write out in later definitions, so we can turn to substituting expressions to reduce: let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an n-tuple of nonnegative integers. Then we set

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdots x_n^{\alpha_n}.$$

When $\alpha = (0, \ldots, 0)$ we see that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1 + \cdots + \alpha_n$ denote the total degree of the monomial x^α.

Definition 17. *A **polynomial** f in $x_1, \ldots, x_n$ with coefficients in k is a finite linear combination (with coefficients in k) of monomials. We will write a polynomial f in the form*

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in k,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

When dealing with polynomials in a smaller number of variables, we will usually dispense with subscripts. Thus, polynomials in one, two, and three variables lie in $k[x], k[x, y]$, and $k[x, y, z]$, respectively. For example,

$$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$$

is a polynomial in $\mathbb{Q}[x, y, z]$. We will usually use the letters f, g, h, p, q, r to refer to polynomials.

We use the following terminology in dealing with polynomials.

Definition 18. *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial $k[x_1, \ldots, x_n]$.*
   (i) *We call a_α the **coefficient** of the monomial x^α.*
   (ii) *If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a **term** of f.*
   (iii) *The **total degree** of f, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient a_α is nonzero.*

Example 9. *The polynomial $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ has four terms and total degree 6, $\deg(f) = 6$.*

Remark 11. *The sum and product of two polynomials is again a polynomial. We say that a polynomial f divides a polynomial g provided that $g = fh$ for some $h \in k[x_1, \ldots, x_n]$.*

One can show that, under addition and multiplication, $k[x_1, \ldots, x_n]$ satisfies all of the field axioms except for the existence of multiplicative inverses (because, for example, $1/x_1$ is not a polynomial). Thus, the mathematical structure of $k[x_1, \ldots, x_n]$ is called a commutative ring, and for this reason we refer to $k[x_1, \ldots, x_n]$ as a *polynomial ring*.

We now proceed to affine spaces.

Definition 19. *Given a field k and a positive integer n, we define the n-dimensional **affine space** over k to be the set*

$$\mathbb{A}_k^n = \{(a_1, \ldots, a_n) : a_i \in k\}.$$

(In general, we call $k^1 = k$ the affine line and k^2 the affine plane.)

To clarify what an n-tuple means, informally: A set of n-numbers is called an n-tuple. ("Tuple" refers to an "ordered list.").

Recall from basic algebra the two-dimensional coordinate system, the x, y plane. Using this two-dimensional system, we denote coordinates on the plane by (x, y). So, an example, $x = 3, y = 5, (3, 5)$. We see that this a set of 2-numbers, so it's called a 2-tuple. You could choose to go one to define the three-dimensional system and find that it's a 3-tuple.

Example 10. *Consider the case $k = \mathbb{R}$. Here we get the affine space $\mathbb{A}_\mathbb{R}^n$.*

Let us see how polynomials relate to affine space.

Discussion 1. *The key idea is that a polynomial $\sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ gives a function*

$$f \colon k^n \to k$$

defined as follows: given $(a_1, \ldots, a_n) \in k^n$, where we replace every x_i by a_i in the expression for f. Since all coefficients also lie on k, this operation gives an element $f(a_1, \ldots, a_n) \in k$. (Note that $f(a_1, \ldots, a_n) \in k$ is the evaluation of the polynomial f in n determinants at the point $(a_1, a_2, \ldots, a_n) \in \mathbb{A}_k^n$.)

The dual nature of polynomials has some unexpected consequences. For example, the question "is $f =?$" now has two potential meanings: is f the zero polynomial? which means that all of its coefficients a_α are zero (e.g., $f = 0x^3 + 0x^2 + 0x$), or is f the zero function?, which means that $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in \mathbb{A}_k^n$. The surprising fact is that these two statements are not equivalent in general. For an example of how they can differ, consider the set consisting of the two elements 0 and 1, which can be made into a field that is denoted by $\mathbb{F}_2$. Now consider the polynomial $x^2 - x = x(x-1) \in \mathbb{F}_2[x]$. Since this polynomial vanishes at 0 and 1:

$$x(x-1) = 0 \implies \text{vanishing at } x = 0, 1,$$

we have found a nonzero polynomial which gives the zero function of the affine space $\mathbb{F}_2^1$

However, this will not continue if we have an infinite field.

Proposition 4. *Let k be an infinite field and let $f \in k[x_1, \ldots, x_n]$. Then $f = 0$ in $k[x_1, \ldots, x_n]$ if and only if $f \colon k^n \to k$ is the zero function.*

Corollary 1. *Let k be an infinite field, and let $f, g \in k[x_1, \ldots, x_n]$. Then $f = g$ in $k[x_1, \ldots, x_n]$ if and only if $f \colon k^n \to k$ and $g \colon k^n \to k$ are the same function.*

Theorem 1 (Fundamental Theorem of Algebra). *Every nonconstant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

"We say that a field k is *algebraically closed* if every nonconstant polynomial in $k[x]$ has a root in k. Thus $\mathbb{R}$ is not algebraically closed (what are the roots of $x^2 + 1$?), whereas the above theorem asserts that $\mathbb{C}$ is algebraically closed. In chapter 4 we prove a powerful generalization of Theorem 1 called the Hilbert Nullstellensatz."

5.2. **Affine Varieties:** We can now define the basic geometric objects studied in *IDA*.

Definition 20. *Let k be a field, and let $f_1, \ldots, f_n$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set*

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n \colon f_1 = f_2 = \cdots = f_s = 0\}.$$

We call $\mathbf{V}(f_1, \ldots, f_s)$ the **affine variety** defined by $f_1, \ldots, f_s$.

Thus, an affine variety $\mathbf{V}(f_1, \ldots, f_s) \subseteq k^n$ is the set of all solutions of the system of equations $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$. We will use the letters V, W, etc... to denote affine varieties.

5.3. **Sheaf.**

5.4. **Schemes.**

6. Appendix A1. Zorn's Lemma and Maximal Ideals

Some great lore from *Topics in Commutative Ring Theory:*

"Our primary goal in this chapter is to show that every ring has a maximal ideal. A proof of this very simple and apparently obvious fact will require the use of something fundamental known as Zorn's lemma. Since it happens to be the case that Zorn's lemma is one of the indispensable tools for the modern mathematician, we will take this opportunity to make a rather roundabout detour from our study of commutative rings in order to explore not only the way Zorn's lemma is used in commutative ring theory but also its larger place in mathematics. We will have a few other occasions to use Zorn's lemma later in the book as well; still, an impatient reader may reasonably choose to bypass this detour and pick up the main route again in the next chapter. It will be Zorn's lemma that allows us to assert with complete confidence that a particular ring that we might have in our hands really does contain a maximal ideal. The situation is not unlike that when Hilbert proved the existence of a finite basis for invariants. We need not actually construct a maximal ideal in our ring — though certainly we often do this as well — we are frequently merely satisfied just to know that such an ideal exists.

Since our goal in this chapter is the existence of maximal ideals, let us first turn to a general discussion of maximal elements. Loosely speaking, something is said to be maximal if there is nothing bigger. So, for example, Mount Everest is maximal. Of course, one problem is that you don't always have maximal elements in a given system. For example, there is no maximal integer — that is, there is not an integer n with the property that no integer m is larger than n. As we have seen, Dedekind's idea was to look at the integers in a new way and to focus on ideals rather than numbers as the primary objects. Thus, if we use set inclusion to measure the size of ideals within the integers, then we do have maximal elements, after all. For example, the ideal (3) will be said to be bigger than the ideal (6) because $(6) \subset (3)$. In fact, in this sense, (3) is maximal, as we have seen, since no other proper ideal is bigger. On the other hand, some ideals, such as (3) and (5), can't be compared with one another by means of set inclusion, so we can't say that either one is larger than the other.

In order to state and subsequently use Zorn's lemma in our search for maximal elements, we need to make precise exactly how we compare things. This leads us to the notion of a partial order: "

Definition 21. *A **partial order** on a set S is a relation $\leq$ on S which is*

    1. reflexive — that is, for all $x \in S$,
$$x \leq x;$$

    2. antisymmetric — that is, for all $x, y \in S$,
$$x \leq y,\ y \leq x \text{ implies } x = y;$$

    3. transitive — that is, for all $x, y, z \in S$,
$$x \leq y,\ y \leq z \text{ implies } x \leq z.$$

Example 11. *Let S be the set of integers $\mathbb{Z}$. We define the standard partial order $\leq$ on S as follows, for $x, y \in S$:*
$$x \leq y \text{ if and only if } y - x \text{ is non-negative}$$

Example 12. *Let S be a collection of sets. We define the standard partial order $\leq$ on S as follows, where $A, B \in S$:*
$$A \leq B \text{ if and only if } A \subseteq B.$$

Example 13. *Let S be a collection of sets. This time we will define another quite natural order $\leq$ on S, called reverse inclusion, as follows, where $A, B \in S$:*
$$A \leq B \text{ if and only if } A \supseteq B.$$

Example 14. *Let S be the set $C(\mathbb{R})$ of continuous real-valued functions on the real line. We define the standard partial order $\leq$ on S as follows, where $f, g \in S$:*

$$f \leq g \text{ if and only if } f(x) \leq g(x) \text{ for all } x \in \mathbb{R}.$$

This is to say that the graph of g never dips below the graph of f for $f \leq g$.

A little bit of motivation for the next definition:

"Note also that in the first partial order above, any two elements of the set S can be compared — that is, for any two integers x and y, either $x \leq y$ or $y \leq x$. This is not the case for the other partial orders. For example, given two sets A and B, it is certainly possible for neither to be contained in the other, so that we have neither $A \leq B$ nor $B \leq A$. Similarly, the functions f and g given by $f(x) = x^2$ and $g(x) = x^3$ are not comparable, since their graphs cross. This, of course, is why we use the term partial order. In the particularly nice situation where any two elements in a set can be compared to one another we have the following:"

Definition 22. *A partial order $\leq$ on a set S is a **total order**, or a **linear order**, if for any $x, y \in S$, either $x \leq y$ or $y \leq x$. In particular, if $\leq$ is a partial order on a set S and C is a subset of S, then we say that the set C is a **chain** if $\leq$ is a total order on C.*

Example 15. *The standard order on $\mathbb{R}$ is a total order. In particular, this means that any subset of $\mathbb{R}$ is a chain.*

Remark 12. *You should think of an arbitrary chain, with the elements of the chain all strung out before you in a row, like the real numbers.*

Example 16. *Let S be a set with the standard partial order given by inclusion — that is, the order given in Example 4. Let $A_1, A_2, A_3, \ldots$ be subsets of S. The set*

$$C = \{A_1, A_1 \cup A_2, A_1 \cup A_2 \cup A_3, \ldots\}$$

is a chain, since given any two sets in C, one is contained in the other.
We can make the total of such a chain more apparent by writing the chain as follows:

$$A_1 \subseteq A_1 \cup A_2 \subseteq A_1 \cup A_2 \cup A_3 \subseteq \cdots$$

*This is an example of an **ascending** chain.*

Example 17. *Let $C([0, 1])$ be the set of all continuous real-valued functions on the closed interval $[0, 1]$ with the standard partial order given in Example 6.*
Then the set of function

$$\cdots \leq x^3 \leq x^2 \leq x$$

is a chain, which we have displayed by the usual way with bigger things on the right (don't forget: these functions are only defined on $[0, 1]$).
However, we will often write such a chain as

$$x \geq x^2 \geq x^3 \geq \cdots$$

*since it is a **descending** chain.*

Remark 13. *The previous examples (Examples 8 and 9) — as well as the term "chain" — give the impression that chains are countable, but they need not be. For example, the irrationals $\mathbb{R} \setminus \mathbb{Q}$ form an uncountable chain in $\mathbb{R}$. In fact, we need to be careful not to assume countability in a proof using chains.*

Definition 23. *Let $\leq$ be a partial order on a set S. Let A be a subset of S. An **upper bound** of the set A is an element $s \in S$ such that $a \leq s$, for all $a \in A$.*

Definition 24. *Let $\leq$ be a partial order on a set S. An element $m \in S$ is a **maximal element** of S if there is no element $s \in S$, $s \neq m$, such that $m \leq s$.*

In other words, a maximal element of a set S is simply an element of S such that no other element in S is larger. In particular, though, a maximal element of a set must actually be in the set. Some partially ordered sets have maximal elements and some don't. For example, with the standard order for real numbers, the closed interval $S = [0, 1]$ has a maximal element, whereas the open interval $T = (0, 1)$ does not. Some partially ordered sets even have more than one maximal element! For example, the set S of proper ideals in the ring $\mathbb{Z}$ has lots of maximal elements — namely, the maximal ideals $(2), (3), (5), \ldots$ corresponding to the prime numbers. This last example also explains our normal use of the term *maximal ideal* since what we mean when we say an ideal is a maximal ideal is precisely that it is a maximal element in the set S of proper ideals with the standard partial order of set inclusion.

Recall that our goal is to show the existence of maximal ideals. Zorn's lemma provides us with a way of guaranteeing the existence of maximal elements in a partial order. It turns out that all we have to do is check that any chain has an upper bound:

Theorem 2 (Zorn's Lemma). *Let $\leq$ be a partial order on a non-empty set S. If every chain in S has an upper bound in S, then S contains a maximal element.*

Theorem 3. *Every nonzero ring has at least one maximal ideal.*

Proof. Let R be a nonzero ring. Let S be the set of all proper ideals of R, together with the standard partial order of set inclusion. The set S is non-empty since (0) is a proper ideal of R — this is an innocent looking but seemingly forgotten step that is often crucial in any application of Zorn's lemma. Clearly, a maximal element of the set S is a maximal ideal of R (which is the reason we chose the set S in the way we did).

In order to apply Zorn's lemma we need only show that any chain in S has an upper bound in S. Let C be a chain in S. Since S is a set of ideals (a family of ideals, if you prefer this description instead), C is in fact a chain consisting of ideals, and we have a rather obvious candidate for an upper bound of C: the union U of *all* the ideals in the chain C. Clearly, any ideal in the chain C is contained in U, so U is the upper bound we are looking for, as long as U is in the set S — that is, provided that U is in fact a proper ideal of R.

So, we need to show that U is a proper ideal of R. First, let $a, b \in U$. We must show that $a - b \in U$. Since $a \in U$ and U is the union of all the ideals in C, the element a is in some ideal I in the chain C. Similarly, $b \in J$ for some ideal J in C. But, by definition, the chain C is totally ordered, so I and J are comparable. Either $I \subseteq J$ or $J \subseteq I$. We may as well assume that $I \subseteq J$. Therefore, $a \in I \subseteq J$, but $b \in J$, so $a - b \in J$, since J is an ideal. Thus $a - b \in U$, since U is the union of all the ideals in the chain C and, as such, contains J.

Next, let $a \in U$, and let $r \in R$. We must show that $ra \in U$ — if you haven't gotten it yet, we're first showing that U is an ideal, then after, a proper ideal. But $a \in I$ for some ideal I in the chain C. Thus $ra \in I$, since I is an ideal, and so $ra \in U$. Therefore, U is an ideal of R.

Finally, U is a *proper* ideal of R since $1 \notin U$. This is, of course, because 1 isn't contained in any ideals in the chain C, since, by assumption, these are proper ideals.

Thus, the chain C has an upper bound in S, and so, by Zorn's lemma, S has a maximal element, which in turn is a maximal ideal of the ring R. $\square$

Corollary 2. *Every nonzero ring has at least one prime ideal*

Proof. Direct consequence of Proposition 12 and Theorem 12. $\square$

It is worth noting that the upper bound U that we in the preceding proof is merely an upper bound for the chain C and need not itself be a maximal element. We still do not have a way to construct maximal ideals; we just know they exist.

As some further lore: the key to any successful use of Zorn's lemma is making appropriate choices of the set S and the partial order $\leq$. These need to be chosen so that when Zorn's lemma gives you a maximal element within this framework, this maximal element is in fact what you were looking for. For

example, in the above proof, a maximal element of S turns out to be a maximal ideal, which is exactly what we were looking for.

Exercise 1. *Every proper ideal of a ring is contained in a maximal ideal.*

Proof. Let R be a nonzero ring. Let S be the set of all proper ideals of R, together with the standard partial order of set inclusion. Then, by Theorem 12, R has a maximal ideal, say M. By the well-ordering principle, S has a least element, say J_0. So, $J_0 \leq I_i$ for all $I_i \in S$. But since $M \in S$, $J_0 \leq M$. Therefore, $J_0 \subseteq M$. (This was a bad attempt)

Suppose R is a ring and J is a proper ideal of R. Now, define the set $S = \{\mathfrak{a} \colon J \subseteq \mathfrak{a}\}$ where $\mathfrak{a}$ is a proper ideal of R. Moreover, S is a partially ordered set under inclusion. Note that S is non-empty since J itself is a proper ideal of R that contains J, i.e., $J \in S$, so $S \neq \varnothing$. Let C be a chain of S. Then, we can take the union of all proper ideals in C, $\bigcup \mathfrak{a}_i$, and get an upperbound for C: very simple to see since $\mathfrak{a}_i \leq \bigcup \mathfrak{a}_i$ clearly. Furthermore, we need to have that $\bigcup \mathfrak{a}_i \in S$, by Definition 20. So, let $a, b \in \bigcup \mathfrak{a}_i$. Then $a \in \mathfrak{a}_\alpha$ for some ideal $\mathfrak{a}_\alpha \in \bigcup \mathfrak{a}_i$, and similarly, $b \in \mathfrak{a}_\omega$ for some $\mathfrak{a}_\omega \in \bigcup \mathfrak{a}_i$. Moreover, since C is totally ordered, then $\mathfrak{a}_\alpha$ and $\mathfrak{a}_\omega$ are comparable — don't forget that $\mathfrak{a}_\alpha, \mathfrak{a}_\omega \in C$. WLOG, suppose $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\omega$. Then we have that $a \in \mathfrak{a}_\omega$, so $a - b \in \mathfrak{a}_\omega$ since $\mathfrak{a}_\omega$ is an ideal. Thus, $a - b \in \bigcup \mathfrak{a}_i$.

Now, take an $r \in R$ and $a \in \bigcup \mathfrak{a}_i$. Then $a \in \mathfrak{a}_\Lambda$ for some $\mathfrak{a}_\Lambda \in C$. So, $ra \in \mathfrak{a}_\Lambda$, and thus $ra \in \bigcup \mathfrak{a}_i$. Therefore, $\bigcup \mathfrak{a}_i$ is an ideal.

Since $\bigcup \mathfrak{a}_i$ is the union of all the proper ideals C, then clearly 1 must not be in $\bigcup \mathfrak{a}_i$. Thus making $\bigcup \mathfrak{a}_i$ proper.

By Zorn's lemma, we have a maximal ideal existing in S, say M. But, by the definition of S, we must have that $M = \mathfrak{a}_\Sigma$ such that $J \subseteq M = \mathfrak{a}_\Sigma$. Therefore J is contained in a maximal ideal. $\qquad\square$

Exercise 2. Let I be an ideal of a ring R that is contained in a prime ideal Q. Use Zorn's lemma to prove that there is a prime ideal $\mathfrak{p}$ of R such that

$$I \subseteq \mathfrak{p} \subseteq Q,$$

and there are *no* prime ideals between I and $\mathfrak{p}$. We will can such a prime $\mathfrak{p}$ a **minimal prime over** I.

Proof. To reaffirm, let I an ideal of a ring R, and let $\mathfrak{F}$ be a prime ideal of R for which $I \subseteq \mathfrak{F}$. Let $S = \{\mathfrak{A} \mid I \subseteq \mathfrak{A} \subseteq \mathfrak{F}\}$ where $\mathfrak{A}$ is a prime ideal of R, together with reverse inclusion; that is, if $A, B \in S$, then $A \leq B$ if and only if $B \subseteq A$. S is nonempty since $\mathfrak{F} \in S$. Let $\mathfrak{C}$ be a chain of S. Then we can claim that the intersection of all ideals in S is a lower bound of $\mathfrak{C}$. So, let $\mathfrak{K} = \bigcap \mathfrak{A}_i$ for $i \in \mathbb{N}$. For $\mathfrak{K}$ to be a lower bound bound, if $\mathfrak{A}_\aleph \in \mathfrak{C}$, then $\mathfrak{A}_\aleph \leq \mathfrak{K}$, which is clearly true — think about the zero element. Now, we need also $\mathfrak{K}$ to be in S for it to be a lower bound so we proceed as follows.

Let $a, b \in \mathfrak{K}$. Then $a \in \mathfrak{A}$ and $b \in \mathfrak{B}$ for some ideals $\mathfrak{A}, \mathfrak{B} \in \mathfrak{C}$. Since $\mathfrak{C}$ is a complex, then $\mathfrak{A}$ and $\mathfrak{B}$ are comparable. WLOG, suppose $\mathfrak{A} \subseteq \mathfrak{B}$. Then we have $a \in \mathfrak{B}$ as well, so $a - b \in \mathfrak{B}$, and thus $a - b \in \mathfrak{K}$ since $\mathfrak{B} \subseteq \mathfrak{K}$.

Let $a \in \mathfrak{K}$, and let $r \in R$. Then $a \in \mathfrak{A}$ for some $\mathfrak{A} \in \mathfrak{C}$. Thus, $ra \in \mathfrak{A}$, and so $ra \in \mathfrak{K}$.

Now, by a famous result, we know that $\mathfrak{K}$ is also prime. Thus $\mathfrak{K}$ is a prime ideal. Moreover, since $\mathfrak{K} = \mathfrak{A}_1 \cap \mathfrak{A}_2 \cap \cdots$ where $\mathfrak{A}_i \in \mathfrak{C}$, then, for every $\mathfrak{A}_i$, $I \subseteq \mathfrak{A}_i \subseteq \mathfrak{F}$, and so we must have that $I \subseteq \mathfrak{K} \subseteq \mathfrak{F}$.

Therefore, $\mathfrak{K} \in S$. And so, by Zorn's lemma, S has a minimal element, say $\mathfrak{P}$; thus $I \subseteq \mathfrak{P} \subseteq \mathfrak{F}$. Lastly, by the minimality of $\mathfrak{P}$, we cannot have another prime ideal in between I and $\mathfrak{P}$. $\qquad\square$

Remark 14. *By choosing the reverse inclusion given in Example 5, we were in fact seeking a minimal element in S rather than a maximal, so instead of fixing an upper bound, we were in fact fixing a lower bound.*

Exercise 3. *Every nonzero ring has at least one minimal prime ideal — that is to say, a prime ideal that contains no other prime ideal.*

Proof. Let R be a nonzero ring. $\mathrm{Spec}(R)$, which is the set of all prime ideals of R, is non-empty by Corollary 2. Let's pair $\mathrm{Spec}(R)$ with the partial order of reverse inclusion. Let $\mathfrak{C}$ be a chain of $\mathrm{Spec}(R)$.

In order to apply Zorn's lemma, we need only to show that $\mathfrak{C}$ has a lower bound, so we proceed as follows: For all $\mathfrak{A}_i \in \mathrm{Spec}(R)$ with $i \in \mathbb{N}$, let $\mathfrak{K} = \bigcap \mathfrak{A}_i$. Then, for $\mathfrak{K}$ to be a lower bound, we need $\mathfrak{A}_i \leq \mathfrak{K}$ — can be intuitively thought of as $\mathfrak{K} \leq \mathfrak{A}_i$ with standard inclusion. Clearly $0 \in \mathfrak{K}$; so, moreover, if $\omega \in \mathfrak{K}$, then ω must be in every prime ideal of $\mathrm{Spec}(R)$, and thus we see that $\mathfrak{K}$ can indeed play the role of a lower bound.

The work showing that $\mathfrak{K}$ is a prime ideal is trivial after doing Exercise 6.

Therefore $\mathfrak{K} \in \mathrm{Spec}(R)$, and so $\mathrm{Spec}(R)$ has a minimal prime ideal, which is in turn is a minimal prime ideal of R. $\qquad\square$

7. Appendix A2. Localization

7.1. **Appendix A2.1. Relation Machinery.**

Definition 25. *A relation $\cong$ on a set S is called an **equivalence relation** if it is*

    1. *reflexive — that is, for $x \in S$,*
$$x \cong x;$$

    2. *symmetric — that is, for all $x, y \in S$,*
$$x \cong y \implies y \cong x;$$

    3. *transitive — that is, for all $x, y, z \in S$,*
$$x \cong y, y \cong z \implies x \cong z.$$

Example 18. *Let I be an ideal of a ring R. We can define an equivalence relation on R by saying that two elements of R are equivalent if they are in coset of I — that is, we define*

$$a \cong b \text{ if and only if } a - b \in I \text{ for } a, b \in R.$$

It is worth noting that, for $I = (n)$ in $\mathbb{Z}$,

$$a \cong b \text{ if and only if } a - b \in (n) \text{ for } a, b \in \mathbb{Z}.$$

So, $a - b = nr$ for some $r \in R$. We normally write this equivalence relation as $a \equiv b \pmod{n}$, and we say that a and b are congruent mod n. More generally then, we write $a \equiv b \pmod{I}$ if $a - b \in I$, and we say the obvious.

Example 19. *Let S be the set of fractions a/b such that $a, b \in \mathbb{Z}$ and $b \neq 0$. The standard equivalence relation on this set of fractions is one that we use without even thinking about it. The equivalence relation on fractions is given by*

$$\frac{a}{b} \cong \frac{c}{d} \text{ if and only if } ad = bc \text{ for } a, b, c, d \in \mathbb{Z} \text{ and } b, d \neq 0.$$

This explains precisely what we are doing when we think of $3/4$ and $6/8$ as being the same number, since $3 \cdot 8 = 4 \cdot 6$. In fact, any fraction that is equivalent to $3/4$, such as $132/176$, is also thought of as representing the same rational number. Note that we are thinking of a <u>single</u> rational number as being represented by various fraction such as $3/4$ or $6/8$ or $132/176$. This leads us to the following definition.

Definition 26. *Let $\cong$ be an equivalence relation on a set S. Let $a \in S$. We define the **equivalence class** of a to be*

$$[a] = \{x \in S \mid x \cong a\}$$

that is, $[a]$ is the set of all elements of S that are equivalent to a.

For example 13, let $a \in R$. Then an element $b \in R$ is in the equivalence class $[a]$ if and only if $b \cong a$ – that is, if and only if $b - a \in I$. In other words, $b \in [a]$ if and only if the cosets $b + I$ and $a + I$ are equal. We conclude that $[a] = a + I$. Thus, the equivalence classes are just the cosets.

In example 14, the equivalence class $[3/4]$, for example, is the set of all fractions a/b such that $4a = 3b$ and $b \neq 0$, a condition that we normally write as $a/b = 3/4$. This is the sense in which the two fractions

3/4 and 6/8 are "equal": they are representatives of the same equivalence class. The key idea, then, is to *equate the equivalence class* [3/4] *with a single rational number.*

Definition 27. *A **partition** of a set S is a family of disjoint nonempty subsets of S, whose union is S.*

Theorem 4 (The Basic Properties of Equivalence Classes). *Let $\cong$ be an equivalence relation on a set S. Then the equivalence classes of S have the following basic properties:*

1. *each element $a \in S$ is in some equivalence class — namely, $[a]$;*
2. *$[a] = [b]$ if and only if $a \cong b$;*
3. *$[a] \cap [b] = \varnothing$ if and only if $a \not\cong b$;*
4. *two equivalence classes are either identical or disjoint;*
5. *the equivalence relation $\cong$ partitions the set S into equivalence classes.*

Proof. (1) Since $a \cong a$, $a \in [a]$.
(2) Suppose $[a] = [b]$, then $[a] = \{x \in S \mid x \cong a\} = \{y \in S \mid y \cong b\} = [b]$. Thus, since $a \in [a]$, then $a \cong b$. Conversely, suppose $a \cong b$. Then $a \in [b]$. But then, by the symmetry, we have $b \in [a]$. Thus, $[a] = [b]$.
(3) Clearly, if $[a] \cap [b] = \varnothing$, then $a \not\cong b$. Now, suppose $[a] \cap [b] \neq \varnothing$; then let $c \in [a] \cap [b]$. It follows easily that $c \cong a$ and $c \cong b$, but then by transitivity, we have $a \cong b$. (The contrapositive was used in proving $\Leftarrow$; that is, if $[a] \cong [b] \neq \varnothing$, then $a \cong b$ — this statement is logically equivalent to (3).)
(4) Suppose $[a]$ and $[b]$ are equivalence classes. Then we either have that $a \cong b$ or $a \not\cong b$. So, if $a \cong b$, then by (2), $[a] = [b]$; if $a \not\cong b$, then by (3), $[a] \cap [b] = \varnothing$.
(5) This follows from (1) and (4). $\qquad\square$

Example 20. *Let $\cong$ be the equivalence relation defined on $\mathbb{Z}$ by*

$$a \cong b \text{ if and only if } a \equiv b \pmod 5$$

Then there are five equivalence classes: $[0], [1], [2], [3],$ and $[4]$. These five sets are disjoint, and their union is the entire set $\mathbb{Z}$. Furthermore, any other equivalence classes, such as $[1729]$, is identical to one of these sets. Thus, this equivalence relation partitions $\mathbb{Z}$ into these five sets.

We have seen how the rational numbers can be thought of merely as equivalence classes of fractions under a completely natural equivalence relation. We now describe this same procedure once more, but this time more precisely and in a slightly more general setting. Our goal is to create a field F beginning with an arbitrary integral domain D by imitating the process of creating the rationals $\mathbb{Q}$ from the integers $\mathbb{Z}$. This field F will be called the *quotient field* of the domain D. So, for example, $\mathbb{Q}$ will be the quotient field of $\mathbb{Z}$. (You need to be very careful with this terminology, and not confuse this concept with that quotient rings).

We begin firstly by defining an equivalence relation on an integral domain D. Let D be an integral domain. We define an equivalence relation of the set S of "fractions" (very similar to the definition of $\mathbb{Q}$) using elements of D,

$$S = \left\{ \frac{a}{b} \mid a, b \in D, b \neq 0 \right\},$$

by

$$\frac{a}{b} \cong \frac{c}{d} \text{ if and only if } ad = bc \text{ for all } a, b, c, d \in D, b, d \neq 0.$$

Showing that this in fact an equivalence relation:

1. reflexive: $\frac{a}{b} \cong \frac{a}{b}$, since $ab = ba$;
2. symmetric: $\frac{a}{b} \cong \frac{c}{d}$ implies $ad = bc$, and so $cb = da$, and $\frac{c}{d} \cong \frac{a}{b}$;
3. transitive: Suppose $\frac{a}{b} \cong \frac{c}{d}$ and $\frac{c}{d} \cong \frac{e}{f}$. Then $ad = cb$ and $cf = de$, so $adf = cbf = cfb$, which implies, $adf = deb$, so $d(af - eb) = 0$, and since D is an integral domain and $d \neq 0$, then we must have $af = eb$; thus, $\frac{a}{b} \cong \frac{e}{f}$.

This equivalence relation on the set S of "fractions" from an integral domain determine a set F of equivalence classes of the form $[a/b]$, where $a, b \in D$ and $b \neq 0$ We wish to turn this set F of equivalence classes into a ring (in fact, F will be a field). In order to do this, we need to define two operations on the set F, addition and multiplication (keep in mind $\mathbb{Q}$).

The natural definitions are

$$[a/b] + [c/d] = [(ad + bc)/bd]$$

and

$$[a/b] \cdot [c/d] = [ac/bd].$$

Next, we must attend to the tedious details of showing that these operations are well defined — this means that the result of an addition or a multiplication does not depend upon the choice of the representatives for the equivalence classes being added or multiplied.

Suppose $[a/b] = [a'/b']$ and $[c/d] = [c'/d']$. We must show that $[a/b] + [c/d] = [a'/b'] + [c'/d']$ and that $[a/b] \cdot [c/d] = [a'/b'] \cdot [c'/d']$.

We know that $ab' = ba'$ and $cd' = dc'$, so

$$(ad + bc)b'd' = adb'd' + bcb'd' = (ab')dd' + bb'(cd')$$
$$= (ba')dd' + bb'(dc') = bd(a'd' + b'c').$$

Thus, $[(ad + bc)/bd] = [(a'd' + b'c')/b'd']$, as desired, so addition is well defined.

Similarly,

$$acb'd' = (ab')(cd') = (a'b)(c'd) = bda'c',$$

and so $[ac/bd] = [a'c'/b'd']$, and multiplication is also well defined.

This set F is indeed a ring.

Definition 28. *Let D be an integral domain. The above field F of equivalence classes of fractions from D, with addition and multiplication defined as above, is called the **quotient field** of D.*

Thus, the field $\mathbb{Q}$ of rational numbers is the quotient field of the ring $\mathbb{Z}$ of integers. It is standard practice to blur the distinction between a fraction and the equivalence class represented by that fraction. That is, we usually write a/b when we mean $[a/b]$. In addition, we even think of the domain D as being contained in its quotient field F, just as we think of $\mathbb{Z}$ as being contained in $\mathbb{Q}$. We do this by identifying an element $a \in D$ with the fraction $a/1$ — that is, with $[a/1] \in F$.

What we have succeeded in doing above is to show that we can always embed an integral domain in a field — that is, if D is an integral domain, then there exists a field F such that D is a subring of F. But, what if we begin with an arbitrary ring R? Can we always embed R in a field? One answer is: obviously not if R has zero-divisors, since a field has no zero-divisors, and so R could not be a subring of a field. This is exactly why we restricted the foregoing process to integral domains.

The main point of embedding a domain in a field is to create inverses for the elements of the domain — that is, to be able to divide by any nonzero element. This is what we achieved by creating the rationals from the integers. However, for an arbitrary ring we cannot hope to construct an inverse for a zero-divisor (why not?). But we can hope to construct inverses for any element that is not a zero-divisor. This is what we do next. First, we give a name to those elements in a ring that are not zero-divisors.

Definition 29. *Let R be a ring. An element $a \in R$ is a **regular element** if it is not a zero-divisor.*

If a refresher is needed:

Definition 30. *In a ring R, a nonzero element $a \in R$ is said to be a **zero divisor** if there exists a nonzero $b \in R$ such that $a \cdot b = 0$.*

So, can we always divide by regular elements? Let's look at some examples.

Example 21. *In particular, 0 is not a regular element any nonzero ring. Not surprising since we don't expect to be able to divide by 0 anyway.*

Example 22. *Consider the ring* $\mathbb{Z} \times \mathbb{Z}$ *— that is, all ordered pairs* (a, b) *with* $a, b \in \mathbb{Z}$, *and with addition and multiplication defined componentwise. Then an element* (a, b) *is regular if and only if* $a \neq 0$ *and* $b \neq 0$. *However, the only elements of* $\mathbb{Z} \times \mathbb{Z}$ *that have inverses are* $(1, 1), (1, -1), (-1, 1)$, *and* $(-1, -1)$.

7.2. **Appendix A2.2. Quotient Field.** So, the answer is that you can't always divide by regular elements, but the very good news is that we will now show that any ring R can be embedded in a ring $Q(R)$ such that every regular element of R does have an inverse in $Q(R)$. An equivalence relation can be defined on an appropriate set S of "fractions" using elements of R,

Definition 31. *Let* R *be a ring. The above ring* $Q(R)$ *of equvialence classes of fractions from* R *whose denominators are regular elements, with addition and multiplication defined as above, is called the **total quotient ring** of* R.

In the special case that the ring R is an integral domain, we shall continue to use the term quotient field. Once again, I remind you not to confuse the two very different concepts of quotient ring, Q/R, and total quotient ring, $Q(R)$.

It may seem that we have pushed this idea of constructing inverses for elements in a ring about as far as we can. Nonetheless, the construction of quotient fields and of total quotient rings are but special cases of a still more general procedure called localization. Localization represents one of the most fundamental techniques in commutative ring theory. In the case of a quotient field, we allow denominators to be any nonzero element; in the case of a total quotient ring we allow denominators to be any regular element; and, in the case of an arbitrary ring, we now allow denominators to be any element from what is called a multiplicative system.

Definition 32. *Let* R *be a ring. A subset* T *of* R *is a **multiplicative system** if* $1 \in T$, *and if* $a, b \in T$ *implies that* $ab \in T$ *— that is,* T *is multiplicatively closed and contains* 1.

For example, in an integral domain the set of nonzero elements is a multiplicative system. More generally, in any ring the set of regular elements is a multiplicative system. One other example of a multiplicative system that is very important in commutative ring theory is the complement of a prime ideal.

If T is a multiplicative system of a ring R, then an equivalence relation can be defined on an appropriate set S of "fractions" using elements of R,

$$S = \{a/b \mid a, b \in R, \text{and } b \in T\}$$

by

$$\frac{a}{b} \cong \frac{c}{d} \text{if and only if } t(ad - bc) = 0 \text{ for some } t \in T.$$

The $\cong$ defined above is indeed an equivalence relation on the set S of fraction whose denominators lie in the multiplicative system T.

This equivalence relation on the set S of fractions from R whose denominators are elements of the multiplicative system T determines a set R_T of equivalence classes of the form $[a/b]$, where $a, b \in R$, and $b \in T$. We wish to turn this set R_T of equivalence classes into a ring. In order to do this, we need to define two operations on the set R_T, addition and multiplication. Once again, the natural definitions are

$$[a/b] + [c/d] = [(ad + bc)/bd]$$

and

$$[a/b] \cdot [c/d] = [ac/bd].$$

And, once again, the definitions of multiplication and addition are well defined, and R_T is a ring — together with the operations defined above, and the zero element of R_T being $[0/1]$ and the multiplicative identity is $[1/1]$ (it is also standard practice to ignore the distinction between a fraction and the equivalence class represented by that fraction — that is, we normally write a/b instead of $[a/b]$).

7.3. **Appendix A2.3. Localization Definition.**

Definition 33. *Let R be a ring, and let T be a multiplicative system of R. The above ring R_T of equivalence classes of fractions from R whose denominators are elements of T, with addition and multiplication defined as above, is called the **localization** of R with respect to T, and which we read as "R localized at T."*

Example 23. *Let T be the set of odd integers in $\mathbb{Z}$. Then $1 = 2(0) + 1 \in T$ and if $a, b \in T$, then $a = 2k_1 + 1$ and $b = 2k_2 + 1$ for some $k_1, k_2 \in \mathbb{Z}$, and so $ab = 4k_1 k_2 + 2k_1 + 2k_2 + 1 = 2(2k_1 k_2 + k_1 + k_2) + 1$; thus, $ab \in T$ and T is a multiplicative system. The localization $\mathbb{Z}_T$ consists of all fractions a/b such that b is odd. Note that $a/b \cong c/d$ if and only if $t(ad - bc) = 0$ for some odd integer T, but since $\mathbb{Z}$ is an integral domain, then this condition is equivalent to $ad - bc = 0$ (since $0 \notin T$ and so $t \neq 0$), which is just the usual condition for two fractions to be equal. Thus, $\mathbb{Z}_T$ is the subring of the rationals $\mathbb{Q}$ consisting of fractions having odd denominators.*

Example 24. *Let p be a prime number. Let T be the set of integers in $\mathbb{Z}$ that are relatively prime to p; that is, $T = \{x \in \mathbb{Z} \mid \gcd(x, p) = 1\}$. Then T is a multiplicative system in $\mathbb{Z}$. The localization $\mathbb{Z}_T$ consists of all rational numbers a/b such that b is relatively prime to p.*

Example 25. *We can generalize these last two examples. Let P be a prime ideal of a ring R. Let $T = R\,P$. Then T is a multiplicative system. The localization R_T consists of all fractions a/b, such that b is not in the ideal P. This situation is common enough that we have a special notation: rather than use $R_{R \backslash P}$, which is correct but awkward, we use instead R_P. Thus, the rings of Examples 9 and 10 are written, respectively, as $Z_{(2)}$ and $Z_{(p)}$.*

Observation 1. *Let R be a ring, Z be a multiplicative system of R, and I an ideal of R. Then $I_Z = \{x/z \mid x \in I, z \in Z\}$ is an ideal of the ring R_Z (R localized at Z).*

Proof. Let $x/z, y/s \in I_Z$ — $x, y \in I$ and $z, s \in Z$. Then

$$\frac{x}{z} - \frac{y}{s} = \frac{xs - zy}{zs},$$

and so $zs \in Z$ since Z is a multiplicative system, and $xs - zy \in I$ since I is an ideal; thus $(xs - zy)/zs \in I_T$. Moreover, take $x/z \in I_T$ and let $a/s \in R_Z$. Then

$$\frac{a}{s} \cdot \frac{x}{z} = \frac{ax}{sz} \in I_T;$$

thus I_T is an ideal of R_T as claimed. $\qquad\square$

Remark 15. *Therefore, for any ideal I of the ring R we can associate with I — in a very natural way — an ideal I_T of the ring R_T.*

Observation 2. *Let J be an ideal of the localized ring R at Z. Let $I = \{x \in R \mid x/1 \in J\}$. Then the set I is an ideal of the ring R.*

Proof. Let $x, y \in I$; then, $x/1, y/1 \in J$, so

$$\frac{x - y}{1} = \frac{x}{1} - \frac{y}{1} \in J,$$

since J is an ideal; thus, $x - y \in I$. Similarly, let $r \in R$, and $x \in I$; then $a/1 \in R_Z$ and $x/1 \in J$, so

$$\frac{ax}{1} = \frac{a}{1} \cdot \frac{x}{1} \in J,$$

since J is an ideal; thus, $ax \in I$.

Therefore I is an ideal of R. $\qquad\square$

Remark 16. *Therefore, for an ideal J of the ring R_Z we can associate with J an ideal of I of the ring R.*

We can summarize the discussion thus far by saying that we have successfully defined two functions. The first is a function Φ:

$$\Phi\colon \mathrm{Heg}(R) \to \mathrm{Heg}(R_Z)$$

defined by

$$\Phi\colon I \mapsto I_Z.$$

The second is a function Ψ in the other direction:

$$\Psi\colon \mathrm{Heg}(R_Z) \to \mathrm{Heg}(R)$$

defined by

$$\Psi\colon J \mapsto I,$$

where $I = \{x \in R \mid x/1 \in J\}$.
So,

$$\mathrm{Heg}(R) \xrightarrow{\quad\Phi\quad} \mathrm{Heg}(R_Z)$$
$$\Psi$$

The immediate question is: what happens if we begin with an ideal I in R, and carry this ideal to an ideal I_Z in R_Z, and then back again to an ideal in R in the natural fashion described above? Do we get back to the ideal I we started with in the first place, or not? Similarly, we could ask the same question beginning with an ideal J in R_Z. This is to say, symbolically, is it always true that $\Psi(\Phi(I)) = I$, and that $\Phi(\Psi(J)) = J$.

Happily, we can easily show that starting in one direction everything is as it should be. That is, if we let J be an ideal in R_Z, then it is in fact true that $\Phi(\Psi(J)) = J$. Let $I = \Psi(J)$ — that is, $I = \{x \in R \mid x/1 \in J\}$. Since $\Phi(I) = I_Z$, we need to show that $I_Z = J$.

First, let $x/z \in I_Z$, where $x \in I$ and $z \in Z$. We need to show that $x/z \in J$. But $x \in I$ mean that $x/1 \in J$, and so, since $1/z \in R_Z$ and J is an ideal of $_Z$,

$$\frac{x}{z} = \frac{1}{z} \cdot \frac{x}{1} \in J,$$

so $I_Z \subseteq J$.

Now let $x/z \in J$, where $x \in R$ and $z \in Z$. We must show that $x/t \in I_Z$ — that is, we must show that $x \in I$. But, $t/1 \in R_Z$ and J is an ideal of R_Z, so

$$\frac{x}{1} = \frac{t}{1} \cdot \frac{x}{t} \in J,$$

which means that $x \in I$. Thus, $J \subseteq I_Z$. And so it follows that $J = I_Z$ and $\Phi(\Psi(J)) = J$.

Sad news is that it not always true that $\Psi(\Phi(I)) = I$. But, luckily, we may impose some restriction on the correspondence to actually get it to function as want.

Theorem 5. *Let R be a ring, and let T be a multiplicative system of R. There is a one-to-one order-preserving correspondence between the prime ideals of the localization R_T and the prime ideals of R which are disjoint from T.*

8.1. **Appendix A3.1. Topological Spaces.**

Definition 34. *Let X be a non-empty set. A set $\mathcal{O}$ of subsets of X is said to be a* **topology** *on X if*

(i) *X and the empty set, $\varnothing$, belong to $\mathcal{O}$, i.e., $X, \varnothing \in \mathcal{O}$;*

(ii) *the union of any (finite or infinite) number of sets in $\mathcal{O}$ belong to $\mathcal{O}$ again; and*

(iii) *the intersection of any two sets in $\mathcal{O}$ belongs to $\mathcal{O}$.*

The pair $(X, \mathcal{O})$ is called a **topological space**.

Example 26. *Let $X = \{a, b, c, d, e, f\}$ and $\mathcal{O}_1 = \{X, \varnothing, \{a\}, \{c, d\}, \{a, c, d\}, \{b, c, d, e, f\}\}$. Then $\mathcal{O}_1$ satisfies all the three conditions, so $\mathcal{O}_1$ is a topology and $(X, \mathcal{O}_1)$ is a topological space.*

Example 27. *Let $X = \{a, b, c, d, e\}$ and $\mathcal{O}_2 = \{X, \varnothing, \{a\}, \{c, d\}, \{a, c, e\}, \{b, c, d\}\}$. Then $\mathcal{O}_2$ is not a topology on X since the union $\{c, d\} \cup \{a, c, e\} = \{a, c, d, e\}$ of two members of $\mathcal{O}_2$ does belong to $\mathcal{O}_2$; that is, $\mathcal{O}_2$ doesn't satisfy condition* (ii) *of Definition 1. (There are in fact more issues with the members of $\mathcal{O}_2$ than the preceding two chosen.)*

Definition 35. *Let X be any non-empty set and let $\mathcal{O}$ be the collection of all subsets of X. Then $\mathcal{O}$ is called the* **discrete topology** *on the set X. The topological space $(X, \mathcal{O})$ is called the* **discrete space**.

"We note that $\mathcal{O}$ is Definition 2. does satisfy the conditions of Definition 1 and so it is indeed a topology."

Definition 36. *Let X be any non-empty set and $\mathcal{O} = \{X, \varnothing\}$. Then $\mathcal{O}$ is called the* **indiscrete topology** *and $(X, \mathcal{O})$ is said to be an* **indiscrete space**

Once again, $\mathcal{O}$ in Definition 3. satisfies the conditions of a topology in Definition 1, so it is indeed a topology.

Proposition 5. *If $X = \{a, b, c\}$ and $\mathcal{O}$ is a topology on X with $\{a\} \in \mathcal{O}$, $\{b\} \in \mathcal{O}$, and $\{c\} \in \mathcal{O}$, then $\mathcal{O}$ is the discrete topology.*

Proof. Suppose $X = \{a, b, c\}$ and $\mathcal{O}$ is a topology on X with $\{a\} \in \mathcal{O}$, $\{b\} \in \mathcal{O}$, and $\{c\} \in \mathcal{O}$. Then, since $\mathcal{O}$ is a topology on X, then $\mathcal{O}$ must contain the elements $\varnothing$ and X; moreover, since $\mathcal{O}$ is a topology with $\{a\}$, $\{b\}$, and $\{c\}$, they must fit the conditions of Definition 1., so $\{a, b\}, \{a, c\}, \{b, c\} \in \mathcal{O}$ as well. Thus, $\mathcal{O} = \{X, \varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$, and so $\mathcal{O}$ is the collection of all subsets of X. Therefore $\mathcal{O}$ is a discrete topology. $\square$

A more powerful and general version of Proposition 1:

Proposition 6. *If $(X, \mathcal{O})$ is a topological space such that, for every $x \in X$, the singleton set $\{x\}$ is in $\mathcal{O}$, then $\mathcal{O}$ is a discrete topology.*

Proof. Suppose $(X, \mathcal{O})$ is a topological space such that for every $x \in X$, the singleton set $\{x\} \in \mathcal{O}$. Note that every set is the union of all its singleton subsets, and so if S is any subset of X, then

$$S = \bigcup_{x \in S} \{x\}.$$

Since we are given that each $\{x\} \in \mathcal{O}$, Definition 1. (ii) and the above equation imply that $S \in \mathcal{O}$. As S is an arbitrary subset of X, we have that $\mathcal{O}$ is the discrete topology. $\square$

Note that the equation $S = \bigcup_{x \in S} \{x\}$ holds even when $S = \varnothing$ — this is called the **empty union** and its result is simply $\varnothing$.

Proposition 7. *Let $(X, \mathcal{O})$ be any topological space. Then the intersection of any finite number of members of $\mathcal{O}$ is a member of $\mathcal{O}$.*

Proof. Since $(X, \mathcal{O})$ is a topological space, then it must work for the case of two sets. More generally, $\bigcap_{x \in \mathcal{O}}^{n} x_i$ for $i = 1, 2, \ldots, n$. Suppose $\bigcap_{x \in \mathcal{O}}^{k} x_i \in \mathcal{O}$ for some natural number k. Then assume that $x_{k+1} \in \mathcal{O}$, and so $\bigcap_{x \in \mathcal{O}}^{k+1} x_i = \bigcap_{x \in \mathcal{O}}^{k} x_i \cap x_{k+1}$, and thus $\bigcap_{x \in \mathcal{O}}^{k+1} x_i \in \mathcal{O}$, by definition that the intersection of any two sets in $\mathcal{O}$ belongs to $\mathcal{O}$ again. $\qquad\square$

Open Sets:

Rather than continually referring to "members of $\mathcal{O}$," we find it more convenient to give them the name "open sets." We shall also name the complements of open sets. They will be called "closed sets."

Definition 37. *Let $(X, \mathcal{O})$ be any topological space. Then the members of $\mathcal{O}$ are said to be* **open sets**.

Proposition 8. *If $(X, \mathcal{O})$ is any topological space, then*
  (i) *X and $\mathcal{O}$ are open sets;*
  (ii) *the union of any (finite or infinite) number of open sets is an open set; and*
  (iii) *the intersection of any finite number of open sets is an open set.*

Proof. The first two properties fall from Definition 1, and three falls from Proposition 3. $\qquad\square$

Definition 38. *Let $(X, \mathcal{O})$ be a topological space. A subset S of X is said to be a* **closed set** *in $(X, \mathcal{O})$ if its complement in X, namely $X \setminus S = \{x \mid x \in X \wedge x \notin S\}$, is open in $(X, \mathcal{O})$.*

Example 28. *From Example 1, let $X = \{a, b, c, d, e, f\}$ and $\mathcal{O}_1 = \{X, \varnothing, \{a\}, \{c, d\}, \{a, c, d\}, \{b, c, d, e, f\}\}$ — clearly a topology. Now, to find the closed sets of X take $X \setminus X = \varnothing$; $X \setminus \varnothing = X$; $X \setminus \{a\} = \{b, c, d, e, f\}$; $X \setminus \{c, d\} = \{a, b, e, f\}$; $X \setminus \{a, c, d\} = \{b, e, f\}$; $X \setminus \{b, c, d, e, f\} = \{a\}$. So, we see that $\varnothing, X, \{b, c, d, e, f\}, \{a, b, e, f\}, \{b, e, f\}, \{a\}$, are closed sets, respectively to $(X, \mathcal{O}_1)$.*